



**SCHOOL TECHNOLOGY  
SERVICES**

IT GOVERNANCE

SERVICE MANAGEMENT

SECURITY

# **SCHOOL TECHNOLOGY SERVICES**

## *Self-Evaluation Guide*

*June 2011*

**Government of Alberta ■**

Copyright © 2011 Crown in Right of the Province of Alberta, as represented by the Minister of Education.

Permission is hereby given by the copyright holder to use, reproduce, store or transmit this material for educational purposes and on a non-profit basis. However, Crown copyright is to be acknowledged. If this material is to be used, reproduced, stored or transmitted for commercial purposes, first arrange for consent by contacting:

School Technology Sector  
Alberta Education  
10th Floor, 44 Capital Boulevard  
10044–108 Street  
Edmonton, AB T5J 5E6  
Telephone: (780) 422–6931 or toll-free in Alberta by dialing 310–0000  
Fax: (780) 644–2665

#### ALBERTA EDUCATION CATALOGUING IN PUBLICATION DATA

Alberta. Alberta Education. School Technology Sector.  
School technology services self-evaluation guide.

ISBN 978-0-7785-9103-0 (print)  
ISBN 978-0-7785-9104-7 (online)

Available online: <http://education.alberta.ca/admin/technology/schooltechservices.aspx>

1. Educational technology – Alberta.
2. Information technology – Study and teaching – Alberta.
3. Computer-assisted instruction – Alberta. I. Title.

LB1028.43 A333 2010

371.334

# Table of Contents

Introduction	5
School Technology Services Self-Evaluation Guide	5
Understanding the Format of the School Technology Services Self-Evaluation Guide	6
Using the School Technology Services Self-Evaluation Guide	9
Acknowledgements	10
<b>IT Governance</b>	<b>12</b>
Create and Maintain an IT Strategic Plan	12
Determine Technology Direction	20
Define IT Relationship, Organization and Processes	28
Manage IT Investments	37
Communicate Management Aims and Direction	45
Manage IT Human Resources	53
Assess and Manage IT Risk	61
Monitor and Evaluate IT Performance	69
Monitor and Evaluate Internal Processes	77
Manage Compliance with External Requirements	85
<b>IT Service Management</b>	<b>94</b>
Manage Service Levels	94
Manage Incidents	102
Manage Problems	110
Manage Changes	118
Manage IT Service Continuity and Availability	126
<b>Information Security Management</b>	<b>177</b>
Govern Information Security	177
Protect Information	186
Monitor and Report on Information Security	194
Ensure End User Security	202
Manage System Vulnerabilities	210
Manage End User Identity and Access	218
Protect Networks	226

# INTRODUCTION

# Introduction

## School Technology Services Self-Evaluation Guide

### Background

Technology is playing an increasingly important role in the K-12 education system in Alberta. Together, Alberta Education and school jurisdictions have made significant investments in Information Technology (IT) to support learning and teaching. Additionally, IT is increasingly used to support collaboration, sharing, and the effective and efficient administration of education.

As schools incorporate more technology into learning and teaching, and as technology continues to advance, decisions about technology become increasingly important and more complex. School jurisdiction leaders not only have to consider the technology itself, but also how they will support it, what value it provides, and what risks are associated with it. These decisions can have long-term effects on a school jurisdiction. Jurisdiction IT departments are expected to ensure that:

- IT decisions support the educational goals of the jurisdiction;
- Financial investments in IT provide the value that users expect;
- The IT department is able to support the chosen directions;
- IT assets, information, and people operate in a safe and secure educational environment;
- Critical information is communicated within the jurisdiction;
- IT risks are understood and managed; and
- The IT department is continuously improving to support education.

School jurisdiction leaders can benefit from a set of processes that support and guide the implementation of policies, plans, procedures and organizational structures that are suited to the individual IT needs of the jurisdiction. The School Technology Self-Evaluation Guide was developed to help provide guidance to jurisdiction leaders.

### Description

The School Technology Services Self-Evaluation Guide is a tool for jurisdictions to self-assess and develop their own improvement initiatives in three domains of IT management:

- IT Governance - A set of processes centred on ensuring that the expectations of IT are met and that the risks associated with IT directions are understood and accepted or mitigated.
- IT Service Management - A set of processes centred on the effective and efficient provision of IT services that focus on the objectives of the organization.
- Information Security - A set of processes used to ensure information and systems are safe from unauthorized access, use, disclosure, disruption, modification or destruction.

The guide presents a number of high-level processes that will assist jurisdictions in determining the current state of maturity in each of these three domains, as it has been developed in a maturity model format. The maturity model can be thought of in much the same way as an educational rubric, as it provides jurisdiction leadership with a clear set of criteria with which to measure their current IT practices and provides the opportunity for reflection and improvement.

When using the maturity model, it is not always required or desirable to achieve the highest level of maturity. Each jurisdiction must decide what level of maturity is most appropriate in any particular process based on local circumstances and resources.

During the development of this guide, several internationally-recognized frameworks of best practice were referenced, including *Control Objectives for Information and related Technologies* (COBIT) 4.1 and *IT Infrastructure Library* (ITIL) v3.

Permission to reproduce content from ISO/IEC 27001:2005 and ISO/IEC 27002:2005 is provided by Standards Council of Canada. No further reproduction is permitted without prior written approval from Standards Council of Canada.

## Target Audiences

The School Technology Services Self-Evaluation Guide is intended for senior leadership and IT leaders. Other school jurisdiction personnel may need to be consulted to understand the current level of maturity depending on the process being discussed.

The guide refers to the following roles:

1. **Senior leadership** (e.g., Superintendent, Deputy/Associate/Assistant Superintendent, Secretary-Treasurer)
2. **IT leadership** (e.g., Associate Superintendent of IT, IT Director, IT Manager)
3. **IT staff** (e.g., Technician, Help Desk Analyst, Programmer, Network Analyst)
4. **School administrators** (e.g., Principal, Assistant/Vice Principal)
5. **Trustees** (e.g., elected member of the school board)
6. **End users** (e.g., school jurisdiction personnel, teachers, students and school staff)

## Understanding the Format of the School Technology Services Self-Evaluation Guide

The School Technology Services Self-Evaluation Guide is divided into three distinct but interconnected sections:

1. **IT Governance** (Green);
2. **IT Service Management** (Blue)
3. **Information Security** (Pink)

Each of the three sections follows the same format and includes:

- **Name of the process** - (e.g. Create and Maintain an IT Strategic Plan)
- **Description** - A general description of what the process is.
- **Value** - Describes what the value of the process is to the jurisdiction.
- **Goals** - Describes the intended outcome of the process.
- **Audience** - Describes who should be involved in defining the maturity level of the process.
- **Key Activities** - Describes activities that are performed to achieve the goals and to realize the value of the process.
- **RACI chart** - Outlines the key activities to be performed as part of the process and indicates who is Responsible, Accountable, Consulted and Informed during each activity.

**Responsible** – the person or group who is responsible for performing a task

**Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)

**Consulted** – the person or group communicated with prior to a task being performed

**Informed** – the parties who are notified about an activity before, during or after it is performed.

Each school jurisdiction will have unique job roles to represent the individuals who are responsible,

accountable, consulted or informed about the activities outlined in each RACI chart. For this reason, the roles section of the RACI chart in each of the processes has been left blank.

## The Process Maturity Model

The left side of the maturity model describes the *objectives of the process* grouped by areas of focus. The three areas of focus are:

### People

People are critical to the implementation, support, maintenance and effective management of IT in school jurisdictions. The objectives of this area are:

- awareness, understanding and communication
- skills and expertise
- responsibility and accountability.

### Process

Process is a particular course of action formalized in documentation and may include measures used to inform decision making and continuous improvement. The objectives of this area are:

- process, plans and procedures
- goal setting and measurement.

### Tools

Tools describe what techniques are being used to automate and standardize a process within a jurisdiction. The objective of this area is:

- Tools and automation.

The top row of each maturity model describes the levels of maturity. Each maturity level is the foundation for the next level. The desired or required level of maturity will vary between jurisdictions, based on their size, needs, resources, capability and the alignment of the process with the jurisdiction's strategic plan. It is not necessary to assume that a jurisdiction should be at a Level 5 in all or any processes.

### Level 1 – Initial

At this level, processes and specific activities are typically informal or ad hoc. They are generally reactive in nature and undocumented. Success largely depends upon the capabilities and efforts of individuals. Processes are not sufficiently defined or understood to allow them to be performed in a repeatable way. Senior leadership or IT leadership recognizes that issues exist and should be addressed, but may not communicate this requirement consistently.

### Level 2 – Repeatable

At this level, there is awareness among senior leadership and IT leadership that formalized processes are required and this requirement is communicated consistently. Some processes and activities are repeatable, but may not be consistently performed. Exceptions to the “way of doing things” generally are not noticed and, when they are, corrective action is generally not taken.

### Level 3 – Defined

At this level, all critical processes have been defined and documented. Stakeholders understand and accept the need for formal approaches to IT governance, service management and information security management. IT leadership and IT staff have a solid understanding of the processes, activities and documentation required. Continuous improvement methods are emerging.

#### Level 4 – Managed

At this level, all activities are defined, documented and communicated for a given process and are supported by training. Variations in performance of processes are noticed, but corrective action is not consistently taken.

#### Level 5 – Optimized

At this level, processes and activities are often automated. There is a focus on improving process performance through incremental and innovative technological or process changes. Exceptions to how a process is performed are noticed and analyzed. Corrective action is consistently taken.

		Maturity Level				
Attributes		1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized
PEOPLE	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li>□ IT leadership is aware of the need for strategic planning.</li> </ul>	<ul style="list-style-type: none"> <li>□ Senior leadership discusses IT strategic planning at senior leadership meetings when issues emerge.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT strategic planning is performed on a regular basis, is formalized and involves a range of stakeholders.</li> </ul>	<ul style="list-style-type: none"> <li>□ Senior leadership and IT leadership understand the full requirements for IT strategic planning.</li> </ul>	<ul style="list-style-type: none"> <li>□ Senior leadership and IT leadership have a detailed and forward-looking understanding of IT strategic planning, tactical planning and IT portfolio management.</li> </ul>
	Skills and Expertise					
	Responsibility and Accountability					
PROCESS	Policies, Plans and Procedures					
	Goal Setting and Measurement					

*Note: Sample model is deliberately incomplete.*

## Using the School Technology Services Self-Evaluation Guide

The School Technology Services Self-Evaluation Guide describes the attributes of mature IT Governance, IT Services Management and Information Security Management processes. It does not describe how these are implemented, or provide specific guidance for the development of policies and procedures. Instead it is intended to serve as a shared reference to support collaborative work to improve these processes.

School authority senior leadership and IT leaders can use this guide as the basis for dialogue about how technology is governed, managed and secured in their school jurisdiction. It can be used to support target setting, self-assessment, and ongoing monitoring and reporting of improvements.

School authority IT leadership and IT staff can use the guide to engage in process improvement activities. It can be used to identify capability gaps, and support improvement planning and monitoring.

The guide can also be used to support collaboration across school authorities. Using the guide as a common point of reference, school authority personnel can collaboratively develop policies and processes for use across school authority boundaries.

The guide can be used alongside more detailed standards, such as:

- *IT Infrastructure Library (ITIL) v3*
- *Control Objectives for Information and related Technologies (COBIT) 4.1*
- *Val IT Framework 2.0*
- *Risk IT*
- *ISO/IEC 27001:2005 Information technology - Security techniques - Information security systems requirements*
- *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management*

## Questions or Comments?

IF you have any questions or comments, please contact the School Technology Sector, Alberta Education at (780)427-9001, toll-free within Alberta by calling 310-0000 first.

## Acknowledgements

Alberta Education, in partnership with education stakeholders developed the School Technology Services Self Assessment Guide in 2009/2010.

We gratefully acknowledge the contributions of the following individuals and school boards to the creation of this guide.

### 2009/2010 Development Team

Peter Balding	Black Gold Regional Division No. 18
Robert Barrett	Fort Vermilion School Division No. 52
Dr. Jim Brandon	College of Alberta School Superintendents
Darcy Bromling	Peace Wapiti School Division No. 76
Clint Carrell	Grande Prairie Roman Catholic Separate School District No. 28
Brian Celli	Wild Rose School Division No. 66
Daniel Chamczuk	Elk Island Public Schools Regional Division No. 14
Joseph De Almeida	Red Deer Catholic Regional Division No. 39
Todd Diakow	Palliser Regional Division No. 26
Daniel Durand	Edmonton Catholic Separate School District No. 7
Daryl Hoey	Buffalo Trail Public Schools Regional Division No. 28
Danny Houssian	Edmonton Catholic Separate School District No. 7
Donna Holloway	St. Paul Education Regional Division No. 1
Dean Jarvey	Calgary Roman Catholic Separate School District No. 1
Todd Kennedy	Pembina Hills Regional Division No. 7
Shawn LeBleu	Holy Spirit Roman Catholic Separate Regional Division No. 4
Jaymon Lefebvre	Wild Rose School Division No. 66
Jim Malenczak	Edmonton School District No. 7
Mike Rinkel	Calgary School District No. 19
Ken Robitaille	Battle River School Division No. 31
Kurt Scobie	Grande Yellowhead Public School Division No. 77
Cindy Seibel	Calgary School District No. 19
Gary Spence	Wolf Creek School Division No. 72
Rolf Traichel	Medicine Hat Catholic Separate Regional Division No. 20
Loralei Turner	Calgary School District No. 19
Norman Yanitski	Alberta Education – Learning Supports

### Alberta Education Staff

Angie Tarasoff	School Technology Services Program Manager
Qin Chang	Project Manager – Information Security
Dave Hauschildt	Project Manager – IT Service Management
Jeff Rawlings	Project Manager – IT Governance

### Consultants

Lesli Flaman  
Peter Lijnse  
Mark Linton  
Rhys Morgan  
Dejan Slokar

### Editor

Darlene Cann



# IT Governance

## Create and Maintain an IT Strategic Plan

### Description

An IT Strategic Plan helps jurisdictions ensure that IT resources and investments as well as jurisdiction strategic goals are coherent and cohesive. This document helps answer the question, “is IT doing the right things?” IT tactical plans are derived from the IT Strategic Plan and describe how the strategy will be carried out in greater detail. Tactical planning partially addresses the question, “is IT doing the things right?”

This process area includes the development and maintenance of the IT Strategic Plan and the tactical plans that support it.

### Value

- Builds common understanding among stakeholders about how investments in technology will be used to support the work of the school jurisdiction.
- Ensures that IT operations and initiatives are correctly aligned to jurisdiction strategy.
- Supports informed decision making, with respect to IT resource allocation and investment.

### Goals

- Align IT investments, resources and activities with jurisdiction strategic goals and priorities.
- Ensure that sufficient resources are available to achieve the outcomes stated in the IT Strategic Plan.

### Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

### Key Activities

**Ensure there is a clear and direct link between IT goals and jurisdiction objectives.**

- Implement a process to enable regular communication and stakeholder involvement in IT strategic planning.

**Assess current capabilities and performance of IT solutions and service delivery** to establish a baseline against which future requirements can be compared.

- Implement a process to measure current performance of IT services in terms of their contribution to jurisdiction goals.
- Implement a process to measure IT service functionality, stability, complexity, costs, strengths and weaknesses.
- Communicate results to inform development and maintenance of the IT Strategic Plan.

**Create a long-term IT Strategic Plan**, in cooperation with stakeholders, that defines how IT will contribute to the jurisdiction’s objectives and that outlines related costs and risks.

- Implement a process to regularly review and update the IT Strategic Plan.

**Create IT tactical plans** to achieve objectives outlined in the IT Strategic Plan.

- Implement a process to ensure that each IT tactical plan identifies an owner and includes resource requirements, costs, timelines, activities, project plans and performance measurements.

### RACI Chart

	Roles				
<b>Activities</b>					
Ensure there is a clear and direct link between IT goals and jurisdiction objectives.					
Assess current capabilities and performance of IT solutions and service delivery.					
Create a long-term IT Strategic Plan.					
Create IT tactical plans.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

### Maturity Model – Create and Maintain an IT Strategic Plan

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p style="text-align: right;"><b>PEOPLE</b></p> <p><i>Attributes</i></p>	<p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for IT strategic planning.</li> <li><input type="checkbox"/> The need for IT strategic planning is communicated inconsistently.</li> <li><input type="checkbox"/> IT strategic planning is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT strategy is sporadic and usually in response to issues.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need for IT strategic planning.</li> <li><input type="checkbox"/> IT leadership understands the requirements of an effective IT strategic planning process.</li> <li><input type="checkbox"/> The need for IT strategic and tactical planning is communicated consistently.</li> <li><input type="checkbox"/> IT strategic planning is discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about IT strategy occurs periodically.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the requirements of an effective IT strategic planning process.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of a sound IT strategic planning process.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss IT strategic and tactical planning on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about the IT Strategic Plan occurs on a regular basis and in a formal way.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership discusses the IT Strategic Plan on a regular basis and in a formal way.</li> <li><input type="checkbox"/> The IT Strategic Plan is developed in collaboration with senior leadership, IT leadership and jurisdiction stakeholders.</li> <li><input type="checkbox"/> Communication to stakeholders about IT strategic planning is regular, formal and includes a report of results.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership and have an advanced and forward-looking understanding of IT strategic and tactical planning.</li> <li><input type="checkbox"/> Understanding of IT strategic goals is widespread throughout the jurisdiction.</li> </ul>
	<p>Awareness, Understanding and Communication</p>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of IT strategic and tactical planning exists in isolation.</li> <li>□ Minimum skills required to perform IT strategic and tactical planning have not been identified.</li> <li>□ Training needs for IT strategic and tactical planning have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership has the skills and expertise to perform basic IT strategic and tactical planning.</li> <li>□ Minimum skill requirements to perform basic IT infrastructure planning have been identified.</li> <li>□ Training in IT strategic planning is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership has the skills and expertise to perform all key IT strategic and tactical planning processes.</li> <li>□ Skill requirements for all aspects of IT strategic and tactical planning have been defined and documented.</li> <li>□ A formal training plan for IT strategic and tactical planning has been developed.</li> <li>□ Formal training in IT strategic and tactical planning is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the expertise to perform all IT strategic and tactical planning processes.</li> <li>□ Proficiency in critical aspects of IT strategic and tactical planning is ensured for individuals who perform these processes.</li> <li>□ A formal training plan for IT strategic and tactical planning is implemented.</li> <li>□ Skill requirements for IT infrastructure planning are reviewed and updated on a regular basis.</li> <li>□ Formal training for IT strategic and tactical planning is required for individuals who perform these processes.</li> <li>□ Certification in IT strategic and tactical planning is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of IT strategic and tactical planning is ensured for individuals who perform these processes.</li> <li>□ The jurisdiction encourages formal training in IT strategic and tactical planning, based upon personal and jurisdiction goals.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into the IT Strategic Plan and tactical plans.</li> </ul>
	Skills and Expertise				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>Allocation of responsibility for IT strategic and tactical planning is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for IT strategic and tactical planning is done informally.</li> <li>Individuals assume responsibility for IT strategic and tactical planning.</li> <li>There is confusion about who is responsible and accountable for IT strategic and tactical planning when issues arise.</li> <li>Ownership of the IT Strategic Plan is viewed as resting with the IT department.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability and responsibility for IT strategic and tactical planning have been formally assigned and documented.</li> <li>IT strategic and tactical planning process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>IT strategic and tactical planning process owners have the level of authority required to fulfill their responsibilities.</li> <li>Ownership of the IT Strategic Plan is viewed as resting with senior leadership.</li> </ul>	<ul style="list-style-type: none"> <li>IT strategic and tactical planning process owners are empowered to make decisions and to take action.</li> <li>IT strategic and tactical planning process owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability				

PEOPLE (continued)

Maturity Level	
<b>1: Initial</b>	<b>5: Optimized</b>
<b>2: Repeatable</b>	<b>4: Managed</b>
<b>3: Defined</b>	<b>5: Optimized</b>
<b>1: Initial</b>	<b>4: Managed</b>
<b>2: Repeatable</b>	<b>4: Managed</b>
<b>3: Defined</b>	<b>4: Managed</b>
<b>4: Managed</b>	<b>5: Optimized</b>
<b>5: Optimized</b>	<b>5: Optimized</b>

Attributes

Policies, Plans and Procedures

**PROCESS**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Some IT strategic and tactical planning goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> IT strategic goals are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> The performance of IT strategic and tactical planning is monitored informally.</li> <li><input type="checkbox"/> The link between IT strategic goals and jurisdiction objectives is indirect.</li> <li><input type="checkbox"/> Measures reflected in IT strategic and tactical plans are stated almost exclusively as objectives or financial measures.</li> <li><input type="checkbox"/> Measures used to assess IT strategic and tactical planning are derived from the defaults available in software-based tools.</li> <li><input type="checkbox"/> IT leadership provides basic reports about the status of strategic and tactical plans.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> The performance of IT strategic and tactical planning is monitored regularly.</li> <li><input type="checkbox"/> The link between IT strategic goals and jurisdiction objectives is clear and direct.</li> <li><input type="checkbox"/> Measures in the IT Strategic Plan and tactical plans reflect a mixture of financial, non-financial and educational objectives, as appropriate.</li> <li><input type="checkbox"/> IT leadership regularly reports to senior leadership about the status of the IT Strategic Plan and tactical plans.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Measures reflected in the IT Strategic Plan and tactical plans reflect a mixture of leading and lagging indicators.</li> <li><input type="checkbox"/> Performance measures in the IT Strategic Plan are used to inform decision making and continuous improvement.</li> <li><input type="checkbox"/> Senior leadership is provided with regular and formalized reports of the status of the IT Strategic Plan and tactical plans.</li> <li><input type="checkbox"/> Risks and benefits of major strategic decisions are formally recognized, monitored and measured.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into IT strategic planning, linking IT performance to jurisdiction objectives.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for IT strategic and tactical planning is performed.</li> <li><input type="checkbox"/> IT strategic and tactical planning processes are monitored and measured.</li> </ul>	
	<p style="text-align: right;">Goal Setting and Measurement</p>				

PROCESS (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT strategic and tactical planning; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support IT strategic and tactical planning.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT strategic and tactical planning has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT strategic and tactical planning is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools have been implemented.</li> <li>□ Integration of tools to support IT strategic and tactical planning is emerging.</li> <li>□ There is a formal and structured approach to tool use.</li> <li>□ Tools are used in key areas to automate and formalize IT strategic and tactical planning.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used, jurisdiction wide, to support IT strategic and tactical planning.</li> <li>□ IT strategic and tactical planning tools are integrated with other jurisdiction planning tools.</li> </ul>
	Tools and Automation				

**TOOLS**

## Determine Technology Direction

### Description

The jurisdiction's technology direction, combined with technical standards and guidelines, strike a balance between provision of efficient support for IT services and ensuring that the jurisdiction's strategic and operational goals are met.

Technology standards and guidelines minimize the complexity of the technology environment. Effective processes for handling exceptions ensure that jurisdiction operational and strategic objectives are not a consideration secondary to standards.

This process area includes setting a technological direction, creating an IT Infrastructure Plan, and creating and maintaining technology standards and guidelines.

### Value

- Sets and manages clear and realistic expectations of what IT can offer, in terms of services, given the degree of variation in the technology environment.
- Creates transparency around the process used to make decisions about IT standards and guidelines.
- Supports purposeful decision making about what technology standards should be implemented and how exceptions will be handled.

### Goals

- Balance efficiency of IT operations and effectiveness of IT services to support the jurisdiction's strategic and operational goals and objectives.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

### Key Activities

#### Plan the technological direction.

- Implement a process to create and maintain a plan for the technological direction of the jurisdiction that addresses systems architecture, migration strategies, technology acquisition and contingency arrangements.

#### Create and maintain an IT Infrastructure Plan that supports the IT Strategic Plan.

- Ensure that changes in the educational environment, staffing, technology investments and the interoperability of technology platforms and applications are considered when developing or maintaining the IT Infrastructure Plan.

#### Analyze and monitor trends, including existing and emerging technologies, best practices in other school jurisdictions, and legal and regulatory requirements.

- Implement a process to monitor technology trends, emerging educational practices and regulations that may contribute to or impact the jurisdiction's technological direction.

**Create and maintain technology standards and guidelines.**

- Implement a process to seek input from relevant stakeholders into technology standards and guidelines for the jurisdiction.
- Implement a process to evaluate, formally decide upon and monitor exceptions to standards and guidelines.
- Document, communicate and gain commitment to standards and guidelines.
- Review and revise standards and guidelines on a regular basis.

**RACI Chart**

Activities	Roles				
Plan the technological direction.					
Create and maintain an IT Infrastructure Plan.					
Analyze and monitor trends.					
Create and maintain technology standards and guidelines.					

**RACI Responsibilities**

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

### Maturity Model – Determine Technology Direction

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> 1: Initial	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need to set a technological direction and to plan infrastructure.</li> <li><input type="checkbox"/> The need to set a technological direction and to plan infrastructure is communicated inconsistently.</li> <li><input type="checkbox"/> Technological direction and IT infrastructure planning are discussed at IT leadership meetings in response to issues or requests for information.</li> <li><input type="checkbox"/> Communication to stakeholders about IT standards, guidelines and technology trends is sporadic.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership communicates commitment to the jurisdiction's technological direction.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss technological direction and the IT Infrastructure Plan on a regular basis.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss the impact of the technological direction and the IT Infrastructure Plan on the process of education.</li> <li><input type="checkbox"/> Communication to stakeholders about the technological direction, the IT Infrastructure Plan, standards and guidelines occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership, IT leadership and school administrators discuss and review the potential educational impact of technological change.</li> <li><input type="checkbox"/> Communication to stakeholders about the technological direction, standards and guidelines occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of the requirements for the jurisdiction's technological direction and IT Infrastructure Plan.</li> <li><input type="checkbox"/> Communication of emerging trends and issues occurs in a formal and proactive way.</li> </ul>
		<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to set a technological direction.</li> <li><input type="checkbox"/> IT leadership understands the requirements to set a technological direction and to develop an IT Infrastructure Plan.</li> <li><input type="checkbox"/> The need to set a technological direction and to plan the infrastructure is communicated consistently.</li> <li><input type="checkbox"/> Technological direction and IT infrastructure planning are discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about the technological direction, the IT Infrastructure Plan, standards and guidelines occurs periodically.</li> </ul>			

PEOPLE

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of IT infrastructure planning exists in isolation.</li> <li>□ Minimum skills required to perform IT infrastructure planning have not been identified.</li> <li>□ Training needs for IT infrastructure planning have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the expertise to perform basic IT infrastructure planning.</li> <li>□ Minimum skill requirements to perform basic IT infrastructure planning have been identified.</li> <li>□ Training in IT infrastructure planning is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all key IT infrastructure planning processes.</li> <li>□ Skill requirements for IT infrastructure planning processes have been defined and documented.</li> <li>□ A formal training plan for IT infrastructure planning has been developed.</li> <li>□ Formal training for IT infrastructure planning is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the expertise to perform all IT infrastructure planning processes.</li> <li>□ Proficiency in critical aspects of IT infrastructure planning is ensured for individuals who perform these processes.</li> <li>□ A formal training plan for IT infrastructure planning is implemented.</li> <li>□ Skill requirements for IT infrastructure planning are reviewed and updated on a regular basis.</li> <li>□ Formal training for IT infrastructure planning is required for individuals who perform these processes.</li> <li>□ Certification in IT infrastructure planning is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of IT infrastructure planning is ensured for individuals who perform these processes.</li> <li>□ The jurisdiction encourages formal training in IT infrastructure planning, based upon personal and jurisdiction goals.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into the IT Infrastructure Plan.</li> </ul>
	Skills and Expertise				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for IT infrastructure planning is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT infrastructure planning is done informally.</li> <li>□ Individuals assume responsibility for IT infrastructure planning.</li> <li>□ There is confusion about who is responsible and accountable for IT infrastructure planning when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT infrastructure planning have been formally assigned and documented.</li> <li>□ IT infrastructure planning process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT infrastructure owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT infrastructure planning process owners are empowered to make decisions and to take action.</li> <li>□ IT infrastructure planning process owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability	<b>PEOPLE (continued)</b>			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT infrastructure planning activities are based upon individual IT staff practices.</li> <li><input type="checkbox"/> Development of the technological direction and IT infrastructure planning occur in isolation from IT strategic planning.</li> <li><input type="checkbox"/> Evaluation of emerging technologies, trends and best practices occurs in an unplanned, ad hoc way.</li> <li><input type="checkbox"/> Technology standards and guidelines are developed in response to issues and in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT infrastructure planning are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT infrastructure planning policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Compliance with IT infrastructure standards and guidelines is left to the individual's discretion.</li> <li><input type="checkbox"/> A consistent approach to planning infrastructure and developing standards and guidelines is followed.</li> <li><input type="checkbox"/> Decisions related to technological direction and the IT Infrastructure Plan are made on a project-by-project basis.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all key IT infrastructure planning activities are defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> IT leadership develops infrastructure plans, standards and guidelines with input from IT staff.</li> <li><input type="checkbox"/> There is a process in place to regularly review and update the IT Infrastructure Plan and existing standards and guidelines.</li> <li><input type="checkbox"/> There is a process in place to assess, decide upon and monitor exceptions to standards and guidelines.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT infrastructure planning activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> Senior leadership approves policies and procedures for IT infrastructure planning.</li> <li><input type="checkbox"/> Senior leadership and school jurisdiction stakeholders are involved in setting the jurisdiction's technological direction and technology standards and guidelines.</li> <li><input type="checkbox"/> Migration plans to introduce new technologies are developed when planning the technological direction.</li> <li><input type="checkbox"/> A process is implemented to regularly evaluate evolving and emerging technologies.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT infrastructure planning is coordinated with IT strategic planning.</li> <li><input type="checkbox"/> Generally accepted best practices and standards for IT infrastructure planning are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT infrastructure planning policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT infrastructure planning policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				
<b>PROCESS</b>					

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>Some IT infrastructure planning goals are set and monitored inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li>The effectiveness of IT infrastructure planning, and standards and guidelines development is monitored regularly.</li> <li>There is a clear link between the IT Infrastructure Plan and the IT Strategic Plan.</li> <li>Measurement of cost and value of the technology infrastructure is emerging.</li> <li>Senior leadership is provided with regular reports about the status and effectiveness of the IT infrastructure.</li> </ul>	<ul style="list-style-type: none"> <li>IT infrastructure planning, and standards and guidelines development performance metrics are formally defined and approved, and align to the IT Strategic Plan.</li> <li>Measures of the effectiveness of the IT Infrastructure Plan and related standards and guidelines are used to inform decision making and continuous improvement.</li> <li>There is a process in place to address deviations from technology standards.</li> </ul>	<ul style="list-style-type: none"> <li>Peer- and sector-based benchmarking for IT infrastructure planning is performed.</li> <li>The processes used to develop the technological direction, IT Infrastructure Plan, and standards and guidelines are monitored and measured.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT infrastructure planning; they are generally based upon standard desktop tools.</li> <li>□ There is a formal approach to using tools to support the development of the technological direction, IT Infrastructure Plan, standards or guidelines.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to IT infrastructure planning and the development of standards and guidelines, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support IT infrastructure planning and the development of standards and guidelines are emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT infrastructure planning and the development of standards and guidelines has been developed.</li> <li>□ The basic level of functionality in tools and templates to support IT infrastructure planning and the development of standards and guidelines is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT infrastructure planning and the development of standards and guidelines have been implemented.</li> <li>□ Integration of tools to support IT infrastructure planning and the development of standards and guidelines is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT infrastructure planning and the development of standards and guidelines.</li> <li>□ Tools are used in key areas to automate and formalize IT infrastructure planning and the development of standards and guidelines.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support the development of the technological direction, IT infrastructure planning and the development of standards and guidelines.</li> </ul>
	Tools and Automation				

**TOOLS**

## Define IT Relationship, Organization and Processes

### Description

There is no one “right” way to position IT within an organization. Nor is there a one-size-fits-all design for the organization of the IT department itself. Both are driven by how the IT department is seen as contributing to the strategic objectives of the jurisdiction. The relationship required for an IT department that is seen as strictly functional (i.e., providing efficient support for technology needs) is vastly different than that required when IT is viewed as supporting transformation in the jurisdiction.

Functional	Differentiating	Contributing	Differentiating	Transformational
IT manages and operates technology systems and resources efficiently.	IT builds and operates systems defined by the jurisdiction.	IT uses technology proactively to enhance operations and to raise jurisdiction performance.	IT helps the jurisdiction leverage technology resources to provide new services for stakeholders.	IT operates at the cutting edge of transformation and technology to support transformation of educational practice.

*Adapted from “Organizing for Success”, Gartner, Inc. March 2010.*

The capability level of the IT organization is a critical factor in determining its position within the organization. An IT department with functional capabilities is not ready to fill a transformational role.

This process area includes evaluation of the current and the desired state of operations for the IT department, in the context of jurisdiction IT strategy, and evaluation of the capabilities, organizational structures and processes required to reach the desired state.

During this process, specific attention must be paid to risk management, delegation of information and systems ownership, and quality assurance.

### Value

- Provides clear and appropriate direction to the IT department.
- Supports oversight by senior leadership.

### Goals

- Establish a clear reporting relationship and delegation of authority between senior leadership and the IT department.
- Provide a means to clearly communicate IT leadership expectations.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

## Key Activities

**Position the IT department in the jurisdiction's organizational structure** in consideration of how IT is viewed as contributing to strategic objectives and the overall capability level of the IT department.

**Establish an IT department organizational structure** that best supports the jurisdiction's objectives.

- Implement a process to periodically review the IT organizational structure to adjust resource requirements to meet the jurisdiction's objectives and changing circumstances.

**Establish IT governance committees**, engaging stakeholders, where appropriate, to provide oversight and direction to the IT department.

- Provide a forum to receive advice and feedback relating to strategic direction, IT priorities and initiatives, technological direction, information security and service levels and to ensure that IT governance is addressed

**Implement an IT process framework** that supports execution of IT strategic and tactical plans.

- Articulate an IT process structure and the relationships between processes to address gaps and overlaps.

**Define and implement IT roles and responsibilities**, including supervision and segregation of duties.

- Communicate the roles of IT staff and end users, in relation to authority, responsibilities and accountability for meeting the jurisdiction's needs.
- Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether staff have sufficient authority and resources to execute their roles and responsibilities, and to provide oversight.
- Implement a division of roles and responsibilities to reduce the possibility of a single individual compromising a critical process.
- Ensure that IT staff perform only the duties authorized and relevant to their position.

**Identify system and data owners** and empower them to address their responsibilities.

**Assign responsibility for risk, security and compliance.**

- Ensure that responsibility for IT-related risks is delegated explicitly and appropriately.

## RACI Chart

Activities	Roles				
Position the IT department in the jurisdiction's organizational structure.					
Establish an organizational structure for the IT department.					
Establish IT governance committees.					
Implement an IT process framework.					
Define and implement IT roles and responsibilities.					
Identify system and data owners.					
Assign responsibility for risk, security and compliance.					

## RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Define IT Relationships, Organization and Processes

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> Awareness, Understanding and Communication	<b>1: Initial</b> IT leadership is aware of the need to position the IT department within the jurisdiction, in accordance with the strategic and operational importance of IT.  IT leadership is aware of the need for an IT governance committee and an IT process framework.  The need for appropriate positioning of the IT department within the jurisdiction, an IT governance committee and an IT process framework is communicated inconsistently.  Communication channels within the IT department are unclear to end users and stakeholders.	Senior leadership is aware of the need to position the IT department within the jurisdiction, in accordance with the strategic and operational importance of IT.  IT leadership understands the requirements to implement basic IT structures, processes and procedures.  The IT structure, processes, procedures and regulations are communicated to stakeholders periodically.	Senior leadership is aware of IT relationships, organization and processes.  IT leadership is aware of the requirements to implement IT structures, processes and procedures.  Communication to stakeholders about IT structure, processes, procedures and regulations occurs on a regular basis and in a formal way.  IT staff are aware of their roles and responsibilities for information systems and data.  End users understand their responsibilities for information security.	Senior leadership has a full understanding of the IT relationships, organization and processes.  IT leadership informs senior leadership of the effectiveness of IT relationships, organization and processes on a regular basis.  Communication to stakeholders about IT relationships, organization and processes occurs on a regular basis and in a formal way.  End users understand their responsibilities and accountabilities for data and data ownership.  Relationships with external third parties are formalized.	IT leadership has an advanced and forward-looking understanding of IT relationships, organization and processes, and how they support jurisdiction objectives.  End users understand the roles and responsibilities of the IT department and understand the relationship of IT to senior leadership and rest of the organization.  Senior leadership understands the relationship of external third parties to the jurisdiction in general and to the IT department specifically.
	<b>PEOPLE</b>				

Maturity Level		5: Optimized			
Attributes		4: Managed	3: Defined	2: Repeatable	1: Initial
PEOPLE (continued)		Skills and Expertise			
<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT process frameworks and how to implement them exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to implement an IT process framework have not been identified.</li> <li><input type="checkbox"/> Training needs for implementing an IT process framework have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the skills and expertise to implement basic IT structures, processes and procedures.</li> <li><input type="checkbox"/> Minimum skill requirements for basic aspects of implementing IT structures, processes and procedures have been identified.</li> <li><input type="checkbox"/> Training in the implementation of IT structures, processes and procedures is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the skills and expertise to perform all processes related to defining IT organization and processes.</li> <li><input type="checkbox"/> IT staff have the skills and expertise to perform all key aspects of defining IT processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of defining IT organization and processes is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for defining IT organization and processes have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for defining IT organization and processes has been developed.</li> <li><input type="checkbox"/> Formal training for defining IT organization and processes is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the skills and expertise to perform all processes related to defining IT organization and processes.</li> <li><input type="checkbox"/> IT staff have the skills and expertise to perform all aspects of defining IT processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of defining IT organization and processes is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for defining IT organization and processes are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for defining IT organization and processes is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in defining IT organization and processes is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff have the skills and expertise to implement and monitor IT processes.</li> <li><input type="checkbox"/> Proficiency in all aspects of defining IT organization and processes is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in defining IT organization and processes, based on personal and jurisdictional goals.</li> <li><input type="checkbox"/> External experts are engaged to provide advice and input into the jurisdiction's IT organization and processes.</li> </ul>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Allocation of responsibility and accountability for the implementation of IT structures, processes and procedures is done informally.</li> <li><input type="checkbox"/> Individuals assume responsibility for implementing IT structures, processes and procedures.</li> <li><input type="checkbox"/> There is confusion about who is responsible and accountable for IT structures, processes and procedures when issues arise.</li> <li><input type="checkbox"/> Ad hoc committees are convened to provide input into IT strategic planning or IT operations.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Accountability and responsibility for defining IT organization and processes have been formally assigned and documented.</li> <li><input type="checkbox"/> IT organization and process design process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> <li><input type="checkbox"/> Duties that relate to information security are segregated, when required.</li> <li><input type="checkbox"/> Formal IT governance committees are in place and serve in an advisory capacity.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT organization and process design process owners have the level of authority required to fulfill their responsibilities.</li> <li><input type="checkbox"/> Ownership of information and systems is clearly articulated and authority to act has been delegated.</li> <li><input type="checkbox"/> System owners are held accountable for their systems and data ownership.</li> <li><input type="checkbox"/> Formal governance committees provide guidance and oversight.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is engaged in defining the IT organizational structure.</li> <li><input type="checkbox"/> Roles and responsibilities of IT governance committee members are defined, documented and communicated.</li> <li><input type="checkbox"/> End users are accountable for their use of information systems and data.</li> </ul>	
	<ul style="list-style-type: none"> <li><input type="checkbox"/> Allocation of responsibility for implementing an IT process framework is done in an ad hoc way.</li> <li><input type="checkbox"/> System and data ownership is not clearly assigned.</li> <li><input type="checkbox"/> Responsibility and accountability for risk, security and compliance are not clearly assigned.</li> <li><input type="checkbox"/> Roles and responsibilities for defining IT organization and processes are not clearly defined.</li> </ul>	<p style="text-align: right;">Responsibility and Accountability</p>			

**PEOPLE (continued)**

**PROCESS**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>□ Implementation of portions of an IT process framework occurs in isolation and is based upon individual IT staff practices.</li> <li>□ Definition of the IT department's relationship to the jurisdiction is performed reactively and informally.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for the implementation of IT structures, processes and procedures are defined, but not documented.</li> <li>□ Compliance with policies for the implementation of IT structures, processes and procedures is left to the individual's discretion.</li> <li>□ Basic IT processes and procedures have been defined, but not documented.</li> </ul>	<ul style="list-style-type: none"> <li>□ Organization of the IT department is defined, documented and communicated.</li> <li>□ Key activities related to IT operations and management have been defined and documented in the IT process framework.</li> <li>□ Policies and procedures in the process framework are based upon generally accepted good practices.</li> </ul>	<ul style="list-style-type: none"> <li>□ The organization of the IT department appropriately reflects educational needs and objectives, and contains capabilities required to meet those objectives.</li> <li>□ Most activities related to IT operations have been defined and documented in the IT process framework; activities are formally approved and regularly reviewed and updated.</li> <li>□ Standard processes to define IT organization and processes are consistently followed.</li> </ul>	<ul style="list-style-type: none"> <li>□ Generally accepted best practices and standards for procedure and policy development are used.</li> <li>□ Policies and procedures are standardized and integrated.</li> <li>□ The IT department adapts to the jurisdiction's changing needs and objectives.</li> </ul>	
	<p>Policies, Plans and Procedures</p>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some goals for the implementation of an IT process framework are set and monitored inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li>□ Implementation of IT structures, processes and procedures is monitored informally.</li> <li>□ Measures for implementation of IT structures, processes and procedures emphasize achievement of objectives.</li> <li>□ IT leadership provides basic status reports about the implementation of IT structures, processes and procedures.</li> </ul>	<ul style="list-style-type: none"> <li>□ The effectiveness of IT processes and relationships is monitored regularly.</li> <li>□ Senior leadership and IT governance committee members seek input related to the effectiveness and efficiency of the IT governance committee.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance goals are formally defined and approved, and align to the IT Strategic Plan.</li> <li>□ Measures of the effectiveness of the IT organization and process framework are used to inform decision making and continuous improvement.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance goals are monitored.</li> <li>□ Peer- and sector-based benchmarking of the IT organization and processes is performed.</li> <li>□ IT organization and processes are monitored and measured.</li> </ul>
	Goal Setting and Measurement	<p style="text-align: right;"><b>PROCESS (continued)</b></p>			

Maturity Level		Attributes			
<b>TOOLS</b>	<b>1: Initial</b>	<b>2: Repeatable</b>	<b>3: Defined</b>	<b>4: Managed</b>	<b>5: Optimized</b>
	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support implementation of the IT process framework; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no consistent approach to using tools to support implementation of the IT process framework.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Basic tools and templates, specific to implementing IT structures, processes and procedures, have been developed and implemented.</li> <li><input type="checkbox"/> Common approaches to the use of tools to support implementation of IT structures, processes and procedures are emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan to acquire and implement tools to support the development and maintenance of the IT process framework, and to design, monitor and manage the IT organization has been developed.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates to support development and maintenance of the IT process framework, and to design, monitor and manage the IT organization is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support the development and maintenance of the IT process framework and to design, monitor and manage the IT organization have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support the development and maintenance of the IT process framework and to design, monitor and manage the IT organization is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support the development and maintenance of the IT process framework and to design, monitor and manage the IT organization.</li> <li><input type="checkbox"/> Tools are used in key areas to formalize the development and maintenance of the IT process framework and to design, monitor and manage the IT organization.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support the development and maintenance of the IT process framework.</li> </ul>

Tools and Automation

## Manage IT Investments

### Description

There is no single right answer for how much investment in technology is enough in the K-12 education sector. School jurisdictions determine the appropriate levels of investment in technology by evaluating the costs, risks and expected benefits of initiatives.

IT investments are defined in this context as capital investment in technology. They include required (operational) and discretionary (initiatives) spending. IT spending can be further categorized into three areas: run (keep the lights on), grow (devise new services for stakeholders) and transform (support transformation of teaching and learning practices).

Mature IT investment management processes ensure that individual investments are considered in the context of a larger portfolio. For example, investment in maintaining a school jurisdiction's student information system should be balanced against investments in classroom technologies that support student learning, rather than evaluated in isolation.

This process area includes identifying and analyzing opportunities, based upon cost, benefit and risk, prioritization and ongoing monitoring.

### Value

- Ensures that IT investments are managed to maximize value realized and minimize risks and costs and that investments are aligned to jurisdiction strategic and operational goals.
- Enables senior leadership to sustain a comprehensive understanding of the jurisdiction's IT investments.
- Provides insight for senior leadership into the expected and actual value to be realized by implementing technology.

### Goals

- Ensure effective and efficient use of jurisdiction resources.
- Promote transparency and accountability for IT investment, from selection to reporting benefits realization.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

### Key Activities

**Establish and maintain a financial management framework for IT** to manage the overall investment and cost of IT resources and services.

**Evaluate, prioritize and select services** to receive IT funding.

**Establish and maintain IT budgeting processes** to support preparation of a budget that reflects established IT priorities, upcoming projects, ongoing costs of operation and maintenance of existing services.

**Monitor and manage IT expenditures**, comparing actual costs to budgets.

- Implement a process to monitor and report IT expenditures.
- Identify, assess, address and report budget variances in a timely manner.

**Monitor and report on IT benefits and value realization** delivered by the current IT portfolio of services.

- Implement a process to regularly identify and communicate the value realization of IT investments that further jurisdiction objectives.
- Ensure that the performance of the portfolio of IT investments is regularly reviewed and optimized.

**Manage the portfolio of IT enabled investments** required to achieve jurisdiction goals.

- Implement a process to define, evaluate, prioritize, select and initiate the required IT services.
- Implement a process to regularly review and adjust the IT portfolio.

### RACI Chart

Activities	Roles				
Establish and maintain a financial management framework for IT.					
Evaluate prioritize and select services.					
Establish and maintain IT budgeting processes.					
Monitor and manage IT expenditures.					
Monitor IT benefits and value realization.					
Manage the portfolio of IT-enabled investments.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Manage IT Investments

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> 1: Initial Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need to manage IT investments.</li> <li><input type="checkbox"/> The need to manage IT investments is communicated inconsistently.</li> <li><input type="checkbox"/> IT investment management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of IT and the performance of IT investments is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to manage IT investments.</li> <li><input type="checkbox"/> IT leadership understands the requirements of an effective IT investment management process.</li> <li><input type="checkbox"/> The need for an IT investment management process is communicated consistently.</li> <li><input type="checkbox"/> IT investment management is discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about IT investment value and benefits realization occurs periodically.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership understands the requirements of an effective IT investment management process.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of a sound IT investment management process.</li> <li><input type="checkbox"/> Senior leadership and IT leadership discuss IT investments on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about IT investment plans occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership actively participates in managing IT investments.</li> <li><input type="checkbox"/> Communication to stakeholders about IT investment performance occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of IT investments.</li> <li><input type="checkbox"/> The IT governance committee governs and manages IT investments.</li> <li><input type="checkbox"/> The IT governance committee is regularly briefed on the performance of IT investments.</li> </ul>

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT investment management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to manage IT investments have not been identified.</li> <li><input type="checkbox"/> Training needs for IT investment management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the skills and expertise to perform basic IT investment planning.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic IT investment planning have been identified.</li> <li><input type="checkbox"/> Training in IT investment planning is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key IT investment management processes.</li> <li><input type="checkbox"/> Skill requirements are defined for all areas of IT investment management.</li> <li><input type="checkbox"/> A formal training plan has been developed for IT investment management.</li> <li><input type="checkbox"/> Formal training for IT investment management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all IT investment management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT investment management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> A formal training plan for IT investment management is implemented.</li> <li><input type="checkbox"/> Skill requirements for IT investment management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for IT investment management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT investment management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT investment management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT investment management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into IT investment selection.</li> </ul>
	<p style="text-align: right;"><b>PEOPLE (continued)</b></p>	Skills and Expertise			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for IT investment management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT investment management is done informally.</li> <li>□ Individuals assume responsibility for IT investment management.</li> <li>□ There is confusion about who is responsible and accountable for IT investment management when issues arise.</li> <li>□ Ownership of IT investments is viewed as resting with the IT department.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT investment management have been formally assigned and documented.</li> <li>□ IT investment management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT investment management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT investment management process owners are empowered to make decisions and to take action.</li> <li>□ IT investment process owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT investment management are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT investment management policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Reactive, tactical and cost-focused budgeting decisions occur.</li> <li><input type="checkbox"/> A process to monitor and report on IT benefits realization is emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key IT investment management and budgeting processes are defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> Investment decisions are evaluated within the context of the entire IT investment portfolio.</li> <li><input type="checkbox"/> IT budgeting and investment selection decisions are aligned with the IT Strategic Plan.</li> <li><input type="checkbox"/> Formal approval of IT investment decisions occurs.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT investment activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> Senior leadership approves policies and procedures for IT investment management.</li> <li><input type="checkbox"/> A formalized process for IT investment selection and budgeting is consistently followed.</li> <li><input type="checkbox"/> Formal costing analysis that includes calculation of direct and indirect costs, over the entire life cycle of proposed and operational services, is consistently performed.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT investment management is coordinated and integrated into the jurisdiction's financial management practices.</li> <li><input type="checkbox"/> IT investment benefits realization plans are documented and implemented.</li> <li><input type="checkbox"/> IT projects are cancelled when they do not realize expected benefits.</li> <li><input type="checkbox"/> Exceptions to IT investment management processes are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT investment management policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT investment management activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> A process to evaluate, prioritize and select services to receive IT funding does not exist.</li> <li><input type="checkbox"/> IT investments are justified, on an as-needed basis, usually in response to requests.</li> <li><input type="checkbox"/> Technology investment decisions are made on a project-by-project basis.</li> <li><input type="checkbox"/> A process to monitor and report on IT benefits and value realization does not exist.</li> </ul>			

## PROCESS

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some IT investment performance goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> IT investment goals are unclear or vaguely defined.</li> <li><input type="checkbox"/> Performance of IT investments is measured primarily on the basis of cost.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of the IT investment management process is monitored informally.</li> <li><input type="checkbox"/> Metrics for the performance of the IT investment management process are informally defined.</li> <li><input type="checkbox"/> Informal monitoring of the benefits and value realized by IT investments occurs inconsistently.</li> <li><input type="checkbox"/> Metrics for the benefits and value of IT investments are defined informally.</li> <li><input type="checkbox"/> Basic reporting on the performance of IT investments is defined and used inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of IT investments is monitored regularly.</li> <li><input type="checkbox"/> The link between IT investment goals and the IT Strategic Plan is clear and direct.</li> <li><input type="checkbox"/> Measures of IT investment performance reflect a mix of financial, non-financial and educational objectives, as appropriate.</li> <li><input type="checkbox"/> Benefits are tracked and reported, using measures of financial value, strategic alignment and risk.</li> <li><input type="checkbox"/> IT leadership provides senior leadership and the IT governance committee with regular reports about the performance of IT investments.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT investment metrics are formally defined and align to the IT Strategic Plan.</li> <li><input type="checkbox"/> IT investment metrics reflect a mixture of leading and lagging indicators.</li> <li><input type="checkbox"/> Measures of the effectiveness of IT investment management is used to inform decision making and continuous improvement and to ensure that planned benefits are achieved, sustained and optimized.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Peer- and sector-based benchmarking for IT investment performance and management is used to identify areas for improvement.</li> <li><input type="checkbox"/> IT investment management processes are monitored and measured.</li> </ul>
	<p style="text-align: right;">Goal Setting and Measurement</p>				

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT investment management; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support IT investment management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to IT investment management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support IT investment management are emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT investment management has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT investment management is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT investment management have been implemented.</li> <li>□ Integration of tools to support IT investment management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT investment management.</li> <li>□ Tools are used in key areas to automate and formalize IT investment management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support IT investment management.</li> <li>□ IT investment management tools are integrated with other jurisdiction financial management tools.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

## Communicate Management Aims and Direction

### Description

The overall vision and strategic direction for the use of technology in school jurisdictions must be communicated clearly and effectively to all staff. Through ongoing communication and clearly defined policies and procedures, staff have a clearer understanding of what is expected of them and senior leadership has a greater degree of assurance that staff understand what is expected.

This process area includes directional communications that describe how technology should be used in the classroom and operational communications that set standards for behaviour, such as security policies and procedures, and guidelines for acceptable use.

This process area supports the development of the policies, procedures, standards and guidelines for every other process area described in the School Technology Services Framework. It addresses:

- authorization to create a new policy, procedure, guideline, standard or strategy
- identification of and consultation with stakeholders
- development, review and revision of documents to communicate the new policy, procedure, guideline, standard or strategy
- approval and communication of the new policy, procedure, guideline, standard or strategy.

### Value

- Provides assurance to senior leadership that policies, strategic direction and expectations are communicated clearly and consistently.
- Ensures that leadership and stakeholders understand and are aware of the aims and direction for IT and the expectations for its use in the school jurisdiction.
- Reduces the time required to develop policies, procedures, guidelines, standards and so forth by outlining a consistent process to be followed.

### Goals

- Ensure awareness and understanding of policies, procedures and regulations related to the support and use of technology.
- Mitigate IT risks.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

## Key Activities

**Establish and maintain IT policies** that are consistent with jurisdiction philosophy, objectives and operating style.

- Implement a framework of policies that addresses expectations and requirements regarding delivery of value from IT investments, approach to risk, integrity, ethical use and IT staff and end user accountability and responsibility.

**Implement and maintain an IT process framework** that supports the jurisdiction in meeting its objectives while managing risk, cost and value.

- Implement a process to regularly review and update IT procedures.

**Communicate the IT policy and process framework**, IT strategy, objectives and direction to appropriate stakeholders in a timely way.

## RACI Chart

Activities	Roles				
Establish and maintain IT policies.					
Implement and maintain an IT process framework.					
Communicate the IT policy and process framework.					

## RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Communicate Management Aims and Direction

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> Awareness, Understanding and Communication	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for an IT policy and process framework.</li> <li><input type="checkbox"/> The need for an IT policy and process framework is communicated inconsistently.</li> <li><input type="checkbox"/> IT policies and processes are discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT policies, processes and procedures is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the requirements for an effective IT process framework.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development and implementation of a sound IT process framework.</li> <li><input type="checkbox"/> Critical IT processes are documented and communicated.</li> <li><input type="checkbox"/> Senior leadership and IT leadership communicate the importance of IT security awareness on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership assume responsibility for communicating IT policies and procedures.</li> <li><input type="checkbox"/> End users understand the objectives of the IT department and IT policies and processes that affect them.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of the requirements for the IT process framework.</li> <li><input type="checkbox"/> Communication of issues that may affect compliance with policies and procedures is proactive.</li> <li><input type="checkbox"/> End users are aware of emerging issues that may affect compliance with policies and procedures.</li> </ul>
	<b>PEOPLE</b>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT policy and process framework development and implementation exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to develop and implement an IT policy and process framework have not been identified.</li> <li><input type="checkbox"/> Training needs for IT policy and process framework development and implementation have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key IT process framework development processes.</li> <li><input type="checkbox"/> Skill requirements for all IT process framework development processes have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for IT process framework development has been developed.</li> <li><input type="checkbox"/> Formal training in IT process framework development is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all IT process framework development and management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT process framework development and management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> A formal training plan for IT process framework development and management is implemented.</li> <li><input type="checkbox"/> Formal training for IT process framework development and management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT process framework development and management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT process framework development and management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT process development and management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into the IT process framework.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>Allocation of responsibility for IT policy and process framework development and implementation is assumed or done in an ad hoc way.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for developing, maintaining and managing the IT policy process framework is done informally.</li> <li>Individuals assume responsibility for developing, maintaining and managing parts of the IT policy and process framework.</li> <li>There is confusion about who is responsible and accountable for developing, maintaining and managing IT policies and procedures when issues arise.</li> <li>Ownership of IT policies is viewed as resting with the IT department.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li>Accountability and responsibility for IT process framework development, management and communication have been formally assigned and documented.</li> <li>IT process framework development process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li>IT process framework management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>IT process framework development and management process owners are empowered to make decisions and to take action.</li> <li>IT process framework development and management process owners escalate issues, according to a defined escalation process.</li> </ul>	
	<p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>Allocation of responsibility for IT policy and process framework development and implementation is assumed or done in an ad hoc way.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for developing, maintaining and managing the IT policy process framework is done informally.</li> <li>Individuals assume responsibility for developing, maintaining and managing parts of the IT policy and process framework.</li> <li>There is confusion about who is responsible and accountable for developing, maintaining and managing IT policies and procedures when issues arise.</li> <li>Ownership of IT policies is viewed as resting with the IT department.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li>Accountability and responsibility for IT process framework development, management and communication have been formally assigned and documented.</li> <li>IT process framework development process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li>IT process framework management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>IT process framework development and management process owners are empowered to make decisions and to take action.</li> <li>IT process framework development and management process owners escalate issues, according to a defined escalation process.</li> </ul>

Responsibility and Accountability

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><b>Attributes</b></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>□ Development of IT policies, processes and procedures occurs in isolation and is based upon individual IT staff practices.</li> <li>□ Policies and procedures are developed and documented on an ad hoc basis.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for basic development, maintenance and management of the IT policy and process framework are defined, but not documented.</li> <li>□ Compliance with policies and procedures for the development, maintenance and management of the IT policy and process framework is left to the individual's discretion.</li> <li>□ Development of IT policies, processes and procedures considers cost, risk or value, but not all three.</li> </ul>	<ul style="list-style-type: none"> <li>□ A common, formal process for the approval of IT policies and procedures has been developed, documented and implemented.</li> <li>□ Formal requirements of an effective information control environment for the jurisdiction are documented.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for the approval of IT policies and procedures are defined, documented and regularly reviewed.</li> <li>□ IT leadership approves policies and procedures for IT process framework and management.</li> <li>□ Jurisdiction stakeholders, including end users, are involved in defining and reviewing IT policies and procedures.</li> </ul>	<ul style="list-style-type: none"> <li>□ The IT process framework supports the IT Strategic Plan and is regularly reviewed, updated and improved.</li> <li>□ Generally accepted best practices and standards are incorporated into the IT process framework.</li> <li>□ IT process framework development procedures are regularly reviewed and improved.</li> </ul>	
	<p>Policies, Plans and Procedures</p>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li>□ Some goals for IT policy process framework development and implementation are set and monitored inconsistently.</li> </ul>		<ul style="list-style-type: none"> <li>□ Development, maintenance, and implementation of the IT policy and process framework are monitored informally.</li> <li>□ Metrics for the development, maintenance, management and implementation of the IT policy and process framework are defined informally.</li> </ul>	<ul style="list-style-type: none"> <li>□ Compliance with critical processes included in the IT process framework is monitored regularly.</li> <li>□ Basic measures are based upon lagging indicators, such as rate of non-compliance.</li> <li>□ Compliance monitoring is consistent for all areas of the IT process framework.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT process framework development and management metrics are formally defined and approved, and align to the IT Strategic Plan.</li> <li>□ Measures of the effectiveness of the IT process framework are used to inform decision making and continuous improvement.</li> <li>□ There is a process in place to address incidences of non-compliance.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance management is incorporated into the IT process framework.</li> <li>□ Peer- and sector-based benchmarking for the IT process framework is used to identify areas for improvement.</li> <li>□ IT policy and procedure monitoring, self-assessment and compliance checking occurs consistently.</li> <li>□ IT process framework development, management and implementation processes are monitored and measured.</li> <li>□ Effectiveness of the communication of the IT process framework is measured and monitored.</li> </ul>
	Goal Setting and Measurement <b>PROCESS (continued)</b>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>TOOLS</b>	<i>Attributes</i>	<b>1: Initial</b>	<b>3: Defined</b>	<b>4: Managed</b>	<b>5: Optimized</b>
	Tools and Automation	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support the development and implementation of an IT policy and process framework; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no consistent approach to using tools to support the development and implementation of an IT policy and process framework.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan to acquire and implement tools to support the development, management and implementation of the IT policy and process framework has been developed.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates to support the development, maintenance, management and implementation of the IT policy and process framework is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support the development, management and implementation of the IT policy and process framework have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support the development, management and implementation of the IT policy and process framework is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support the development, management and implementation of the IT policy and process framework.</li> <li><input type="checkbox"/> Tools are used in key areas to automate the development, management and implementation of the IT policy and process framework.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support the development and communication of IT policies and procedures.</li> <li><input type="checkbox"/> Tools for IT process framework development and communication are integrated with tools used to develop and communicate other jurisdiction policies, procedures and regulations.</li> </ul>

## Manage IT Human Resources

### Description

Effective, efficient and well-managed IT services are delivered by skilled IT staff. Ensuring that the jurisdiction has an appropriate complement of IT staff available to meet operational and strategic objectives is critical.

In the K-12 education sector, the ideal is to have IT staff that possess skills in the technical, management and education sectors. The depth of expertise required in each of these domains varies by job role.

This process area includes identifying the skills required to meet strategic and operational needs and then ensuring that those skills are available, when needed, through training, hiring and/or contracting. The process of managing IT human resources supports increasing maturity in skills and expertise in all other process areas.

### Value

- Ensures that high quality, responsive IT services that meet current and future jurisdiction objectives are available, when required.

### Goals

- Ensure that appropriately skilled staff are available, when required, to meet the strategic and operational requirements of the jurisdiction.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership School Administrators IT Staff

### Key Activities

**Identify IT skills, expertise and core competencies** needed to realize jurisdiction objectives.

- Develop and maintain position descriptions for IT staff.
- Regularly verify that IT staff have the required competencies to fulfill their responsibilities, considering their education, training, certifications and experience.
- Develop and maintain an IT human resource recruitment plan.

**Implement a process for IT staff recruitment and retention** that aligns with the overall jurisdiction personnel policies and procedures.

- Implement a process to review IT staff responsibilities.
- Develop and implement a compensation framework for IT staff.

**Provide training for IT staff.**

- Implement an IT staff orientation process for new hires.
- Ensure that IT staff receive ongoing training to maintain and enhance their knowledge, skills and abilities to levels required to meet current and future jurisdiction requirements.

**Minimize key IT staff dependencies** through documentation, knowledge sharing, cross training, succession planning and IT staff backup.

- Identify key IT staff roles and implement procedures to minimize risk exposure.

**Monitor, supervise and evaluate IT staff**, based on their position description and responsibilities.

- Perform regular and timely IT staff evaluations, based upon individual objectives, established standards, specific job responsibilities and professional expectations.

**Implement an IT job change and termination process** to ensure that service continuity, knowledge transfer, reassigned responsibilities and removal of access rights are addressed.

### RACI Chart

Activities	Roles				
Implement a process for IT staff recruitment and retention.					
Identify IT skills, expertise and core competencies.					
Provide training for IT staff.					
Minimize key IT staff dependencies.					
Monitor, supervise and evaluate IT staff.					
Implement an IT job change and termination process.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Manage IT Human Resources

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<input type="checkbox"/> IT leadership is aware of the need to manage IT human resources and of the impact that rapid technology changes and increasing technological complexity have on IT staff's need for new skills and competencies.	<input type="checkbox"/> Senior leadership is aware of the need to manage IT human resources.	<input type="checkbox"/> IT leadership understands the full requirements for IT human resources management.	<input type="checkbox"/> Senior leadership and IT staff understand the requirements for human resources management.	<input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of requirements for IT human resources management.
	<input type="checkbox"/> The need for a consistent approach to manage IT human resources is communicated inconsistently.	<input type="checkbox"/> IT leadership understands the requirements for developing an effective IT human resources management process.	<input type="checkbox"/> IT staff discuss IT human resources on a regular basis.	<input type="checkbox"/> IT human resources processes are developed with input from IT staff.	<input type="checkbox"/> IT staff and other jurisdiction stakeholders are engaged in developing IT human resources management strategy, policies and procedures.
<b>PEOPLE</b> Awareness, Understanding and Communication	<input type="checkbox"/> IT human resources management is discussed in response to issues or requests for information from senior leadership.	<input type="checkbox"/> The need to establish an IT human resources management process is communicated consistently.	<input type="checkbox"/> The IT Strategic Plan includes IT human resources management.		
	<input type="checkbox"/> Communication to stakeholders about IT human resources management is sporadic and usually in response to issues.	<input type="checkbox"/> IT human resources management is discussed periodically.	<input type="checkbox"/> IT staff are aware of IT human resources management policies and procedures.	<input type="checkbox"/> Communication to IT staff about IT human resources processes occurs on a regular basis and in a formal way.	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT human resources management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform IT human resources management have not been identified.</li> <li><input type="checkbox"/> Minimum skill requirements for IT staff have not been identified.</li> <li><input type="checkbox"/> Training needs for IT human resources management have not been identified.</li> <li><input type="checkbox"/> Minimum skills required for IT staff have not been identified.</li> <li><input type="checkbox"/> Training requirements for IT staff have not been fully identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the skills and expertise to perform basic IT human resources management.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic IT human resources management have been identified.</li> <li><input type="checkbox"/> Training in IT human resources management is provided in response to emerging needs or requests from individuals.</li> <li><input type="checkbox"/> Minimum skill requirements for IT staff have been identified and incorporated into job descriptions.</li> <li><input type="checkbox"/> Informal training for new IT staff occurs.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the expertise to perform all key activities related to IT human resources management.</li> <li><input type="checkbox"/> Skill requirements for all IT human resources management processes have been defined and documented.</li> <li><input type="checkbox"/> Formal training in IT human resources management is available.</li> <li><input type="checkbox"/> Skill requirements have been identified for all IT roles.</li> <li><input type="checkbox"/> A formal IT training plan, designed to meet the needs of IT human resources, has been defined and implemented.</li> <li><input type="checkbox"/> Cross training between IT staff is encouraged.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has the skills and expertise to perform all IT human resources management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT human resources management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Formal training in IT human resources management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT human resources management is encouraged for individuals who perform these processes.</li> <li><input type="checkbox"/> A formal training program to increase technical, leadership and management capacity among IT staff has been implemented.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT human resources management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT human resources management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into the jurisdiction's IT human resources plan.</li> <li><input type="checkbox"/> IT staff are required to possess certification to perform processes identified as critical.</li> </ul>
	<p style="text-align: right;"><b>PEOPLE (continued)</b></p>	Skills and Expertise			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for IT human resources management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT human resources management is done informally.</li> <li>□ Individuals assume responsibility for IT human resources management.</li> <li>□ There is confusion about who is responsible and accountable for IT human resources management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT human resources management have been formally assigned and documented.</li> <li>□ IT human resources management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT human resources management owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT human resources management process owners are empowered to make decisions and to take action.</li> <li>□ IT human resources management process owners escalate issues, according to a defined escalation process.</li> </ul>
	PEOPLE (continued)	Responsibility and Accountability			

Maturity Level		5: Optimized			
Attributes		4: Managed		3: Defined	
1: Initial		2: Repeatable		1: Initial	
<p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT human resources management activities are based upon individual IT leadership and IT staff practices.</li> <li><input type="checkbox"/> The process of managing IT human resources is reactive and informal.</li> <li><input type="checkbox"/> The IT human resources management process is focused on the short-term operational requirement of hiring and supervising IT staff.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT human resources management are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT human resources management policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> A consistent approach to IT human resources management is followed.</li> <li><input type="checkbox"/> Hiring and managing IT staff are driven by tactical, project-specific needs.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key IT human resources management processes have been developed and documented.</li> <li><input type="checkbox"/> IT human resources management processes are based upon generally accepted good practices.</li> <li><input type="checkbox"/> An IT human resources management plan exists.</li> <li><input type="checkbox"/> A formal orientation of new IT staff is defined and implemented.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT human resources management processes are developed, documented and regularly reviewed.</li> <li><input type="checkbox"/> Senior leadership approves policies and procedures for IT human resources management.</li> <li><input type="checkbox"/> The IT human resources management plan ensures that operational and strategic capabilities are available, when required.</li> <li><input type="checkbox"/> IT human resources management processes are integrated into the overall human resources management framework.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The IT human resources management plan supports the IT Strategic Plan.</li> <li><input type="checkbox"/> The IT human resources management plan is regularly reviewed and revised.</li> <li><input type="checkbox"/> A formal IT staff succession plan for the jurisdiction's critical IT processes is defined and implemented.</li> <li><input type="checkbox"/> Generally accepted best practices and standards for IT human resources management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT human resources policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT human resources management policies and procedures are regularly reviewed and improved.</li> </ul>	<p>Policies, Plans and Procedures</p>
PROCESS					

Maturity Level		3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some IT human resources management goals are set and monitored inconsistently.</li> <li>□ IT staff performance management is performed sporadically and responsively.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance of IT human resources management processes is monitored informally.</li> <li>□ IT leadership provides basic reports about the state of IT human resources management.</li> <li>□ IT staff performance is evaluated inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance of IT human resources management metrics are formally defined and approved, and align to the IT Strategic Plan.</li> <li>□ Measures of the effectiveness of IT human resources management are used to inform decision making and continuous improvement.</li> <li>□ IT staff performance management is performed on an ongoing basis to support continuous improvement.</li> <li>□ Measures for IT staff performance evaluation are linked to the IT Strategic Plan.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance management is incorporated into IT human resources management processes.</li> <li>□ Peer- and sector-based benchmarking for IT human resources management, IT staff performance and IT staff compensation is performed.</li> <li>□ IT human resources management processes are monitored and measured.</li> </ul>
	Goal Setting and Measurement	<ul style="list-style-type: none"> <li>□ Performance of IT human resources management is monitored regularly.</li> <li>□ The link between IT human resources management goals and IT strategic goals is clear and direct.</li> <li>□ IT human resource management metrics are based upon measures of cost.</li> <li>□ IT staff performance is evaluated on a regular basis.</li> <li>□ Measures of IT staff performance are linked to operational requirements.</li> </ul>		

PROCESS (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT human resource management; they are generally based upon standard desktop tools.</li> <li>□ There is no consistent approach to using tools to support IT human resources management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT human resources management has been developed.</li> <li>□ The basic level of functionality in these tools is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT human resources management have been implemented.</li> <li>□ Integration of tools to support IT human resources management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT human resources management.</li> <li>□ Tools are used in key areas to automate and formalize IT human resources management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support IT human resources management.</li> <li>□ IT human resources management tools are integrated with other jurisdiction human resources management tools.</li> </ul>
	Tools and Automation				

## Assess and Manage IT Risk

### Description

Protection of the jurisdiction’s reputation and financial, technological and information assets is a critical activity. Every investment in technology, regardless of size, should be assessed, based upon cost, benefit and risk.

Even minor changes to the technological environment that cost little can pose significant risks. For example, a software update to a server operating system may create a security hole or result in a loss of service if it fails. Even routine activities, such as taking a laptop home from work, expose the jurisdiction to risk. Therefore, IT risk management is a process area that should be embedded throughout the jurisdiction and incorporated into the normal way of doing things.

This is achieved by developing a consistent understanding of the jurisdiction’s appetite for risk, evaluating IT services, operations and assets to determine their associated risk exposure, and then mitigating those risks. It is supported through consistent and well-defined programs of communication intended to help all jurisdiction stakeholders understand and manage IT risks.

### Value

- Protects the jurisdiction’s reputation and financial, technological and information assets.

### Goals

- Ensure stakeholder awareness of IT-related risks.
- Manage risks to an acceptable level, balancing cost, benefits and jurisdiction objectives.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

### Key Activities

**Develop an IT risk management framework** that is aligned with the jurisdiction’s risk management framework.

- Provide guidance related to the context in which the risk management framework is applied in realize appropriate outcomes.
- Implement a process to determine the internal and external context for each risk assessment, the goal of the assessment and the criteria used to evaluate and prioritize risks.

**Identify IT risks.**

- Implement processes to identify IT-related threats or events that may have a negative impact on jurisdiction objectives, legal or regulatory compliance, reputation or operations.
- Implement a process to determine, document and communicate the nature of the threat.

**Assess the impact of identified risks** on a regular basis.

- Implement a process to assess the probability and impact of identified risks, using qualitative and quantitative methods.

**Respond to risks.**

- Implement a process to formulate a cost-effective approach to mitigate exposure by accepting, avoiding, mitigating or transferring risks.

**Maintain and monitor a risk action plan.**

- Prioritize and plan control activities to ensure that risk responses are implemented appropriately.
- Ensure that costs, benefits and responsibilities for each risk response are identified.
- Monitor and report on the execution of the risk action plan to senior leadership.

**RACI Chart**

Activities	Roles				
Develop an IT risk management framework.					
Identify IT risks.					
Assess the impact of identified risks.					
Respond to risks.					
Maintain and monitor a risk action plan.					

**RACI Responsibilities**

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Assess and Manage IT Risk

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> Awareness, Understanding and Communication	<b>1: Initial</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for and importance of IT risk management.</li> <li><input type="checkbox"/> The need to manage IT risks is communicated inconsistently.</li> <li><input type="checkbox"/> IT risk management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT risk management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the requirements of an effective IT risk management process.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of a sound IT risk management process.</li> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff discuss IT risk on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about IT risk and IT risk management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is engaged in IT risk management and is advised of changes in the jurisdiction and IT environment that could significantly impact IT risk management scenarios.</li> <li><input type="checkbox"/> IT leadership has a full understanding of IT risks and their potential impact on the jurisdiction.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of requirements for IT risk management.</li> <li><input type="checkbox"/> Formal committees exist to govern IT risk; they are regularly briefed on IT-related risk.</li> <li><input type="checkbox"/> IT risk management is integrated into jurisdiction and IT operations.</li> <li><input type="checkbox"/> The potential impact of all IT risks are analyzed, documented and communicated to stakeholders.</li> </ul>	
	<b>PEOPLE</b>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT risk management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform IT risk management have not been identified.</li> <li><input type="checkbox"/> Training needs for IT risk management have not been identified.</li> </ul>	<b>2: Repeatable</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic IT risk management.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic IT risk management have been identified.</li> <li><input type="checkbox"/> Informal training in IT risk management is provided in response to emerging needs or requests from individuals.</li> </ul>	<b>3: Defined</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the expertise to perform all key IT risk management processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of IT risk management have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for IT risk management has been developed.</li> <li><input type="checkbox"/> Formal training in IT risk management is available.</li> </ul>	<b>4: Managed</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all IT risk management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT risk management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> A formal training plan for IT risk management is implemented.</li> <li><input type="checkbox"/> Skill requirements for IT risk management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training in IT risk management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT risk management is encouraged for individuals who perform these processes.</li> </ul>	<b>5: Optimized</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT risk management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT risk management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into IT risk management.</li> </ul>	
	<b>Skills and Expertise</b>				

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for IT risk management is assumed or done in an ad hoc way.</li> <li>□ Management of operational and project-based IT risks are sporadically assigned to specific personnel.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT risk management is done informally.</li> <li>□ Individuals assume responsibility for IT risk management.</li> <li>□ There is confusion about who is responsible and accountable for IT risk management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT risk management have been formally assigned and documented.</li> <li>□ IT risk management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT risk management process owners have the level of authority required to fulfill their responsibilities.</li> <li>□ Senior leadership sets the levels of risk that the jurisdiction will tolerate.</li> <li>□ IT risks have an identified owner.</li> <li>□ IT risk owners have the level of authority required to manage the risk.</li> <li>□ Job descriptions include IT risk management responsibilities, where appropriate.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT risk management process owners and risk owners are empowered to make decisions and to take action.</li> <li>□ IT risk management process owners and risk owners escalate issues, according to a defined escalation process.</li> <li>□ End users understand their responsibilities for managing IT and information risks.</li> </ul>
	PEOPLE (continued)	Responsibility and Accountability			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><b>Attributes</b></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>□ IT risk management activities occur in isolation and are based upon individual IT staff practices.</li> <li>□ Identification, assessment and treatment of operational or project-based IT risks are performed sporadically and informally.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for IT risk management are defined, but not documented.</li> <li>□ Risk management activities are high level and are applied to major projects or in response to issues.</li> <li>□ Risk mitigation processes are emerging for identified risks.</li> <li>□ Compliance with IT risk management policies and procedures is left to the individual's discretion.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for key IT risk management processes are defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ A jurisdiction-wide risk management policy defines the frequency and type of risk assessment to be performed.</li> <li>□ Key risks to the jurisdiction are identified and addressed in the risk management framework.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all IT risk management processes are defined, documented and regularly reviewed.</li> <li>□ An IT risk response plan is created for identified risks.</li> <li>□ Risk is assessed and mitigated at the IT operational level and at the project level.</li> <li>□ A process to evaluate emerging and operational IT risks, on a regular basis, has been implemented.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT risk management is formally and fully integrated into the jurisdiction's risk management practices.</li> <li>□ IT leadership continually assesses IT risk and mitigation strategies.</li> <li>□ Generally accepted best practices and standards for IT risk management are used to inform policy and procedure development.</li> <li>□ Exceptions to IT risk management processes are noticed and corrective action is taken.</li> <li>□ IT risk management policies and procedures are regularly reviewed and improved.</li> </ul>	
	<p>Policies, Plans and Procedures</p> <p style="text-align: right;"><b>PROCESS</b></p>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some IT risk management goals are set and monitored inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance of IT risk management processes is monitored informally.</li> <li>□ IT leadership provides basic reports about the state of and planning for IT risk management.</li> <li>□ Informal and irregular checks to identify and assess risk events are performed.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance of IT risk management is monitored regularly.</li> <li>□ IT risk targets and thresholds have been defined and documented.</li> <li>□ IT leadership provides senior leadership with regular reports about the status of IT risk management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Metrics for IT risk management are defined, documented and approved.</li> <li>□ Measures of the effectiveness of IT risk management are used to inform decision making and continuous improvement.</li> <li>□ Standard measures for assessing risk and determining risk/return ratios have been defined and documented.</li> <li>□ Measurement of the IT risk environment is based on current and anticipated risks.</li> <li>□ There is a process in place to address deviations from IT risk management standards, targets and thresholds.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance management is incorporated into IT risk management processes.</li> <li>□ Peer- and sector-based benchmarking for IT risk management and mitigation performance is performed.</li> <li>□ IT risk management processes are monitored and measured.</li> </ul>
	Goal Setting and Measurement	<p style="text-align: right;"><b>PROCESS (continued)</b></p>			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT risk management; they are generally based upon standard desktop tools.</li> <li>□ There is no consistent approach to using tools to support IT risk management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT risk management has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT risk management is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT risk management have been implemented.</li> <li>□ Integration of tools to support IT risk management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT risk management.</li> <li>□ Tools are used in key areas to automate and formalize IT risk management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support IT risk management.</li> <li>□ IT risk management tools are integrated with other jurisdiction risk management tools.</li> <li>□ Capture, analysis and reporting risk management information are automated processes.</li> </ul>
	Tools and Automation				

## Monitor and Evaluate IT Performance

### Description

One challenge faced by senior leadership in school jurisdictions is that they are responsible for providing oversight to IT—an area in which they are not likely to have deep expertise. From the perspective of senior leadership, funding goes in and work is done, but the value of that work is ambiguous.

Monitoring and evaluating IT performance provides stakeholders—particularly senior leadership—with assurance that the right things are being done and that they are being done in line with jurisdiction goals, policies and expectations.

This process area includes defining appropriate performance indicators, systematic and timely reporting of performance, and taking prompt action to address deviations.

### Value

- Provides assurance to stakeholders that the activities of the IT department are in line with jurisdiction goals, policies and procedures, and that appropriate work is undertaken.

### Goals

- Provide transparency and insight into IT costs, benefits, strategy, policies, and service levels.
- Support continuous improvement of IT services.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

### Key Activities

#### Establish a framework to monitor IT.

- Define the scope and process for monitoring IT services and measuring the contribution of IT to achieving jurisdiction objectives.

#### Define and collect measurement data.

- Implement a process to define a balanced set of performance targets and have them approved by senior leadership.
- Define benchmarks against which performance can be assessed.
- Identify data to be collected to measure IT performance.
- Implement processes to collect timely and accurate data that supports the measurement and monitoring of IT performance.

#### Implement an IT performance monitoring method.

- Implement a process to monitor IT performance that records targets, captures measurements and provides a succinct view into IT performance.
- Ensure that the IT performance monitoring method fits within the jurisdiction's performance monitoring system.

**Assess and improve performance**, review performance against targets, analyze the cause of deviations and take action to address the underlying causes.

- Identify and initiate remedial actions or improvement efforts, based upon performance monitoring, assessment and reporting.
- Review, negotiate and implement management responses.
- Assign responsibility for implementing remedial actions.
- Monitor implementation of remedial actions to ensure timely resolution.

**Report IT performance** about IT’s contribution to the achievement of the jurisdiction’s goals to senior leadership and stakeholders.

- Implement a process to report on the performance of the portfolio of IT investments and services.
- Include updates about achievement of planned objectives, budgeted resources used, performance targets met and risks mitigated.
- Implement a process to gather feedback from senior leadership.

### RACI Chart

Activities	Roles				
Establish a framework to monitor IT.					
Define and collect measurement data.					
Implement a performance monitoring method.					
Assess and improve performance.					
Report IT performance.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Monitor and Evaluate IT Performance

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> 1: Initial Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need to monitor and evaluate IT performance.</li> <li><input type="checkbox"/> The need to monitor and evaluate IT performance is communicated inconsistently.</li> <li><input type="checkbox"/> IT performance monitoring and evaluation is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT performance is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to monitor and evaluate IT performance.</li> <li><input type="checkbox"/> IT leadership understands the requirements for monitoring and evaluating IT performance.</li> <li><input type="checkbox"/> The need to monitor and evaluate IT performance is communicated consistently.</li> <li><input type="checkbox"/> The need to evaluate and monitor IT performance is discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about IT performance occurs periodically.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership commits resources to the development of an effective process to monitor and evaluate IT performance.</li> <li><input type="checkbox"/> IT performance is regularly reported to senior leadership and IT leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT performance occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> The IT performance monitoring framework is communicated to senior leadership.</li> <li><input type="checkbox"/> Senior leadership understands the impact of IT performance on the processes of teaching and learning, and educational management.</li> <li><input type="checkbox"/> Senior leadership and stakeholders are engaged in developing IT performance metrics.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of requirements for IT performance monitoring.</li> <li><input type="checkbox"/> IT leadership reports IT performance metrics that demonstrate the value of IT and its contribution to the jurisdiction's strategic goals.</li> </ul>
	<b>PEOPLE</b>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT performance monitoring and evaluation exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to monitor and evaluate IT performance have not been identified.</li> <li><input type="checkbox"/> Training needs for IT performance monitoring and evaluation have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic IT performance monitoring and evaluation.</li> <li><input type="checkbox"/> Minimum skill requirements to monitor and evaluate IT performance, on a basic level, have been identified.</li> <li><input type="checkbox"/> Training in IT performance monitoring and evaluation is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key IT performance monitoring and evaluation processes.</li> <li><input type="checkbox"/> Skill requirements for all areas of IT performance monitoring and evaluation have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for IT performance monitoring and evaluation has been developed.</li> <li><input type="checkbox"/> Formal training in IT performance monitoring and evaluation is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the expertise to perform all IT performance monitoring and evaluation processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT performance monitoring and evaluation is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> A formal plan for IT performance monitoring and evaluation is implemented.</li> <li><input type="checkbox"/> Skill requirements for IT performance monitoring and evaluation are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training in IT performance monitoring and evaluation is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT performance monitoring and evaluation is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT performance monitoring and evaluation is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT performance monitoring and evaluation, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into IT performance monitoring.</li> </ul>
	Skills and Expertise				

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for IT performance monitoring and evaluation is assumed or done in an ad hoc way.</li> <li>□ Monitoring and evaluation of the financial performance of IT may be assigned to the jurisdiction's finance department.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT performance monitoring and evaluation is done informally.</li> <li>□ Individuals assume responsibility for IT performance monitoring and evaluation.</li> <li>□ There is confusion about who is responsible and accountable for IT performance monitoring and evaluation when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT performance monitoring and evaluation have been formally assigned and documented.</li> <li>□ IT performance monitoring and evaluation process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT performance monitoring and evaluation process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT performance monitoring process owners are empowered to make decisions and to take action.</li> <li>□ IT performance monitoring process owners escalate issues, according to a defined escalation process.</li> </ul>
	PEOPLE (continued)	Responsibility and Accountability			

<b>Maturity Level</b>		<b>2: Repeatable</b>	<b>3: Defined</b>	<b>4: Managed</b>	<b>5: Optimized</b>
<i>Attributes</i>	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT performance monitoring and evaluation are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT performance monitoring and evaluation policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Interpretation of monitoring and evaluation results is performed inconsistently.</li> <li><input type="checkbox"/> A planned approach to gathering information for IT performance monitoring and evaluation does not exist.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key IT performance monitoring and evaluation processes are defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures for IT performance monitoring and evaluation are based upon generally accepted good practices.</li> <li><input type="checkbox"/> A framework for measuring IT performance is defined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT performance monitoring and evaluation processes are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> Senior leadership approves policies and procedures for IT performance monitoring and evaluation.</li> <li><input type="checkbox"/> Senior leadership and IT leadership evaluate IT performance, based on mutually agreed-upon criteria, operating targets, thresholds and metrics.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT performance monitoring is formally and fully integrated into all IT processes.</li> <li><input type="checkbox"/> Generally accepted best practices and standards for IT performance monitoring are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT performance monitoring and evaluation processes are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT performance monitoring and evaluation policies and procedures are regularly reviewed and improved.</li> </ul>
		<ul style="list-style-type: none"> <li><input type="checkbox"/> IT performance monitoring and evaluation activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> IT performance monitoring for some IT processes or projects is implemented inconsistently.</li> <li><input type="checkbox"/> IT performance monitoring is implemented in response to issues.</li> </ul>			

Policies, Plans and Procedures

Maturity Level	
<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some IT performance goals are set and monitored inconsistently.</li> </ul>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li>□ Performance of IT monitoring and evaluation reporting processes is monitored informally.</li> <li>□ IT leadership provides basic reports about the performance of IT.</li> <li>□ Performance metrics are defined informally and are primarily financial.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li>□ The monitoring and evaluation of IT performance is monitored regularly.</li> <li>□ IT performance metrics reflect a mixture of financial, non-financial and educational objectives, as appropriate.</li> <li>□ IT leadership provides senior leadership with regular reports about IT performance.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li>□ IT performance metrics are formally defined and approved, and align to the IT Strategic Plan.</li> <li>□ Measures of the effectiveness of IT performance are used to inform decision making and continuous improvement.</li> <li>□ There is a process in place to address deviations from IT performance targets and thresholds.</li> <li>□ IT performance metrics are integrated across all IT processes and projects.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li>□ Peer- and sector-based benchmarking for IT performance monitoring is performed.</li> </ul>

Goal Setting and Measurement

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support IT performance monitoring and evaluation; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no formal approach to using tools to support IT performance monitoring and evaluation.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Basic tools and templates, specific to IT performance monitoring and evaluation, have been developed and implemented.</li> <li><input type="checkbox"/> Common approaches to the use of tools to support IT performance monitoring and evaluation are emerging.</li> <li><input type="checkbox"/> Tools specifically applicable to IT performance monitoring and evaluation are beginning to be implemented.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan is developed to acquire and implement tools to support IT performance monitoring and evaluation.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates for IT performance monitoring and evaluation is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> <li><input type="checkbox"/> Historical IT performance information is collected and maintained.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support IT performance monitoring and evaluation have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support IT performance monitoring and evaluation is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support IT performance monitoring and evaluation.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize IT performance monitoring and evaluation.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support IT performance monitoring and evaluation.</li> <li><input type="checkbox"/> IT performance management tools are integrated with other jurisdiction performance management tools.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

## Monitor and Evaluate Internal Processes

### Description

Process improvements that are measured and monitored are more likely to be incorporated into the normal way of doing things. When there is no incentive or accountability to carry out defined processes, it is less likely that they will be effective or lasting.

At the same time, monitoring and measurement can be used to drive continuous improvement of processes. Measurement and monitoring can help IT leadership and IT staff identify frequently occurring issues or events, and enable preventative action.

An effective program of monitoring and evaluating internal processes includes monitoring, evaluating and reporting on IT processes and process exceptions, self-assessments and third-party reviews.

### Value

- Supports continuous improvement.
- Provides assurance that IT operations are effective, efficient and compliant with applicable laws and regulations.

### Goals

- Establish a culture of continuous improvement.
- Ensure that internal policies, procedures and processes comply with laws, regulations and contracts.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership School Administrators IT Staff

### Key Activities

**Monitor, benchmark and improve the IT process environment**, on a continuous basis, to meet jurisdiction objectives and to obtain assurance of the completeness and effectiveness of established processes.

- Implement a process to evaluate internal IT services and processes as well as those performed by third parties.
- Perform self-assessment to ensure appropriate levels of control are exercised over IT processes, policies and contracts.
- Perform third-party assessments to provide further assurance of the completeness and effectiveness of IT process control.

**Identify and assess IT process exceptions** to identify their underlying root causes.

- Implement a process to escalate process exceptions to senior leadership or IT leadership, as required.

**Implement corrective action** to address process exceptions.

## RACI Chart

Activities	Roles				
Monitor, benchmark and improve the IT process environment.					
Identify and assess IT process exceptions.					
Implement corrective action.					

## RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Monitor and Evaluate Internal Processes

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> 1: Initial Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need to monitor and evaluate internal IT processes.</li> <li><input type="checkbox"/> The need to monitor and evaluate the effectiveness of internal IT processes is communicated inconsistently.</li> <li><input type="checkbox"/> Internal IT process monitoring is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about the effectiveness of internal IT processes is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to monitor and evaluate internal IT processes.</li> <li><input type="checkbox"/> IT leadership understands the requirements for monitoring and evaluating internal IT processes.</li> <li><input type="checkbox"/> The need to monitor and evaluate internal IT processes is communicated consistently.</li> <li><input type="checkbox"/> Exceptions are reported to IT leadership periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about the performance of internal IT processes occurs periodically.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff understand the requirements for monitoring and evaluating internal IT processes.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss internal IT process monitoring and evaluation on a regular basis.</li> <li><input type="checkbox"/> Communication to senior leadership about internal IT process exceptions and the corrective action taken occurs on an as-needed basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff and end users are aware of their role in supporting or implementing effective internal IT processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of requirements for monitoring and evaluating internal IT processes.</li> <li><input type="checkbox"/> Stakeholders are informed of the results of external assurance reviews related to internal IT process monitoring.</li> </ul>
	<b>PEOPLE</b>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of internal IT process monitoring and evaluation exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform monitoring and evaluation of internal IT processes have not been identified.</li> <li><input type="checkbox"/> Training needs for monitoring and evaluating internal IT processes have not been identified.</li> </ul>	<b>Skills and Expertise</b> PEOPLE (continued)	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to monitor and evaluate internal IT processes at a basic level.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic monitoring and evaluation of internal IT processes have been identified.</li> <li><input type="checkbox"/> Training in monitoring and evaluating internal IT processes is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key internal IT process monitoring and evaluation activities.</li> <li><input type="checkbox"/> Skill requirements for all aspects of monitoring and evaluating internal IT processes have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for monitoring and evaluating internal IT processes has been developed.</li> <li><input type="checkbox"/> Formal training in monitoring and evaluating internal IT processes is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all internal IT process monitoring and evaluation processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of internal IT process monitoring and evaluation is ensured for individuals who perform these tasks.</li> <li><input type="checkbox"/> A formal training plan for monitoring and evaluating internal IT processes is implemented.</li> <li><input type="checkbox"/> Skill requirements for monitoring and evaluating internal IT processes are regularly reviewed and updated.</li> <li><input type="checkbox"/> Formal training for internal IT process monitoring and evaluation is required for individuals who perform these tasks.</li> <li><input type="checkbox"/> Certification in internal IT process monitoring and evaluation is encouraged for individuals who perform these tasks.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of monitoring and evaluating internal IT processes is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in monitoring and evaluating internal IT processes, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into monitoring and evaluating internal IT processes.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>Allocation of responsibility for monitoring and evaluating internal IT processes is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>Allocation of responsibility for monitoring and evaluating internal IT processes is done informally.</li> <li>Individuals assume responsibility for monitoring and evaluating internal IT processes.</li> <li>There is confusion about who is responsible and accountable for monitoring and evaluating internal IT processes when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability and responsibility for monitoring and evaluating internal IT processes have been formally assigned and documented.</li> <li>Internal IT process monitoring and evaluation process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Internal IT process monitoring and evaluation process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Internal IT process monitoring and evaluation process owners are empowered to make decisions and to take action.</li> <li>Internal IT process monitoring and evaluation process owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability				

PEOPLE (continued)

Maturity Level	
<b>Attributes</b> <b>1: Initial</b>	<b>2: Repeatable</b>
<b>3: Defined</b>	<b>4: Managed</b>
<b>5: Optimized</b>	

  

PROCESS	Policies, Plans and Procedures
<ul style="list-style-type: none"> <li><input type="checkbox"/> Internal IT process monitoring and evaluation activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> Internal IT process monitoring is implemented in response to issues or incidents.</li> <li><input type="checkbox"/> Internal IT process evaluation is performed sporadically as a part of a larger annual financial and management control audit.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for monitoring and evaluating internal IT processes are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with monitoring and evaluating internal IT policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Critical internal IT processes are monitored and evaluated.</li> <li><input type="checkbox"/> Informal reporting is used to initiate corrective action for internal IT processes.</li> </ul>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key internal IT process monitoring and evaluation processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all internal IT process monitoring and evaluation processes are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> Senior leadership approves policies and procedures for internal IT process monitoring and evaluation.</li> <li><input type="checkbox"/> Senior leadership and IT leadership evaluate the effectiveness of internal IT processes, based on mutually agreed-upon criteria.</li> <li><input type="checkbox"/> Risk assessment procedures are used to determine the level of monitoring and evaluation required for internal IT processes.</li> </ul>
<ul style="list-style-type: none"> <li><input type="checkbox"/> A framework for monitoring and evaluating internal IT processes is implemented and integrated.</li> <li><input type="checkbox"/> Regular assessment of IT processes is performed.</li> <li><input type="checkbox"/> Exceptions to monitoring and evaluation of internal IT processes are noticed and corrective action is taken.</li> <li><input type="checkbox"/> Procedures and policies for monitoring and evaluating internal IT processes are regularly reviewed and improved.</li> </ul>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>Some goals for the effectiveness of internal IT processes are set and monitored inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li>Performance of internal IT processes is monitored informally.</li> <li>IT leadership provides basic reports about the performance of internal IT processes.</li> <li>Metrics for the performance of internal IT processes are defined informally.</li> </ul>	<ul style="list-style-type: none"> <li>Internal IT processes are monitored and evaluated regularly.</li> <li>Targets and thresholds for internal IT processes have been defined, documented and communicated.</li> <li>IT staff inform IT leadership when thresholds are exceeded.</li> </ul>	<ul style="list-style-type: none"> <li>Internal IT process metrics are formally defined and approved.</li> <li>Measures of the effectiveness of internal IT processes are used to inform decision making and continuous improvement.</li> <li>Use of external reviews and benchmarking of internal IT processes is emerging.</li> </ul>	<ul style="list-style-type: none"> <li>Peer- and sector-based benchmarking for internal IT process performance is used to identify areas for improvement.</li> <li>Results of internal IT process evaluations are used to support continuous improvement.</li> <li>Third parties regularly monitor and evaluate internal IT processes.</li> </ul>
	Goal Setting and Measurement				

PROCESS (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support the monitoring and evaluation of internal IT processes; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support the monitoring and evaluation of internal IT processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to monitoring and evaluating internal IT processes, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support the monitoring and evaluation of internal IT processes are emerging.</li> <li>□ Tools specifically applicable to the monitoring and evaluation of internal IT processes are beginning to be implemented.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan is developed to acquire and implement tools to support internal IT process monitoring and evaluation.</li> <li>□ The basic level of functionality in tools and templates for internal IT process monitoring and evaluation is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Historical information related to internal IT processes is collected and maintained.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support monitoring and evaluating internal IT processes have been implemented.</li> <li>□ Integration of tools to support the monitoring and evaluation of internal IT processes is emerging.</li> <li>□ There is a formal and structured approach to using tools to support the monitoring and evaluation of internal IT processes.</li> <li>□ Tools are used in key areas to automate the monitoring and evaluation of internal IT processes and to detect exceptions.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support internal IT process monitoring.</li> <li>□ Internal IT process monitoring tools are integrated with other jurisdiction process monitoring tools.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

## Manage Compliance with External Requirements

### Description

IT is subject to legal, regulatory and contractual requirements that are highly complex and constantly changing. The school jurisdiction’s senior leadership is ultimately accountable for compliance with these requirements, but must delegate responsibility to IT leadership and IT staff.

In order to minimize the risks associated with being non-compliant with legal, regulatory or contractual requirements, it is necessary to identify and analyze requirements, implement a response and obtain assurance that requirements have been met.

### Value

- Provides assurance to senior leadership that IT operations are in compliance with legal, regulatory and contractual requirements.

### Goals

- Ensure compliance with laws, regulations and contractual requirements.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership School Administrators IT Staff

### Key Activities

#### Identify compliance requirements.

- Implement a process to continuously review local and international laws, regulations and other external compliance requirements.
- Identify and maintain documentation related to the regulatory requirements applicable to each information system planned or in use.

#### Evaluate IT policies, plans and procedures to confirm compliance.

- Evaluate methods of deterring users from performing acts of non-compliance.
- Adjust policies, plans and procedures to ensure that legal, regulatory and contractual requirements are addressed and communicated.

#### Report positive assurance of compliance.

- Implement a process to obtain and report on compliance of IT policies, plans and procedures with legal, regulatory or contractual agreements.
- Ensure that any corrective actions taken to address compliance gaps have been taken in a timely manner by the responsible process owner.

## RACI Chart

Activities	Roles				
Identify compliance requirements.					
Evaluate IT policies, plans and procedures to confirm compliance.					
Report positive assurance of compliance.					

## RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Manage Compliance

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
PEOPLE	Attributes	<ul style="list-style-type: none"> <li>□ IT leadership is aware of compliance management requirements that impact the jurisdiction.</li> <li>□ Compliance management issues that impact the jurisdiction are discussed in response to issues or requests for information from senior leadership.</li> <li>□ Communication to stakeholders about regulatory, contractual and legal compliance requirements that impact the jurisdiction is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li>□ Senior leadership is aware of the requirements of an effective IT compliance management process.</li> <li>□ Senior leadership commits resources to the development of a sound IT compliance management process.</li> <li>□ Communication to stakeholders about regulatory, legal and contractual compliance requirements, policies and procedures occurs on a regular basis and in a formal way.</li> <li>□ IT leadership informs senior leadership of incidences of non-compliance and of the corrective actions taken.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have a comprehensive understanding of the requirements for contractual, legal and regulatory compliance.</li> <li>□ The need to ensure compliance with relevant legislation, regulations and contracts is understood throughout the jurisdiction.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership has extensive knowledge of applicable external requirements, including future trends, anticipated changes and the need for new solutions.</li> <li>□ Compliance assurance reports are regularly discussed at the senior leadership level.</li> <li>□ Understanding of the jurisdiction's external compliance obligations is widespread throughout the jurisdiction.</li> </ul>
	Awareness, Understanding and Communication				

Maturity Level		3: Defined		4: Managed		5: Optimized	
<b>PEOPLE (continued)</b>	Attributes	Skills and Expertise					
	1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized	5: Optimized	5: Optimized
	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of compliance management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform compliance management have not been identified.</li> <li><input type="checkbox"/> Training needs for compliance management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to manage compliance at a basic level.</li> <li><input type="checkbox"/> Minimum skill requirements to manage compliance have been identified.</li> <li><input type="checkbox"/> Training in managing compliance is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key compliance management processes.</li> <li><input type="checkbox"/> Skill requirements for all areas of compliance management have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for compliance management has been developed.</li> <li><input type="checkbox"/> Training for compliance management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all compliance management activities.</li> <li><input type="checkbox"/> Proficiency in critical aspects of compliance management is ensured for individuals who perform these tasks.</li> <li><input type="checkbox"/> Skill requirements for compliance management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for compliance management is required for individuals who perform these tasks.</li> <li><input type="checkbox"/> Certification in compliance management is encouraged for individuals who perform these tasks.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of compliance management is ensured for individuals who perform these tasks.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in compliance management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into compliance management.</li> <li><input type="checkbox"/> Ongoing training is provided to ensure that end users understand legal, regulatory or contractual changes that affect them.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of compliance management is ensured for individuals who perform these tasks.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in compliance management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into compliance management.</li> <li><input type="checkbox"/> Ongoing training is provided to ensure that end users understand legal, regulatory or contractual changes that affect them.</li> </ul>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li>Allocation of responsibility for compliance management is assumed or done in an ad hoc way.</li> </ul>	<b>PEOPLE (continued)</b> Responsibility and Accountability	<ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for compliance management is done informally.</li> <li>Individuals assume responsibility for compliance management.</li> <li>There is confusion about who is responsible and accountable for compliance management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability and responsibility for compliance management have been formally assigned and documented.</li> <li>Compliance management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Compliance management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Compliance management process owners are empowered to make decisions and to take action to ensure compliance with legal, regulatory and contractual requirements.</li> <li>Compliance management process owners escalate issues, according to a defined escalation process.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><b>Attributes</b></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>□ Activities to ensure legal, regulatory and contractual compliance occur in isolation and are based upon individual IT staff practices.</li> <li>□ Monitoring of processes to ensure compliance with legal, regulatory and contractual requirements is implemented in response to issues.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li>□ Common and informal policies and procedures ensure compliance with legal, regulatory and contractual requirements are defined, but not documented.</li> <li>□ Compliance with policies that ensure compliance with legal, regulatory and contractual requirements is left to the individual's discretion.</li> <li>□ Where compliance is a recurring requirement, individual compliance procedures have been developed and are followed on a year-to-year basis.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li>□ Formal policies and procedures for key compliance management processes have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li>□ Formal policies and procedures for all compliance management activities are defined, documented and regularly reviewed.</li> <li>□ Senior leadership approves policies and procedures for compliance management.</li> <li>□ A process to regularly review the environment to identify external requirements and ongoing changes has been implemented.</li> <li>□ Standardized internal good practices are used for specific needs, such as standing regulations and recurring service contracts.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>□ A framework for compliance management is implemented and integrated.</li> <li>□ Generally accepted best practices and standards for compliance management are used to inform policy and procedure development.</li> <li>□ Exceptions to compliance management policies and procedures are noticed and corrective action is taken.</li> <li>□ The framework includes a self-assessment process for compliance management.</li> <li>□ Compliance management policies and procedures are regularly reviewed and updated.</li> </ul>	
	<p>Policies, Plans and Procedures</p>				

**PROCESS**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some legal, regulatory and contractual compliance goals are set and monitored inconsistently.</li> </ul>	<ul style="list-style-type: none"> <li>□ Compliance with legal, regulatory and contractual requirements is monitored informally.</li> <li>□ IT leadership informally reports to senior leadership about legal, regulatory and contractual compliance.</li> </ul>	<ul style="list-style-type: none"> <li>□ Compliance management is monitored regularly.</li> <li>□ Targets and thresholds for compliance management have been defined and documented.</li> <li>□ IT leadership informs senior leadership about compliance management in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Compliance management metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of compliance management policies and procedures are used to inform decision making and continuous improvement.</li> <li>□ There is a process in place to monitor incidences of non-compliance, identify root causes and implement corrective action.</li> </ul>	<ul style="list-style-type: none"> <li>□ Compliance management is integrated into appropriate IT policies and procedures.</li> <li>□ Compliance management processes are monitored and measured.</li> </ul>
	Goal Setting and Measurement	<b>PROCESS (continued)</b>			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support legal, regulatory and contractual compliance activities; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support legal, regulatory and contractual compliance activities.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan is developed to acquire and implement tools to support compliance management activities.</li> <li>□ The basic level of functionality in tools and templates for compliance management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Standard pro forma contracts and legal processes are used to minimize risks associated with contractual liability.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support compliance management have been implemented.</li> <li>□ Integration of tools to support IT compliance management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support compliance management.</li> <li>□ Tools are used in key areas to automate and formalize compliance management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of automated tools and formalized techniques is used, jurisdiction wide, to support compliance management.</li> </ul>

# IT Service Management

# IT Service Management

## Manage Service Levels

### Description

Managing service levels is about understanding the importance of a service and ensuring that resources are available to meet agreed-upon performance expectations.

This process area includes communicating what a service is, negotiating with senior leadership to determine appropriate levels of service, keeping records of those services in a service catalogue, and monitoring and reporting to senior leadership on actual service levels.

### Value

- Ensures that services are provided to the jurisdiction at an appropriate level and cost.
- Enables effective communication about IT services between senior leadership, IT leadership and end users.

### Goals

- Facilitate agreement between senior leadership and end users about IT service target levels.
- Maintain a single, consistent source of information about available IT services.

### Target Audience

Primary	Secondary
Senior Leadership School Administrators IT Leadership	IT Staff

### Key Activities

#### Implement service level agreement structures.

- Develop and implement a policy for creating and maintaining Service Level Agreements.
- Implement a policy to create, review and monitor underpinning agreements, such as Operating Level Agreements, with internal departments and contracts with external parties.

#### Develop and document Service Level Agreements.

- Implement a process to define, in consultation with stakeholders, service level requirements for new services.
- Agree upon and document service definitions in a Service Catalogue.
- Ensure that the Service Catalogue is accessible to end users.
- Document underpinning agreements related to the service.

#### Monitor and revise Service Level Agreements.

- Monitor service performance against metrics, based upon the Service Level Agreement, and provide regular service reports.
- Implement a process to assess end user satisfaction with service levels.
- Implement a process to regularly review and identify possible improvements and to revise Service Level Agreements, as necessary.

### RACI Chart

Activities	Roles				
Implement Service Level Agreement structures.					
Develop and document Service Level Agreements.					
Maintain a Service Catalogue.					
Monitor and revise Service Level Agreements.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

### Maturity Model – Manage Service Levels

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	1: Initial	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for service level and service catalogue management.</li> <li><input type="checkbox"/> The need for service level and service catalogue management is communicated inconsistently.</li> <li><input type="checkbox"/> Communication to stakeholders about service levels and the Service Catalogue is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for service level and service catalogue management.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss Service Level Agreements and the Service Catalogue on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about the Service Catalogue and Service Level Agreements occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of service level and service catalogue management.</li> <li><input type="checkbox"/> IT leadership and IT staff understand the importance of meeting Service Level Agreements.</li> <li><input type="checkbox"/> Senior leadership and IT leadership understand the interrelationship between service levels and resources, and manage supply and demand accordingly.</li> <li><input type="checkbox"/> The Service Catalogue is defined, documented and communicated to stakeholders.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of service level requirements.</li> <li><input type="checkbox"/> Understanding of service level and service catalogue items is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about service level and service catalogue management issues is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need for service level management.</li> <li><input type="checkbox"/> IT leadership understands the requirements for service level and service catalogue management.</li> <li><input type="checkbox"/> The need to establish Service Level Agreements and service definitions is communicated consistently.</li> <li><input type="checkbox"/> Service levels are discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about service levels occurs periodically.</li> <li><input type="checkbox"/> The relationship between service levels and education processes is communicated to and understood by IT staff.</li> </ul>			

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> Skills and Expertise	<b>1: Initial</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of service level and service catalogue management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform service level and service catalogue management have not been identified.</li> <li><input type="checkbox"/> Training needs for service level and service catalogue management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic service level and service catalogue management.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic service level and service catalogue management have been identified.</li> <li><input type="checkbox"/> Training in service level and service catalogue management is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key service level and service catalogue management processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of service level and service catalogue management has been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for service level and service catalogue management has been developed.</li> <li><input type="checkbox"/> Formal training in service level and service catalogue management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all service level and service catalogue management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of service level and service catalogue management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for service level and service catalogue management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for service level and service catalogue management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in service level and service catalogue management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of service level and service catalogue management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in service level and service catalogue management, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into service level and service catalogue management processes and outputs.</li> </ul>
	<b>PEOPLE (continued)</b>				

Maturity Level	
<b>PEOPLE (continued)</b>	<b>Responsibility and Accountability</b>
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li>□ Allocation of responsibility for service level and service catalogue management is assumed or done in an ad hoc way.</li> </ul>	<b>2: Repeatable</b> <ul style="list-style-type: none"> <li>□ Allocation of responsibility for service level and service catalogue management is done informally.</li> <li>□ Individuals assume responsibility for service level and service catalogue management.</li> <li>□ There is confusion about who is responsible and accountable for service level and service catalogue management when issues arise.</li> </ul>
<b>3: Defined</b> <ul style="list-style-type: none"> <li>□ Accountability and responsibility for service level and service catalogue management have been formally assigned and documented.</li> <li>□ Service level and service catalogue management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<b>4: Managed</b> <ul style="list-style-type: none"> <li>□ Service level and service catalogue management owners have the level of authority required to fulfill their responsibilities.</li> </ul>
<b>5: Optimized</b> <ul style="list-style-type: none"> <li>□ Service level and service catalogue management process owners are empowered to make decisions and to take action.</li> <li>□ Service level and service catalogue management process owners escalate issues, according to a defined escalation process.</li> </ul>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Service definition and negotiation of Service Level Agreements occur in isolation and are based upon individual IT staff practices.</li> <li>□ Policies and procedures for creating and maintaining Service Level Agreements do not exist.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies for service level and service catalogue management are defined, but not documented.</li> <li>□ Compliance with service level and service catalogue management policies and procedures is left to the individual's discretion.</li> <li>□ Rudimentary Service Level Agreements and service definitions have been developed.</li> <li>□ Service Level Agreements are operationally and technically focused, with limited emphasis on strategic and educational requirements.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for key service level and management processes have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ Service level and service catalogue management procedures ensure that educational requirements are captured and met, when appropriate.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all service level and management activities are defined, documented and regularly reviewed.</li> <li>□ IT leadership approves policies and procedures for service level and service catalogue management.</li> <li>□ Service level and service catalogue management processes are linked with change management processes to enable continuous improvement.</li> <li>□ Service definitions and Service Level Agreements are used in other processes.</li> <li>□ Service Level Agreements and Operating Level Agreements are defined for most IT services.</li> </ul>	<ul style="list-style-type: none"> <li>□ Service level and service catalogue management processes and outputs support the implementation of the IT Strategic Plan.</li> <li>□ Generally accepted best practices and standards for service level and service catalogue management are used to inform policy and procedure development.</li> <li>□ Exceptions to service level and service catalogue management policies and procedures are noticed and corrective action is taken.</li> <li>□ Service level and service catalogue management policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				
<b>PROCESS</b>					

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some service level management goals are set and monitored inconsistently.</li> <li>□ Service level management goals are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance of service level and service catalogue management is monitored informally.</li> <li>□ IT leadership provides senior leadership with basic reports about the state of service levels.</li> <li>□ The response to issues identified in reports is inconsistent and reactive.</li> <li>□ Initial goals for service level and service catalogue management are defined, but are not clearly linked to educational requirements or jurisdiction goals.</li> </ul>	<ul style="list-style-type: none"> <li>□ Service Level Agreements are monitored regularly.</li> <li>□ Targets and thresholds for IT services have been defined and documented in Service Level Agreements.</li> <li>□ IT leadership provides senior leadership with regular reports about service levels.</li> </ul>	<ul style="list-style-type: none"> <li>□ Service level and service catalog management metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of service level and management policies and procedures are used to inform decision making and continuous improvement.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance management is integrated into service level and service catalog management.</li> <li>□ Peer- and sector-based benchmarking for service level and service catalog management is performed.</li> <li>□ Service level and service catalog management processes are monitored and measured.</li> </ul>
	<p>Goal Setting and Measurement</p>				

PROCESS (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support service level management; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support service level management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan is developed to acquire and implement tools to support service level and service catalogue management.</li> <li>□ The basic level of functionality in tools and templates for service level and service catalogue management is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support service level and service catalogue management have been implemented.</li> <li>□ Integration of tools to support service level and service catalogue management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support service level and service catalogue management.</li> <li>□ Tools are used in key areas to automate and formalize service level and service catalogue management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support service level and service catalogue management.</li> </ul>
	TOOLS	Tools and Automation			

## Manage Incidents

### Description

Incidents will occur—despite all best efforts. Having a defined process to manage incidents, from reporting to closure, minimizes service disruptions.

The incident management process includes setting up a single point of contact (often called the service desk or help desk) for end users. It is here that calls are recorded, escalated to the correct group, resolved and closed. By managing incidents, all end user queries, issues and requests are managed through their life cycle.

### Value

- Increases productivity and improved end user satisfaction through quick resolution to queries and efficient handling of service requests.

### Goals

- Ensure timely and effective response to end user queries, issues and requests.
- Restore normal service operation efficiently and effectively.

### Target Audience

Primary	Secondary
IT Leadership IT Staff	School Administrators

### Key Activities

#### Identify, record and classify incidents.

- Record and track incidents and service requests (referred to as incidents).
- Classify incidents by service categories and priorities.
- Inform end users of the status of incidents they report.

#### Perform initial diagnosis of incidents and escalate.

- Define and implement an incident escalation process that includes agreed-upon levels of escalation and response times and that takes Service Level Agreement (SLA) targets into account.
- Identify solutions or workarounds for reported incidents and escalate the incident, as appropriate.
- Inform end users of escalation and update the incident record.

#### Investigate and address incidents.

- Implement a process to investigate and diagnose incidents to determine the root cause and resolution.
- Implement a process to document investigations undertaken and the steps taken to resolve the incident.

#### Resolve incidents and recover data.

- Define and establish a process to implement resolutions to incidents. Follow change management processes, as applicable.
- Ensure data is recovered.
- Close the incident record.

**Close incidents.**

- Define and implement a process to verify that the incident is resolved and that end users are satisfied.

**Monitor and report on incidents.**

- Define incident metrics, and report and review them regularly.

**RACI Chart**

Activities	Roles				
Identify, classify and record incidents.					
Diagnose and escalate incidents.					
Perform initial diagnosis and escalation.					
Investigate and address incidents.					
Resolve incidents and recover data.					
Close incidents.					
Monitor and report on incidents.					

**RACI Responsibilities**

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage Incidents**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction’s strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to manage incidents and service requests.</li> <li><input type="checkbox"/> The need for a formal approach to manage incidents and service requests is communicated inconsistently.</li> <li><input type="checkbox"/> Incident and service request management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about incident and service management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for incident and service request management.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound incident and service request management process.</li> <li><input type="checkbox"/> The service desk or help desk is the formal and first point of contact for all IT incident reports and service requests.</li> <li><input type="checkbox"/> Communication to stakeholders about incident and service management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of incident and service request management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of using incident and service request management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of incident and service request management.</li> <li><input type="checkbox"/> Understanding of incident and service request management processes is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about incident and service request management is formal and proactive.</li> </ul>
	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to manage incidents and service requests.</li> <li><input type="checkbox"/> IT leadership understands the requirements for managing incidents and service requests.</li> <li><input type="checkbox"/> The need for a formal approach to manage incidents and service requests is communicated consistently.</li> <li><input type="checkbox"/> A first point of contact (i.e., service desk, help desk) is introduced in the organization to handle incidents and service requests.</li> <li><input type="checkbox"/> Communication to stakeholders about incident and service request management occurs periodically.</li> <li><input type="checkbox"/> End users begin to use the services of the first point of contact.</li> </ul>			

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of formal incident and service request management practices exists in isolation.</li> <li>□ Minimum skills required to perform incident and service request management have not been identified.</li> <li>□ Training needs for incident and service request management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT staff have the skills and expertise to perform all key incident and service request management processes.</li> <li>□ Skill requirements for all aspects of incident and service request management have been defined and documented.</li> <li>□ A formal training plan for incident and service requests management has been developed.</li> <li>□ Formal training in incident and service request management is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all incident and service request management processes.</li> <li>□ Proficiency in critical aspects of incident and service request management is ensured for individuals who perform these processes.</li> <li>□ Skill requirements for incident and service request management are reviewed and updated on a regular basis.</li> <li>□ Formal training for incident and service request management is required for individuals who perform these processes.</li> <li>□ Certification in incident and service request management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of incident and service request management is ensured for individuals who perform these processes.</li> <li>□ The jurisdiction encourages formal training in incident and service request management, based on personal and jurisdiction goals.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into incident and service request management.</li> </ul>
	<b>PEOPLE (continued)</b>	Skills and Expertise			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> 1: Initial	Allocation of responsibility for incident and service request management is assumed or done in an ad hoc way.	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for incident management is done informally.</li> <li>□ Individuals assume responsibility for incident management.</li> <li>□ There is confusion about who is responsible and accountable for incident management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for incident and service request management have been formally assigned and documented.</li> <li>□ Incident and service request management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Incident and service request management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Incident and service request management process owners are empowered to make decisions and to take action.</li> <li>□ Incident and service request management process owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Incident and service request management occurs informally and is based upon individual IT staff practices.</li> <li>□ Policies and procedures for incident and service request management are undefined.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all key incident and service request management processes have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ A formal procedure for managing major incidents has been defined, documented and communicated.</li> <li>□ Procedures include steps to record, prioritize, identify impact, classify, update, escalate and formally close incidents.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all incident and service request activities are defined, documented and regularly reviewed.</li> <li>□ IT leadership approves policies and procedures for incident and service request management.</li> <li>□ There are clear and documented links between change, incident and problem management and management processes.</li> <li>□ End users are informed of the progress of reported incidents or service requests and are alerted, in advance, if service levels cannot be met.</li> <li>□ IT staff share incident resolutions and workarounds consistently.</li> </ul>	<ul style="list-style-type: none"> <li>□ Generally accepted best practices and standards for incident and service request management are used to inform policy and procedure development.</li> <li>□ Incident and service request models are defined in automated workflows.</li> <li>□ Exceptions to incident and service request management policies and procedures are noticed and corrective action is taken.</li> <li>□ Incident and service request management policies and procedures are regularly reviewed and improved.</li> </ul>

**PROCESS**

Policies, Plans and Procedures

Maturity Level	
<b>PROCESS (continued)</b>	<b>Goal Setting and Measurement</b>
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>□ Some incident and service request management goals are set and monitored inconsistently.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li>□ The performance of incident management is monitored informally.</li> <li>□ IT leadership provides basic reports to senior leadership about the state of incident management.</li> <li>□ IT staff have basic operational targets for solving incidents and implementing service requests.</li> <li>□ Initial goals are set for incident management, but they are not clearly linked to educational requirements or jurisdiction goals.</li> </ul>
<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li>□ Incident and service request management is monitored regularly.</li> <li>□ Targets and thresholds for incident and service request management are defined, documented and communicated.</li> <li>□ IT leadership provides regular reports to senior leadership about the status of incident and service request management.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li>□ Incident and service request management metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of incident and service request management policies and procedures are used to inform decision making and continuous improvement.</li> </ul>
<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>□ Performance management is integrated into incident and service request management.</li> <li>□ Peer- and sector-based benchmarking for incident and service request management is performed.</li> <li>□ Incident and service request management processes are monitored and measured.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>□ Performance management is integrated into incident and service request management.</li> <li>□ Peer- and sector-based benchmarking for incident and service request management is performed.</li> <li>□ Incident and service request management processes are monitored and measured.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support incident and service request management; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support incident and service request management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to incident management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support incident management are emerging.</li> <li>□ A call-tracking tool is implemented for the first point of contact (i.e., service desk, help desk).</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support incident and service request management has been developed.</li> <li>□ The basic level of functionality in tools for incident and service request management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Incidents and service requests are consistently captured, tracked and reported in the incident and service request management tool.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support incident and service request management have been implemented.</li> <li>□ Integration of tools to support incident and service request management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support incident and service request management.</li> <li>□ Tools are used in key areas to automate and formalize incident and service request management.</li> <li>□ Incident reports and service requests are consistently recorded in incident and service request management tools.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support incident and service request management.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Manage Problems

### Description

Incidents that reoccur not only cause disruptions for end users, but they also erode stakeholder confidence in the quality of IT service provided. Identifying the underlying cause of incidents and treating that cause can prevent incident reoccurrence.

Problem management comprises the activities needed to diagnose the underlying root cause of reoccurring incidents and to find a solution for the resulting problem. The process must ensure that the solution is implemented by applying the correct change and release management procedures.

### Value

- Improves reliability of IT services and minimizes service disruptions.
- Sustains stakeholder confidence in IT services.

### Goals

- Prevent problems and resulting incidents from occurring or recurring.
- Minimize the impact of non-preventable incidents.

### Target Audience

Primary	Secondary
IT Leadership IT Staff	

### Key Activities

#### Identify and classify problems.

- Implement a process to detect, record and classify problems.

#### Investigate and address problems.

- Implement a process to diagnose the root cause of problems.
- Develop workarounds or solutions for problems.
- Create a record of the problem.

#### Resolve problems.

- Implement resolutions to problems, using the processes outlined in Manage Change.
- Review and close problems.

### RACI Chart

Activities	Roles				
Identify and classify problems.					
Investigate and address problems.					
Resolve problems.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage Problems**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	1: Initial	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to manage problems.</li> <li><input type="checkbox"/> The need for a formal approach to manage problems is communicated inconsistently.</li> <li><input type="checkbox"/> Formal approaches to problem management are discussed in response to issues.</li> <li><input type="checkbox"/> Communication to stakeholders about problem management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff understand the requirements of an effective problem management process.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound problem management process.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss problem management on a regular basis.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of problem management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of using problem management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of the requirements for problem management.</li> <li><input type="checkbox"/> Understanding of problem management processes is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about problem management issues is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership understands the requirements for managing problems.</li> <li><input type="checkbox"/> The need for problem management is communicated consistently.</li> <li><input type="checkbox"/> Known errors and workarounds are communicated among IT staff.</li> <li><input type="checkbox"/> IT staff can differentiate between incidents and problems, and address each accordingly.</li> </ul>			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of formal approaches to problem management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform problem management have not been identified.</li> <li><input type="checkbox"/> Training needs for problem management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic problem management.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic problem management have been identified.</li> <li><input type="checkbox"/> Training in problem management is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key problem management processes.</li> <li><input type="checkbox"/> Skill requirements for all problem management processes have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for problem management has been developed.</li> <li><input type="checkbox"/> Formal training in problem management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all problem management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of problem management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for problem management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for problem management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in problem management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of problem management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in problem management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide advice and input into problem management processes.</li> </ul>
	Skills and Expertise				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for problem management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for problem management is done informally.</li> <li>□ Individuals assume responsibility for problem management.</li> <li>□ There is confusion about who is responsible and accountable for problem management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for problem management have been formally assigned and documented.</li> <li>□ Problem management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Problem management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Problem management process owners are empowered to make decisions and to take action.</li> <li>□ Problem management processes owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Problem management activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> Policies and processes for managing problems are undefined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key problem management processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Problem management processes are linked with change management processes to enable continuous improvement.</li> <li><input type="checkbox"/> A formal procedure for managing major problems has been defined, documented and communicated.</li> <li><input type="checkbox"/> Procedures include steps to record, prioritize, identify impact, classify, update, escalate and formally close problems.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all problem management activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> IT leadership approves policies and procedures for problem management.</li> <li><input type="checkbox"/> There are clear and documented links between change, incident processes and problem management processes.</li> <li><input type="checkbox"/> End users are informed of the progress of reported problems and known errors and are alerted, in advance, if service levels cannot be met.</li> <li><input type="checkbox"/> IT staff consistently share problem resolutions, known errors and workarounds.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Generally accepted best practices and standards for problem management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to problem management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> Problem management processes have been defined in automated workflows.</li> <li><input type="checkbox"/> Problem management policies and procedures are regularly reviewed and improved.</li> </ul>

**PROCESS**

Policies, Plans and Procedures

Maturity Level	
<b>PROCESS (continued)</b>	<b>Attributes</b>
<b>1: Initial</b>	<p>Some problem management goals are set and monitored inconsistently.</p> <p>Problem management goals are unclear or vaguely defined.</p>
<b>2: Repeatable</b>	<p>Performance of problem management is monitored informally.</p> <p>IT leadership receives basic problem management reports.</p> <p>Basic operational targets are set to solve problems and apply workarounds.</p> <p>Initial problem management goals are defined, but they are not clearly linked to educational objectives or jurisdiction goals.</p>
<b>3: Defined</b>	<p>Problem management is monitored regularly.</p> <p>Targets and thresholds for problem management have been defined and documented.</p> <p>IT staff provide regular reports to IT leadership about problem management.</p>
<b>4: Managed</b>	<p>Problem management metrics are formally defined and approved.</p> <p>Measures of the effectiveness of problem management policies and procedures are used to inform decision making and continuous improvement.</p>
<b>5: Optimized</b>	<p>Performance management is integrated into problem management policies and procedures.</p> <p>Peer- and sector-based benchmarking for problem management is performed.</p> <p>Problem management processes are monitored and measured.</p>
Goal Setting and Measurement	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support problem management; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no formal approach to using tools to support problem management.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Basic tools and templates, specific to problem management, have been developed and implemented.</li> <li><input type="checkbox"/> Common approaches to the use of tools to support problem management are emerging.</li> <li><input type="checkbox"/> Problem management tools are implemented and used in a limited way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan is developed to acquire and implement tools to support problem management.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates for problem management is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> <li><input type="checkbox"/> Use of automation for problem models is emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support problem management have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support problem management is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support incident and service request management.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize problem management.</li> <li><input type="checkbox"/> Problem reports and known errors are consistently recorded in problem management tools.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools is used to support problem management.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Manage Changes

### Description

The jurisdiction is dependent on the reliability and continuity of IT services. Service and infrastructure changes have an impact on jurisdiction IT services and must be controlled so that exposure to risks and service disruptions is minimized and changes are implemented successfully.

This process area includes initiating, planning, implementing and validating changes to the IT environment.

### Value

- Reduces the number of service disruptions and the amount of re-work caused by failed changes.

### Goals

- Respond to evolving requirements and maximize value while reducing incidents, disruption and re-work.
- Ensure that changes are managed in a controlled manner.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership School Administrators IT Staff

### Key Activities

#### Initiate requests for change in a controlled manner.

- Implement a process to record, assess and authorize all changes prior to implementation, including changes to procedures, processes, systems and service parameters.
- Evaluate the overall risk, complexity, priority and remediation plans prior to implementing the change.

#### Have changes of significant complexity, risk or cost evaluated by a Change Advisory Board.

- Determine thresholds for escalation of changes to the Change Advisory Board.

#### Implement changes in a controlled manner.

- Implement a process to schedule, test and implement changes.
- Develop risk mitigation strategies for changes.

#### Implement a process to review and close requests for change.

- Implement a process to collect and file all appropriate change documentation.
- Review all changes against planned outcomes after implementation.

#### Manage emergency changes.

- Implement a process to evaluate the impact, risk and benefit of performing emergency changes.
- Implement a process to test emergency changes, when feasible.
- Authorize, perform and close emergency changes, ensuring that the change is adequately documented.

**Monitor and report on change metrics.**

- Measure and report on the efficiency, effectiveness and frequency of planned and emergency changes.

**RACI Chart**

Activities	Roles				
Initiate requests for change in a controlled manner.					
Have changes of significant complexity, risk or cost evaluated by a Change Advisory Board.					
Implement changes in a controlled manner.					
Manage emergency changes.					
Monitor and report change metrics.					

**RACI Responsibilities**

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage Changes**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction’s strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to manage changes.</li> <li><input type="checkbox"/> The need for a formal approach to manage changes is communicated inconsistently.</li> <li><input type="checkbox"/> Change management is discussed in response to issues.</li> <li><input type="checkbox"/> Communication to stakeholders about changes to the IT environment and their impact is sporadic and usually in response to issues.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to manage changes.</li> <li><input type="checkbox"/> IT leadership understands the requirements for managing changes.</li> <li><input type="checkbox"/> The need to manage changes, in a controlled way, is communicated consistently.</li> <li><input type="checkbox"/> Change management is discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about change management occurs periodically.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership understands the requirements for managing changes.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound change management process.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss change management on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about change management occurs on a regular basis and in a formal way.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of change management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of following change management processes occurs on a regular basis and in a formal way.</li> <li><input type="checkbox"/> Communication to stakeholders about unplanned changes occurs in a formal way.</li> <li><input type="checkbox"/> IT leadership conducts change meetings and change management review meetings with stakeholders, as appropriate.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of change management requirements.</li> <li><input type="checkbox"/> Understanding of change management processes is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> All stakeholders in the process are aware of the need for formal change management.</li> </ul>	
	<p>Awareness, Understanding and Communication</p>				

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized	
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of formal change management processes exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to formally perform change management have not been identified.</li> <li><input type="checkbox"/> Training needs for a formal approach to change management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic change management.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic change management have been identified.</li> <li><input type="checkbox"/> Training in change management is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all change management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of change management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of change management have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for change management has been developed.</li> <li><input type="checkbox"/> Formal training in change management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all change management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of change management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for change management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for change management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in change management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of change management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in change management, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into change management processes.</li> </ul>
	<b>PEOPLE (continued)</b>	Skills and Expertise				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for change management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for change management have been formally assigned and documented.</li> <li>□ Change management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Change management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Change management process owners are empowered to make decisions and to take action.</li> <li>□ Change management process owners escalate issues, according to a defined escalation process.</li> </ul>

Responsibility and Accountability

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<input type="checkbox"/> Change management activities occur in isolation and are based upon individual IT staff practices.	<input type="checkbox"/> Common and informal policies and procedures for change management are defined, but not documented.	<input type="checkbox"/> Formal policies and procedures for key change management processes have been defined, documented and communicated.	<input type="checkbox"/> Formal policies and procedures for all change management activities are defined, documented and regularly reviewed.	<input type="checkbox"/> Generally accepted best practices and standards for change management are used to inform policy and procedure development.
	<input type="checkbox"/> Policies and procedures for change management are undefined.	<input type="checkbox"/> Compliance with change management policies and procedures is left to the individual's discretion.	<input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.	<input type="checkbox"/> There are clear and documented links between incident and problem management processes.	<input type="checkbox"/> Exceptions to change management policies and procedures are noticed and corrective action is taken.
	<input type="checkbox"/> The need for approvals of certain changes is not consistently understood; as a result, approvals are not consistently obtained for changes.	<input type="checkbox"/> A formal procedure for managing emergency changes has been defined, documented and communicated.	<input type="checkbox"/> There are clear and documented links between change processes and capacity management processes.	<input type="checkbox"/> Change management policies and procedures are regularly reviewed and improved.	
	<input type="checkbox"/> Impact assessment sometimes occurs before the change is implemented.	<input type="checkbox"/> Procedures include steps to record, prioritize, identify impact, classify, authorize, implement and review changes.	<input type="checkbox"/> End users are informed of the progress of changes and are alerted, in advance, if service levels cannot be met.		
	<input type="checkbox"/> A process for planning changes is emerging.				
	Policies, Plans and Procedures				
<b>PROCESS</b>					

Maturity Level	
<b>PROCESS (continued)</b>	<i>Attributes</i>
<b>1: Initial</b>	<b>1: Initial</b>
<b>2: Repeatable</b>	<b>2: Repeatable</b>
<b>3: Defined</b>	<b>3: Defined</b>
<b>4: Managed</b>	<b>4: Managed</b>
<b>5: Optimized</b>	<b>5: Optimized</b>

Goal Setting and Measurement

- Some change management goals are set and monitored inconsistently.
- Change management goals are unclear or vaguely defined.

- Performance of change management is monitored informally.
- IT leadership receives basic reports about the status of the change management process.
- Initial change management goals have been defined.

- Change management is monitored regularly.
- Targets and thresholds for change management have been defined and documented.
- IT staff provide IT leadership with regular reports about change management.
- IT leadership provides senior leadership with regular reports about change management.

- Change management metrics are formally defined and approved.
- Measures of the effectiveness of change management policies and procedures are used to inform decision making and continuous improvement.

- Performance management is integrated into change management.
- Peer- and sector-based benchmarking for change management is performed.
- Change management processes and procedures are monitored and measured.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support change management; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no formal approach to using tools to support change management.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Basic tools and templates, specific to change management, have been developed and implemented.</li> <li><input type="checkbox"/> Common approaches to the use of tools to support change management are emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan is developed to acquire and implement tools to support change management.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates for change management is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> <li><input type="checkbox"/> Changes are consistently captured, tracked and reported in the change management tool.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support change management have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support change management is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support change management.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize change management.</li> <li><input type="checkbox"/> Tools are used to enable change auditing.</li> <li><input type="checkbox"/> Changes are consistently recorded in the change management tool.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support change management.</li> <li><input type="checkbox"/> Tools to detect unlicensed and unlicensed software are used.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Manage IT Service Continuity and Availability

### Description

School jurisdictions are increasingly dependent upon IT services to support day-to-day activities. The process of managing IT service continuity and availability ensures that IT services are available and that IT services are restored in a timely and appropriate way when major events, such as a fire or flood, occur.

Provision of continuous IT services requires a reliable infrastructure and the development, maintenance and testing of IT continuity plans.

This process area includes handling continuity issues, where normal service operation is no longer possible, and ensuring that services are available, when required, during normal operations.

### Value

- Minimizes the likelihood and impact of a major IT service interruption to key jurisdiction functions and processes.
- Ensures the IT department delivers the required level of service by making services available at agreed-upon levels.

### Goals

- Ensure the required IT technical and service facilities can be restored within agreed-upon timelines.
- Ensure the level of service availability delivered is cost effective and meets or exceeds the jurisdiction's current and future agreed-upon needs.

### Target Audience

Primary	Secondary
IT Leadership School Administrators	Senior Leadership IT Staff

### Key Activities

#### Define and implement a policy for service continuity.

- Define senior leadership's intention and objectives for service continuity.
- Specify the scope of the service continuity policy.

#### Implement an IT service continuity management process.

- Implement a process to determine service continuity requirements, including business impact analysis and risk analysis.
- Implement a process to regularly review, test and update the IT Continuity Plan.
- Ensure end users and IT staff receive training in service continuity management and recovery procedures.

**Implement an availability management process** to ensure that services are available, when needed, and as defined in Service Level Agreements.

- Implement a process to identify vital services in the jurisdiction.
- Perform component failure impact analysis, in addition to risk analysis and management.
- Design services to meet availability requirements.
- Test for availability.

- Plan preventative maintenance to comply with availability requirements.
- Implement a process to monitor, measure, analyze and report on the availability of services.
- Evaluate service failures and periods of unavailability to determine root causes and to address issues.

### RACI Chart

Activities	Roles				
Define and implement a policy for service continuity.					
Implement an IT service continuity management process.					
Implement an availability management process.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

### Maturity Model – Manage IT Service Continuity and Availability

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to IT service continuity and availability management.</li> <li><input type="checkbox"/> The need for a formal approach to IT service continuity and availability is communicated inconsistently.</li> <li><input type="checkbox"/> Service continuity and availability management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about service continuity and availability is sporadic and usually in response to issues.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need for IT service continuity and availability management.</li> <li><input type="checkbox"/> IT leadership understands the requirements for IT service continuity and availability management.</li> <li><input type="checkbox"/> The need for IT service continuity and availability management is communicated consistently.</li> <li><input type="checkbox"/> IT service continuity and availability management is discussed periodically.</li> <li><input type="checkbox"/> Communication to stakeholders about IT service continuity and availability management occurs periodically.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the requirements for service continuity management.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound service continuity management process.</li> <li><input type="checkbox"/> IT staff understand the importance of service continuity management.</li> <li><input type="checkbox"/> Communication to stakeholders about service continuity occurs on a regular basis and in a formal way.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of IT service continuity and availability management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of IT service continuity and availability management occurs on a regular basis and in a formal way.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of the requirements for IT service continuity and availability management.</li> <li><input type="checkbox"/> Senior leadership and key stakeholders understand critical IT service continuity and availability management processes.</li> <li><input type="checkbox"/> Communication to stakeholders about IT service continuity and availability management issues is formal and proactive, when possible.</li> </ul>	
	<p>Awareness, Understanding and Communication</p>				

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of service continuity and availability management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform service continuity and availability management have not been identified.</li> <li><input type="checkbox"/> Training needs for service continuity and availability management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key service continuity management processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of service continuity management have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for service continuity management has been developed.</li> <li><input type="checkbox"/> Formal training in service continuity management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all IT service continuity and availability management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT service continuity and availability management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for IT service continuity and availability management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for IT service continuity and availability management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT service continuity and availability management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT service continuity and availability management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT service continuity and availability management, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into IT service continuity and availability management processes.</li> </ul>
	<b>PEOPLE (continued)</b>				

Skills and Expertise

Maturity Level	
<b>Attributes</b> <b>1: Initial</b>	<b>2: Repeatable</b> <ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT service continuity and availability management is done informally.</li> <li>□ Individuals assume responsibility for IT service continuity and availability management.</li> <li>□ There is confusion about who is responsible and accountable for IT service continuity and availability management when issues arise.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for service continuity management have been formally assigned and documented.</li> <li>□ Service continuity management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li>□ IT service continuity and availability management owners have the level of authority required to fulfill their responsibilities.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li>□ IT service continuity and availability management process owners are empowered to make decisions and to take action.</li> <li>□ IT service continuity and availability management process owners escalate issues, according to a defined escalation process.</li> </ul>

Responsibility and Accountability

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT service continuity and availability management are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT service continuity and availability management policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Most continuity issues are solved without using change management processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key service continuity management processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> A formal procedure for managing availability has been defined, documented and communicated.</li> <li><input type="checkbox"/> Service continuity management processes are linked with the change management process to enable continuous improvement.</li> <li><input type="checkbox"/> Procedures include steps to develop and maintain the IT Service Continuity Plan and the availability plan.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT service continuity and availability management activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> Senior leadership approves policies and procedures for service continuity and availability management.</li> <li><input type="checkbox"/> The IT Service Continuity Plan is defined, documented and tested on a regular basis.</li> <li><input type="checkbox"/> IT service continuity and availability are included in the design of new services.</li> <li><input type="checkbox"/> IT service continuity processes are linked with change management processes to enable continuous improvement.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT service continuity and availability management plans support the jurisdiction's business continuity plan.</li> <li><input type="checkbox"/> Generally accepted best practices for IT service continuity and availability management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT service continuity and availability management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT service continuity and availability management are regularly reviewed and updated.</li> </ul>
	<p style="text-align: right;">Policies, Plans and Procedures</p> <p style="text-align: right;"><b>PROCESS</b></p>				

Maturity Level	
<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some IT service continuity and availability management goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> IT service continuity and availability management goals are unclear or vaguely defined.</li> </ul>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of IT service continuity and availability management is monitored informally.</li> <li><input type="checkbox"/> IT leadership receives basic reports about IT service continuity and availability management.</li> <li><input type="checkbox"/> Initial goals for IT service continuity and availability management are defined, but not clearly linked to educational requirements or jurisdiction goals.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT service continuity is monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for IT service continuity have been defined and documented.</li> <li><input type="checkbox"/> IT staff provide regular reports to IT leadership about IT service continuity management.</li> <li><input type="checkbox"/> IT leadership provides regular reports to senior leadership about IT service continuity management.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT service continuity and availability metrics have been formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of IT service continuity and availability management are used to inform decision making and continuous improvement.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into IT service continuity and availability management.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for IT service continuity and availability management is performed.</li> <li><input type="checkbox"/> IT service continuity and availability management are monitored and measured.</li> </ul>
<b>PROCESS (continued)</b>	Goal Setting and Measurement
<i>Attributes</i>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT service continuity and availability management; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support IT service continuity and availability management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to IT service continuity and availability management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support IT service continuity and availability management are emerging.</li> <li>□ Basic availability monitoring tools have been implemented and are used.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT service availability management has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT service continuity management is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT service continuity management have been implemented.</li> <li>□ Integration of tools to support IT service continuity and availability management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT service continuity and availability management.</li> <li>□ Tools are used in key areas to automate and formalize IT service continuity and availability management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support IT service continuity and availability management.</li> <li>□ Tools to automate recovery of information and restoration of service have been implemented, where feasible.</li> </ul>
	Tools and Automation				

**TOOLS**

## Manage Capacity

### Description

Availability of adequate IT capacity prevents incidents and service disruptions. Capacity management provides assurance that information resources that support business requirements are continually available.

This process area includes reviewing the current performance and capacity of IT resources periodically and forecasting future needs, based on workload, storage and contingency requirements.

### Value

- Ensures that the IT services that support the jurisdiction's business objectives have adequate capacity, when needed, but limit costs related to excess capacity.

### Goals

- Ensure that IT capacity is matched to the current and future agreed-upon needs of the jurisdiction, in a timely manner and at an appropriate cost.

### Target Audience

Primary	Secondary
IT Leadership	School Administrators IT Staff

### Key Activities

To achieve the goal of capacity management for IT resources, the jurisdiction should document key activities, with clear roles and responsibilities assigned.

**Manage business capacity** to ensure that the demand for IT services is considered and understood.

- Translate educational requirements and plans into requirements for services and IT infrastructure.
- Estimate future requirements for IT service capacity by using data on current resource usage and by developing trends, forecasts or models to predict changes, based on anticipated business events and growth.

**Manage service capacity** to ensure that each service meets the agreed-upon capacity service targets.

- Manage, control and predict the end-to-end performance and capacity of operational IT services use and workloads.
- Ensure that the performance of all services, as detailed in service targets within Service Level Agreements (SLAs) and Service Level Requirements (SLRs), is monitored and measured, and that the collected data is recorded, analyzed and reported.
- Respond to changing demands to ensure that the performance of all services meets agreed-upon educational requirements.

**Manage resource capacity** to ensure that discrete service components, including infrastructure hardware and software, meet existing and future needs.

- Ensure that all components within the IT infrastructure that have finite resources are monitored and measured, and that the collected data is recorded, analyzed and reported.

### RACI Chart

Activities	Roles				
Manage business capacity.					
Manage service capacity.					
Manage resource capacity.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage Capacity**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	1: Initial	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to IT capacity management.</li> <li><input type="checkbox"/> The need for a formal approach to IT capacity management is communicated inconsistently.</li> <li><input type="checkbox"/> IT capacity management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT capacity management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for IT capacity management.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound IT capacity management process.</li> <li><input type="checkbox"/> Communication to stakeholders about IT capacity management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of IT capacity management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of using IT capacity management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of IT capacity management requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about IT capacity management issues is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication				

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT capacity management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform IT capacity management have not been identified.</li> <li><input type="checkbox"/> Training needs for IT capacity management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key IT capacity management processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of IT capacity management have been defined and documented.</li> <li><input type="checkbox"/> Skill requirements are differentiated for business, service and component capacity management.</li> <li><input type="checkbox"/> A formal training plan for IT capacity management has been developed.</li> <li><input type="checkbox"/> Formal training in IT capacity management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all IT capacity management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT capacity management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for IT capacity management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for IT capacity management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT capacity management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT capacity management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT capacity management, based upon personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into IT capacity management.</li> </ul>
	<b>PEOPLE (continued)</b>	Skills and Expertise			

Maturity Level		1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>PEOPLE (continued)</b> Attributes	Responsibility and Accountability	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for IT capacity management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT capacity management is done informally.</li> <li>□ Individuals assume responsibility for IT capacity management.</li> <li>□ There is confusion about who is responsible and accountable for IT capacity management when issues arise.</li> <li>□ There is no delineation in responsibilities between business, service and component capacity management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT capacity management have been formally assigned and documented.</li> <li>□ Responsibilities are differentiated between business, service and component capacity management.</li> <li>□ IT capacity management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT capacity management owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT capacity management process owners are empowered to make decisions and to take action.</li> <li>□ IT capacity management process owners escalate issues, according to a defined escalation process.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT capacity management activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> IT capacity management activities are undertaken after capacity-related incidents occur.</li> <li><input type="checkbox"/> Policies and procedures for IT capacity management are undefined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT capacity management are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT capacity management policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Policies and procedures emphasize component capacity management.</li> <li><input type="checkbox"/> Few policies and procedures are developed for business and service capacity management.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key IT capacity management processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> IT capacity management processes are linked with change management processes.</li> <li><input type="checkbox"/> IT capacity management processes ensure that education requirements are captured and met, as appropriate.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT capacity management activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> IT leadership approves policies and procedures for IT capacity management.</li> <li><input type="checkbox"/> IT capacity management processes are linked with change management processes to enable continuous improvement.</li> <li><input type="checkbox"/> The Capacity Plan is used to support other IT service management processes.</li> <li><input type="checkbox"/> There are clear and documented links between change and capacity management processes.</li> <li><input type="checkbox"/> The Capacity Plan is regularly reviewed and updated.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> The Capacity Plan supports the implementation of the IT Strategic Plan.</li> <li><input type="checkbox"/> Generally accepted best practices and standards for capacity management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT capacity management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT capacity management policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				
<b>PROCESS</b>					

Maturity Level	
<b>PROCESS (continued)</b>	<b>Goal Setting and Measurement</b>
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li>□ Some IT capacity management goals are set and monitored inconsistently.</li> <li>□ IT capacity management goals are unclear or vaguely defined.</li> </ul>	<b>2: Repeatable</b> <ul style="list-style-type: none"> <li>□ Performance of IT capacity management is monitored informally.</li> <li>□ IT leadership provides basic reports to senior leadership about the state of IT component capacity.</li> <li>□ IT leadership receives basic operational capacity management reports.</li> <li>□ Initial goals for IT capacity management are defined, but not clearly linked to educational requirements or jurisdiction goals.</li> </ul>
<b>3: Defined</b> <ul style="list-style-type: none"> <li>□ IT capacity and IT capacity management are monitored regularly.</li> <li>□ Targets and thresholds for IT capacity have been defined and documented.</li> <li>□ IT staff provide regular reports to IT leadership about IT capacity.</li> <li>□ IT leadership provides regular reports to senior leadership about IT capacity.</li> </ul>	<b>4: Managed</b> <ul style="list-style-type: none"> <li>□ IT capacity management metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of IT capacity management policies and procedures are formally defined and approved.</li> </ul>
<b>5: Optimized</b> <ul style="list-style-type: none"> <li>□ Performance management is integrated into IT capacity management.</li> <li>□ Peer- and sector-based benchmarking for IT capacity management is performed.</li> <li>□ IT capacity management processes are monitored and measured.</li> </ul>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT capacity planning; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support IT capacity planning.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to IT capacity management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support IT capacity management are emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT capacity management has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT capacity management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ A capacity plan template is developed and implemented.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT capacity management have been implemented.</li> <li>□ Integration of tools to support IT capacity management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT capacity management.</li> <li>□ Tools are used in key areas to automate and formalize IT capacity management processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support IT capacity management.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Manage Release and Deployment

### Description

Once development is complete, new and enhanced services need to be made operational. Effective deployment requires planning, scheduling and controlling the implementation of releases, first into a test environment, and then into the production environment.

This includes:

- testing in an environment designed to minimize the impact of incidents that may occur during testing
- testing with relevant test data
- preparing rollout and migration instructions, including a back-out plan
- deploying the release
- reviewing the implementation to ensure that changes meet agreed-upon expectations.

### Value

- Reduces the frequency of end user and service disruptions.
- Minimizes risks associated with implementing new services.

### Goals

- Ensure that the integrity of the operational environment is protected, that the correct components are released and that end users are properly informed of changes before they are made.

### Target Audience

Primary	Secondary
IT Leadership IT Staff	

### Key Activities

**Plan IT service deployment** before a new or changed service is put into production—the rigour of such planning will depend upon the size and complexity of the environment and the new or changed services.

- Implement a process to evaluate the complexity of a new or changed service to determine how much planning is required.
- Develop pass/fail criteria, build and test plans, release package compilation and build plans, deployment plans or financial plans, as appropriate.

**Verify the new or changed IT service** against specifications before starting the build, test and deployment process.

- Manage common services and infrastructure components to minimize any impact on the build and test of the new or changed service.
- Locate and review available release documentation.
- Acquire, implement and test all release components.
- Compile the release information.

**Coordinate IT service testing and pilot efforts.**

- Ensure that the test environment is stable.
- Ensure that sensitive data in the test environment is protected.

- Release the service to the test environment.
- Run tests and pilot efforts.

**Prepare for IT service deployment.**

- Prepare the release package for implementation.
- Review implementation risks and plan appropriate mitigating steps.
- Train end users and IT staff on the new IT service.
- Make any approved last minute changes.

**Transfer and deploy the IT service release.**

- Review service performance by testing.
- Complete performance tests.
- Verify the configuration of service assets.
- Update the Service Catalogue.
- Inform end users of any activities underway that relate to the service and the status of deployment.
- Deliver or distribute service components, according to the Service Deployment Plan.
- Transfer financial assets.
- Publish documentation.
- Transfer management capability.
- Transfer the service to operations.

**Verify the IT service deployment** to ensure that end users are able to use the new service.

**Provide early IT service support** for incidents and problems that arise from the new service or change.

- Update documentation, known errors and FAQs.

**Review and close the IT service release.**

- Verify the quality of knowledge transfer activities, training and documentation.

## RACI Chart

Activities	Roles				
Plan IT service deployment.					
Verify the new or changed IT service.					
Coordinate IT service testing and pilot efforts.					
Prepare for IT service deployment.					
Transfer and deploy the IT service release.					
Verify the IT service deployment.					
Provide early IT service support.					
Review and close the IT service release.					

## RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

## Maturity Model – Manage Release and Deployment

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> Awareness, Understanding and Communication	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to release management.</li> <li><input type="checkbox"/> The need for a formal approach to release management is communicated inconsistently.</li> <li><input type="checkbox"/> Release management is discussed in response to issues.</li> <li><input type="checkbox"/> Communication to stakeholders about release management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for release and deployment management.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound release and deployment management process.</li> <li><input type="checkbox"/> Communication to stakeholders about release and deployment occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of release and deployment management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of using release and deployment management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of release and deployment management requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about release and deployment management issues is formal and proactive, when possible.</li> </ul>
	<b>PEOPLE</b>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized	
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of release management practices exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform release management, in a formal way, have not been identified.</li> <li><input type="checkbox"/> Training needs for release management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic release and deployment management.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic release and deployment management have been identified.</li> <li><input type="checkbox"/> Training in release and deployment management is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all release and deployment management processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of release and deployment management have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for release and deployment management has been developed.</li> <li><input type="checkbox"/> Formal training in release and deployment management is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all release and deployment management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of release and deployment management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for release and deployment management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training in release and deployment management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in release and deployment management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of release and deployment management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in release and deployment management, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into release and deployment management.</li> </ul>

Skills and Expertise

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>Allocation of responsibility for capacity management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for release and deployment management is done informally.</li> <li>Individuals assume responsibility for release and deployment management.</li> <li>There is confusion about who is responsible and accountable for release and deployment management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability and responsibility for release and deployment management have been formally assigned and documented.</li> <li>Release and deployment management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Release and deployment management owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Release and deployment management process owners are empowered to make decisions and to take action.</li> <li>Release and deployment management process owners escalate issues, according to a defined escalation process.</li> </ul>
	Responsibility and Accountability				

PEOPLE (continued)

Maturity Level	
<b>PROCESS</b>	<b>Attributes</b>
<p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Release management activities occur and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> Policies and procedures for release management are undefined.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal release and deployment management policies and procedures have been defined, but not documented.</li> <li><input type="checkbox"/> Compliance with release and deployment management policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Approval for releases and deployments is not consistently obtained.</li> </ul>
<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all key release and deployment management processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> A formal procedure for testing releases has been defined, documented and communicated.</li> <li><input type="checkbox"/> A formal procedure for managing major releases has been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> Procedures include steps to plan, build, test, deploy and formally close releases.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all release and deployment management activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> IT leadership approves policies and procedures for release and deployment management.</li> <li><input type="checkbox"/> End users are informed about the progress of releases and are alerted, in advance, if service levels cannot be met.</li> </ul>
<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Generally accepted best practices and standards for release and deployment management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to release and deployment management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> Release and deployment management policies and procedures are regularly reviewed and improved.</li> <li><input type="checkbox"/> Release strategies are automated, when feasible.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Generally accepted best practices and standards for release and deployment management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to release and deployment management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> Release and deployment management policies and procedures are regularly reviewed and improved.</li> <li><input type="checkbox"/> Release strategies are automated, when feasible.</li> </ul>

Policies, Plans and Procedures

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some release management goals are set and monitored inconsistently.</li> <li>□ Goals for release management are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li>□ Release and deployment management is monitored regularly.</li> <li>□ Targets and thresholds for release management have been defined and documented.</li> <li>□ IT staff provide regular reports to IT leadership about release and deployment management.</li> <li>□ IT leadership provides regular reports to senior leadership about release and deployment management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Release and deployment management metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of release and deployment management policies and procedures are used to inform decision making and continuous improvement.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance management is integrated into release and deployment management.</li> <li>□ Peer- and sector-based benchmarking for release and deployment management is performed.</li> <li>□ Release and deployment management processes are monitored and measured.</li> </ul>
	Goal Setting and Measurement				

PROCESS (continued)

Maturity Level	
<b>Attributes</b>	<b>1: Initial</b>
<b>2: Repeatable</b>	<b>3: Defined</b>
<b>4: Managed</b>	<b>5: Optimized</b>

  

<b>TOOLS</b>	Tools and Automation
--------------	----------------------

  

<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support release management; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> Basic release implementation tools exist.</li> <li><input type="checkbox"/> Release control is tool-driven.</li> <li><input type="checkbox"/> There is no formal approach to using tools to support release management, implementation and control.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan to acquire and implement tools to support release and deployment management has been developed.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates for release and deployment management is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> <li><input type="checkbox"/> Use of push or pull technology to automate release and deployment is emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support release and deployment management have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support release and deployment management is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support release and deployment management.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize release and deployment management.</li> <li><input type="checkbox"/> Releases and test results are consistently recorded in release and deployment management tools.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support release and deployment management.</li> <li><input type="checkbox"/> A standardized set of tools is used to automate release and deployment management.</li> </ul>
---	---	---	--

## Manage Operations

### Description

IT operations management enables the ongoing management and maintenance of the jurisdiction's IT infrastructure to ensure delivery of the agreed-upon level of services to the jurisdiction. IT processing requires effective management of processing procedures and diligent maintenance of hardware.

This process area includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware.

### Value

- Reduces the risk of downtime caused by infrastructure failure.

### Goals

- Achieve consistency in the jurisdiction's day-to-day IT processes and activities.
- Maintain stability through regular examination of, and improvements to, operational IT components.
- Apply operational skills to diagnose and resolve any IT operations failures.

### Target Audience

Primary	Secondary
IT Leadership IT Staff	

### Key Activities

**Define, implement and maintain operating procedures and instructions** for IT operations, ensuring that IT staff are familiar with all operations tasks relevant to them.

- Operational procedures cover shift hand-over (i.e., formal hand-over of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) to support agreed-upon service levels and to ensure continuous operations.

**Define and implement IT infrastructure monitoring procedures** to monitor the IT infrastructure and related events.

- Ensure that sufficient chronological information is stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and other activities that surround or support operations.

**Define and implement preventive maintenance for hardware procedures** to ensure timely maintenance of infrastructure and to reduce the frequency and impact of failures or performance degradation.

**Develop central observation and monitoring capability** through console management. Use the consoles to monitor and control operations.

**Segregate duties and facilities** to ensure key operational roles are appropriately separated from each other.

- Develop and implement policies for segregation of duties and facilities.

- Implement compensating controls to review the operational activities of these roles when segregation is not possible.
- Separate test and production processing facilities to reduce the risks of unauthorized or unintentional changes or access to the jurisdiction's production data and systems.

**Maintain a media library management system** of stored and archived media to ensure their accessibility, usability and integrity.

**Define and implement policies and procedures for disposal of IT assets** to ensure that business requirements for the protection of sensitive data and software are met when data or hardware are disposed of or transferred.

**Define and implement policies and procedures for backup and restoration of systems, applications, data and documentation** that is in line with jurisdictional requirements as well as the Continuity Plan.

## RACI Chart

Activities	Roles				
Define, implement and maintain operating procedures and instructions.					
Define and implement IT infrastructure monitoring procedures.					
Define and implement preventive maintenance for hardware procedures.					
Develop central observation and monitoring capability.					
Segregate duties and facilities.					
Maintain a media library management system.					
Define and implement policies and procedures for the disposal of IT assets.					
Define and implement policies and procedures for the backup and restoration of systems, applications, data and documentation.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage Operations**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	1: Initial	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to IT operations management.</li> <li><input type="checkbox"/> The need for a formal approach to IT operations management is communicated inconsistently.</li> <li><input type="checkbox"/> IT operations management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about IT operations management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for IT operations management.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound IT operations management process.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss IT operations management on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about IT operations occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of IT operations management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of IT operations management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of IT operations management requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about IT operations management issues is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication				

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of IT operations management exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform IT operations management have not been identified.</li> <li><input type="checkbox"/> Training needs for IT operations management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic IT operations management.</li> <li><input type="checkbox"/> Minimum skill requirements for IT operations management have been identified.</li> <li><input type="checkbox"/> Training in IT operations management is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all IT operations management processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of IT operations management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for IT operations management are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for IT operations management is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in IT operations management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of IT operations management is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in IT operations management, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into IT operations management.</li> </ul>
	<b>PEOPLE (continued)</b>				

Skills and Expertise

Maturity Level	
<b>1: Initial</b>	<p>Allocation of responsibility for IT operations management is assumed or done in an ad hoc way.</p>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for IT operations management is done informally.</li> <li>□ Individuals assume responsibility for IT operations management.</li> <li>□ There is confusion about who is responsible and accountable for IT operations management when issues arise.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT operations management have been formally assigned and documented.</li> <li>□ IT operations management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li>□ IT operations management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li>□ IT operations management process owners are empowered to make decisions and to take action.</li> <li>□ IT operations management process owners escalate issues, according to a defined escalation process.</li> </ul>
<b>PEOPLE (continued)</b>	Responsibility and Accountability

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><b>Attributes</b></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT operations management activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> IT operating procedures and instructions are undefined and undocumented.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT operations management are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT operations management policies and procedures is left to the individual's discretion.</li> </ul>	<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key IT operations management processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> Procedures include steps to schedule jobs, backup and restore data, monitor operations, perform console management, and manage print and output.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for all IT operations management activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> IT leadership approves policies and procedures for IT operations management.</li> <li><input type="checkbox"/> End users are informed about the progress of their jobs or prints and are alerted, in advance, if service levels cannot be met.</li> <li><input type="checkbox"/> Operations incidents are managed according to the incident management process.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Generally accepted best practices and standards for IT operations management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT operations management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT operations management policies and procedures are regularly reviewed and improved.</li> <li><input type="checkbox"/> All IT operations management jobs are defined in automated workflows.</li> </ul>	
	<p>Policies, Plans and Procedures</p>				

**PROCESS**

Maturity Level	
<b>PROCESS (continued)</b>	<b>Attributes</b>
<b>1: Initial</b>	<p>Some IT operations management goals are set and monitored inconsistently.</p> <p>IT operations management goals are unclear or vaguely defined.</p>
<b>2: Repeatable</b>	<p>Performance of IT operations management is monitored informally.</p> <p>IT leadership provides basic reports to senior leadership about IT operations management.</p> <p>IT leadership receives basic operation management reports.</p> <p>Basic targets for IT operations management are set.</p> <p>Initial goals for IT operations management are defined, but are not clearly linked to educational requirements or jurisdiction goals.</p>
<b>3: Defined</b>	<p>IT operations are monitored regularly.</p> <p>Targets and thresholds for IT operations have been defined and documented.</p> <p>IT staff provide regular reports to IT leadership about IT operations.</p> <p>IT leadership provides regular reports to senior leadership about IT operations.</p>
<b>4: Managed</b>	<p>IT operations management metrics are formally defined and approved.</p> <p>Measures of the effectiveness of IT operations management are used to inform decision making and continuous improvement.</p>
<b>5: Optimized</b>	<p>Performance management is integrated into IT operations management.</p> <p>Peer- and sector-based benchmarking for IT operations management is performed.</p> <p>IT operations management are monitored and measured.</p>
<b>Goal Setting and Measurement</b>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support IT operations management; they are generally based upon standard desktop tools.</li> <li>□ Basic monitoring tools exist and are used inconsistently.</li> <li>□ There is no formal approach to using tools to support IT operations management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to IT operations management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support IT operations management are emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT operations management has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT operations management is used.</li> <li>□ The use of tools to automate IT operations is emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT operations management have been implemented.</li> <li>□ Integration of tools to support IT operations management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT operations management.</li> <li>□ Tools are used in key areas to automate and formalize IT operations management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support IT operations management.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				
TOOLS					

## Manage Facilities

### Description

Protection for computer equipment requires well-designed and well-managed physical facilities<sup>1</sup>.

The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities and designing effective processes to monitor environmental factors and manage physical access.

### Value

- Protects the confidentiality, reliability and availability of the jurisdiction's IT systems and information.

### Goals

- Maintain IT-related facilities to achieve stability in day-to-day IT processes and activities in the jurisdiction.

### Target Audience

Primary	Secondary
IT Leadership	School Administrators IT Staff

### Key Activities

#### Evaluate candidate sites and layouts.

- Implement a process to evaluate risks, such as natural and man-made disasters, and to assess relevant laws and regulations, such as occupational health and safety regulations, when selecting and laying out sites for IT facilities.

**Implement physical security measures** that are in line with the jurisdiction's requirements to secure the physical location and assets. Evaluate physical security measures to effectively prevent, detect and mitigate risks, such as:

- theft
- temperature
- fire
- smoke
- water
- vibration
- acts of terror or vandalism
- power outages
- chemicals
- explosives.

#### Design and implement measures to protect against environmental factors.

- Install specialized equipment and devices to monitor and control the environment, as appropriate.

<sup>1</sup> The term "facilities" is being used, in this document, in its widest sense. This process area includes any place where shared equipment is located in the jurisdiction.

**Secure IT facilities.**

- Implement policies and processes to grant, limit or revoke access to the premises, buildings and areas, according to the jurisdiction’s needs.
- Ensure that the policies and processes apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or other third parties.
- Implement policies related to equipment security to ensure equipment is not removed from the jurisdiction’s premises, unless authorized, and to ensure that equipment is secure after removal.
- Define and implement processes to ensure that sensitive data is removed from equipment prior to disposal.

**Manage physical facilities**, including power and communications equipment, in compliance with laws and regulations, technical and jurisdiction requirements, vendor specifications, and health and safety guidelines.

- Define and implement equipment maintenance policies.

**RACI Chart**

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Select site and layout.					
Implement physical security measures.					
Design physical access.					
Protect against environmental factors.					
Manage physical facilities.					

**RACI Responsibilities**

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage Facilities**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction’s strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to facilities management.</li> <li><input type="checkbox"/> The need for a formal approach to facilities management is communicated inconsistently.</li> <li><input type="checkbox"/> Facilities management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about facilities management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for IT facilities management.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss IT facilities management on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about IT facilities management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of IT facilities management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of IT facilities management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of IT facilities management requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about IT facilities management issues is formal and proactive, where possible.</li> </ul>
	Awareness, Understanding and Communication				

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of facilities management practices exists in isolation.</li> <li>□ Minimum skills required to perform facilities management have not been identified.</li> <li>□ Training needs for facilities management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all key IT facilities management processes.</li> <li>□ Skill requirements for all aspects of IT facilities management have been defined and documented.</li> <li>□ A formal training plan for IT facilities management has been developed.</li> <li>□ Formal training in IT facilities management is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all IT facilities management processes.</li> <li>□ Proficiency in critical aspects of IT facilities management is ensured for individuals who perform these tasks.</li> <li>□ Skill requirements for IT facilities management are reviewed and updated on a regular basis.</li> <li>□ Formal training for IT facilities management is required for individuals who perform these tasks.</li> <li>□ Certification in IT facilities management is encouraged for individuals who perform these tasks.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of IT facilities management is ensured for individuals who perform these tasks.</li> <li>□ The jurisdiction encourages formal training in IT facilities management, based on personal and jurisdiction goals.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into IT facilities management.</li> </ul>

PEOPLE (continued)

Skills and Expertise

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for facilities management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for IT facilities management have been formally assigned and documented.</li> <li>□ IT facilities management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT facilities management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT facilities management process owners are empowered to make decisions and to take action.</li> <li>□ IT facilities management process owners escalate issues, according to a defined escalation process.</li> </ul>

Responsibility and Accountability

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Facilities management activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> Policies and procedures for facilities management are undefined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for IT facilities management are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with IT facilities management policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> A consistent approach to IT facilities management is followed.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key IT facilities management processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> Procedures include steps to take physical security measures, design site layout, manage facilities and protect against environmental issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Policies and procedures for all IT facilities management activities are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> IT leadership approves policies and procedures for IT facilities management.</li> <li><input type="checkbox"/> Facilities incidents are managed according to the incident management process.</li> <li><input type="checkbox"/> Facilities changes are managed according to the change management or service request management process.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT facilities management plans support the implementation of the IT Strategic Plan.</li> <li><input type="checkbox"/> Generally accepted best practices and standards for IT facilities management are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to IT facilities management policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> IT facilities management policies and procedures are regularly reviewed and improved.</li> </ul>
	<p style="text-align: right;">Policies, Plans and Procedures</p>				

**PROCESS**

Maturity Level	
<b>PROCESS (continued)</b>	<b>Attributes</b>
<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some facilities management goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> Facilities management goals are unclear or vaguely defined.</li> </ul>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of IT facilities management is monitored informally.</li> <li><input type="checkbox"/> IT leadership provides basic reports to senior leadership about the state of IT facilities and facilities management.</li> <li><input type="checkbox"/> Initial goals for IT facilities management are defined, but not clearly linked to educational requirements or jurisdiction goals.</li> <li><input type="checkbox"/> Basic operational targets for IT facilities management have been set.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT facilities management is monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for IT facilities management have been defined and documented.</li> <li><input type="checkbox"/> IT staff provide regular reports to IT leadership about IT facilities management.</li> <li><input type="checkbox"/> IT leadership provides regular reports to senior leadership about IT facilities management.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT facilities management metrics are formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of IT facilities management policies and procedures are used to inform decision making and continuous improvement.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into IT facilities management.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for IT facilities management is performed.</li> <li><input type="checkbox"/> IT facilities management is monitored and measured.</li> </ul>
Goal Setting and Measurement	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support facilities management; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support facilities management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to IT facilities management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support IT facilities management are emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support IT facilities management has been developed.</li> <li>□ The basic level of functionality in tools and templates for IT facilities management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Use of tools to automate IT facilities management tasks is emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support IT facilities management have been implemented.</li> <li>□ Integration of tools to support IT facilities management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support IT facilities management.</li> <li>□ Tools are used in key areas to automate and formalize IT facilities management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and automated techniques is used to support IT facilities management.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Train End Users

### Description

This section focuses on planning for and providing training about how to operate, support and use technology, within the context of jurisdiction IT policies and procedures.

This section **is not** about planning for or providing professional development related to the integration of technology into the instructional process.

### Value

- Increases effective, efficient use of technology within the context of jurisdiction IT policies and procedures.
- Reduces end user errors, incidents of non-compliance with security controls and frequency of support requests.

### Goals

- Design and implement a jurisdiction IT training strategy for end users that addresses existing IT services and the release of new IT services.

### Target Audience

Primary	Secondary
IT Leadership School Administrators	IT Staff

### Key Activities

#### Develop a comprehensive end user training program.

- Implement a process to identify training needs for each group of jurisdiction employees, considering proposed, new and existing IT services, changes to technology policies and procedures, and commonly recurring, preventable incidents.
- Develop a set of course offerings that meets identified training needs.

#### Deliver training to end users.

#### Monitor, evaluate and improve end user training.

- Evaluate each course offering for relevance, quality, cost and value.
- Evaluate training outcomes to determine the effectiveness of the training program.
- Report effectiveness of the training program.
- Regularly review and adjust the end user training program to ensure that it continues to meet jurisdiction goals.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Develop a comprehensive end user training program.					
Deliver training to end users.					
Monitor, evaluate and improve end user training.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Train End Users**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>PEOPLE</b>	<i>Attributes</i>	<b>1: Initial</b>	<b>3: Defined</b>	<b>4: Managed</b>	<b>5: Optimized</b>
	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to end user training.</li> <li><input type="checkbox"/> The need for a formal approach to end user training is communicated inconsistently.</li> <li><input type="checkbox"/> End user training is discussed in response to issues, requests for information from senior leadership or project requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about end user training is sporadic and usually in response to issues or project requirements.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for a formal approach to end user training.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a formal approach to end user training.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss end user training on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about end user training occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of formal approaches to train end users.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of end user training occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of end user training requirements.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of end user training practices exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to train end users have not been identified.</li> <li><input type="checkbox"/> Training needs for IT staff to provide end user training have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff have the skills and expertise to perform basic training for end users on some applications.</li> <li><input type="checkbox"/> Minimum skill requirements to perform basic end user training have been identified.</li> <li><input type="checkbox"/> IT staff are provided training to develop their skills as trainers in response to emerging needs or requests from individuals.</li> <li><input type="checkbox"/> Informal end user training is provided in response to emerging needs or project-based needs.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key end user training processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of end user training have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for end user training has been developed. (Note: These requirements cover "train-the-trainer" and not the skill requirements of end users.)</li> <li><input type="checkbox"/> Formal training in methods to train end users is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all end user training processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of end user training is ensured for individuals who perform these tasks.</li> <li><input type="checkbox"/> Skill requirements for end user training are reviewed and updated on a regular basis. (Note: These requirements cover "train-the-trainer" and not the skill requirements of end users.)</li> <li><input type="checkbox"/> Formal training to train end users is required for individuals who perform these tasks.</li> <li><input type="checkbox"/> Certification in end user training is encouraged for individuals who perform these tasks.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of end user training is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in end user training techniques, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into end user training.</li> </ul>
	<p style="text-align: right;"><b>PEOPLE (continued)</b></p>	Skills and Expertise			

Maturity Level	
<b>PEOPLE</b> <i>(continued)</i>	Responsibility and Accountability
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Allocation of responsibility for end user training is assumed or done in an ad hoc way.</li> </ul>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Allocation of responsibility and accountability for end user training is done informally.</li> <li><input type="checkbox"/> Individuals assume responsibility for end user training.</li> <li><input type="checkbox"/> There is confusion about who is responsible and accountable for end user training when issues arise.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Accountability and responsibility for end user training have been formally assigned and documented.</li> <li><input type="checkbox"/> End user training process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> End user training process owners have the level of authority required to fulfill their responsibilities.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> End user training process owners are empowered to make decisions and to take action.</li> <li><input type="checkbox"/> End user training process owners escalate issues, according to a defined escalation process.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<input type="checkbox"/> End user training activities occur in isolation and are based upon individual IT staff practices.	<input type="checkbox"/> Common and informal policies and procedures for end user training are defined, but not documented.	<input type="checkbox"/> Formal policies and procedures for key end user training processes have been defined, documented and communicated.	<input type="checkbox"/> Formal policies and end user training processes are defined, documented and regularly reviewed.	<input type="checkbox"/> The end user training plan supports implementation of the IT Strategic Plan.
	<input type="checkbox"/> Policies and procedures for end user training have not been defined.	<input type="checkbox"/> Compliance with end user training policies and procedures is left to the individual's discretion.	<input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.	<input type="checkbox"/> Senior leadership approves policies and procedures for end user training.	<input type="checkbox"/> Generally accepted best practices and standards for end user training are used to inform policy and procedure development.
			<input type="checkbox"/> End user training procedures include steps to develop the training plan, deliver training and evaluate the training.	<input type="checkbox"/> End user training plans are consistently reviewed before, during and after implementation.	<input type="checkbox"/> Exceptions to end user training policies and procedures are noticed and corrective action is taken.
					<input type="checkbox"/> End user training policies and procedures are regularly reviewed and improved.

**PROCESS**

Policies, Plans and Procedures

Maturity Level	
<b>Attributes</b>	<b>1: Initial</b>
<b>PROCESS (continued)</b>	Goal Setting and Measurement
<b>2: Repeatable</b>	<b>3: Defined</b>
<b>4: Managed</b>	<b>5: Optimized</b>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Some end user training goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> End user training goals are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> End user training is monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for end user training have been defined and documented.</li> <li><input type="checkbox"/> IT staff provide regular reports to IT leadership about end user training.</li> <li><input type="checkbox"/> IT leadership provides regular reports to senior leadership about end user training.</li> </ul>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of end user training is monitored informally.</li> <li><input type="checkbox"/> IT leadership provides basic reports to senior leadership about the state of end user training.</li> <li><input type="checkbox"/> Initial goals for end user training are defined, but not clearly linked to educational requirements or jurisdiction goals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> End user training metrics are formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of end user training are used to inform decision making and continuous improvement.</li> </ul>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into end user training.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for end user training is performed.</li> <li><input type="checkbox"/> End user training processes are measured and monitored.</li> </ul>	

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support end user training; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support end user training.</li> </ul>	<ul style="list-style-type: none"> <li>□ Simple tools and templates, specific to end user training, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support end user training are emerging.</li> <li>□ More robust tools to directly enable end user training are implemented and used by key individuals.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support end user training has been developed.</li> <li>□ The basic level of functionality in tools and templates to support end user training is used.</li> <li>□ Tools in use are not fully integrated.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support end user training have been implemented.</li> <li>□ Integration of tools to support end user training is emerging.</li> <li>□ There is a formal and structured approach to using tools to support end user training.</li> <li>□ Tools are used in key areas to automate and formalize end user training.</li> <li>□ End user training requests are consistently recorded in end user training management tools.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support end user training.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

# Information Security Management

# Information Security Management

## Govern Information Security

### Description

Information security governance helps jurisdictions strike an effective balance between educational goals, risk management and security implementation costs. Outcomes of an effective information security management process include:

- alignment of information security with jurisdiction strategic and educational goals
- effective risk management, monitoring and mitigation
- effective and efficient use of security knowledge and infrastructure
- regular measurement, monitoring and reporting of security governance metrics to provide assurance that jurisdiction objectives are met.

Information security governance includes establishing a framework that defines structures, processes, leadership, roles and responsibilities for governing information security in the jurisdiction.

### Value

- Provides reasonable assurance to jurisdiction leadership and stakeholders that information risks are appropriately managed.

### Goals

- Enable the jurisdiction to balance the potential benefits of accepting information security risks against the costs of managing those risks.
- Establish an effective management process that can be used to identify and address information risks.

### Target Audience

Primary	Secondary
IT Leadership Senior Leadership	Trustees

### Key Activities

**Establish organizational structures for information security** by defining structures, processes and mechanisms to control the implementation of information security within the jurisdiction.

- Assign security roles and responsibilities to coordinate and review the implementation of security across the jurisdiction.
- Assign accountability and responsibility to monitor information security trends, issues and risks on an ongoing basis.

**Establish responsibility for information assets** by identifying information assets, assigning owners to those assets and empowering them to make decisions about controls to be implemented.

**Develop information security policy**, in accordance with jurisdiction requirements and applicable legal and regulatory requirements.

- Issue, communicate and maintain an information security policy to demonstrate support for, and commitment to, information security.

**Assess information risk** by identifying, quantifying and prioritizing information risks against a set of criteria for risk acceptance, including an estimation of probability and impact.

**Treat information risk** by making and documenting treatment decisions, using the jurisdiction's risk acceptance criteria.

- Select and implement appropriate controls to ensure that risks are reduced to an acceptable level, where appropriate.

**Govern information security with third parties** by performing a risk assessment to determine security implications and any control requirements.

- Describe the controls to be used in an agreement between the jurisdiction and the external party.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Establish organizational structures for information security.					
Establish responsibility for information assets.					
Develop information security policy.					
Assess information security risk.					
Treat information security risk.					
Govern information security with third parties.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Govern Information Security**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	1: Initial	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need for information security governance.</li> <li><input type="checkbox"/> The need for information security governance is communicated inconsistently.</li> <li><input type="checkbox"/> Information security governance is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about information security governance is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for information security governance and risk management.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of sound information security governance and risk management processes.</li> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff discuss information security governance and risk management on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders and end users about information security governance and risk management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff have a comprehensive understanding of information security governance and risk management.</li> <li><input type="checkbox"/> Communication to stakeholders about information risks and policies occurs on a regular basis and in a formal way.</li> <li><input type="checkbox"/> Communication to third parties about their responsibilities for information security governance and risk management for jurisdiction information occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of information security governance and risk management requirements.</li> <li><input type="checkbox"/> Understanding of information risks and risk management is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about information risk and management issues is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need for information security governance.</li> <li><input type="checkbox"/> The need for information security governance is communicated inconsistently.</li> <li><input type="checkbox"/> Information security governance is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about information security governance is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for information security governance and risk management.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of sound information security governance and risk management processes.</li> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff discuss information security governance and risk management on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders and end users about information security governance and risk management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff have a comprehensive understanding of information security governance and risk management.</li> <li><input type="checkbox"/> Communication to stakeholders about information risks and policies occurs on a regular basis and in a formal way.</li> <li><input type="checkbox"/> Communication to third parties about their responsibilities for information security governance and risk management for jurisdiction information occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership and IT leadership have an advanced and forward-looking understanding of information security governance and risk management requirements.</li> <li><input type="checkbox"/> Understanding of information risks and risk management is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about information risk and management issues is formal and proactive, when possible.</li> </ul>

Maturity Level		3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <input type="checkbox"/> Some knowledge of information security governance practices exists in isolation. <input type="checkbox"/> Minimum skills required to provide information security governance have not been identified. <input type="checkbox"/> Training needs for information security governance have not been identified.	<b>2: Repeatable</b> <input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic information risk management and security policy management. <input type="checkbox"/> Senior leadership has the skills and expertise to perform basic information risk assessment. <input type="checkbox"/> IT staff have the skills and expertise to perform basic risk treatment. <input type="checkbox"/> Minimum skill requirements to perform information risk management and security policy management have been identified. <input type="checkbox"/> Training in information risk management and security policy management is provided in response to emerging needs or requests from individuals. <input type="checkbox"/> External advice is sought when gaps in expertise are evident.	<b>3: Defined</b> <input type="checkbox"/> Senior leadership has the skills and expertise to make informed information risk management decisions. <input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key information security governance and risk management processes. <input type="checkbox"/> Skill requirements for all aspects of information security governance and risk management have been defined and documented. <input type="checkbox"/> Information asset owners have the skills and expertise to perform information risk assessments. <input type="checkbox"/> A formal training plan for information security governance and risk management is developed. <input type="checkbox"/> Formal training in information security governance and risk management is available.	<b>4: Managed</b> <input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all information security governance and risk management processes. <input type="checkbox"/> Proficiency in critical aspects of information security governance and risk management is ensured for individuals who perform these processes. <input type="checkbox"/> Skill requirements for information security governance and risk management are reviewed and updated on a regular basis. <input type="checkbox"/> Formal training for information security governance and risk management is required for individuals who perform these processes. <input type="checkbox"/> Certification in information security governance and risk management is encouraged for individuals who perform these processes.	<b>5: Optimized</b> <input type="checkbox"/> Proficiency in all aspects of information security governance and risk management is ensured for individuals who perform these processes. <input type="checkbox"/> The jurisdiction encourages formal training in information security governance and risk management, based on personal and jurisdiction goals. <input type="checkbox"/> Certification in information security governance and risk management is required for individuals who perform these processes. <input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into information security governance and risk management processes and outputs.
	<b>PEOPLE (continued)</b> Skills and Expertise			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>Allocation of responsibility for information security governance is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for information security governance and risk management is done informally.</li> <li>Individuals assume responsibility for information security governance and risk management.</li> <li>There is confusion about who is responsible and accountable for information security governance and risk management when issues arise.</li> <li>Information asset ownership is informally assigned to functional areas of the organization.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability and responsibility for conducting information risk management activities are formally assigned to information asset owners.</li> <li>Information security governance and risk management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> <li>Third parties have formally accepted accountability and responsibility for information security governance and risk management.</li> </ul>	<ul style="list-style-type: none"> <li>Information security governance and risk management process owners have the level of authority required to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>Information security governance and risk management process owners are empowered to make decisions and to take action.</li> <li>Information security governance and risk management process owners and information asset owners escalate issues, according to a defined escalation process.</li> </ul>
	<p>Responsibility and Accountability</p>				

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Information security governance and risk management activities occur in isolation and are based upon individual IT staff practices.</li> <li>□ Policies and procedures for information security governance and risk management have not been defined.</li> <li>□ Information risks are identified and treated informally.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for information security governance and risk management are defined, but not documented.</li> <li>□ Compliance with information security governance and risk management policies and procedures is left to the individual's discretion.</li> <li>□ Information risk assessment and management procedures are informal, but can be used to identify significant risks.</li> <li>□ Third-party information security governance and risk management requirements are managed informally.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for key information security governance and risk management processes have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ Procedures include steps to identify significant risks and the security controls needed to mitigate them.</li> <li>□ Third-party security requirements are managed using contract management procedures.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all information security governance and risk management activities are defined, documented and regularly reviewed.</li> <li>□ Senior leadership approves policies and procedures for information security governance and risk management.</li> <li>□ Information security governance and risk management policies are integrated with other IT and jurisdiction governance and risk management policies and procedures.</li> </ul>	<ul style="list-style-type: none"> <li>□ Procedures to identify, implement and operate security controls are integrated with other jurisdiction compliance procedures.</li> <li>□ Generally accepted best practices and standards for information security governance and risk management are used to inform policy and procedure development.</li> <li>□ Exceptions to information security governance and risk management are noticed and corrective action is taken.</li> <li>□ Information security governance and risk management policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				

**PROCESS**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Information security governance and risk management goals are set and monitored inconsistently.</li> <li>□ Information security governance and risk management goals are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance of information security governance and risk management is monitored informally.</li> <li>□ IT leadership provides basic reports to senior leadership about the state of information security governance and risk management.</li> <li>□ Initial goals for information security governance and risk management are defined, but not clearly linked to educational requirements or jurisdiction goals.</li> </ul>	<ul style="list-style-type: none"> <li>□ Information security governance and risk management is monitored regularly.</li> <li>□ Targets and thresholds for information security governance and risk management have been defined and documented.</li> <li>□ IT staff and information asset owners provide reports to IT leadership about the number and types of information risks being managed.</li> <li>□ IT leadership provides senior leadership with regular reports about information security governance and risk management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Information security governance and risk management metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of information security risk management are used to inform decision making and continuous improvement.</li> <li>□ Measures include indicators of the effectiveness of security controls relative to cost and jurisdiction risk tolerance levels.</li> </ul>	<ul style="list-style-type: none"> <li>□ Performance management is integrated into information security governance and risk management.</li> <li>□ Peer- and sector-based benchmarking for information security governance and risk management is performed.</li> <li>□ Information security governance and risk management processes are monitored and measured.</li> </ul>
	<p>Goal Setting and Measurement</p>				

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support information security governance and risk management activities; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support information security governance and risk management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates, specific to information security governance and risk management, have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support information security governance and risk management are emerging.</li> <li>□ Third-party security responsibilities and requirements are included in contract documentation.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan to acquire and implement tools to support information security governance and risk management has been developed.</li> <li>□ The basic level of functionality in tools and templates for information security governance and risk management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Risks are consistently captured, tracked and reported in the risk management tool.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support information security governance and risk management have been implemented.</li> <li>□ Integration of tools to support information security governance and risk management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support information security governance and risk management.</li> <li>□ Tools are used in key areas to automate and formalize information security governance and risk management.</li> <li>□ Information security risks, mitigation strategies and issues are consistently recorded in information security governance and risk management tools.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support information security governance and risk management.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Protect Information

### Description

Information protection provides assurance to jurisdiction stakeholders that sensitive information is adequately protected as it is collected, stored, used and shared by jurisdiction staff and partners.

This process area includes the mechanisms and infrastructure used to support the collection, storage and processing of information as well as the information required to understand the threats and common conditions that lead to incidents and losses.

### Value

- Provides reasonable assurance to jurisdiction leadership and stakeholders that sensitive information is appropriately protected.

### Goals

- Address potential threats to jurisdiction information and reduce the risk of loss, unauthorized disclosure or unauthorized alteration of information.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	IT Staff

### Key Activities

**Classify information** by defining and applying a policy and model to classify data, in terms of its sensitivity, seriousness and value to the jurisdiction, and assign ownership of that data appropriately.

**Protect against malicious code** by implementing procedures and tools to detect, prevent and remove malicious code within the appropriate layers of IT infrastructure.

**Manage media** used to store sensitive information to prevent unauthorized disclosures and losses; implement controls to protect all storage and archived media that contain sensitive information, including physical media, such as paper-based print-outs.

**Protect information during exchange** by implementing controls to minimize the risk that sensitive information may be lost or misused.

## RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Classify information.					
Protect against malicious code.					
Manage media.					
Protect information during exchange.					

## RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Protect Information**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need to protect information.</li> <li><input type="checkbox"/> The need to protect information is communicated inconsistently.</li> <li><input type="checkbox"/> Information protection is discussed in response to issues or requests for information from senior leadership.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements to protect sensitive information.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of a sound information protection process.</li> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff discuss information protection on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about information protection occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of information protection.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of information protection occurs on a regular basis and in a formal way.</li> <li><input type="checkbox"/> A structured awareness program about information protection is implemented for IT staff and end users.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of information protection requirements.</li> <li><input type="checkbox"/> Understanding of information protection is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about information protection is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to protect sensitive information.</li> <li><input type="checkbox"/> IT leadership understands the requirements for protecting sensitive information.</li> <li><input type="checkbox"/> The need to protect sensitive information is communicated consistently.</li> <li><input type="checkbox"/> Information protection policies and processes are communicated periodically and informally.</li> <li><input type="checkbox"/> Information protection requirements are informally communicated to third parties.</li> </ul>			

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <input type="checkbox"/> Some knowledge of information protection practices exists in isolation. <input type="checkbox"/> Minimum skills required to protect information have not been identified. <input type="checkbox"/> Training needs for protection of information have not been identified.	Skills and Expertise	<input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic information protection. <input type="checkbox"/> Minimum skill requirements to perform information protection have been identified. <input type="checkbox"/> Training in information protection is provided in response to emerging needs or requests from individuals. <input type="checkbox"/> External advice is sought when gaps in expertise are evident.	<input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key information protection processes. <input type="checkbox"/> Skill requirements for all aspects of information protection have been defined and documented. <input type="checkbox"/> A formal training plan for information protection has been developed. <input type="checkbox"/> Formal training in information protection is available.	<input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all information protection processes. <input type="checkbox"/> Proficiency in critical aspects of information protection is ensured for individuals who perform these processes. <input type="checkbox"/> Skill requirements for information protection are reviewed and updated on a regular basis. <input type="checkbox"/> Formal training for information protection is required for individuals who perform these processes. <input type="checkbox"/> Certification in information protection is encouraged for individuals who perform these processes.	<input type="checkbox"/> Proficiency in all aspects of information protection is ensured for individuals who perform these processes. <input type="checkbox"/> The jurisdiction encourages formal training in information protection, based on personal and jurisdiction goals. <input type="checkbox"/> Certification in information protection is required for individuals who perform these processes. <input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into information protection processes.
		<b>PEOPLE (continued)</b>			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for the protection of information and ownership of information is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for information protection have been formally assigned and documented.</li> <li>□ Information owners have been formally assigned and documented.</li> <li>□ Information owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Information protection process owners have the level of authority required to fulfill their responsibilities.</li> <li>□ IT staff have the level of authority required to implement, operate and enforce policies and procedures related to information protection.</li> </ul>	<ul style="list-style-type: none"> <li>□ Information protection process owners are empowered to make decisions and to take action.</li> <li>□ Information protection process owners escalate issues, according to a defined escalation process.</li> </ul>
		Responsibility and Accountability			

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Information protection activities occur in isolation and are based upon individual IT staff practices.</li> <li><input type="checkbox"/> Policies and procedures for information protection have not been defined.</li> <li><input type="checkbox"/> Instances of virus infections and loss of information, through loss of storage media and exchange, are identified only when brought to the attention of IT staff.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Common and informal policies and procedures for information protection are defined, but not documented.</li> <li><input type="checkbox"/> Compliance with information protection policies and procedures is left to the individual's discretion.</li> <li><input type="checkbox"/> Repeatable processes for managing virus protection, information storage media and exchanges of information exist.</li> <li><input type="checkbox"/> Basic requirements for information protection controls are documented at a basic level.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and procedures for key information protection processes have been defined, documented and communicated.</li> <li><input type="checkbox"/> Policies and procedures are based upon generally accepted good practices.</li> <li><input type="checkbox"/> Procedures cover antivirus controls and mechanisms to protect information media and information exchanges.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Formal policies and information protection processes are defined, documented and regularly reviewed.</li> <li><input type="checkbox"/> IT leadership approves policies and procedures for information protection.</li> <li><input type="checkbox"/> Procedures include provisions to ensure that virus, media protection and information exchange controls are implemented according to policies and procedures.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Antivirus protection and information media controls are automated, when possible, to ensure controls are current.</li> <li><input type="checkbox"/> Generally accepted best practices and standards for information protection are used to inform policy and procedure development.</li> <li><input type="checkbox"/> Exceptions to information protection policies and procedures are noticed and corrective action is taken.</li> <li><input type="checkbox"/> Information protection policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				
<b>PROCESS</b>					

Maturity Level	
<b>Attributes</b>	<b>1: Initial</b>
<b>2: Repeatable</b>	<b>3: Defined</b>
<b>4: Managed</b>	<b>5: Optimized</b>
<b>Attributes</b>	<b>1: Initial</b>
<b>2: Repeatable</b>	<b>3: Defined</b>
<b>4: Managed</b>	<b>5: Optimized</b>

Goal Setting and Measurement

**PROCESS (continued)**

Some information protection goals are set and monitored inconsistently.

Information protection goals are unclear or vaguely defined.

Investigations into control failures are inconclusive.

Performance of information protection is monitored informally.

IT leadership provides basic reports to senior leadership about the state of information protection.

Initial goals for information protection are defined, but not clearly linked to educational requirements or jurisdiction goals.

Information protection is monitored regularly.

Targets and thresholds for information protection have been defined and documented.

IT leadership provides regular reports to senior leadership about information protection.

Antivirus controls are examined regularly to ensure they are current.

An inventory of information storage media is available and current.

A current list of electronic commerce and sensitive information exchanges is available.

Information protection metrics are formally defined and approved.

Measures of the effectiveness of information protection policies and procedures are used to inform decision making and continuous improvement.

Information protection controls are tested to ensure that they comply with policies and procedures.

Performance management is integrated into information protection.

Peer- and sector-based benchmarking for information protection is performed.

Information protection processes are monitored and measured.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support protection of information; they are based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no formal approach to using tools to support information protection.</li> <li><input type="checkbox"/> Desktop and server operating systems have a variety of antivirus and malware controls installed that utilize basic configuration settings.</li> <li><input type="checkbox"/> Information exchanges include unprotected protocols and techniques, such as FTP, TELNET and HTTP.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Most desktop and server operating systems have antivirus and malware controls installed.</li> <li><input type="checkbox"/> Configurations of antivirus and malware software are known and used, but not documented.</li> <li><input type="checkbox"/> Standardization of information storage media devices is emerging.</li> <li><input type="checkbox"/> Tools are available to purge media of sensitive information.</li> <li><input type="checkbox"/> Information exchanges use protected protocols and techniques, such as SFTP, SCP and HTTPS.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> All desktop and server operating systems have antivirus and malware controls implemented and updated regularly.</li> <li><input type="checkbox"/> Standards exist and are regularly reviewed and updated for information storage devices.</li> <li><input type="checkbox"/> Controls may be used to prevent unauthorized storage media from being used.</li> <li><input type="checkbox"/> Information exchanges are only enabled using standardized protection methods.</li> <li><input type="checkbox"/> Configurations of all information protection controls are formally defined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support information protection have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support information protection is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support information protection.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize information protection.</li> <li><input type="checkbox"/> All desktop and server operating systems are required to have antivirus and malware controls implemented that are updated automatically.</li> <li><input type="checkbox"/> Tools to detect non-compliant information storage devices are used.</li> <li><input type="checkbox"/> Information exchange mechanisms are monitored to ensure compliance.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support information protection.</li> <li><input type="checkbox"/> Automated antivirus and malware tools are integrated across all platforms and with other security tools.</li> <li><input type="checkbox"/> Tools to automate the preparation, use and destruction of information media are used consistently.</li> <li><input type="checkbox"/> Tools to automate the deployment of information exchange protections are integrated with other security tools.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

TOOLS

## Monitor and Report on Information Security

### Description

Security monitoring and reporting enable jurisdictions to identify and respond to information security issues. They encompass:

- security monitoring across the jurisdiction's IT platforms
- a process to ensure all staff and third parties can identify and report issues
- the procedures used to investigate and follow up on reported security incidents.

### Value

- Provides reasonable assurance to jurisdiction leadership and stakeholders that the jurisdiction's information and technology assets are adequately protected.

### Goals

- Ensure information regarding potential security issues is collected, analyzed and reported in a timely manner.
- Proactively identify potential and actual security incidents in order to prevent or detect and address the cause of these incidents.

### Target Audience

Primary	Secondary
IT Leadership IT Staff	Senior Leadership

### Key Activities

**Monitor security** by recording and archiving information security events to detect unauthorized information processing activities and to verify the effectiveness of security controls.

- Identify and comply with legal requirements applicable to IT's information security monitoring and logging activities.

**Report information security events and weaknesses** in a timely and effective way to ensure they are dealt with promptly.

- Inform all staff and stakeholders of the procedures to report security events that impact the security of jurisdiction information systems.

**Manage and improve procedures related to information security incidents** in order to respond to reports of security events and weaknesses in a timely and effective manner.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Monitor security.					
Report information security events and weaknesses.					
Manage and improve procedures.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Monitor and Report on Information Security**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to monitor, report and respond to security issues.</li> <li><input type="checkbox"/> The need for a formal approach to monitor, report and respond to security issues is communicated inconsistently.</li> <li><input type="checkbox"/> Monitoring, reporting and responding to security issues are discussed in response to issues or requests from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about monitoring, reporting and responding to security issues is sporadic and usually in response to issues.</li> </ul>	<p><b>PEOPLE</b></p>	<p>Awareness, Understanding and Communication</p>			
		<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of the need to identify, report and respond to security issues.</li> <li><input type="checkbox"/> IT leadership understands the requirements for security monitoring.</li> <li><input type="checkbox"/> The need for security monitoring and reporting is communicated consistently.</li> <li><input type="checkbox"/> Information security monitoring and reporting policies are communicated to end users and third parties periodically and informally.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for security monitoring.</li> <li><input type="checkbox"/> Senior leadership commits resources to the development of a sound security monitoring process.</li> <li><input type="checkbox"/> Formal communication channels for reporting and responding to information security issues have been implemented.</li> <li><input type="checkbox"/> Senior leadership, IT leadership and IT staff discuss security monitoring and reporting on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about responsibilities and expected actions related to identifying and reporting security issues occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of security monitoring and reporting.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of security monitoring and reporting occurs on a regular basis and in a formal way.</li> <li><input type="checkbox"/> Security incident reports are collected and shared with stakeholders to raise awareness of issues, resolutions and good practices.</li> <li><input type="checkbox"/> Security incident reports are collected from third parties to raise awareness of issues, resolutions and good practices.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of security monitoring and reporting requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about security monitoring and reporting is formal and proactive, when possible.</li> <li><input type="checkbox"/> Security incident reports are shared with external third parties to increase community awareness of issues, resolutions and good practices.</li> </ul>

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of security monitoring and reporting practices exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to monitor, report and respond to security issues have not been identified.</li> <li><input type="checkbox"/> Training needs to support monitoring, reporting and responding to security issues have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic security monitoring and reporting.</li> <li><input type="checkbox"/> IT staff have the expertise to perform system security logging and reporting.</li> <li><input type="checkbox"/> Minimum skill requirements to perform security monitoring and reporting have been identified.</li> <li><input type="checkbox"/> Training in security monitoring and reporting is provided in response to emerging needs or requests from individuals.</li> <li><input type="checkbox"/> External advice is sought when gaps in expertise are evident.</li> <li><input type="checkbox"/> IT staff understand the basic security logging and reporting capabilities of significant systems.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key security monitoring and reporting processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of security monitoring and reporting have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for security monitoring and reporting has been developed.</li> <li><input type="checkbox"/> Formal training in security monitoring is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all security monitoring and reporting processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of security monitoring and reporting is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> Skill requirements for security monitoring and reporting are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for security monitoring and reporting is required for individuals who perform these processes.</li> <li><input type="checkbox"/> Certification in security monitoring and reporting is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of security monitoring and reporting is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in security monitoring and reporting, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> Certification in security monitoring and reporting is required for individuals who perform these processes.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into security monitoring and reporting processes.</li> </ul>
	Skills and Expertise				

**PEOPLE (continued)**

Maturity Level		3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for monitoring, reporting and responding to security issues is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for security monitoring and reporting have been formally assigned and documented.</li> <li>□ Security monitoring and reporting process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Security monitoring and reporting process owners have the level of authority required to fulfill their responsibilities.</li> <li>□ Measures are in place to encourage security incident reporting.</li> </ul>	<ul style="list-style-type: none"> <li>□ Security monitoring and reporting process owners are empowered to make decisions and to take action.</li> <li>□ Security monitoring and reporting process owners escalate issues, according to a defined escalation process.</li> </ul>
	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for security monitoring and reporting is done informally.</li> <li>□ Individuals assume responsibility for security monitoring and reporting.</li> <li>□ There is confusion about who is responsible and accountable for security monitoring and reporting when issues arise.</li> </ul>			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Activities related to monitoring, reporting and responding to security issues occur in isolation and are based upon individual IT staff practices.</li> <li>□ Security issues are identified only when brought to the attention of IT staff.</li> <li>□ Policies and procedures for monitoring, reporting and responding to security issues have not been defined.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for security monitoring and reporting are defined, but not documented.</li> <li>□ Compliance with security monitoring and reporting policies and procedures is left to the individual's discretion.</li> <li>□ Requirements for information systems include basic documentation about security monitoring and reporting.</li> <li>□ Third-party security monitoring and reporting requirements are managed informally.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for key security monitoring and reporting processes have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ Procedures outline monitoring, identifying, reporting and responding to information security events and incidents.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all security monitoring and reporting processes are defined, documented and regularly reviewed.</li> <li>□ Senior leadership approves policies and procedures for security monitoring and reporting.</li> </ul>	<ul style="list-style-type: none"> <li>□ Generally accepted best practices for security monitoring and reporting are used to inform policy and procedure development.</li> <li>□ Exceptions to security monitoring and reporting are noticed and corrective action is taken.</li> <li>□ Security monitoring and reporting procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				

**PROCESS**

Maturity Level	
<p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>□ Some goals for monitoring, reporting and responding to security issues are set and monitored inconsistently.</li> <li>□ Goals for monitoring, reporting and responding to security issues are unclear or vaguely defined.</li> <li>□ Investigations into security incidents, if performed, are inconclusive.</li> </ul>	<p><b>2: Repeatable</b></p> <ul style="list-style-type: none"> <li>□ Performance of security monitoring and reporting is monitored informally.</li> <li>□ IT leadership provides basic reports to senior leadership about security monitoring and reporting.</li> <li>□ Logging and other system monitoring is periodically reviewed to ensure they are operational.</li> <li>□ Initial goals for security monitoring and reporting are defined, but not clearly linked to educational requirements or jurisdiction goals.</li> </ul>
<p><b>3: Defined</b></p> <ul style="list-style-type: none"> <li>□ Security monitoring and reporting are monitored regularly.</li> <li>□ Targets and thresholds for security monitoring and reporting have been defined and documented.</li> <li>□ The number of security events and incidents is reported.</li> <li>□ The number and severity of security incidents that result in a response are reported.</li> <li>□ Security logs are analyzed to identify trends.</li> <li>□ IT staff provide IT leadership with regular reports about security monitoring.</li> <li>□ IT leadership provides senior leadership with regular reports about security monitoring.</li> </ul>	<p><b>4: Managed</b></p> <ul style="list-style-type: none"> <li>□ Security monitoring and reporting metrics are formally defined and approved.</li> <li>□ Measures of the effectiveness of security monitoring and reporting are used to inform decision making and continuous improvement.</li> <li>□ Security monitoring and reporting processes are assessed, on a regular basis, to ensure compliance with policies and procedures.</li> </ul>
<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>□ Performance management is integrated into security monitoring and reporting.</li> <li>□ Peer- and sector-based benchmarking for security monitoring and reporting is performed.</li> <li>□ Security monitoring and reporting processes are monitored and measured.</li> </ul>	<p><b>5: Optimized</b></p> <ul style="list-style-type: none"> <li>□ Performance management is integrated into security monitoring and reporting.</li> <li>□ Peer- and sector-based benchmarking for security monitoring and reporting is performed.</li> <li>□ Security monitoring and reporting processes are monitored and measured.</li> </ul>

Goal Setting and Measurement

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b> <ul style="list-style-type: none"> <li>□ Tools may exist to support monitoring, reporting and responding to security issues; they are generally based on standard desktop tools.</li> <li>□ There is no formal approach to using tools to monitor, report and respond to security issues.</li> <li>□ IT staff manually review security logs of information systems, if available, on an occasional basis.</li> <li>□ Security logging and reporting capability within systems may be in use if a vendor enables this functionality by default.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates for security monitoring and reporting have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support security monitoring and reporting are emerging.</li> <li>□ Security logging is locally enabled in significant IT systems and components; IT staff review the security events in these systems periodically.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan is developed to acquire and implement tools to support security monitoring and reporting.</li> <li>□ The basic level of functionality in tools and templates for security monitoring is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Systems are deployed with security logging capability.</li> <li>□ Consolidation of security monitoring of multiple systems, using automated tools, is emerging.</li> <li>□ Use of automated log analysis to identify security events is emerging.</li> <li>□ Security events are consistently captured, tracked and reported, using automated tools.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support security monitoring and reporting have been implemented.</li> <li>□ Integration of tools to support security monitoring and reporting is emerging.</li> <li>□ There is a formal and structured approach to using tools to support security monitoring and reporting.</li> <li>□ All new systems comply with security logging and monitoring standards.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support security monitoring and reporting.</li> <li>□ Security event logging and monitoring for all platforms is consolidated.</li> <li>□ Normalization, correlation and advanced automated analytics are used to identify security issues.</li> <li>□ Automated responses to security events are enabled through integration between security controls.</li> </ul>	
	Tools and Automation				

**TOOLS**

## Ensure End User Security

### Description

School jurisdictions rely on end users to ensure the security of information and IT assets. End users must be aware of their responsibilities for information and IT asset security and knowledgeable about applicable legislation and jurisdiction policies and procedures.

This process area includes establishing and managing expected behaviours of individuals who access and interact with the jurisdiction's IT services.

### Value

- Provides reasonable assurance to jurisdiction leadership and stakeholders that end user security is appropriately managed.

### Goals

- Ensure that all jurisdiction staff members, including IT staff, understand their responsibilities and interact with, use, enable and support IT services in an ethical and appropriate manner.

### Target Audience

Primary	Secondary
Senior Leadership IT Leadership	School Administrators IT Staff

### Key Activities

**Identify and address security responsibilities** in job descriptions, confidentiality, non-disclosure or acceptable use agreements prior to employment or provision of access to IT services.

- Identify and regularly review requirements for Confidentiality Agreements, Non-disclosure Agreements or Acceptable Use Agreements.
- Implement a process to ensure that information security responsibilities are described appropriately and are regularly maintained in job descriptions.

**Ensure that end users of jurisdiction IT services understand their responsibilities for protecting sensitive information.**

- Require end user commitment to meet assigned information security roles and responsibilities while using the jurisdiction's IT services.
- Raise awareness of security threats, responsibilities and liabilities among end users, including contractors and third party users of jurisdiction IT services.
- Provide end users, including contractors and other third parties, with appropriate, relevant and ongoing education and training for security procedures and the correct use of IT services.
- Establish and maintain a formal disciplinary process to handle information security breaches.

**Define and assign responsibilities to manage end user access** during new hire, employment or contract termination, change of employment or student transfer out of the jurisdiction.

**Adequately screen end users** of jurisdiction IT services, including staff, contractors and other third-party users, prior to providing access to jurisdiction IT services.

- Implement a process to ensure that all changes, including termination, to end users' ability to use IT services are performed in a timely and controlled manner.

- Implement a process to ensure that all jurisdiction and school information and IT assets are returned upon termination or change of employment.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Identify and address security responsibilities.					
Adequately screen end users.					
Ensure that all end users of jurisdiction IT services understand their responsibilities for protecting sensitive information.					
Define and assign responsibilities for end user access.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Ensure End User Security**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for end user security.</li> <li><input type="checkbox"/> The need for end user security is communicated inconsistently.</li> <li><input type="checkbox"/> End user security is discussed in response to issues.</li> <li><input type="checkbox"/> Communication to stakeholders about end user security is sporadic and usually in response to issues.</li> <li><input type="checkbox"/> Jurisdiction end users, contractors and other third parties have limited awareness of their responsibilities that relate to security.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for ensuring end user security.</li> <li><input type="checkbox"/> IT leadership commits resources to the development of a sound end user security management process.</li> <li><input type="checkbox"/> Formal communication channels for reporting and responding to end user security issues have been implemented.</li> <li><input type="checkbox"/> End users formally accept their information security responsibilities.</li> <li><input type="checkbox"/> Third party arrangements and contracts include standard security responsibility acceptance criteria.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of ensuring end user security.</li> <li><input type="checkbox"/> Communication to stakeholders about end user security occurs on a regular basis and in a formal way.</li> <li><input type="checkbox"/> A structured awareness program about security is implemented for end users.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of the requirements for ensuring end user security.</li> <li><input type="checkbox"/> Understanding of end user security requirements and responsibilities is widespread throughout the jurisdiction and beyond to external parties.</li> <li><input type="checkbox"/> Communication to stakeholders about ensuring end user security is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of end user security requirements and practices exists in isolation.</li> <li>□ Minimum skills required to support end user security have not been identified.</li> <li>□ Training needs for end user security have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and HR staff have the skills and expertise to ensure basic end user security.</li> <li>□ Minimum skill requirements to ensure end user security have been identified.</li> <li>□ Training in specific processes required to ensure end user security, such as adding accounts, terminating accounts and migrating users to new roles, is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all key security monitoring and reporting processes.</li> <li>□ Jurisdiction staff have the skills and expertise to perform employee screening and background checks.</li> <li>□ Skill requirements for all aspects of managing end user security have been defined and documented.</li> <li>□ A formal training plan for managing end user security has been developed.</li> <li>□ Formal training in managing end user security is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all end user security processes.</li> <li>□ Proficiency in critical aspects of end user security is ensured for individuals who perform these processes.</li> <li>□ Skill requirements for end user security are reviewed and updated on a regular basis.</li> <li>□ Formal training for end user security is required for individuals who perform these processes.</li> <li>□ Certification in end user security is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of ensuring end user security is ensured for individuals who perform these processes.</li> <li>□ The jurisdiction encourages formal training in ensuring end user security, based on personal and jurisdiction goals.</li> <li>□ Certification in ensuring end user security is required for individuals who perform these processes.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into processes to ensure end user security.</li> </ul>
	<p style="text-align: right;">Skills and Expertise</p>				

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for end user security is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for end user security have been formally assigned and documented.</li> <li>□ End user security process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ End user security process owners have the level of authority required to fulfill their responsibilities.</li> <li>□ IT staff have the level of authority to implement, operate and enforce policies and procedures related to end user security.</li> </ul>	<ul style="list-style-type: none"> <li>□ End user security process owners are empowered to make decisions and to take action.</li> <li>□ End user security process owners escalate issues, according to a defined escalation process.</li> </ul>
		<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for ensuring end user security and enforcing end user security policies is done informally.</li> <li>□ Individuals assume responsibility for ensuring end user security.</li> <li>□ There is confusion about who is responsible and accountable for ensuring end user security when issues arise.</li> </ul>			

Responsibility and Accountability

PEOPLE (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ End user security activities occur in isolation and are based upon individual IT staff and end user practices.</li> <li>□ Policies and procedures for end user security are undefined.</li> <li>□ Instances of end user security issues are identified only when brought to the attention of IT staff.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for ensuring end user security are defined, but not documented.</li> <li>□ Compliance with policies and procedures for ensuring end user security is left to the individual's discretion.</li> <li>□ Agreements, such as Acceptable Use Agreements, Confidentiality Agreements and Non-disclosure Agreements, are reviewed and revised periodically.</li> <li>□ IT staff and HR staff collaborate informally to ensure that end user security issues are managed appropriately.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies, procedures and processes that define acceptable controls for end user security have been documented.</li> <li>□ IT and HR procedures for end user security are cross referenced to ensure consistency.</li> <li>□ Procedures cover the creation of new end user accounts, migration of end users to new roles and termination of accounts as well as regular review and revision of agreements, such as Acceptable Use Agreements, Confidentiality Agreements and Non-disclosure Agreements.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all end user security processes are defined, documented and regularly reviewed.</li> <li>□ Senior leadership approves policies and procedures for end user security.</li> </ul>	<ul style="list-style-type: none"> <li>□ Generally accepted best practices and standards for ensuring end user security are used to inform policy and procedure development.</li> <li>□ Exceptions to ensuring end user security are noticed and corrective action is taken.</li> <li>□ End user security policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				
<b>PROCESS</b>					

Maturity Level	
<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some end user security goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> End user security goals are unclear or vaguely defined.</li> <li><input type="checkbox"/> Investigations into end user security incidents are inconclusive, if performed.</li> </ul>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Processes to ensure end user security are monitored informally.</li> <li><input type="checkbox"/> End user accounts are periodically checked to ensure they are properly managed and configured.</li> <li><input type="checkbox"/> Issues related to inappropriate use of school authority technology resources are documented and archived occasionally.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> End user security is monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for end user security have been defined and documented.</li> <li><input type="checkbox"/> The number and severity of end user security incidents and related security events and incidents are reported to senior leadership and IT leadership.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> End user security metrics are formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of end user security policies are used to inform decision making and continuous improvement.</li> <li><input type="checkbox"/> End user security controls are tested to ensure that they comply with policies and procedures.</li> <li><input type="checkbox"/> Investigations and evidence of end user security policy breaches are consistently tracked and reported.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into ensuring end user security.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for ensuring end user security is performed.</li> <li><input type="checkbox"/> End user security processes are monitored and measured.</li> </ul>
<b>Attributes</b>	Goal Setting and Measurement

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support end user security processes; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support end user security processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates to ensure end user security have been developed and implemented.</li> <li>□ Common approaches to the use of tools to ensure end user security are emerging.</li> <li>□ End user permissions and access are managed, using profiles defined by end user responsibility.</li> <li>□ End user security incidents are investigated manually.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan is developed to acquire and implement tools to support end user security management</li> <li>□ The basic level of functionality in tools and templates for end user security management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ Use of automated tools to support end user monitoring and investigations is emerging.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support end user security have been implemented.</li> <li>□ Integration of tools to support end user security is emerging.</li> <li>□ There is a formal and structured approach to using tools to support end user security.</li> <li>□ Tools are used in key areas to automate and formalize end user security.</li> <li>□ End user security incidents are consistently tracked and investigated, using automated tools.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to help ensure end user security.</li> <li>□ Normalization, correlation and advanced automated analytics are used to identify end user security issues.</li> <li>□ Automated responses to end user security events are enabled through integration with other security tools.</li> </ul>
	<p style="text-align: right;">Tools and Automation</p>				

**TOOLS**

## Manage System Vulnerabilities

### Description

Threats to information security are constantly evolving and changing. A proactive approach to monitoring the environment for threats and responding accordingly is necessary to limit system downtime and to prevent loss of information confidentiality, integrity or availability. The implementation of system and vulnerability management controls supports this proactive approach.

This process area includes monitoring the environment for new and emerging threats to information security, and implementing and managing measures to address threats.

### Value

- Provides reasonable assurance to jurisdiction leadership and stakeholders that risks associated with system vulnerabilities are appropriately managed.

### Goals

- Ensure that jurisdiction information systems remain secure and free of vulnerabilities, at a cost that is proportionate to the identified risks.
- Reduce technical issues that could result in losses due to inadvertent or intentional exploitation of information system weaknesses.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership IT Staff

### Key Activities

**Manage technical vulnerabilities** by obtaining timely information about system vulnerabilities and responding in an effective, systematic and repeatable way.

- Implement a process to obtain timely information about technical vulnerabilities, evaluate the jurisdiction's exposure to such vulnerabilities and take appropriate measures to address the associated risk.
- Monitor, measure and report on this objective to provide assurance that it is being effectively managed.

**Manage cryptographic controls** by implementing a policy for the use of cryptographic controls within the jurisdiction to maximize benefits and to prevent inappropriate or incorrect use of controls.

- Implement a process to manage cryptographic keys and mechanisms, and to protect against modification, loss, destruction or unauthorized disclosure.

**Ensure security** of system files and source codes by implementing a process to control the installation of software on operational systems.

- Implement a process to monitor and supervise outsourced software development.

**Protect sensitive data** in test environments by selecting test data carefully and by using it in a controlled manner.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Ensure security of system files.					
Protect sensitive data.					
Manage technical vulnerabilities.					
Manage cryptographic controls.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete (Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage System Vulnerabilities**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	1: Initial	<ul style="list-style-type: none"> <li>□ IT leadership is aware of the need for a formal approach to managing systems and vulnerabilities.</li> <li>□ The need for a formal approach to managing systems and vulnerabilities is communicated inconsistently.</li> <li>□ System vulnerability management is discussed in response to issues.</li> <li>□ Communication to stakeholders about system vulnerability management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership commits resources to the implementation of a sound system vulnerability management process.</li> <li>□ IT leadership and IT staff discuss system vulnerability management.</li> <li>□ Communication to stakeholders about system vulnerabilities occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have a comprehensive understanding of system vulnerability management.</li> <li>□ Communication to stakeholders about the value of system vulnerability management occurs on a regular basis and in a formal way.</li> <li>□ A structured awareness program about system and vulnerability management is implemented for IT staff and end users.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership has an advanced and forward-looking understanding of system vulnerability management requirements.</li> <li>□ Understanding of system vulnerability management is widespread throughout the jurisdiction.</li> <li>□ Communication to stakeholders about system vulnerability management is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of system vulnerability management practices exists in isolation.</li> <li>□ Minimum skills required to perform system vulnerability management have not been identified.</li> <li>□ Training needs for system vulnerability management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform basic management of system vulnerabilities.</li> <li>□ Minimum skill requirements to manage system vulnerabilities have been identified.</li> <li>□ Training in the management of system vulnerabilities is provided in response to emerging needs or requests from individuals.</li> <li>□ External advice is sought when gaps in expertise are evident.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all key system vulnerability management processes.</li> <li>□ Skill requirements for all aspects of system vulnerability management have been defined and documented.</li> <li>□ A formal training plan for system vulnerability management has been developed.</li> <li>□ Formal training in system vulnerability management is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all system vulnerability management processes.</li> <li>□ Proficiency in critical aspects of system vulnerability management is ensured for individuals who perform these processes.</li> <li>□ Skill requirements for system vulnerability management are reviewed and updated on a regular basis.</li> <li>□ Formal training for system vulnerability management is required for individuals who perform these processes.</li> <li>□ Certification in system vulnerability management is required for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of system vulnerability management is ensured for individuals who perform these processes.</li> <li>□ The jurisdiction encourages formal training in system vulnerability management, based on personal and jurisdiction goals.</li> <li>□ Certification in system vulnerability management is required for individuals who perform these processes.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into system vulnerability management processes.</li> </ul>
	Skills and Expertise				

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<p><i>Attributes</i></p> <p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li>Allocation of responsibility for system vulnerability management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>Allocation of responsibility and accountability for system vulnerability management is done informally.</li> <li>Individuals assume responsibility for system vulnerability management.</li> <li>There is confusion about who is responsible and accountable for information security governance when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>Accountability and responsibility for system vulnerability management have been formally assigned and documented.</li> <li>System vulnerability management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>System vulnerability management process owners have the level of authority required to fulfill their responsibilities.</li> <li>IT staff have the level of authority to implement, operate and enforce policies and procedures related to system vulnerability management.</li> </ul>	<ul style="list-style-type: none"> <li>System vulnerability management process owners are empowered to make decisions and to take action.</li> <li>System vulnerability management process owners escalate issues, according to a defined escalation process.</li> </ul>	
	<p>Responsibility and Accountability</p> <p><b>PEOPLE (continued)</b></p>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ System vulnerability management activities occur in isolation and are based upon individual IT staff practices.</li> <li>□ Policies and procedures for system vulnerability management have not been defined.</li> <li>□ Instances of system management issues, technical vulnerabilities and inappropriate or inadequate use of cryptography are identified only when brought to the attention of IT staff.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for managing and administering systems, identifying and addressing system vulnerabilities and managing applicable cryptographic controls are defined, but not documented.</li> <li>□ Compliance with policies and procedures for system and vulnerability management is left to the individual's discretion.</li> <li>□ Requirements for system and vulnerability management controls are documented at a basic level.</li> <li>□ The security of significant IT systems and components, and the identification of vulnerabilities in these systems are reviewed periodically.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for system vulnerability management have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ Procedures cover managing and administering systems, identifying and addressing system vulnerabilities and managing applicable cryptographic controls.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all system vulnerability management processes are defined, documented and regularly reviewed.</li> <li>□ IT leadership approves policies and procedures for system vulnerability management.</li> <li>□ Procedures include provisions to ensure appropriate system management, identification and management of vulnerabilities, and management and operation of cryptographic controls.</li> </ul>	<ul style="list-style-type: none"> <li>□ Generally accepted best practices and standards for system vulnerability management are used to inform policy and procedure development.</li> <li>□ Exceptions to system vulnerability management are noticed and corrective action is taken.</li> <li>□ System vulnerability management policies and procedures are regularly reviewed and improved.</li> </ul>
	Policies, Plans and Procedures				

**PROCESS**

Maturity Level	
<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Goals for system vulnerability management are set and monitored inconsistently.</li> <li><input type="checkbox"/> Goals for system vulnerability management are unclear or vaguely defined.</li> <li><input type="checkbox"/> Investigations into control failures, if performed, are inconclusive.</li> </ul>
<b>2: Repeatable</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of system vulnerability management is monitored informally.</li> <li><input type="checkbox"/> Cryptographic controls are periodically reviewed to ensure they function correctly.</li> </ul>
<b>3: Defined</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> System vulnerabilities are monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for system vulnerability management have been defined and documented.</li> <li><input type="checkbox"/> A current inventory of cryptographic controls and processes is available.</li> </ul>
<b>4: Managed</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> System vulnerability management metrics are formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of system vulnerability management policies and procedures are used to inform decision making and continuous improvement.</li> <li><input type="checkbox"/> System vulnerability management controls are tested to ensure they comply with policies and procedures.</li> </ul>
<b>5: Optimized</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into system vulnerability management.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for system vulnerability management is performed.</li> <li><input type="checkbox"/> System vulnerability management processes are monitored and measured.</li> </ul>

Attributes

Goal Setting and Measurement

PROCESS (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Tools may exist to support system vulnerability management; they are generally based upon standard desktop tools.</li> <li>□ There is no formal approach to using tools to support system vulnerability management.</li> <li>□ Cryptographic controls included by product and software vendors (by default) may be implemented.</li> </ul>	<ul style="list-style-type: none"> <li>□ Basic tools and templates for system vulnerability management have been developed and implemented.</li> <li>□ Common approaches to the use of tools to support system vulnerability management are emerging.</li> <li>□ Cryptographic controls have been implemented in significant IT systems.</li> </ul>	<ul style="list-style-type: none"> <li>□ A formal plan is developed to acquire and implement tools to support system vulnerability management.</li> <li>□ The basic level of functionality in tools and templates for system vulnerability management is used.</li> <li>□ Tools in use are not fully integrated.</li> <li>□ System administration tasks are consistently recorded in system vulnerability management tools.</li> <li>□ Use of automated tools to identify system vulnerabilities is emerging.</li> <li>□ Cryptographic controls are consistently used and standardized.</li> </ul>	<ul style="list-style-type: none"> <li>□ Tools to support system vulnerability management have been implemented.</li> <li>□ Integration of tools to support system vulnerability management is emerging.</li> <li>□ There is a formal and structured approach to using tools to support system vulnerability management.</li> <li>□ Tools are used in key areas to automate and formalize system vulnerability management.</li> <li>□ Auditable records of system administration are maintained, using tools to support system vulnerability management.</li> </ul>	<ul style="list-style-type: none"> <li>□ A standardized and integrated set of tools and formalized techniques is used to support system vulnerability management.</li> <li>□ System vulnerability management tools are integrated to enable proactive and automatic responses to threats.</li> <li>□ Strong vulnerability prevention techniques, such as white-listing, are used on critical systems.</li> <li>□ Cryptographic tools are integrated and tested for technical compliance with recognized industry standards.</li> </ul>
	Tools and Automation				

**TOOLS**

## Manage End User Identity and Access

### Description

School jurisdictions implement policies to balance access to information with the need for security and privacy. These policies are supported through effective end user identity and access processes.

This process area includes controlling access to the jurisdiction's information and to the jurisdiction's physical IT assets and facilities.

### Value

- Ensures that authorized end users have timely and appropriate access to information systems.
- Reduces the risk of loss of confidentiality, integrity or availability of jurisdiction information.

### Goals

- Manage the allocation and use of access rights to the jurisdiction's IT services and physical assets.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership School Administrators IT Staff

### Key Activities

For a school jurisdiction to achieve these benefits, there are some key activities that should be considered and documented, with clear roles and responsibilities assigned.

**Control access to jurisdiction information and information-processing facilities** by implementing a policy, based upon administration and education requirements, security requirements and jurisdiction policies for information dissemination and authorization.

**Manage end user access** to jurisdictional information systems and services by implementing a process to control the allocation of access rights, from the initial registration of new end users to the final de-registration of end users who no longer require access.

**Manage end user passwords** by controlling allocation of passwords through implementation of a formal process.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Control access to jurisdiction information and information-processing facilities.					
Manage end user access.					
Manage end user passwords					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Manage End User Identity and Access**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>PEOPLE</b>	<i>Attributes</i>	<p><b>1: Initial</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to identity and access management.</li> <li><input type="checkbox"/> The need for a formal approach to identity and access management is communicated inconsistently.</li> <li><input type="checkbox"/> Identity and access management is discussed in response to issues or requests for information from senior leadership.</li> <li><input type="checkbox"/> Communication to stakeholders about identity and access management is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Senior leadership is aware of access control policies and the rationale behind them.</li> <li><input type="checkbox"/> IT staff understand the requirements for identity and access management.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss identity and access management on a regular basis.</li> <li><input type="checkbox"/> Communication to stakeholders about identity and access management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of identity and access management.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of identity and access management occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of identity and access management requirements.</li> <li><input type="checkbox"/> Communication to stakeholders about identity and access issues is formal and proactive, when possible.</li> </ul>
	<i>Awareness, Understanding and Communication</i>				

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Some knowledge of best practices for identity and access management exists in isolation.</li> <li>□ Minimum skills required to perform identity and access management have not been identified.</li> <li>□ Training needs for end user identity and access management have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform basic identity and access management.</li> <li>□ IT staff understand the configuration requirements for operating system and application access controls and have the expertise to configure these systems, as required.</li> <li>□ Minimum skill requirements to perform identity and access management have been identified.</li> <li>□ Training in identity and access management is provided in response to emerging needs or requests from individuals.</li> <li>□ External advice is sought when gaps in expertise are evident.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all key identity and access management processes.</li> <li>□ Skill requirements for all aspects of identity and access management have been defined and documented.</li> <li>□ A formal training plan for identity and access management has been developed.</li> <li>□ Formal training in identity and access management is available.</li> </ul>	<ul style="list-style-type: none"> <li>□ IT leadership and IT staff have the skills and expertise to perform all identity and access management processes.</li> <li>□ Proficiency in critical aspects of identity and access management is ensured for individuals who perform these processes.</li> <li>□ Skill requirements for identity and access management are reviewed and updated on a regular basis.</li> <li>□ Formal training for identity and access management is required for individuals who perform these processes.</li> <li>□ Certification in identity and access management is encouraged for individuals who perform these processes.</li> </ul>	<ul style="list-style-type: none"> <li>□ Proficiency in all aspects of identity and access management is ensured for individuals who perform these processes.</li> <li>□ The jurisdiction encourages formal training in identity and access management, based on personal and jurisdiction goals.</li> <li>□ Certification in identity and access management is required for individuals who perform these processes.</li> <li>□ External experts and industry leaders are engaged to provide guidance and input into identity and access management processes.</li> </ul>
	Skills and Expertise				

**PEOPLE** (continued)

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for identity and access management is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for identity and access management is done informally.</li> <li>□ Individuals assume responsibility for identity and access management.</li> <li>□ There is confusion about who is responsible and accountable for identity and access management when issues arise.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for identity and access management have been formally assigned and documented.</li> <li>□ Identity and access management process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Identity and access management owners have the level of authority required to implement, operate and enforce policies and procedures for identity and access management.</li> <li>□ IT staff have the level of authority required to implement, operate and enforce policies and procedures for identity and access management.</li> </ul>	<ul style="list-style-type: none"> <li>□ Identity and access management process owners are empowered to make decisions and to take action.</li> <li>□ Identity and access management process owners escalate issues, according to a defined escalation process.</li> </ul>
	<p style="text-align: right;">Responsibility and Accountability</p>				

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized	
<b>Attributes</b>	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Identity and access management activities occur in isolation and are based upon individual IT staff practices.</li> <li>□ Policies and procedures to manage end user identity and access management are not defined.</li> <li>□ Instances of inappropriate access control are identified only when brought to the attention of IT staff.</li> </ul>	<ul style="list-style-type: none"> <li>□ Common and informal policies and procedures for identity and access management are defined, but not documented.</li> <li>□ Compliance with identity and access management policies and procedures is left to the individual's discretion.</li> <li>□ Requirements for access control for information systems and applications during the development process are documented to a basic level.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for key identity and access processes have been defined, documented and communicated.</li> <li>□ Policies and procedures are based upon generally accepted good practices.</li> <li>□ Procedures include managing end user accounts.</li> </ul>	<ul style="list-style-type: none"> <li>□ Formal policies and procedures for all identity and access processes are defined, documented and regularly reviewed.</li> <li>□ Senior leadership approves policies and procedures for identity and access management.</li> <li>□ Compliance with identity and access control policy requirements and procedures is integrated in the service management life cycle.</li> </ul>	<ul style="list-style-type: none"> <li>□ Generally accepted best practices and standards for identity and access management are used to inform policy and procedure development.</li> <li>□ Exceptions to identity and access management are noticed and corrective action is taken.</li> <li>□ Identity and access management policies and procedures are regularly reviewed and improved.</li> </ul>
		Policies, Plans and Procedures				
<b>PROCESS</b>						

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some identity and access management goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> Identity and access management goals are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance of identity and access management is monitored informally.</li> <li><input type="checkbox"/> Dormant end user accounts and accesses exist; they are deactivated as they are discovered.</li> <li><input type="checkbox"/> Information systems and applications are informally checked for access control before they are used.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Identity and access management is monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for identity and access management have been defined and documented.</li> <li><input type="checkbox"/> IT staff provide reports to IT leadership about identity and access management.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Identity and access management metrics are formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of identity and access management policies and procedures are used to inform decision making and continuous improvement.</li> <li><input type="checkbox"/> Identity and access management controls are tested to ensure they comply with policies and procedures.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into identity and access management.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for identity and access management is performed.</li> <li><input type="checkbox"/> Identity and access management are monitored and measured.</li> </ul>
	<p style="text-align: right;">Goal Setting and Measurement</p>				

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Basic tools and templates to support identity and access management have been developed and implemented.</li> <li><input type="checkbox"/> Common approaches to the use of tools to support identity and access management are emerging.</li> <li><input type="checkbox"/> Most operating systems and applications in use have access control capabilities.</li> <li><input type="checkbox"/> Common access control configuration settings are used on most platforms.</li> <li><input type="checkbox"/> Use of automated tools to support end registration and management is emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan is developed to acquire and implement tools to support identity and access management.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates for identity and access management is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> <li><input type="checkbox"/> Operating systems and applications are used to define access control capabilities.</li> <li><input type="checkbox"/> Common access control configuration settings have been documented and implemented on all platforms.</li> <li><input type="checkbox"/> Tools for end user registration and management have been implemented.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support identity and access management have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support identity and access management is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support identity and access management.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize identity and access management.</li> <li><input type="checkbox"/> Tools to automate end user registration and management are integrated across platforms.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools and formalized techniques is used to support identity and access management.</li> <li><input type="checkbox"/> End user access provisioning and management processes are automated, when possible.</li> <li><input type="checkbox"/> Automated tools are used to support investigation and resolution of identity and access management issues.</li> <li><input type="checkbox"/> Identity and access management tools are optimized to alert IT staff about potential issues.</li> </ul>
	Tools and Automation	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support identity and access management; they are generally based upon standard desktop tools.</li> <li><input type="checkbox"/> There is no formal approach to using tools for identity and access management.</li> <li><input type="checkbox"/> Operating systems and applications may have basic access control capabilities.</li> <li><input type="checkbox"/> Access controls use basic configuration settings and vary from platform to platform.</li> <li><input type="checkbox"/> Tools for end user registration and management are not used.</li> <li><input type="checkbox"/> Information is not available to support investigations into failures of access control or failures of identity management controls.</li> </ul>			

**TOOLS**

## Protect Networks

### Description

End users connect to computer networks to access information and applications, and to communicate with others. Network connections are vulnerable to weaknesses in their design and deployment, particularly when they are available for remote and mobile users.

This process area includes identification and management of network vulnerabilities.

### Value

- Provides reasonable assurance to jurisdiction leadership and stakeholders that network-related risks are appropriately managed.

### Goals

- Ensure that authorized end users have timely and appropriate network access to information systems while reducing the potential for loss of information confidentiality, integrity or availability.

### Target Audience

Primary	Secondary
IT Leadership	Senior Leadership IT Staff

### Key Activities

**Manage and control network security** by implementing a policy that balances security risks and jurisdiction requirements with appropriate end user access to jurisdiction networks and network services.

**Control network access** by implementing controls to prevent unauthorized access to the jurisdiction's networked services.

### RACI Chart

The position titles used in this process are for illustration purposes only. The actual titles for the various roles will be unique to each school jurisdiction and should be specified in the RACI chart.

Activities	Roles				
Manage and control network security.					
Control network access.					
Implement a process to authenticate remote and mobile end users.					
Implement a process to identify and remove equipment not permitted to connect to the network.					
Implement a process to ensure that ports, services and similar facilities are accessible only as required.					
Implement a process to segregate information services, end users and information systems on networks.					

### RACI Responsibilities

- Responsible** – the person or group who is responsible for performing a task
- Accountable** – the person who is held accountable for the task being complete  
(Ideally, accountability is assigned to only one role for each process.)
- Consulted** – the person or group communicated with prior to a task being performed
- Informed** – the parties who are notified about an activity before, during or after it is performed.

**Maturity Model – Protect Networks**

Note: The required or desired level of maturity will vary between jurisdictions, based on the size, needs, costs, capability and alignment with the jurisdiction's strategic plan. It is not necessary to assume that any jurisdiction should be at a Level 5 in all or any of these activities.

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>PEOPLE</b>	<i>Attributes</i>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership is aware of the need for a formal approach to network protection.</li> <li><input type="checkbox"/> The need for a formal approach to network protection is communicated inconsistently.</li> <li><input type="checkbox"/> Network protection is discussed in response to issues.</li> <li><input type="checkbox"/> Communication to stakeholders about network protection is sporadic and usually in response to issues.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT staff understand the requirements for network protection.</li> <li><input type="checkbox"/> IT leadership commits resources to the implementation of a sound network protection process.</li> <li><input type="checkbox"/> IT leadership and IT staff discuss network protection on a regular basis.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have a comprehensive understanding of network protection.</li> <li><input type="checkbox"/> Communication to stakeholders about the value of network protection occurs on a regular basis and in a formal way.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership has an advanced and forward-looking understanding of network protection requirements.</li> <li><input type="checkbox"/> Understanding of network protection is widespread throughout the jurisdiction.</li> <li><input type="checkbox"/> Communication to stakeholders about network protection is formal and proactive, when possible.</li> </ul>
	Awareness, Understanding and Communication				

**PEOPLE**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some knowledge of formal network protection approaches exists in isolation.</li> <li><input type="checkbox"/> Minimum skills required to perform network protection have not been identified.</li> <li><input type="checkbox"/> Training needs for network protection have not been identified.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform basic network protection.</li> <li><input type="checkbox"/> Minimum skill requirements to perform network protection have been identified.</li> <li><input type="checkbox"/> Training in network protection is provided in response to emerging needs or requests from individuals.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all key network protection processes.</li> <li><input type="checkbox"/> Skill requirements for all aspects of network protection have been defined and documented.</li> <li><input type="checkbox"/> A formal training plan for network protection has been developed.</li> <li><input type="checkbox"/> Formal training in network protection is available.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> IT leadership and IT staff have the skills and expertise to perform all network protection processes.</li> <li><input type="checkbox"/> Proficiency in critical aspects of network protection is ensured for individuals who perform these tasks.</li> <li><input type="checkbox"/> Skill requirements for network protection are reviewed and updated on a regular basis.</li> <li><input type="checkbox"/> Formal training for network protection is required for individuals who perform these tasks.</li> <li><input type="checkbox"/> Certification in network protection is encouraged for individuals who perform these tasks.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Proficiency in all aspects of network protection is ensured for individuals who perform these processes.</li> <li><input type="checkbox"/> The jurisdiction encourages formal training in network protection, based on personal and jurisdiction goals.</li> <li><input type="checkbox"/> Certification in network protection is required for individuals who perform these tasks.</li> <li><input type="checkbox"/> External experts and industry leaders are engaged to provide guidance and input into network protection processes.</li> </ul>
	<p style="text-align: right;">Skills and Expertise</p>				

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
Attributes	<b>1: Initial</b>	<ul style="list-style-type: none"> <li>□ Allocation of responsibility for network protection is assumed or done in an ad hoc way.</li> </ul>	<ul style="list-style-type: none"> <li>□ Accountability and responsibility for network protection have been formally assigned and documented.</li> <li>□ Network protection process owners are identified, but may not have sufficient authority to fulfill their responsibilities.</li> </ul>	<ul style="list-style-type: none"> <li>□ Network protection process owners have the level of authority required to implement, operate and enforce policies and procedures related to network protection.</li> <li>□ IT staff have the level of authority required to implement, operate and enforce policies and procedures related to network protection.</li> </ul>	<ul style="list-style-type: none"> <li>□ Network protection process owners are empowered to make decisions and to take action.</li> <li>□ Network protection process owners escalate issues, according to a defined escalation process.</li> </ul>
		<ul style="list-style-type: none"> <li>□ Allocation of responsibility and accountability for network protection is done informally.</li> <li>□ Individuals assume responsibility for network protection.</li> <li>□ There is confusion about who is responsible and accountable for network protection when issues arise.</li> </ul>			

Responsibility and Accountability

**PEOPLE (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<input type="checkbox"/> Network protection activities occur in isolation and are based upon individual IT staff practices.	<input type="checkbox"/> Common and informal policies and procedures for network protection are defined, but not documented.	<input type="checkbox"/> Formal policies and procedures for key network protection processes have been defined, documented and communicated.	<input type="checkbox"/> Formal policies and procedures for all network protection processes are defined, documented and regularly reviewed.	<input type="checkbox"/> Generally accepted best practices and standards for network protection are used to inform policy and procedure development.
	<input type="checkbox"/> Policies and procedures for network protection are undefined.	<input type="checkbox"/> Compliance with network protection policies and procedures is left to the individual's discretion.	<input type="checkbox"/> Policies and procedures are based upon generally accepted best practices.	<input type="checkbox"/> IT leadership approves policies and procedures for network protection.	<input type="checkbox"/> Exceptions to network protection policies and procedures are noticed and corrective action is taken.
<b>PROCESS</b>		Policies, Plans and Procedures			

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Some network protection goals are set and monitored inconsistently.</li> <li><input type="checkbox"/> Network protection goals are unclear or vaguely defined.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Network protection is monitored informally.</li> <li><input type="checkbox"/> Dormant end user accounts and accesses exist; they are deactivated as they are discovered.</li> <li><input type="checkbox"/> Information systems access control configuration and policies are checked informally before they are used.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Network protection is monitored regularly.</li> <li><input type="checkbox"/> Targets and thresholds for network protection have been defined and documented.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Network protection metrics are formally defined and approved.</li> <li><input type="checkbox"/> Measures of the effectiveness of network protection policies and procedures are used to inform decision making and continuous improvement.</li> <li><input type="checkbox"/> Network protection controls are tested to ensure they comply with policies and procedures.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Performance management is integrated into network protection.</li> <li><input type="checkbox"/> Peer- and sector-based benchmarking for network protection is performed.</li> <li><input type="checkbox"/> Network protection processes are monitored and measured.</li> </ul>
	<p style="text-align: right;">Goal Setting and Measurement</p>				

**PROCESS (continued)**

Maturity Level		2: Repeatable	3: Defined	4: Managed	5: Optimized
<b>Attributes</b> <b>1: Initial</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools may exist to support network protection; they are generally based on standard desktop tools.</li> <li><input type="checkbox"/> There is no formal approach to using tools to support network protection.</li> <li><input type="checkbox"/> Tools specifically designed for network protection are not used.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Basic tools and templates to support network protection have been developed and implemented.</li> <li><input type="checkbox"/> Common approaches to the use of tools to support network protection are emerging.</li> <li><input type="checkbox"/> Most operating systems and applications in use have access control configured to a basic level.</li> <li><input type="checkbox"/> Common but undocumented access control configuration settings are used on most platforms.</li> <li><input type="checkbox"/> Use of automated tools to support end registration and management is emerging.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A formal plan is developed to acquire and implement tools to support network protection.</li> <li><input type="checkbox"/> The basic level of functionality in tools and templates for network protection is used.</li> <li><input type="checkbox"/> Tools in use are not fully integrated.</li> <li><input type="checkbox"/> Operating systems and applications are used to define access control capabilities.</li> <li><input type="checkbox"/> Common access control configuration settings are documented and implemented on all platforms.</li> <li><input type="checkbox"/> Tools for end user registration and management have been implemented.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Tools to support network protection have been implemented.</li> <li><input type="checkbox"/> Integration of tools to support network protection is emerging.</li> <li><input type="checkbox"/> There is a formal and structured approach to using tools to support network protection.</li> <li><input type="checkbox"/> Tools are used in key areas to automate and formalize network protection.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> A standardized and integrated set of tools is used to support network protection.</li> <li><input type="checkbox"/> Tools are used to support investigation and resolution of network protection issues.</li> <li><input type="checkbox"/> Network protection tools are optimized to alert IT staff about potential issues.</li> </ul>
	Tools and Automation				

**TOOLS**



**SCHOOL TECHNOLOGY**  
SERVICES