

**Office of Information Technology**

**Information Technology Service Management Performance Evaluation**

**February 2022**

**RubinBrown LLP**





**THE MISSION OF THE OFFICE OF THE STATE AUDITOR  
IS TO IMPROVE GOVERNMENT  
FOR THE PEOPLE OF COLORADO**

**LEGISLATIVE AUDIT COMMITTEE**

Senator Jim Smallwood  
Chair

Senator Robert Rodriguez  
Vice Chair

Representative Rod Bockenfeld

Representative Dafna Michaelson Jenet

Senator Julie Gonzales

Representative Dylan Roberts

Representative Colin Larson

Senator Rob Woodward

**OFFICE OF THE STATE AUDITOR**

Kerri L. Hunter

State Auditor

Matt Devlin

Deputy State Auditor

Cindi Radke

IT Audit Manager

Rubin Brown LLP

Contractor

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT

**[WWW.STATE.CO.US/AUDITOR](http://WWW.STATE.CO.US/AUDITOR)**

A BOUND REPORT MAY BE OBTAINED BY CALLING THE

OFFICE OF THE STATE AUDITOR

**303.869.2800**

REFER TO REPORT NUMBER **2150P-IT** WHEN REQUESTING THIS REPORT





1900 16th Street  
Suite 300  
Denver, CO 80202

T: 303.698.1883  
E: info@rubinbrown.com  
www.RubinBrown.com

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS CONSULTANTS

February 25, 2022

Members of the Legislative Audit Committee:

This report contains the results of our evaluation of Information Technology Service Management at the Governor's Office of Information Technology. The evaluation was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology.

We conducted this engagement as an IT performance evaluation, and although we did not attempt to strictly follow generally accepted government auditing standards, we did obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and recommendations based on the evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

A handwritten signature in blue ink, appearing to read "Rob Rudloff".

Rob Rudloff  
Partner  
RubinBrown, LLP



# Contents

Report Highlights ..... 1

CHAPTER 1 ..... 2

*Evaluation Purpose, Scope, and Methodology* ..... 7

CHAPTER 2 ..... 9

**IT Service Management Practices**..... 9

**Recommendation No. 1:** ..... 19

**Recommendation No. 2:** ..... 20

**Recommendation No. 3:** ..... 21

**Recommendation No. 4:** ..... 22





# Report Highlights

## Evaluation of Information Technology Service Management

### Governor's Office of Information Technology

IT Performance Evaluation • February 2022 • 2150P-IT

#### Key Concern

The Governor's Office of Information Technology (OIT) does not have adequate IT Service Management (ITSM) practices implemented in the areas of Idea and Demand Management, Incident Management, Knowledge Management, and IT Asset Management.

#### Key Findings

- *Idea and Demand Management* – OIT does not have a consistent or formalized process in place to ensure its idea and demand management practices are in place and operating effectively.
- *Incident Management* – OIT's incident management practices do not fully comply with OIT policies, and OIT staff are not adequately capturing and documenting all incidents.
- *Knowledge Management* – OIT does not maintain a common knowledge management solution that would aid the various OIT teams in providing customer support, incident resolution, and requests in a timely manner.
- *IT Asset Management* – OIT's IT asset management practices do not address the following key aspects of ITSM leading industry practices:
  - OIT reactively supports agencies with their IT asset needs and does not have a process in place to consistently assist all participating agencies with strategic technology modernization planning.
  - OIT estimates the current unfunded technology debt for executive branch agencies at over \$465 million, but OIT has not provided the agencies with sufficient information and advisory support despite its understanding of the growing debt level.

#### Background

In 2008, the "IT Consolidation Bill" consolidated IT operations under OIT for most of the Executive Branch agencies. As the State's centralized IT service provider responsible for managing IT resources and services for state agencies, OIT's IT Service Management practices and processes are critical to meeting the IT service needs for the supported state agencies.

#### Recommendations Made: 10

#### Responses:

- Agree: 10
- Partially Agree: 0
- Disagree: 0



# CHAPTER 1

## Overview

### *Office of Information Technology*

The Governor's Office of Information Technology (OIT or the Office) is the State's centralized IT service provider responsible for managing IT resources and service delivery for state agencies as consolidated under Senate Bill 08-155. OIT oversees executive branch technology initiatives and works to maximize service delivery efficiency, in a cost-effective manner, through the application of enterprise technology solutions. The Office provides services to state agencies on a cost reimbursement basis, with OIT acting as a vendor. Services provided by OIT include enterprise application management and support, database management, network security and management, communication technology services, data center operations, information security, help desk services, public safety communications, procurement, project management, and IT economic development.

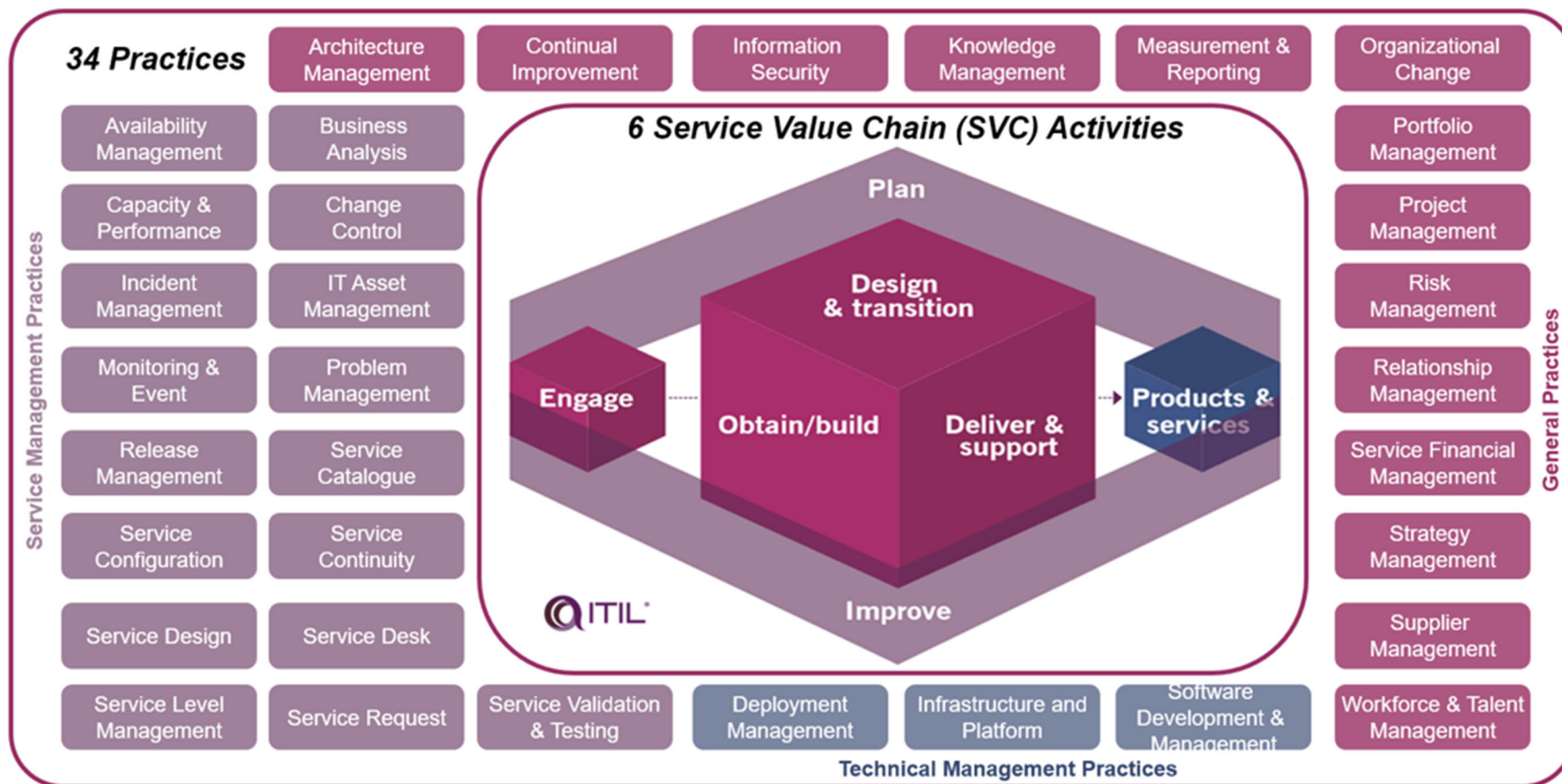
The State's Chief Information Officer (CIO) acts as the head of OIT and oversees all of its activities. As part of the CIO's duties and responsibilities in overseeing OIT, statute [Section 24-37.5-106, C.R.S.] requires OIT to develop policies, standards, specifications, and guidelines for information technology and related procedures to effectively manage and adhere to the State's IT processes. For the Fiscal Year 2020-2021 budget year, OIT was appropriated more than \$301.5 million and more than 1,000 full-time equivalent staff.

OIT has adopted the Information Technology Infrastructure Library (ITIL) as its ITSM framework. ITIL is a set of industry-leading practices for IT Service Management (ITSM) that was originally developed by a government agency in Great Britain in the 1980's as a way to achieve better quality at a lower cost in the IT services it procured. ITIL has been streamlined and adapted and is now recognized internationally for setting the standard for IT service delivery. ITIL focuses on aligning and integrating IT services with the business needs and goals of an organization, as well as encouraging more collaboration and communication between the organization and its IT function. ITIL's ITSM practices can aid the State in managing risks or reducing disruptions or failing to provide adequate IT services, as well as establishing cost-effective approaches and building an environment that allows for growth and change.

ITIL, like other ITSM frameworks, presents a broad set of detailed practices for IT activities that an organization can adopt and customize, as appropriate, for its needs to plan, design, deliver, transition, operate, improve, and control IT services. These practices fall within various areas such as Service Design and Architecture Management. Service Design practices are used to develop services that meet the needs of the user, are cost effective, and are flexible enough to adapt to changes. Architecture Management is focused on the business, service, and technical architectures and the resulting principles, standards, and tools the organization uses to meet its goals.

The following diagrams provide visualizations of the ITSM practices. The first depicts the ITIL practices and how they support the service value chain.

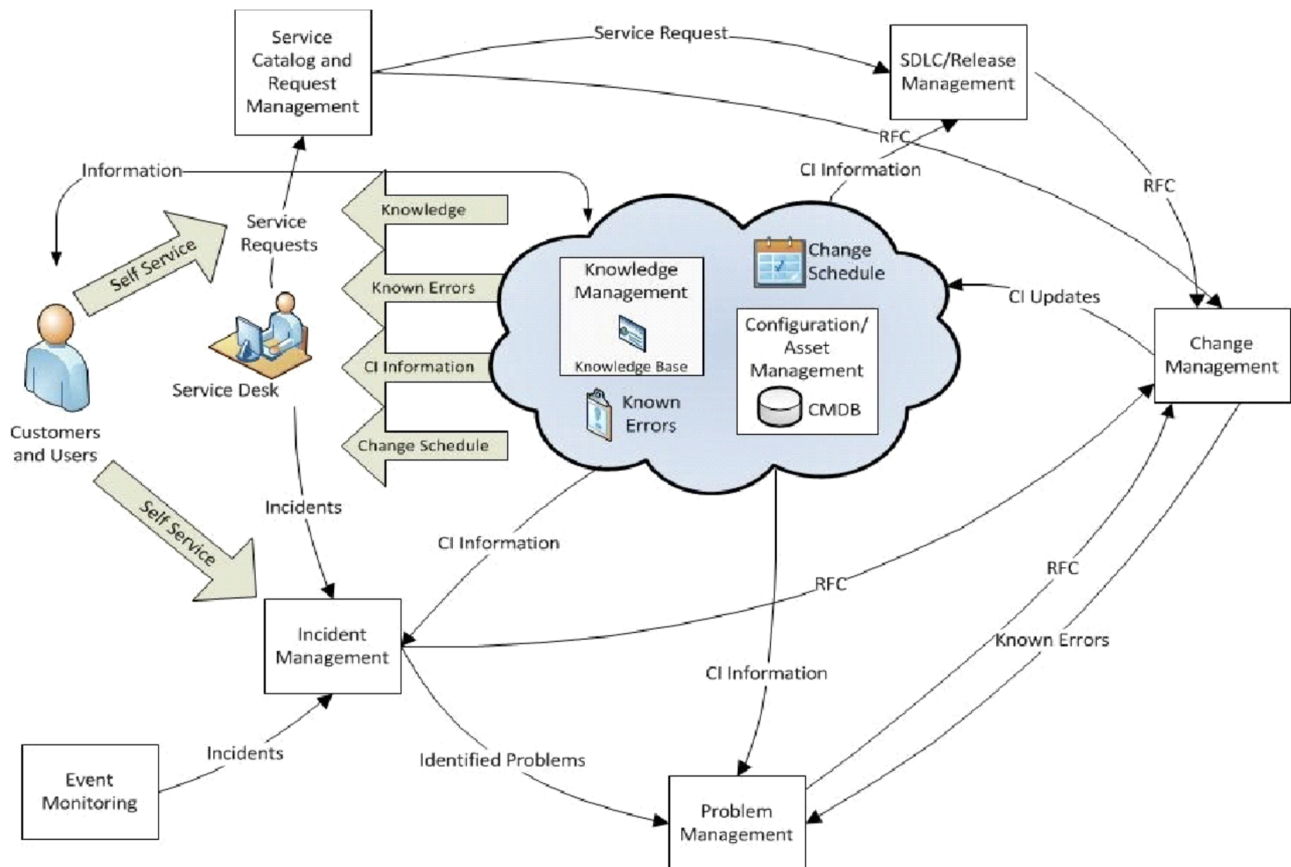
Figure 1 - ITIL Service Value Chain



Source: <https://blog.itil.org/>

The following illustration provides a visual description of ITIL’s ITSM process flows commonly found in IT service organizations between the different practices.

Figure 2 - High-Level Process Flow  
 ITSM Practices and Processes



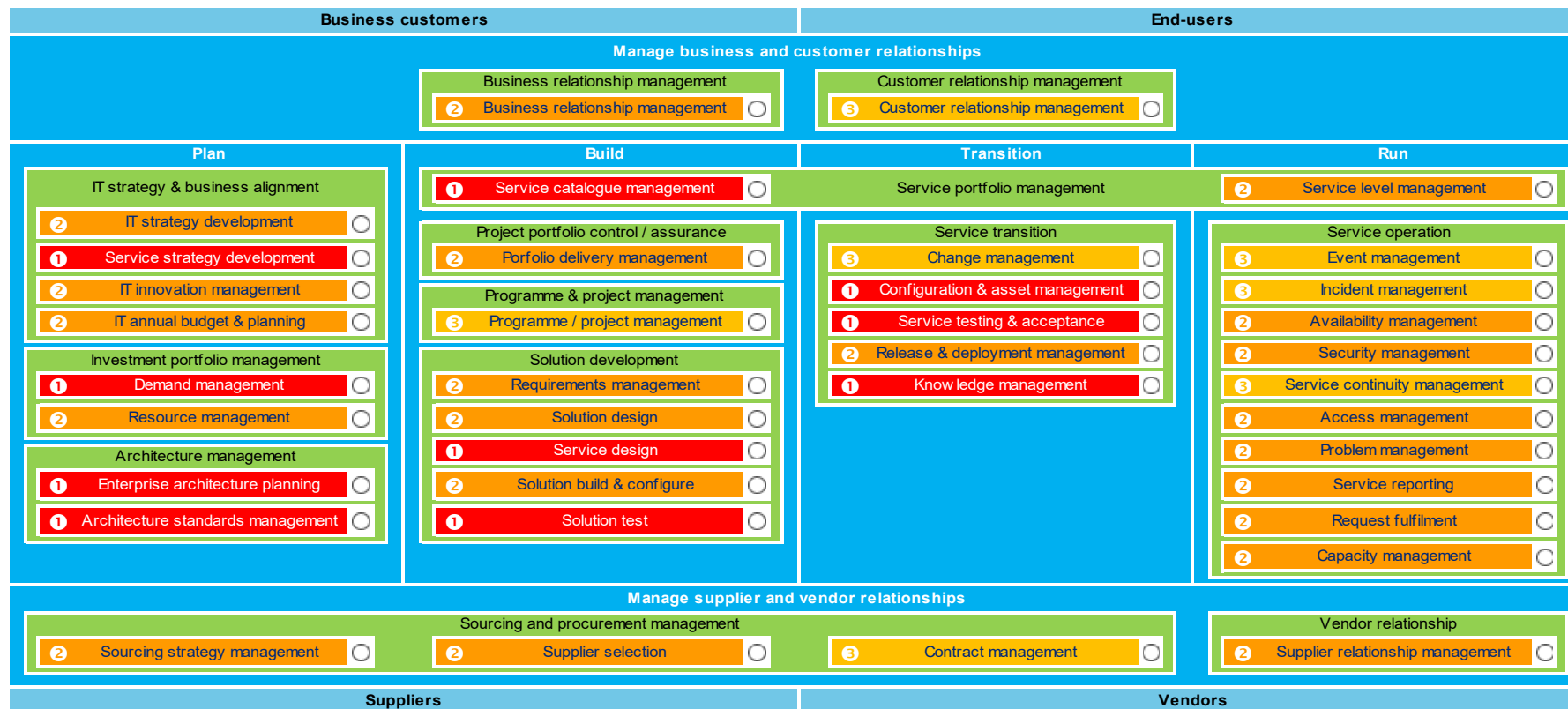
Source: OIT Hardware Asset Management Process Guide, July 2021

*IT Transformation Program*

During 2019, OIT conducted an analysis of the state’s current IT operations and environment to identify gaps in the State’s IT service delivery function, in relation to ITIL and other industry leading practices. During this year-long process, OIT met with state agencies and business and IT leaders to discuss needed improvements to efficiency, transparency, and customer satisfaction. OIT began addressing the identified areas of improvement using small project teams of selected OIT staff assigned by focus area.

In April 2020, OIT performed a self-assessment on its current capabilities to provide services related to specific ITSM categories, based on ITIL, and developed the following heat map indicating the level assessed. The results (Figure 3) changed the direction of OIT’s efforts and contributed to OIT’s IT Transformation (ITT) effort that is currently in progress. As indicated in the Capability Key, dark red colors represent areas where little or no formal detailed process or policies exist, up to dark green areas, which have well-defined and documented processes and policies.

Figure 3 - Governor’s Office of Information Technology  
 IT Service Management Self-Assessment Results  
 April 2020



Capability key:

0	Non-existent
1	Initial
2	Repeatable
3	Defined
4	Managed
5	Optimised

Icon Key:

- Not Outsourced
- ◐ 25% Outsourced
- ◑ 50% Outsourced
- ◒ 75% Outsourced
- ◓ Fully Outsourced

Capability Key Definitions:

0	Non-Existent	Process, policies and procedures do not exist.
1	Initial	Processes are characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
2	Repeatable	Basic policies and procedures are established to track activities. The necessary process discipline is in place to repeat earlier successes for similar efforts.
3	Defined	The policies and procedures are documented, standardized, integrated, and are used.
4	Managed	Detailed measures are collected around processes. These measures are used to quantitatively understand and control the processes.
5	Optimized	Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

Source: Governor’s Office of Information Technology

In August 2020, based on the feedback OIT had received from state agencies and business and IT leaders, as well as its ITSM self-assessment, OIT officially launched its ITT Program that covers the following areas and related goals:

- *IT Leadership and Governance* – Building a structure that supports collaborative IT oversight, strategic direction, and coordinated budgeting.
- *IT Talent* – Increasing alignment with agency business needs supported by strategies for talent growth and retention.
- *IT Financial Management* – Increasing financial transparency to support improved agency financial planning, increased oversight of vendors, and more streamlined processes for IT procurement.
- *Technology* – Improving use of modern technologies to support online and digital government along with defined services and coordination with customers.
- *Security* – Maintaining a robust security organization by a culture of compliance in partnership with agencies.
- *Service Excellence* – Enabling IT to function effectively through defined process and a service catalog.

In a February 2021 presentation to the Colorado General Assembly's Joint Technology Committee, which is the legislative committee that oversees the Office, OIT stated that its current ITT program has a strong focus on process improvement, with a goal to prioritize the following 13 ITSM-related process areas for improvement:

1. Innovation Management
2. Service Catalog Management
3. IT Service Charging
4. People Performance Management
5. Customer Relationship Management
6. Investment Portfolio Management
7. IT Strategy Development
8. Architecture Standards Management
9. Demand Management
10. Configuration and Asset Management
11. Supplier Relationship Management
12. Contract Management
13. Program and Project Management

These areas are linked to the ITSM areas noted in Figure 3 above, but have broader scope and additional areas customized to OIT's requirements and efforts.

OIT is currently implementing a cloud solution (software-as-a-service) ITSM tool called ServiceNow. OIT has branded its instance of ServiceNow as ServiceHub, using both names interchangeably. ServiceHub is intended to tie the various IT service management practices across OIT as part of the ITT program. At the time of the evaluation, OIT had only integrated the Project Management practice (which ties to number 13 above) into ServiceHub.

*Evaluation Purpose, Scope, and Methodology*

The Office of the State Auditor, State of Colorado, engaged RubinBrown LLP to conduct an evaluation of IT Service Management at the Colorado Governor's Office of Information Technology. The purpose of this IT performance evaluation was to determine whether OIT has adequate IT service management practices in place to plan, design, deliver, transition, operate, and control information technology services offered to customers, in accordance with state requirements, OIT's adopted ITSM practices, and other ITSM industry leading practices or standards, as applicable. RubinBrown performed fieldwork procedures from July 15, 2021 through November 2, 2021.

RubinBrown used a combination of interviews, observations, and documentation and data reviews to evaluate OIT's IT service management practices. The evaluation focused on OIT's ability to meet customer requirements, OIT internal requirements, and other ITSM industry leading practices and standards. RubinBrown utilized interviews with senior OIT leadership and documentation reviews to perform a risk assessment and identify areas of specific focus.

Based on our analysis, we identified and focused our review on the following nine key ITSM processes based on ITIL that provide underlying support to OIT's stated goals:

- *Governance* – the systems in place used to direct and control OIT in meeting its operational objectives. Governance sets the tone at the top and provides direction within the organization for supporting and directing each of the OIT goals. Governance links to all ITSM areas targeted by OIT.
- *Idea and Demand Management* – the identification, tracking, development, delivery, and related processes used to capture new ideas, requirements, and opportunities. Idea and demand management provides an avenue for OIT to centralize the intake process, provide transparency of the IT project pipeline, and efficiently react to customer demands. Idea and Demand Management links directly to OIT's Demand Management area.
- *Incident Management* – support management for user disruptions (incidents), to minimize the negative impact, by restoring normal operation as quickly as possible, typically tracked in an IT ticketing system. Incident management is required to effectively meet OIT's stated goals. Incident Management is a core element for ITSM and specifically links with OIT's goals of Service Catalog Management, IT Service Charging, Customer Relationship Management, and Configuration and Asset Management.
- *IT Asset Management* – managing lifecycles and total costs of IT solutions and infrastructure. IT asset management is an underlying support practice for IT service charging, investment management, and proactively managing technology debt, which is defined as the cost of maintaining and replacing out-of-date technology. IT Asset Management links to OIT's goals of Architectural Standards Management and Configuration and Asset Management.
- *IT Service Charging* – the practices and approach used to allocate IT service delivery and management of costs with increased transparency. IT service charging is a key component of a service organization, and OIT has recently launched Real Time Billing to address this area. IT Service Charging is an ITSM concept OIT customized to its needs and is linked to IT Service Charging and Customer Relationship Management.
- *Knowledge Management* – the collection, standardization, and utilization of information across the service organization. Knowledge management is central to supporting all other ITSM efforts, sharing information across the organization, and ongoing continuous improvement efforts. Knowledge Management is an underlying supporting concept linked to all of OIT's goals.



- *Project Management* – ensuring consistent planning, execution, delivery, and closeout of projects across the organization. Project management can impact across other ITSM practices and involves the communication and interaction between OIT and its customers. Project Management is directly linked to OIT's Program and Project Management goal.
- *Relationship Management* – establishing, nurturing, and maintaining relationships with users and stakeholders to facilitate effective and clear communications and decision making. Relationship management is a key component for a service organization to understand in order to deliver quality service. Relationship Management is directly linked to OIT's Customer Relationship Management goal.
- *Workforce and Talent Management* – maintaining, acquiring, and cultivating organizational talent to meet the organization's mission requirements. Workforce and talent management is a critical component in ensuring that the appropriate skills are in-house and continuing to provide a high level of service and commitment to customers. Workforce and Talent Management is directly linked with OIT's People Performance Management goal.

As part of the evaluation effort, RubinBrown conducted 37 interviews and reviewed more than 300 pieces of supporting information provided by OIT. The information was collected and analyzed as it provided insight into OIT's progress in the areas identified above.

As part of our evaluation effort, we developed specific findings addressed to OIT. As discussed above, the evaluation focused on the following nine specific areas:

- Governance
- Idea and Demand Management
- Incident Management
- IT Asset Management
- IT Service Charging
- Knowledge Management
- Project Management
- Relationship Management
- Workforce and Talent Management

While we evaluated all of the practices listed, we did not identify findings in all areas, as we determined that OIT's initiatives that are currently in place and/or in process are adequately addressing issues within the practices. We specifically identified findings in the following four areas:

- Idea and Demand Management
- Incident Management
- Knowledge Management
- IT Asset Management

Our findings are discussed in Chapter 2 of this report.



## CHAPTER 2

### IT Service Management Practices

#### Overview

As part of our evaluation fieldwork, we reviewed and identified issues with OIT's processes related to the following four ITSM practice areas:

- *Idea and Demand Management* – This practice is intended to help OIT identify new user opportunities and technology needs and routing the identified opportunities and technology needs through an appropriate process for consideration, prioritization, and execution. The opportunities and needs may be new functionality, capabilities (e.g., remote video conferencing), or a need for additional technology resources. Ideally, idea and demand management provides a centralized structure and process for submission of new requests, ideas, or needs from OIT's customers.
- *Incident Management* – This practice is focused on minimizing the negative impacts of incidents, by restoring normal service operations as quickly as possible. Within OIT, the Customer Office is responsible for the oversight of the majority of incidents, but incidents can be initiated by, assigned to, addressed by, and closed by any OIT staff member assigned to the incident.
- *Knowledge Management* – This practice includes the concept of maintaining and improving the effective, efficient, and convenient use of information and knowledge across an organization, and provides a structured approach to defining, building, re-using, and sharing knowledge (i.e., information, skills, practices, solutions, and problems) in various forms. Each OIT division maintains its own knowledge bases using a variety of solutions (e.g., wiki, shared drives, Google Hangouts, etc.).
- *IT Asset Management* – This practice focuses on managing the lifecycles and total costs of IT assets, such as IT equipment and infrastructure, and serves the purpose of planning and managing the full lifecycle of all IT assets, to help the organization:
  - Maximize asset values.
  - Control asset costs and the implied cost of additional rework caused by choosing an easy (limited) solution now, instead of using a better approach that would take longer, which is referred to as “technology debt.”
  - Manage risks related to IT assets.
  - Support decision-making about the purchase, re-use, retirement, and disposal of IT assets.
  - Meet regulatory and contractual requirements.

#### **Maturity Ratings and Observation Descriptions:**

RubinBrown has developed a five-level maturity rating system that we utilized when assessing OIT's adoption and integration of IT processes. The five levels with their applicable definitions are noted below:

- *Optimizing* – meets or exceeds organizational requirements, continuous improvement is in place and it is supported by formal documentation.
- *Managed* – meets or exceeds organizational requirements, formal documentation is in place and quality is actively managed via an organization-wide methodology.
- *Defined* – meets organizational requirements, is supported by formal documentation and standardized methodology.

- *Repeatable* – informal practices are in place and discipline exists in the organization to repeat earlier successes.
- *Ad Hoc* – no formal documentation and processes are dependent on individual efforts.

### **Observation Descriptions**

Maturity ratings are augmented with the following Observation Descriptions to further describe the level of implementation for each area assessed:

- *In Place* – Exists and is operating as intended.
- *Distributed* – No central owner or multiple owners with possible inconsistencies in the environment causing confusion.
- *Baseline In Place* – The foundation is present, but it is not stable or still in the final stages of production operation.
- *Under Development* – The development or deployment effort is still in progress.
- *Policy Only* – The policy is formally documented, but no processes or supporting activities are in place.
- *Does Not Exist* – The area is identified as necessary, but lack formal documentation, plans, or detailed designs.

### **What was the purpose of the evaluation and what work was performed?**

The purpose of the evaluation was to identify the existence of ITSM practices within OIT, specifically related to idea and demand management, incident management, knowledge management, and IT asset management, to assess the adequacy of those practices, and to identify areas of improvement necessary to support OIT's stated goals.

We reviewed more than 300 documents across these four ITSM practices, which included, but were not limited to:

- Various Policies, Procedures, and Templates
- Presentations to the Joint Technology Committee
- Project Lifecycle Methodology Knowledge Base
- OIT Fiscal Year 2021-22 Performance Plan

We conducted interviews across several OIT departments and staff, including the following:

- Executive Director and CIO
- Deputy Executive Director
- Chief Technology Officer
- Chief Customer Officer
- Deputy Chief Customer Officer
- Senior Manager - Customer Care
- Senior Director - Infrastructure Operations
- Senior Director - Applications Delivery & Support
- Security Governance Director
- Technology Performance & Planning Director
- Procurement Process Manager

- Senior IT Directors for the following agencies:
  - Colorado Department of Public Health and Environment (CDPHE)
  - Colorado Department of Transportation (CDOT)
  - Department of Corrections (DOC)
  - Department of Revenue

We also conducted interviews across several state departments and staff acting as key liaisons with OIT, including the following agency representatives:

- Environmental Information Manager, CDPHE
- Business Process Architect, CDOT
- Chief Information Officer, DOC
- Chief Administrative Officer, Colorado Department of Public Safety

In relation to our assessment of incident management, we obtained incidents captured by OIT in the Service Desk solution from June through August 2021, totaling 27,920 incidents. “Incidents” refer to unplanned interruptions or requests reported by users and include such items as password resets, access changes, or computer hardware issues. The three months from June to August were selected as a representative sample for analysis. We performed data analytics on the sample of incidents to determine their length of duration to closure, to identify how the incident handling procedures were being performed, and whether they were in conformity with OIT’s procedures.

Lastly, we assigned a maturity rating for each of the four ITSM practices that were the focus of this evaluation. The maturity rating was based on the level of process adoption and integration and included five (5) levels of ratings from Ad Hoc to Optimizing (full details were described in the Overview section). The maturity ratings were supported by observations to describe the level of process implementation with ratings ranging from “Does Not Exist” to “In Place.”

### **How were the results of the work measured?**

Overall, we measured the results of our work against a combination of OIT’s interpretation of the ITSM and ITIL processes and requirements; ITSM industry leading practices, including the ITIL Foundation’s Version 4 framework; OIT policies and procedures related to the specific ITSM practice areas; the Green Book, and our assigned maturity rating and observations descriptions.

The specifics of the criteria are as follows:

**ITSM industry leading practices, including the ITIL Foundation’s Version 4 framework:**

ITSM Practice	ITIL Foundation’s Version 4 Framework and Other Industry Leading Practices
Idea and Demand Management	<ul style="list-style-type: none"> <li>• <i>Identification</i> – capturing, centralizing, and assessing ideas and demands from users.</li> <li>• <i>Tracking and Monitoring</i> – centralizing tracking and reporting into a single source for use by users and the service organization.</li> </ul>
Incident Management	<ul style="list-style-type: none"> <li>• <i>Plan</i> – leveraging incident records for planning activities at the tactical and operational level.</li> <li>• <i>Improve</i> – using incident records as input for improvement activities using frequency and severity levels to prioritize improvements.</li> <li>• <i>Engage</i> – engaging customers through incident communications as the primary and most visible point of interaction with users.</li> </ul> <p>Overall, ITIL recommends activities are in place to ensure all IT assistance efforts are captured in the incident management system, and the data is used to provide metrics and contribute to planning and improvements.</p>
Knowledge Management	<ul style="list-style-type: none"> <li>• <i>Plan</i> – using the existing and known gaps in Knowledge Management to inform strategy, planning, and budgeting.</li> <li>• <i>Deliver and Support</i> – continuously updating and adding to the knowledge base so that known situations can be resolved efficiently and context can be provided for resolutions that may require additional analysis.</li> <li>• <i>Improve</i> – providing context for what has been documented and providing the structure to document changes and improvements in the environment.</li> </ul> <p>Overall, ITIL recommends that a common solution be utilized so that information and knowledge can be efficiently shared and leveraged.</p>
IT Asset Management	<ul style="list-style-type: none"> <li>• <i>Plan</i> – processes designed to forecast maintenance, replacements, upgrades, improvements, and the associated costs related to IT assets.</li> <li>• <i>Improve</i> – processes designed to consider the impact on IT assets, identify necessary versus optional improvements, and manage long term costs.</li> <li>• <i>Design/Build</i> – integration with development and procurement teams, so asset management covers the lifecycle of IT assets.</li> </ul>

**OIT Policies and Procedures:**

In addition, we used OIT process (PROC) and policy (POL) documents PROC 100-03 and POL 100-35 as a basis to analyze a sample of incident tickets. PROC 100-03 requires incidents to be prioritized based on urgency and impact, and categorizes them from Urgent to Medium. The target resolution times range from 15 minutes for Urgent incidents, to no more than 10 days for Medium incidents.

PROC 100-03 also states that when an IT staff transfers an incident/ticket to another person or group:

- The ticket should not be transferred back to the Service Desk,
- The reason for the transfer should be documented, and

- The responsibility of the incident's resolution becomes that of the team receiving the assignment.

### **Standards for Internal Control in the Federal Government (Green Book):**

The Green Book describes the components and principles of internal control, such as:

- *Control Environment* – The foundation for an internal control system that provides the discipline and structure to help an entity achieve its objectives. *Section OV2.04*
  - Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. *Section OV2.09*
    - The organization structure is necessary to enable the entity to plan, execute, control, and assess the organization in achieving its objectives. *Principle 3.02*
    - Management develops an organizational structure with an understanding of the overall responsibilities, and assigns these responsibilities to discrete units. In addition, management also considers the entity's overall responsibilities to external stakeholders and establishes reporting lines that allow the entity to both communicate and receive information from external stakeholders. Management assigns responsibility and delegates authority to key roles throughout the entity. *Principles 3.03, 3.04, and 3.07*
    - Management develops and maintains documentation of its internal control system to provide a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel. *Principles 3.09 and 3.10*
  - Management should hold individuals accountable for their internal control responsibilities. *Section OV2.09*
- *Information and Communication* – The quality information management and personnel communicate and use to support the internal control system. *Section OV2.04*
  - Management should communicate, both internally and externally, the necessary quality information to achieve the entity's objectives. *Section OV2.09*

### **What problems did the work identify?**

Based on our interviews, documentation reviews, and evidence analysis, we identified problems with OIT's ITSM practices in four specific areas, as discussed below.

#### **Idea and Demand Management**

OIT does not have a consistent or formalized process in place to ensure its Idea and Demand Management practices are in place and operating effectively. Specifically, based on our work, we found that OIT has no formal documentation in place, no centralized process to capture and evaluate ideas and demands, and no person or position assigned responsibility for the process. Major project intake is documented and assigned, but is not designed to handle the variances in size and scale for idea and demand management. OIT relies on multiple methods, processes, and activities to gather ideas from users. For example, ideas are currently tracked through a combination of paper, email, and files, providing minimal transparency to the user submitting the request.

#### ***Process and Documentation Levels:***

We assessed the implementation levels of the process area and the documentation related to the process area as **distributed**, or as having no central owner or multiple owners with possible inconsistencies in the environment causing confusion.

***Maturity Rating:***

We assessed the overall maturity level of the process area as **ad hoc**, or as having no formal documentation and processes being dependent on individual efforts.

**Incident Management**

OIT's incident management practices do not fully comply with OIT Policy and OIT staff are not capturing and documenting all incidents, as noted below.

- Some transferred tickets did not comply with OIT policy. Specifically, of the nearly 28,000 incidents reviewed, we found:
  - 1,263 incidents were transferred or reassigned at least 5 times.
  - 79 incidents were transferred or reassigned at least 10 times.
  - 3 incidents, within the 79 incidents, were transferred or reassigned at least 20 times.
- We further analyzed a subset of 129 incidents that were transferred or reassigned at least 5 times and impacted the resolution time frames. Specifically, we found:
  - 41 percent of the incidents did not meet the established resolution timeframe and/or the transfer requirements.
  - Overall, 30 incidents were open for more than 30 days.
- Not all incidents, and their associated support, are documented in the incident management ticketing system. Through our interviews, staff stated that incidents and support are handled without being documented in the incident management ticketing system as an incident. For example, OIT staff assigned full time onsite to an agency reported to us that they sometimes handle support through email, phone calls, or dropping by someone's desk and never enter the information into the incident management system.

***Process and Documentation Levels:***

We assessed the implementation levels of the process area as **distributed**, or as having no central owner or multiple owners with possible inconsistencies in the environment causing confusion. We assessed the documentation related to the process area as **baseline in place**, meaning the foundation is present, but it is not stable or still in the final stages of production operation.

***Maturity Rating:***

We assessed the overall maturity level of the process area as **repeatable**, meaning that informal practices are in place and discipline exists in the organization to repeat earlier successes.

**Knowledge Management**

OIT does not maintain a common knowledge management solution that would aid the various OIT teams in providing customer support, incident resolution, and requests in a timely manner. Currently, information and knowledge may be maintained separately and updated inconsistently in multiple locations since it is not shared across OIT teams, thereby resulting in ineffective and inefficient use of human resources and reducing the level of service provided to agencies. For instance, the Project Lifecycle Management Knowledgebase is stored and maintained separate from other Customer Office knowledge bases, which creates a decentralized storage environment complicating where users can find documentation potentially causing service delays. OIT does not have any formal documentation requiring the use of a central knowledge management solution.



***Process and Documentation Levels:***

We assessed the implementation levels of the process area and the documentation related to the process area as **distributed**, or as having no central owner or multiple owners with possible inconsistencies in the environment, causing confusion.

***Maturity Rating:***

We assessed the overall maturity level of the process area as **ad hoc**, or as having no formal documentation and processes being dependent on individual efforts.

**IT Asset Management**

OIT's IT asset management practices do not address key aspects of ITSM leading industry practices. Specifically,

- OIT does not have a proactive approach to agency support; rather, it reactively supports the agencies and does not have a process in place to consistently assist all participating agencies with strategic technology modernization planning. Technology modernization requirements that are not addressed build up over time and are referred to as technology debt. Technology modernization efforts vary considerably across agencies in regards to planning and improving IT assets within the State. For example, CDOT reported that it receives sufficient funding that aids in minimizing its technical debt but DOC stated it has greater challenges budgeting for technology upgrades, over fulfilling its primary mission. Overall, OIT in its role providing technology support to state agencies should be taking a larger role in advising agencies on technology strategy.
- Based on the September 9, 2021, Office of Information Technology Update to the Joint Technology Committee, OIT estimated the current unfunded technology debt for executive branch agencies at over \$465 million. Each agency is responsible for their own technology debt, but OIT has not provided the agencies with sufficient information and advisory support, despite its understanding of the growing debt level, so that each agency can address their individual technology debt.

***Process and Documentation Levels:***

We assessed the implementation levels of the process area and the documentation related to the process area as **under development**, meaning that the development or deployment effort is still in progress.

***Maturity Rating:***

We assessed the overall maturity level of the process area as **ad hoc**, or as having no formal documentation and processes being dependent on individual efforts.

**Why did the problems occur?**

Overall, the problems we identified have occurred because OIT has not established a strong IT governance model in the areas of control environment (e.g., organizational structure, assigning responsibility, and delegating authority) and information and communication (e.g., quality information communications), which would aid in OIT accomplishing its goals for the ITT Program. The following outlines the specific causes for the issues we identified by ITSM practice:

**Idea and Demand Management**

Rather than implementing a standard, centralized idea and demand management process according to IT industry leading practice, OIT management has allowed multiple, informal, manual, and disparate Idea and

Demand Management processes and coordination paths to exist with agencies. Examples of these informal, disparate methods include:

- Innovation projects within the Chief Technology Officer's division are submitted directly to the group and tracked only within the group.
- Customer Service responding to requests and inquiries often receive new requests but do not have formal guidance on how to process the requests.
- Major project intake process is a defined process, but only appropriate for large, resource intensive, projects.
- IT Directors working with agency contacts regularly receive requests that are routed individually by each IT Director but are not formally tracked.
- Personal relationships within OIT and between OIT staff and agency staff are often leveraged to present ideas and requests outside of formal processes.

Further, OIT has not taken steps to catalog the current processes, design a centralized model, centralize the implementation of formalized processes and/or usage of automated tools, or assign the effort to a specific division and its staff to oversee the effort.

*Governance Area: Control Environment and Information and Communication*

### **Incident Management**

- No thresholds are defined or enforced for the number of times an incident is transferred or reassigned to ensure compliance with established resolution timeframes and transfer requirements. Although PROC 100-35 outlines target resolution timeframes for the various incident categorizations, OIT has not designed the Procedure to ensure that the transfers or reassignments do not impact the resolution time.
- No position or group has the responsibility for monitoring all incidents or authority to enforce the established procedure. Incidents are managed by various teams, including Security Operations, Security Governance, Service Desk, and Infrastructure Operations, and when transferred between groups, the incident monitoring is passed to the new group, and the established procedure is not followed consistently.
- PROC 100-35 does not require all support efforts to be logged as incidents and only requires Service Desk personnel to enter incidents. Staff not in a Service Desk role (e.g., analyst, lead, supervisor, manager, etc.) do not have a formal directive to create incidents.

Users prefer to interact with known IT support staff and are reluctant to engage the Service Desk to enter an incident. In addition, IT staff assigned to a specific agency focus on their Service Level Agreements and agency satisfaction, not OIT centralized processes.

*Governance Area: Control Environment and Information and Communication*

### **Knowledge Management**

OIT leadership has neither identified nor developed a common vision, strategy, process, or solution for knowledge management and has not, therefore, developed the associated policies or procedures.

*Governance Area: Control Environment and Information and Communication*

## **IT Asset Management**

OIT does not have effective, consistent, and transparent processes and solutions in place to assist agencies with strategic replacement plans. In addition, OIT does not use the data and metrics available, combined with standard processes, for the OIT IT Directors to engage the agencies in strategic planning. Other contributing factors include agency variations in funding, inability to hire business technology specialists, and budget conflicts between technology updates and core agency missions.

### *Governance Area: Control Environment and Information and Communication*

In summary, OIT is a large and complex organization. Culturally, OIT has the silos, communications challenges, and relationship management issues common to most IT organizations. The evolution into a single organization has been complicated by teams that were previously part of another agency that are often still serving that same agency, blurring the lines between the organizations and chains of command. Finally, tension between OIT and agency customers has existed for many years, as the agencies demand additional supporting detail from OIT for the costs associated with OIT support, resulting in the current Real Time Billing effort. OIT has a large number of efforts in various stages of development, including the ITT initiative, governance initiatives, organizational changes, customer initiatives, Wildly Important Goals, and day-to-day operational efforts. Continuing to work through the ITT initiative is essential for OIT in order for it to meet its mission of providing high quality, cost efficient, technology services to the agencies.

### **Why do these problems matter?**

Overall, IT service management is the foundation of OIT's purpose to the agencies it supports, as well as ultimately to the citizens of Colorado. Consistent, formalized, and transparent policies and directives are critical elements of IT governance to establish responsibility, authority, and quality expectations. As OIT continues to execute its ITT Program, it has the opportunity to incrementally improve existing processes and establish clear policies and procedures for newly developed processes.

Each of the four ITSM practices assist in providing an overall framework for IT service management and are crucial to OIT's success in meeting its purpose, as noted below:

- *Idea and Demand Management* – Consistent, formalized, and transparent idea and demand management is critical to building trust with agencies and efficiently handling requests, ideas, or needs from the agencies. For example, manually coordinating across multiple departments (using email or paper) can be inefficient and may not provide the level of transparency in the process desired by individual agencies. The lack of transparency to users may erode trust, add to tension levels between OIT and agencies, and could lead to agencies seeking ways to circumvent OIT in the future.
- *Incident Management* – Incident Management practices are critical to continuous process improvement and without leadership focus and direction in place, there is no assurance and enforcement to comply with OIT established procedures and meeting OIT's stated goals. Incident Management is the foundation of IT Service Management, and it has the most immediate impact to most users. The lack of established thresholds and enforcement of requirements for transferred incidents could impact OIT's ability to meet target resolution times and cause disruptions and delays for users. In addition, incidents that stay open far longer than allowed by OIT standards result in degraded customer satisfaction. Failure to continuously improve and optimize the Incident Management function may cause disruption throughout the value chain and increase tension and frustration with OIT users. In addition, incidents handled without documentation do not contribute to the data used for planning and improvements.

- *Knowledge Management* – Knowledge management practices are critical to providing the underlying support needed for OIT in order for it to be a high performing IT services organization, and to meet OIT's stated goals by collecting, managing, and sharing information across the service organization effectively and efficiently to reduce response time and improve value to users. OIT's lack of a central vision, strategy, or process for knowledge management results in redundant and inconsistent knowledge base information, duplicate efforts to create similar information, inefficient use of time, and longer times to resolve some incidents.
- *IT Asset Management* – IT Asset Management processes are critical to managing cost and value over the long term. Mounting technology debt creates a financial risk to the State because of the cost to maintain dated technology, and technical risk from the potential security-risks associated with technology no longer being supported or actively updated.

**Recommendation No. 1:**

The Governor's Office of Information Technology (OIT) should establish or improve, as applicable, its Information Technology (IT) governance structure related to the IT service management practice of Idea and Demand Management by:

- A. Assigning centralized oversight authority and responsibility for Idea and Demand Management to an appropriate OIT division and staff.
- B. Formalizing, implementing, and communicating Idea and Demand Management processes to those responsible or involved in the processes.
- C. Considering the use of OIT's current application platform, or a different tool, to automate and facilitate supporting Idea and Demand Management processes across OIT and its customers/agencies. Areas to be addressed should include, but not be limited to:
  - Intake process customized to size and impact of each idea submitted.
  - Initial triage and consideration by business analysts and solution designers focused on leveraging enterprise solutions.
  - Consideration for innovation efforts for rapid prototyping.
  - Workflow processes that track an Idea through its lifecycle.
  - Status reporting for better transparency of each effort to senior management, agencies, and customers.

**AGENCY RESPONSE**

**GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY**

- A. AGREE. IMPLEMENTATION DATE: December 2022.

OIT intends to centralize oversight, authority and responsibility for idea and demand management as a part of our ongoing IT Transformation program.
- B. AGREE. IMPLEMENTATION DATE: June 2023.

OIT has an active project within its IT Transformation program to improve and formalize idea and demand management processes and is aligning the implementation and communication of these improvements with the ServiceHub roll-out scheduled for this summer and we expect full implementation of these changes by the end of next fiscal year.
- C. AGREE. IMPLEMENTATION DATE: June 2023.

OIT has an active project within its IT Transformation program to improve idea and demand management processes which will include the recommended items. OIT is aligning the implementation and communication of these improvements with the ServiceHub roll-out scheduled for this summer and we expect full implementation of these changes by the end of next fiscal year.

## **Recommendation No. 2:**

The Governor's Office of Information and Technology (OIT) should establish or improve, as applicable, its Information Technology (IT) governance structure related to the IT service management practice of Incident Management by:

- A. Assigning an overall Incident Manager to monitor incidents across all OIT service areas, specifically to enforce incident reporting procedures, monitor long-term trends, identify and provide support for exceptions to documented procedures, and report on the overall incident processing effectiveness for OIT.
- B. Once an Incident Manager has been assigned, as recommended in Part A, they should update the OIT Incident Management Procedure to clarify how, when, and by whom incidents should be created, documented, routed, monitored, and reported.
- C. Developing a communications plan to emphasize incident management procedures, including updates made as recommended in Part B, with OIT staff and the need to capture user support work efforts in OIT's centralized ticketing system. The communications plan should include an agency-directed marketing plan item to emphasize the benefits of engaging the OIT Service Desk to submit and record user incidents.

## **AGENCY RESPONSE**

### **GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY**

- A. AGREE. IMPLEMENTATION DATE: July 2022.

OIT will assign an overall Incident Manager. With the implementation of ServiceNow, OIT expects this role to monitor incidents across all OIT service areas, specifically to enforce incident reporting procedures, monitor long-term trends, identify and provide support for exceptions to documented procedures, and report on the overall incident processing effectiveness for OIT.

- B. AGREE. IMPLEMENTATION DATE: December 2022.

With the implementation of the ServiceNow ITSM modules, OIT will include updating the incident management procedure as noted by the recommendation.

- C. AGREE. IMPLEMENTATION DATE: June 2023.

OIT plans to address the recommendation as noted. Notifications and communications are being further automated and standardized with the implementation of the ServiceNow ITSM module. Incident management, notification, and resolutions will be in a centralized system. In parallel to this system implementation, OIT has completed a stakeholder analysis and overlay our ticketing processes with effective communications.

**Recommendation No. 3:**

The Governor's Office of Information Technology (OIT) should establish or improve, as applicable, its Information Technology (IT) governance structure related to the IT service management practice of Knowledge Management by:

- A. Assigning ownership to an OIT individual who is empowered to lead OIT in developing a common vision or strategy and associated processes to ensure the collection and organization of a comprehensive knowledge base
- B. Implementing a Knowledge Management digital solution, once Part A is implemented, as a single platform for hosting standard operating procedures, historical information, detailed technical solutions, solutions and technologies available, and other information that may assist in providing a higher level of product and service delivery to agencies in a timely manner and facilitate continuous improvement opportunities.

**AGENCY RESPONSE**

**GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY**

- A. AGREE. IMPLEMENTATION DATE: April 2022.

OIT agrees with the need for accountability and governance and will establish appropriate ownership and governance by April 2022. Overall, the ServiceNow Executive Committee has oversight for the ITSM area.

- B. AGREE. IMPLEMENTATION DATE: June 2023.

OIT expects to be substantially complete with implementing the tool to include the items noted in the recommendation by June 2023. Integrations with all peripheral systems may not be complete by June 2023 yet processes will exist to enable ongoing integrations in the future.

**Recommendation No. 4:**

The Governor's Office of Information Technology (OIT) should establish or improve, as applicable, its Information Technology (IT) governance structure related to the IT service management practice of IT Asset Management by:

- A. Developing a set of common practices for OIT Directors to use in engaging and advising agencies about technology replacement planning and budget forecasting.
- B. Assisting the agencies in their strategic planning efforts for technology updates by utilizing available solutions, asset inventories, data and metrics to develop forecasting tools to help normalize funding variations and reduce budgeting conflicts.

**AGENCY RESPONSE**

**GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY**

- A. AGREE. IMPLEMENTATION DATE: August 2023.

Work on this is in progress but will take time given the scale of the recommendation involved. OIT is partnering with executive branch agencies to build out robust Technology Planning Workbooks to meet this recommendation. A critical piece of this is agency buy-in to the process and outcomes.

- B. AGREE. IMPLEMENTATION DATE: August 2023.

This will be an evolutionary process. OIT has begun this work through its IT Roadmaps and deployment of a single IT asset management repository. However, maturing the processes will take time as part of overall IT Transformation. A critical piece of this is agency buy-in to the process and outcomes.