Review of
Critical Systems Standard

November 2018

INTERNAL AUDIT
AND ADVISORY SERVICES

BRITISH COLUMBIA | Ministry of Finance

Project No.: 19−05 CITZ

Review of Critical Systems Standard

Internal Audit & Advisory Services
Ministry of Finance

Date of fieldwork completion: November 2018

Table of Contents

Section **Page No.**

Abbreviations

Checklist	Compliance Checklist
CPPM	Core Policy and Procedures Manual
Guidelines	Critical Systems Guidelines
IM/IT	Information Management and Information Technology
OCIO or Office	Office of the Chief Information Officer
Province or Government	Government of British Columbia
Standard	Critical Systems Standard

Executive Summary

The Office of the Chief Information Officer (OCIO or Office) is the central agency responsible for leading strategy, policies and standards for telecommunications, information technology, cybersecurity, and is accountable for the operation of a broad technology infrastructure for the Government of British Columbia.

Depending on the criticality of the business services that are impacted, disruptions to Information Management and Information Technology (IM/IT) can be costly and can cause significant harm or hardship to stakeholders, including citizens that depend on these services. In March 2015, the Critical Systems Standard was approved with the purpose of helping ministries ensure processes and controls are in place to minimize system disruptions and improve recoverability.

The purpose of this review was to assess the effectiveness of the Critical Systems Standard and its implementation to protect systems that deliver mission critical and business priority services. This review was requested by the OCIO and conducted by Internal Audit & Advisory Services, Ministry of Finance.

Standard Content and Alignment

Under the Critical Systems Standard, critical systems must satisfy a list of requirements that pertain to various IM/IT areas, including incident and change management, and disaster recovery planning.

While the requirements in the Critical Systems Standard generally align with the Core Policy and Procedures Manual, there are a few instances of misalignment identified, such as defining performance metrics that would enable the monitoring and tracking of ministry compliance.

In addition, a few ministries reported that some requirements could not be fully applied due to the use of Agile development approach and the existence of outsourced systems where the accountability is usually placed on service providers. Opportunities exist for the OCIO to provide ministries with additional support to reduce the risk of misinterpreting the applicability of the Critical Systems Standard.

Standard Integration

Several programs and initiatives exist throughout the Government of British Columbia to increase the resiliency of critical services and IM/IT systems against incidents and disasters. These include Emergency Management BC's Business Impact Analysis for ministries to identify and prioritize critical services in case of a disruptive event, the OCIO's Security Strategy to help ministries further mature their information security practices, and the OCIO's Hosting Services that provide options to ministries for increasing data and processing availability.

As the Critical Systems Standard was initially developed as a stand-alone document, there is a need to further integrate its requirements with the aforementioned initiatives to help gain efficiencies, increase synergies, and better leverage resources towards compliance activities.

Identification of Critical Systems

Since ministries were not provided with recommended courses of action for identifying their critical systems, they have defined their own methodologies to identify these assets with various levels of sophistication and documentation.

The inconsistent methodologies used by ministries impact the accuracy and completeness of the corporate inventory, and the allocation of resources to protect critical systems. Ministries would benefit from leveraging their Business Continuity Plans and Business Impact Analyses to identify, prioritize, and regularly review their critical systems.

Compliance Progress

Of the 181 critical systems identified in the OCIO's asset registry, 82 were expected to become compliant as of December 2018; only 6% of these systems were recognized by the Office as being fully compliant.

Low compliance is likely driven by multiple factors, including inaccurate declaration of critical systems by ministries, unclear accountability to ensure prioritization and oversight, and lack of resources dedicated to this process. The OCIO would benefit from enhancing consultation with ministries to address the root causes of the low compliance rate and improve adherence.

Roles and Responsibilities

While the Critical Systems Standard and related guidelines define roles and responsibilities that form part of the compliance activities, they do not define those relevant to executive oversight. To ensure compliance with IM/IT standards, it is vital for the Government of British Columbia to revise the Core Policy and Procedures Manual to clearly establish ministry executives' accountability at the appropriate level.

These roles help to support ministries' continued efforts towards compliance through the appropriate allocation of budget and resources. They are also essential for ensuring that the Government of British Columbia's inventory of critical systems remains accurate and complete.

Standard Awareness, Support and Training

During the initial stages of the compliance activities, the OCIO actively promoted awareness about the Critical Systems Standard's purpose, value and impact to ministries.

The OCIO has attempted to maintain various channels of communication with ministries with limited success. Acknowledging the challenges, the Office is currently developing a Communication Protocol to support compliance and cultural change. It has also initiated a Community of Practice in November 2018 in an effort to address ministries' concerns and benefit different audiences.

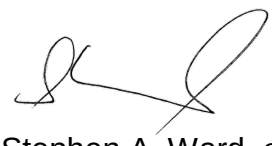
Monitoring and Reporting

Ministries are required to select an Independent Reviewer to attest to the evidence of compliance and the OCIO verifies whether the independent review was completed appropriately before deeming the critical system as compliant. While these reviews are required, they are not reperformed regularly (e.g., every 2 to 3 years).

At the corporate level, a Summary Report with statistics is expected to be distributed to the Assistant Deputy Minister-OCIO Enterprise Services and Ministry Chief Information Officers. However, recent reports have not been routinely made available. While these statistics are obtained from the asset registry, ministry information is not always accurate or complete. Opportunities exist for the OCIO to consult with ministries and establish an integrated process to regularly report on the effectiveness of the Government of British Columbia's compliance activities.

* * *

We would like to thank the management and staff of the OCIO, as well as ministry stakeholders who participated in and contributed to this review, for their cooperation and assistance.



Stephen A. Ward, CPA, CA, CIA
Executive Director
Internal Audit & Advisory Services
Ministry of Finance

Introduction

The Government of British Columbia (Province or Government) increasingly relies on information technology to provide critical services to citizens and to a broad range of organizations. As the technology environment continues to increase in scale, complexity, and dependencies, so does the risk of disruptions to business services.

The Office of the Chief Information Officer (OCIO or Office) is responsible for developing and maintaining corporate-wide Information Management and Information Technology (IM/IT) policy, procedures and standards in areas such as electronic identity management, information management, and information security. The Office is also responsible for monitoring compliance with these IM/IT policies.

To reduce the risk of disruptions to IM/IT systems and critical services, the OCIO introduced the Critical Systems Standard (Standard) in March 2015. An updated version with additional requirements was published in October 2017.

Related compliance activities followed a three-phased approach, as listed below:

- **Phase 1** (March 2015 – October 2015): ministries identified their critical systems.
- **Phase 2** (November 2015 – March 2016): ministries assessed and reported their critical systems' compliance status to the OCIO.
- **Phase 3** (since April 2016): ministries have been working on compliance with the Standard.

As of November 2018, ministries identified 181 systems as critical to deliver ministries' services.

Purpose, Scope and Approach

The purpose of this review was to assess the effectiveness of the Standard and its implementation to protect the systems necessary to deliver mission critical and business priority functions by core government.

The review evaluated and made recommendations to the OCIO's and ministries' processes with a focus on the following areas:

- whether the Standard and its guidelines are sufficient to address OCIO and ministries' purposes;
- whether the Standard and its guidelines are effectively adopted by the OCIO and ministries; and
- the progress of the above organizations towards compliance.

This review, requested by the OCIO, was conducted by Internal Audit & Advisory Services, Ministry of Finance.

Working with senior management, Internal Audit & Advisory Services conducted this engagement with focus on the effectiveness of the Standard. The approach included:

- conducting interviews with key management and staff across the Office and ministries;
- surveying Ministry Coordinators and System Owners involved in the compliance efforts; and
- reviewing the Standard's alignment with best practices and existing government policy and initiatives.

1.0 Standard and Policies

The OCIO develops and maintains corporate IM/IT policy, standards, and guidance to help protect and manage the Province's information and technology resources. Depending on the criticality of the Province's business services that are impacted, IM/IT disruptions can be costly and can cause significant harm or hardship to citizens and businesses that depend on these services.

In March 2015, the OCIO introduced the Standard to address lessons learned from IM/IT disruptions to the Province's critical services that occurred in the previous year. Prior to this, the Province did not have a set of control requirements and guidelines specifically targeting the availability of IM/IT systems that deliver mission critical and business priority services, although policies and standards have existed for managing and protecting the Province's information and technology resources.

The purpose of the Standard is to help ministries ensure that adequate processes and controls are in place to minimize disruptions and improve recoverability of critical applications.

1.1. Standard Content and Integration

Under the Standard, the Province's critical systems must satisfy a list of requirements that pertain to various areas of IM/IT, including system documentation, incident and change management, and disaster recovery planning. The Standard is supplemented by the Critical Systems Guidelines (Guidelines) and the Compliance Checklist (Checklist), which are designed to assist ministries in reaching compliance.

Sufficiency of the Standard and Feasibility of Requirements

This review assessed the sufficiency of the IM/IT areas covered in the Standard against the COBIT 5 framework and determined that they are adequate in serving the purposes of the Standard.

> COBIT 5 is an internationally recognized control framework for effective governance and management of information technology.

The Standard defines a set of requirements for each IM/IT area that it covers. Some of these requirements are further detailed in the Guidelines and Checklist. The requirements were written at a high-level to allow ministries with flexibility to adopt them using their own processes and procedures. However, a few ministries reported that some requirements could not be fully applied due to the use of Agile development approach and the existence of outsourced systems where the accountability is usually placed on service providers.

Opportunities exist for the OCIO to provide additional support to ministries with unique circumstances. This can be achieved through providing contextualized examples, leveraging ministries' successful experiences, and identifying champions reducing the risk of misinterpreting the applicability of the Standard.

Alignment with Legislation and Policies

Alignment of the Standard with legislation and corporate policies supports consistency and reduces redundancy in requirements. The requirements in the Standard, Guidelines and Checklist generally align with Core Policy and Procedures Manual (CPPM), Information Security Policy, and the emergency program legislation and regulation.

There are a few instances where the Standard and Guidelines do not align with CPPM. For example, they do not:

- require Deputy Minister involvement when identifying their critical systems and dependencies,
- define performance metrics that would enable the monitoring and tracking of ministry compliance, and
- require an annual review of disaster recovery plans.

The OCIO would benefit from revising the Standard and Guidelines to further align with CPPM and Information Security Policy, as well as with other existing policies that have a broader or more in-depth coverage of the related IM/IT areas (e.g., back-up management, disaster recovery planning, system monitoring, etc.).

Integration

The Standard was initially developed as a stand-alone document, with minimal alignment with other programs and initiatives. Several corporate initiatives exist throughout the Government to increase the resiliency of critical services and IM/IT systems against incidents and disasters. Integration of the Standard with these initiatives would help minimize inconsistencies and redundancies between requirements, reduce confusion for resource allocation within ministries, and leverage ministries' existing efforts for similar requirements towards the compliance activities.

The following opportunities to further align or integrate the Standard were identified:

- Emergency Management BC has developed a Business Impact Analysis template for ministries to identify and prioritize critical services in case of a disruptive event. It is also working with ministries to define the Government's actions necessary to respond to a catastrophic event (e.g., earthquake, tsunami). Both initiatives involve identifying resources, including IM/IT systems necessary to recover critical services and deliver catastrophic response actions.

- The OCIO has published several security-related standards and guidance and has developed an overarching digital security strategy to help ministries further mature their information security practices. While scopes and objectives differ from the Standard, these initiatives introduce requirements that address common IM/IT areas, such as IT change management and disaster recovery planning processes.

- The Hosting Services branch at the OCIO offers service package subscriptions to meet ministries' application needs, including a standardized set of information technology infrastructure and related support for change management and disaster recovery planning processes. Options are available to ministries to support increasing data and processing availability as well as geographic diversity that can reduce the risk of disruptions to their critical systems.

The integration of the Standard to existing programs and initiatives will ensure that consistent methodologies and services are promoted throughout the Government to identify critical systems and reduce the risk of IM/IT disruptions. The integration of the Standard within an overarching initiative such as the OCIO's Security Strategy will also help the Province gain efficiencies, increase synergies, and better leverage resources towards compliance activities.

Consistency

The OCIO has developed the Guidelines and Checklist to substantiate the Standard requirements and help ministries assess their compliance. While these documents generally align with the Standard requirements, the Guidelines do not cover some key processes that are outlined in the Standard. This includes the processes for ministries to have their compliance assessment and roadmap endorsed, and to report its progress annually. Other inconsistencies reside in referencing outdated tools and unclear roles and responsibilities.

Outdated and inconsistent information can impact compliance efforts and affects ministries' confidence in the relevance of the resources provided by the OCIO. It would be beneficial for the Office to establish an iterative process to improve the Standard, Guidelines and Checklist that considers feedback and suggestions proposed by ministries. This would help improve the consistency of the information provided by the Office and provide ministries with the relevant support that they require.

Recommendations:

(1) **The OCIO should further align the Critical Systems Standard with CPPM.**

(2) **The OCIO should engage Emergency Management BC to align methodologies for identification and prioritization of ministries' critical services and information systems.**

(3) **The OCIO should further integrate the Critical Systems Standard with IM/IT security initiatives and leverage available hosting services to support ministries' progress towards compliance.**

(4) **The OCIO should ensure the consistency of the Critical Systems Guidelines and Compliance Checklist with the Critical Systems Standard.**

1.2. Identification of Critical Systems

As of November 2018, ministries identified 181 systems as necessary for the delivery of the Government's critical services. Some examples include case management applications, as well as health, financial and security systems. British Columbians depend on these systems to receive healthcare, social, and emergency services. Disruption to such services could lead to loss of life or injury, personal hardship to citizens, major damage to the environment, or significant loss of revenue or assets.

Identifying the IM/IT systems that are necessary for the delivery of critical services is the first key step to ensuring these services are mitigated against IM/IT disruptions and could recover within acceptable timeframes. However, the Standard and Guidelines do not provide recommended courses of action for ministries to identify their critical systems.

This review found instances where critical systems were not identified, or where systems were incorrectly classified as critical. This was due to ministries having defined their own methodologies to identify critical systems with various levels of sophistication and documentation. These inconsistent methodologies impact the accuracy and completeness of the Province's inventory and its ability to appropriately allocate resources to protect and recover critical systems.

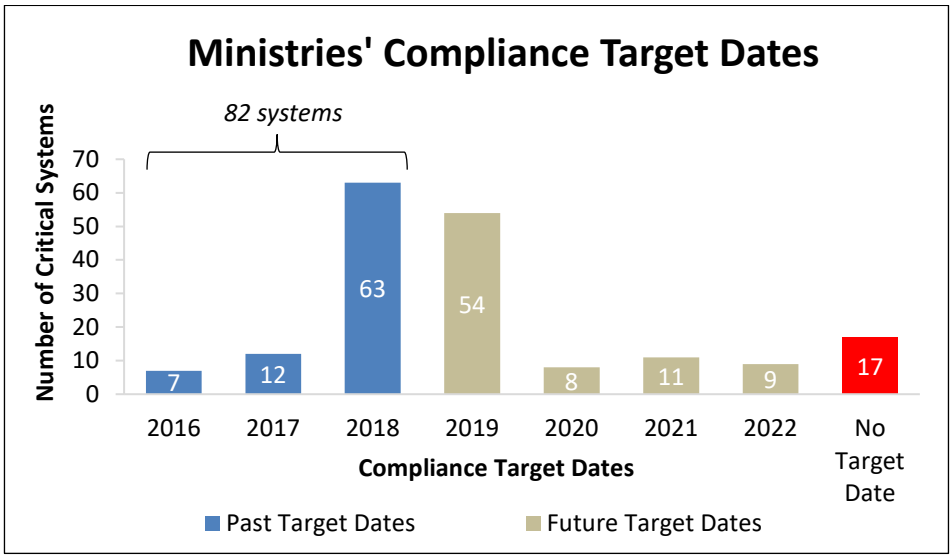
As mentioned in the previous section, ministries would benefit from leveraging their Business Continuity Plans and their Business Impact Analyses to identify, prioritize, and regularly review their critical systems. This would ensure that mitigation of risks and recovery of IM/IT systems are prioritized based on their criticality levels.

1.3. Compliance Progress of Critical Systems

The Standard came into effect in April 2016. By that date, ministries had to declare the following information in a central asset registry:

- list of critical systems;
- status of the system's compliance towards the Standard; and
- target dates for systems that were not compliant.

Of the 181 critical systems identified in the asset registry, 82 were expected to become compliant as of December 2018, as illustrated in the following chart:



Source: OCIO, as of December 31, 2018

Only 6% of the 82 systems expected to be compliant by 2018 were recognized by the Office as being fully compliant. Low compliance is likely driven by multiple factors, including inaccurate declaration of critical systems by ministries, unclear accountability to ensure prioritization and oversight, and lack of resources dedicated to this process. Without proper prioritization, it is unlikely that the remaining systems will become compliant within the time indicated.

Furthermore, some IM/IT systems that are planned to be retired have been excluded from ministries' compliance activities. These systems are still delivering critical services until their retirement. The lack of compliance of these systems with the Standard increases the risk of IM/IT disruptions and inability to recover related critical services within the acceptable timeframe.

Although full compliance may not be feasible or may not be an effective use of resources for IM/IT systems about to be retired, the Province would benefit from establishing a level of compliance that is considered tolerable to ensure that all systems delivering critical services are covered.

Lastly, ministries stated that they place heavy reliance on their service providers' adherence to contractual requirements, sometimes substantiated by third-party reviews (e.g., System and Organization Controls reports), to ensure compliance with the contract. The current attestation process defined by the OCIO does not mention leveraging these third-party reviews to declare compliance with the Standard. The OCIO and ministries would benefit from using these reviews to demonstrate compliance of outsourced critical systems.

Recommendations:

(5) The OCIO should enhance consultation with ministries to address the root causes of the low compliance rate and improve adherence to the Critical Systems Standard.

(6) The OCIO should update the Critical Systems Standard to leverage third-party reviews for outsourced critical systems.

2.0 Governance

The OCIO develops, maintains and evaluates ministry compliance with corporate IM/IT policies and standards. At the ministry level, Ministry Chief Information Officers are responsible for ensuring compliance with these policies and standards.

An appropriate governance model defines activities to evaluate strategic options, assign roles with appropriate authority and monitor performance. A clear governance structure for the implementation and monitoring of the Standard ensures all parties are effectively adopting the related requirements and helps to mitigate the risk of IM/IT disruptions.

2.1. Roles and Responsibilities

The Standard and the Guidelines define roles and responsibilities that form part of the compliance activities. Some of the key roles under the Standard are defined as follows:

- System Owners: are accountable for the overall state of their critical systems.
- Ministry Coordinators: act as an administrative contact between the Office and their ministries.
- OCIO Coordinator: acts as the single point of contact between the Office and Ministry Coordinators.

To achieve compliance, ministries are expected to assign these roles to staff who have the appropriate skills and authority, including the ability to set expectations and to be held accountable for compliance progress. Clearly defined roles and responsibilities are an essential component for the successful implementation of the Standard.

The Standard and Guidelines do not define roles and responsibilities relevant to executive oversight. These roles help to support ministries' continued efforts towards compliance through the appropriate allocation of budget and resources. They are also essential for ensuring that the Government's inventory of critical systems remains accurate and complete. To ensure compliance with IM/IT standards, it is vital for the Government to revise CPPM Chapter 12 and any other relevant chapters to clearly establish the appropriate ministry executives' accountability.

Additionally, some roles are not consistently defined between the Standard and the Guidelines, while other roles have limited responsibilities identified. Examples of these roles include the Independent Reviewer and Business Owner.

It would be beneficial for the OCIO to clarify the key roles and responsibilities that are needed to ensure the success of the Government's compliance activities and to guide ministries to identify an executive sponsor with the appropriate level of authority. A clearer presentation of roles and responsibilities will enhance understanding and help promote individual accountability to reach compliance, including effort prioritization and resource allocation.

Recommendations:

(7) The OCIO should engage with the appropriate parties to review CPPM and to strengthen ministry accountability over compliance with corporate IM/IT standards.

(8) The OCIO should enhance the clarity of key roles and responsibilities within the Critical Systems Standard and Guidelines.

2.2. Standard Awareness, Support and Training

Developing awareness and providing support through training and guidance enable individuals to develop their understanding of the Standard and the competencies necessary to fulfill their responsibilities. This helps clarify their roles and accountabilities, and assists with prioritizing tasks.

Standard Awareness

During the initial stages of the compliance activities in 2015/16, the OCIO actively promoted awareness across the Government about the Standard's purpose, value and impact to ministries. For instance, the Office:

- Delivered a presentation to Ministry Chief Information Officers in September 2015, which provided them with an overview of the Ministry Coordinator role, compliance timeframe and registration requirements.
- Held workshops in the fall of 2015 that provided Ministry Coordinators with an overview of the benefits, impacts, and roles.
- Presented the Standard to the Business Continuity Management Program Advisory Committee in January 2016.

This formal awareness effort was lessened after the implementation of the Standard. As awareness training mostly targeted Ministry Coordinators at the beginning, there has been a noticeable decrease in awareness in ministries who had experienced staff turnover.

Business Owners and ministry executives, who are ultimately accountable for managing the business impacts of IM/IT disruptions, have not been the target audience of the Office in its efforts to raise awareness of the Standard. Obtaining support from those levels would help ministries prioritize compliance efforts according to risks and promote a "tone at the top" in favour of compliance.

OCIO Communication and Support

The OCIO has attempted to maintain channels of communication with ministries through emails, meetings, and workshops with the community of Ministry Coordinators with limited success. Efforts also included assigning an OCIO Coordinator to provide support to ministries when requested and the implementation of a website to promote the sharing of practices between ministries.

At the time of this review, ministries provided the following feedback:

- Ministries would prefer more effective communication with the Office. Some of the issues raised by ministries have yet to be incorporated into the Standard and Guidelines.

- Ministries would like to receive more tailored guidance, clarifications, training and templates from the Office, especially to meet technical requirements under the Standard.

Communication issues between the OCIO and ministries have also impacted the accurate assessment and monitoring of compliance over time as ministries' annual assessments have not been submitted to the Office. A Communication Protocol is being developed by the OCIO to support compliance and cultural change.

In an effort to improve communications and begin to address ministries' concerns, the Office initiated a Community of Practice in November 2018. They intend to continue this initiative and encourage ministries to chair its sessions to foster mutual support. Ministries would benefit from using the Community of Practice to identify common challenges, showcase existing good practices, and delegate ministry champions across Government to assist other ministries. This would help develop good practices and inform different roles within ministries to take ownership over the compliance activities.

Ministry Training

A few ministries have taken some actions to help obtain internal stakeholders' buy-in, such as email communications and workshops. However, ministries have assumed that the Standard awareness and training activities were the responsibility of the OCIO. Each ministry is accountable to ensure internal buy-in and provide necessary training and guidance to its staff.

It would be important for the OCIO to clarify its role within the compliance process and the types of support it can provide to ministries (e.g., training, directing ministries within the compliance process and to other existing support within the OCIO). Ministries would benefit from developing training activities tailored to their needs with support from the Office. This would accelerate and sustain ministry compliance activities and successes. The Community of Practice could be the right forum to co-develop and execute these activities between ministries facing similar challenges.

Recommendations:

(9) The OCIO should finalize the development of the Communication Protocol with ministries to raise awareness of the Critical Systems Standard and support compliance.

(10) The OCIO should engage ministries to further develop the Community of Practice to benefit different audiences.

3.0 Monitoring and Reporting

Monitoring and reporting activities can be established to accurately assess the Province's progress towards compliance with the Standard. These activities would encompass performance measurement targets, risk identification and mitigation, and reporting of reliable information for decision making. They would also support and encourage accountability, oversight and ownership of risks.

3.1. Monitoring and Reporting Processes

The Standard and Guidelines contain requirements that lay the foundation for ministries and the OCIO to monitor and report on compliance activities. The key requirements are:

- Ministries must register their critical systems in the OCIO's asset registry with a compliance target date and keep this information current.
- At registration, ministries must submit a compliance assessment and a roadmap for endorsement, then report annually on their progress.
- Quarterly reports on the effectiveness of compliance activities must be provided to senior executives at the OCIO and ministries.

In May 2018, the OCIO defined a validation process to ensure compliance with the Standard. As part of this process, an Independent Reviewer, selected by ministries, uses the Checklist to attest evidence of compliance. The OCIO receives the attested Checklist and verifies whether the review was completed appropriately before deeming the critical system as compliant.

While independent reviews are required, it is not reperformed regularly (e.g., every 2 to 3 years). The absence of a regular review process for compliance impacts the efforts in maintaining system availability as required by the Standard.

Corporate Level

At the corporate level, the Standard requires a Summary Report to be distributed to the Assistant Deputy Minister-OCIO Enterprise Services and Ministry Chief Information Officers. At the time of this review, recent reports have not been routinely made available to ministries and other senior executives within the OCIO.

The OCIO reports statistics on critical systems and its compliance status, including target dates. While these statistics are obtained from the asset registry, ministry information is not always accurate or complete. Furthermore, the Office has yet to define a procedure to collect ministries' compliance assessments and roadmaps.

The OCIO tracks these statistics over time for trend analysis but generally, qualitative information is less prevalent in its Summary Reports. Root cause analyses, reports on incidents, performance indicators, and other elements of risks are not reported in relation to critical systems. The OCIO's reports could be enhanced to provide the executives and key stakeholders with sufficient information to assess progress towards compliance.

Ministry Level

There is inconsistency with the frequency and quality of information regarding ministries' compliance progress reporting to their executives. This was caused by the following factors:

- absence of roles relevant to executive oversight in the Standard;
- complications faced by System Owners when compiling information required to report on a system's status; and
- Ministry Coordinators' limited authority to access system status information.

Without regular and consistent monitoring and reporting within ministries, there is a risk that compliance efforts will diminish over time. Consequently, the information that the OCIO currently has is not always accurate and up to date.

Opportunities exist for the OCIO to consult with ministries and establish an integrated process to regularly report on the effectiveness of the Province's compliance activities. This process would account for the OCIO's and ministries' needs and include quantitative as well as qualitative information. This would help the executives take remediating actions when necessary.

Recommendations:

(11) The OCIO should implement a requirement for ministries to perform independent reviews on a regular basis to ensure critical systems remain compliant with the Critical Systems Standard.

(12) The OCIO should ensure that regular reports on critical systems and the impact of non-compliance are regularly distributed to ministry executives and key stakeholders.

3.2. Reporting Tool

According to the Standard and Guidelines, the OCIO is required to maintain a formal inventory of all critical systems for the Province. The OCIO uses an asset registry tool to:

- register and maintain a list of identified critical systems;
- collect ministry information on critical systems; and
- monitor and report on compliance.

The OCIO has provided ministries with guidance on how to enter and maintain information in the asset registry. However, a process has not been developed and documented to ensure that critical system information remains accurate over its lifecycle. As a result, roles and responsibilities to maintain the quality of information in the asset registry are not always well understood by ministries, since they tend to see the OCIO as the owner of the information stored in this tool.

While the asset registry has an audit trail to identify history of changes and their authors, the tool has limited controls in place to prevent the entry of inconsistent, inaccurate and incomplete information. In addition, the asset registry does not map dependencies between critical systems. This information would help determine the priority order that critical systems need to be recovered, should a disruption impact several mutually dependent systems.

It would be beneficial for the OCIO to define a process to manage the critical system information lifecycle and explore the features available in the asset registry. If the necessary features are not available, it may be beneficial to explore alternatives that would better support the registration process, monitoring requirements and system prioritization.

Recommendation:

(13) The OCIO should define a process to further enhance the critical system information lifecycle and address data related issues associated with the asset registry.

Appendix 1 - Detailed Action Plan

Rec. #	Recommendations	Management Actions Planned or Taken
1.	The OCIO should further align the Critical Systems Standard with CPPM.	• Develop recommended policy change(s) that will specify Critical Systems accountability at ministry level (by August 2019).
2.	The OCIO should engage Emergency Management BC to align methodologies for identification and prioritization of ministries' critical services and information systems.	• Develop a sub-section of the Critical Systems list, agreed upon by key central agencies, which identifies key mission critical systems and incorporates key enabling IT systems, eg: PayBC (by June, 2019).
3.	The OCIO should further integrate the Critical Systems Standard with IM/IT security initiatives and leverage available hosting services to support ministries' progress towards compliance.	• Establish close collaboration with Information Security Branch to ensure ongoing alignment between CSS and Information Security policy and standards. • Based on the classification of program data, provide a list of relevant links on the CSS that will direct programs to other supporting resources which include specific physical and IT security protocols, along with hosting services that support application and database recoverability (by July, 2019).
4.	The OCIO should ensure the consistency of the Critical Systems Guidelines and Compliance Checklist with the Critical Systems Standard.	• Amalgamate the checklist into the guidelines and develop a version control process that ensures synchronization between the standard and guidelines (by August, 2019).
5.	The OCIO should enhance consultation with ministries to address the root causes of the low compliance rate and improve adherence to the Critical Systems Standard.	• Collaborate with ministries, including via the Critical Systems Standard Community of Practice, to develop a list of actions that will increase the compliance of all ministries to the CSS (by October, 2019).

The Detailed Action Plan represents the Office of the Chief Information Officer's response to the issues identified and the 13 recommendations detailed in the 2019 report: *Review of Critical Systems Standard*. This document was prepared by the Office of the Chief Information Officer and submitted to Internal Audit & Advisory Services to be included as an Appendix to the report.

Rec. #	Recommendations	Management Actions Planned or Taken
6.	The OCIO should update the Critical Systems Standard to leverage third-party reviews for outsourced critical systems.	• Develop specific language in the CSS that references policy and the need to conduct reviews of the mission critical systems' compliance to the standard (by August, 2019). • Engage an independent audit company to conduct annual spot audits on progress towards compliance for our most critical systems (by October, 2019).
7.	The OCIO should engage with the appropriate parties to review CPPM and to strengthen ministry accountability over compliance with corporate IM/IT standards.	• Develop an MOU amongst key stakeholders that details required policy change(s) that will clarify and strengthen IM/IT standards accountability at ministry level – collaborate with OCIO IM/IT Policy team and owner of CPPM (Financial Management Branch, Comptroller General – referred by IAAS) (by September, 2019).
8.	The OCIO should enhance the clarity of key roles and responsibilities within the Critical Systems Standard and Guidelines.	• Develop a section in the CSS that describes governance and specifically details the roles and responsibilities of the ministry and the program area responsible for each critical system (by September, 2019).
9.	The OCIO should finalize the development of the Communication Protocol with ministries to raise awareness of the Critical Systems Standard and support compliance.	• Create a communication framework for engaging the broader government community regarding the importance of continuous adherence to the Critical Systems Standard (by June, 2019).

The Detailed Action Plan represents the Office of the Chief Information Officer's response to the issues identified and the 13 recommendations detailed in the 2019 report: *Review of Critical Systems Standard*. This document was prepared by the Office of the Chief Information Officer and submitted to Internal Audit & Advisory Services to be included as an Appendix to the report.

Rec. #	Recommendations	Management Actions Planned or Taken
10.	The OCIO should engage ministries to further develop the Community of Practice to benefit different audiences.	• Create an engagement framework that will bring key personnel together for the purposes of reviewing current and future practice as well as application status and roadmap (by June, 2019). • Develop Terms of Reference for the CSS Community of Practice (by August, 2019).
11.	The OCIO should implement a requirement for ministries to perform independent reviews on a regular basis to ensure critical systems remain compliant with the Critical Systems Standard.	• Develop specific language in the CSS that references policy and the need to conduct regular reviews of the mission critical systems' compliance to the standard (by August, 2019). • Engage an independent audit company to conduct annual spot audits on progress towards compliance for our most critical systems (leverage IAAS qualified list) (by October, 2019).
12.	The OCIO should ensure that regular reports on critical systems and the impact of non-compliance are regularly distributed to ministry executives and key stakeholders.	• Further develop the work that is being conducted on the C55 executive reporting to include an impact assessment of the business risk of non-compliance (by November, 2019). • Establish process for ministries to maintain accuracy of their Critical Systems information (by August, 2019).

The Detailed Action Plan represents the Office of the Chief Information Officer's response to the issues identified and the 13 recommendations detailed in the 2019 report: *Review of Critical Systems Standard*. This document was prepared by the Office of the Chief Information Officer and submitted to Internal Audit & Advisory Services to be included as an Appendix to the report.

Rec. #	Recommendations	Management Actions Planned or Taken
13.	The OCIO should define a process to further enhance the critical system information lifecycle and address data related issues associated with the asset registry.	• Create streamlined attribute criteria and align the collection and maintenance of that data with the CSS governance, roles and responsibilities section (by November, 2019).

The Detailed Action Plan represents the Office of the Chief Information Officer's response to the issues identified and the 13 recommendations detailed in the 2019 report: *Review of Critical Systems Standard*. This document was prepared by the Office of the Chief Information Officer and submitted to Internal Audit & Advisory Services to be included as an Appendix to the report.