REPORT ON:

Information Technology Change Management Phase I

IAAS | INTERNAL AUDIT & ADVISORY SERVICES

BRITISH COLUMBIA | Ministry of Finance

Table of Contents

Section Page No.

Executive Summary and Overall Conclusion

The Government of British Columbia (Government) increasingly relies on information technology (IT) to provide services to British Columbians. Changes made to the Government's IT environment are required to follow formal processes and procedures. This minimizes the risk of disruption and ensures changes are properly approved.

Within the Ministry of Citizens' Services (CITZ or Ministry), the Enterprise Services Division manages IT changes to the Government's shared IT infrastructure and enterprise systems (e.g. Email, SharePoint) while the Information Management Branch (IMB) manages IT changes to many of the Ministry's IT systems. IMB's responsibility is separate from the Enterprise Services Division's management of the shared IT infrastructure and enterprise systems.

Enterprise Services Division's Process

The Enterprise Services Division has documented its IT change processes and procedures (the Enterprise Services Procedures). The Enterprise Services Procedures cover the process of a Request for Change (RFC) from creation until closure. They also define roles and responsibilities, including the establishment of a change advisory board to oversee IT changes. The Enterprise Services Procedures do not provide details on how changes must be prepared by the Enterprise Services Division's eight Service Delivery Units (SDUs) and moved between the stages that precede final implementation (i.e., planning, developing, testing). Due to the variety of technology, changes are planned, developed and tested as part of SDUs' processes. SDUs have specialized and evolving technical knowledge that cannot be documented by another area. However, the Enterprise Services Procedures provide SDUs with some key requirements and sets the expectation that SDUs develop standards and procedures to address these stages of a change. Most SDUs have limited documentation to guide how these various stages should be managed.

The Enterprise Services Division's process enables SDUs to log their RFCs in the change management application called ITIMS and receive approval before implementing the changes in the shared IT infrastructure and enterprise systems. SDUs are required to record the results of their change assessments (i.e. risk, impact, exposure) in the RFCs. Through predefined rules in ITIMS, this information is used to assign approvers for RFCs. SDUs do not consistently use the criteria of the Enterprise Services Procedures to assess their changes.

According to the Enterprise Services Procedures, SDUs must develop documentation about their changes outside of ITIMS to allow for additional review. While process maturity varies, SDUs generally rely on their staff's experience and the key information contained in ITIMS to conduct changes. Depending on the nature of a change, SDUs would develop documentation to support the change.

Every week, Change Review Groups, including the change advisory board, meet to review the list of scheduled changes. Requirements for their review and approval vary between documents. Changes are reviewed; however, focus is given to unusual and high-risk RFCs as determined by the Change Managers. In addition, Change Review Groups' approvals are not clearly documented in minutes or in ITIMS.

The Enterprise Services Procedures also require that changes go through a post-implementation review to confirm that they have met their objectives. The Enterprise Services Procedures provide limited requirements or guidelines to SDUs on how to conduct this review. Post-implementation reviews vary depending on the nature and exposure of the change. Therefore, SDUs determine how to conduct these reviews. There are opportunities for the Enterprise Services Division to strengthen its process particularly around change assessment, review and approvals by Change Review Groups, post-implementation review. It should also clarify responsibilities and internal control requirements for SDUs.

The Change Management Team oversees change activity and produces monthly activity reports for SDUs' Executive Directors. As SDUs are also expected to monitor their own performance, Change Management Team's reports do not define performance targets or provide trend analysis. Therefore, there is an opportunity for the Enterprise Services Division to strengthen its performance monitoring.

ITIMS and ServiceNow

The Enterprise Services Division uses ITIMS to administer RFCs from creation to closure. This legacy application has limitations that impact the performance of the process, including accessibility for approvers and limited configuration management capacity. The Enterprise Services Division is implementing a new application, ServiceNow IT Service Management, to replace ITIMS. It plans to migrate the current change management process into the new application before deploying further capabilities. The compatibility of some of the new configuration management capabilities with existing IT systems has not yet been assessed.

IMB's Processes

IMB's scope of operations has evolved over time, following Government' successive reorganizations. IMB follows different processes for each business area it supports. Some of these processes were initially developed outside IMB and have remained separate processes with dedicated application management teams and various change management applications. Procedures have been documented for only one of IMB's processes.

IMB's staff are members of change advisory boards of various business areas, while changes for IMB's internal operations are not overseen by a committee. There are no common practices between the existing change advisory boards in regard to terms of reference, agenda setting, documentation of minutes and decisions or change approval. The lack of process standardization and documented processes has resulted in the different teams following processes with various levels of maturity. For areas supported by IMB for which procedures have not been developed, processes and their expectations in terms of assessments, change documentation, reviews and approvals vary according to the area or IT system supported and the nature of the changes.

IMB uses a variety of applications to support its IT change management processes, ranging from a dedicated change management application, a ticket tracking application, to emails. Some of these applications have limited capability and may not capture all necessary information in a consistent way. Using different processes and applications creates a risk that IMB does not consistently apply appropriate change management practices across its service areas. Therefore, it would be beneficial that IMB standardizes and documents its IT change management processes, as well as consolidates its IT change management applications.

Overall Conclusion

The Enterprise Services Division has established an IT change management process and a procedure for changes impacting the Government's shared IT infrastructure and enterprise systems. While these follow best practices, there are opportunities to improve the process. Clarifying expectations and documenting them in the form of defined responsibilities and detailed requirements will help enhance the maturity of the SDUs' processes. Defining criteria to initiate reviews and approvals, and more formally documenting these activities will ensure that changes receive the appropriate level of scrutiny.

While the implementation of a new change management application may improve the consistency of change submissions, there is also an opportunity for the Enterprise Services Division to leverage this implementation to help address the process challenges identified by this review.

IMB follows a variety of change management processes that support different business areas. Process maturity varies as processes are not standardized and procedures are not documented for most of them. Opportunities exist for IMB to standardize its processes and procedures around the stages of IT changes.

We would like to thank the management and staff at the Ministry of Citizens' Services, who participated in and contributed to this review, for their cooperation and assistance.

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

Introduction

The Government of British Columbia (Government) increasingly relies on information technology (IT) to provide services to British Columbians. The Government's IT environment seldomly remains static, as multiple factors can trigger changes. These factors include the evolution of business needs, regulations and technologies, as well as adverse incidents.

Changes made to the Government's IT environment are required to follow formal processes and procedures. IT changes should be appropriately assessed, planned, tested and approved before they are implemented. This process provides key stakeholders (e.g. technical teams and business users) with the necessary information to oversee IT changes. This minimizes the risk of disruption to IT systems and related infrastructure, and ensures changes are properly approved.

The Ministry of Citizens' Services (CITZ or Ministry) provides a range of services to citizens, businesses and public sector organizations. This includes, amongst others, Service BC, property management, and Freedom of Information. Through its Office of the Chief Information Officer, the Ministry also provides the shared IT infrastructure used by the Government and the broader public sector. This shared IT infrastructure consists of key technology solutions, including data centre facilities, hardware (e.g. servers, workstations), network, and the enterprise architecture and security services (e.g. firewalls, intrusion detection systems) to support it, as well as enterprise systems such as Email and SharePoint.

Several areas within CITZ manage the Ministry's IT systems, the Government's shared IT infrastructure, and their respective IT changes, as follows:

- the Enterprise Services Division manages the Government's shared IT infrastructure and enterprise systems;
- the Information Management Branch (IMB) manages some of the Ministry's IT systems, primarily applications; and
- other business areas manage their own applications, such as Service BC and Queen's Printer Publishing Services.

Purpose, Scope and Approach

The purpose of this review was to assess the adequacy of the processes followed by the Enterprise Services Division for managing changes to the Government's existing shared IT infrastructure and enterprise systems. It also assessed the adequacy of the processes followed by IMB for managing changes to Ministry specific existing systems.

The review evaluated and, as appropriate, made recommendations relating to the following:

- whether the processes designed by the Enterprise Services Division and IMB follow best practices for managing regular and emergency changes;
- whether the changes managed by the Enterprise Services Division and IMB comply with their established processes; and
- how the implementation of ServiceNow's IT change management module is expected to enhance the Enterprise Services Division's current practices.

Our approach included:

- reviewing process-related documentation;
- conducting interviews with key management and staff; and
- judgementally sampling IT changes.

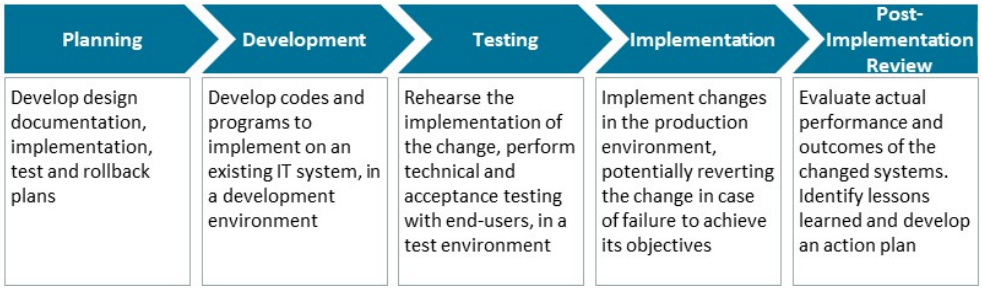
The review was conducted by Internal Audit & Advisory Services (IAAS), Ministry of Finance, and fieldwork was completed in November 2019.

Future phases of the review will cover ministries of the natural resource and social sectors.

1.0 IT Change Management Process

Changes to IT systems happen for multiple reasons; evolution of technology, business needs and regulations are some of the factors that trigger IT changes. Before being implemented into a production environment, IT changes must be prepared and moved between stages, as follows:

Stages of an IT Change



Source: IAAS, adapted from COBIT 2019 framework

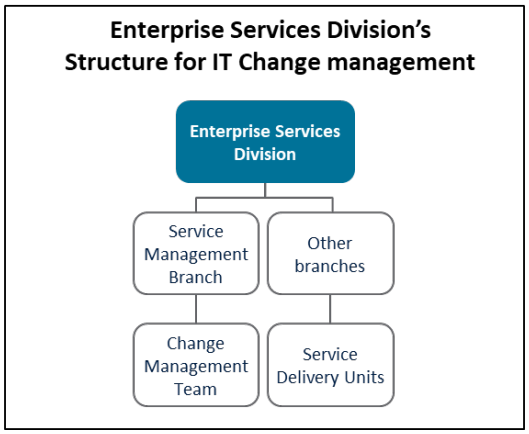
The purpose of IT change management is to enable fast and reliable delivery of IT changes and mitigate the risk that they negatively impact the stability and integrity of the IT environment. An effective process manages all changes in a controlled manner, including emergency changes. Such a process would ensure that changes are:

- assessed and prioritized to enable appropriate review and approval based on priority, risk and benefit, through the submission of a Request for Change (RFC);
- planned, developed, tested and approved before implementation; and
- implemented according to plans or rolled back if necessary, to limit any negative impact on services. Rolling back a change is the process of restoring an IT system to a previous state, typically to recover from an error.

The Government has an Operations Security Standard that defines key principles for IT change management. Ministries must adopt and further develop these principles within their IT change management procedures.

Ministry's Processes

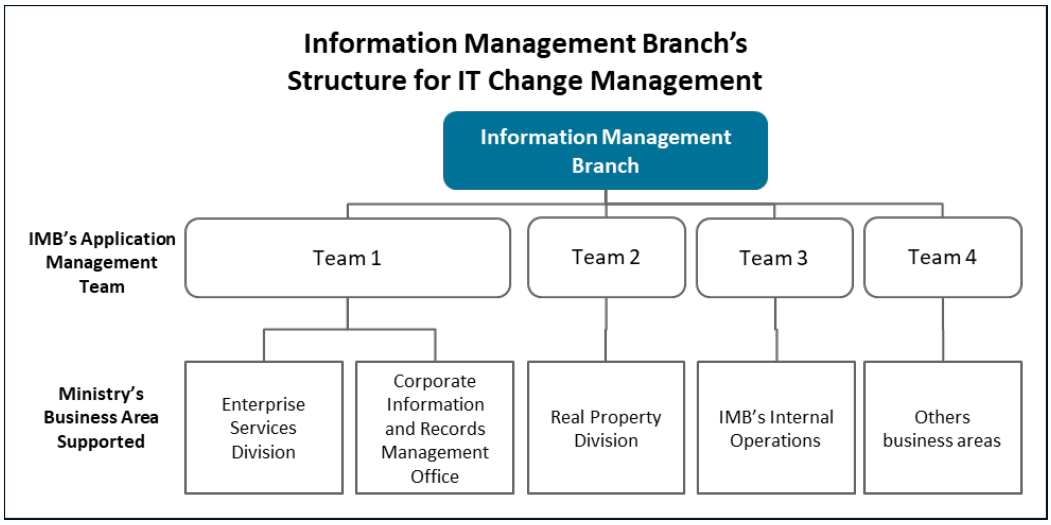
Within the Ministry, two service areas manage most IT changes: the Enterprise Services Division and IMB. Within the Office of the Chief Information Officer, the Enterprise Services Division manages changes to the shared IT infrastructure and enterprise systems used by the Government and the broader public sector. Within the division, eight Service Delivery Units (SDUs) manage various components of the shared IT infrastructure and enterprise systems. They include various service delivery teams and their service providers. The Service Management Branch provides the process that SDUs are to follow to submit their RFCs and receive approvals. The following chart illustrates the structure of the Enterprise Services Division for IT change management:



Source: IAAS, adapted from OCIO Enterprise Services Division

IMB manages IT changes to many of the Ministry's IT systems. These systems include applications used by the Corporate Information and Records Management Office (CIRMO), the Real Property Division and Enterprise Services Division. IMB's responsibility is separate from the management of the Government's shared IT infrastructure and enterprise systems by the Enterprise Services Division. IMB's scope of operations has evolved over time, following Government's successive reorganizations. Some of IMB's IT change management processes were initially developed outside IMB and have remained separate processes since they joined the branch. IMB consists of several teams that support specific business areas.

The following chart illustrates the structure of IMB for IT change management:



Source: IAAS, adapted from Information Management Branch

2.0 Enterprise Services Division

For an IT change management process to be effective several components must be present, including a defined process and a governance structure to oversee it.

2.1 Governance

An appropriate governance model defines activities to evaluate changes, assigns roles with authority, and ensures performance is monitored. A clear governance structure for the implementation and monitoring of IT change management processes includes documented procedures. This helps define objectives and how to achieve them consistently; and roles and responsibilities to establish accountability.

Procedures

Documented procedures allow for a clear and consistent approach to making changes. These documents provide staff with the requirements and expectations they need to manage changes and enable management to review how operations are conducted.

The Enterprise Services Division has documented its IT change management processes and procedures (the Enterprise Services Procedures). The Enterprise Services Procedures cover the process of an RFC from creation, through review and approval, until closure within the change management application called ITIMS.

The Enterprise Services Procedures provide SDUs with some key requirements on how changes must be prepared by SDUs and moved between the stages that precede final implementation (i.e. planning, developing, testing). Due to the variety of technology, changes are planned, developed and tested as part of SDUs' processes as SDUs have the specialized and evolving technical knowledge. The Enterprise Services Procedures set the expectation that SDUs develop standards and procedures to address these stages of a change. Most SDUs have limited documentation to guide how these various stages of the change management process should be managed.

Roles and Responsibilities

Defining roles and responsibilities and setting up a committee to oversee IT changes and the related processes are essential for the successful management of IT changes. It is also a good practice to use change advisory boards (CAB) to bring business and IT stakeholders together to review changes before their implementation.

Some of the key roles and responsibilities in the Enterprise Services Division's IT change management process are as follows:

- SDUs include various service delivery teams (e.g. network, hosting, security) and their service providers. They plan, develop, test and implement the IT changes on their services. They initiate and approve RFCs in ITIMS.

- Change Review Groups are made up of representatives of SDUs. They review and approve changes before implementation. Some of these groups focus on the technical impact of changes while the CAB focuses on the business impact of changes. They meet on a weekly basis.

- Within the Service Management Branch, the Change Management Team manages the IT change management process. It reviews RFCs submitted by SDUs, chairs Change Review Groups' meetings. It also reviews implemented changes before closing RFCs.

The Enterprise Services Procedures also define an Executive CAB that is to be invoked when regular approvers of a change escalate to one or some of the Enterprise Services Division's Executives. This committee was recently established and generally does not convene as a committee to review changes. The Executive CAB can also be invoked to make emergency decisions when major incidents arise. Therefore, the Enterprise Services Division should clarify and document the roles, responsibilities and procedures associated with the Executive CAB, including emergency changes.

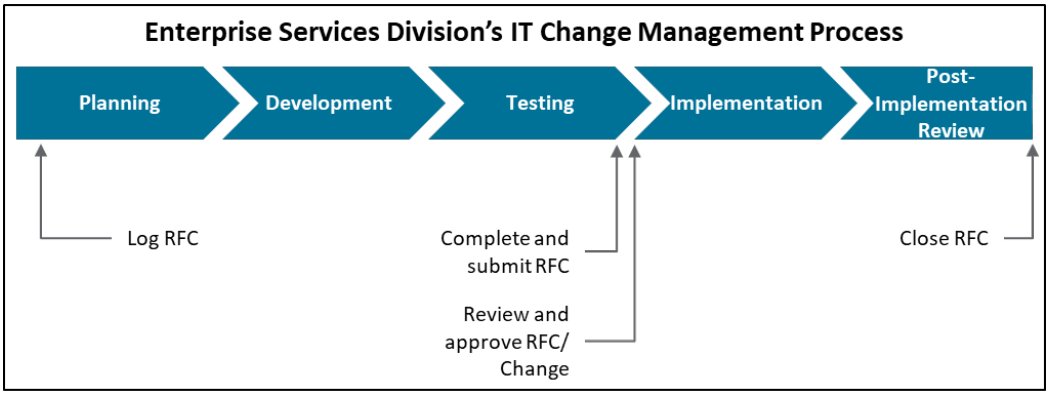
Recommendation:

(1) **The Enterprise Services Division should clarify and document the roles, responsibilities and processes associated with the Executive CAB, including emergency changes.**

2.2 Processes

The Service Management Branch and its Change Management Team manage the Enterprise Services Division's IT change management process, through which approximately 1,200 changes a month are submitted for implementation in the shared IT infrastructure and enterprise systems.

This process enables SDUs to log their RFCs in the change management application ITIMS and receive approval before implementing them. The following chart presents the milestones of a regular IT change and the related RFC in the Enterprise Services Division's change management process.



Source: IAAS, adapted from Enterprise Services Division

The Enterprise Services Division has defined the processes for standard and emergency changes, as follows:

- Standard RFCs are pre-approved in ITIMS. Standard change cases are submitted to the Change Management Team and Change Review Groups for approval.

- SDUs may implement emergency changes without receiving formal approvals when an IT service is down, or degraded and is presenting a risk for the business service. Such changes must be logged and approved in ITIMS after implementation.

RFC Creation & Change Assessment

To initiate the Enterprise Services Division's change management process, SDUs must log their change in ITIMS. They are required to enter key information about their change in the RFC including:

- a description of the change and the asset to be changed;
- the methodology and roll-back method;
- staff assigned to the change; and
- a risk analysis, impact, exposure and priority assessments.

Based on the above information, ITIMS uses the predefined rules to assign approvers for RFCs. These rules depend on the affected IT system and risk-related factors that SDUs enter in their RFCs. Therefore, accurate and consistent risk assessments of changes are essential to ensure that changes receive the review and approval in adequation to their risk level.

SDUs advised that assessment criteria are not clearly defined in the Enterprise Services Procedures and are not consistently used to assess their changes. The current process relies on the Change Management Team to identify and correct inaccurate or inconsistent assessments. It would be beneficial for the Enterprise Services Division to review its assessment criteria and develop further guidance to help SDUs assess their changes.

Change Planning and Testing

According to the Enterprise Services Procedures, SDUs must develop documentation about their changes, including implementation and testing plans as well as have testing results outside of ITIMS to allow for additional review. While process maturity varies, SDUs generally rely on their staff's experience and the key information contained in ITIMS to conduct changes. SDUs have partially documented their internal change management process and operational procedures. Depending on the nature, impact and parties involved in a change, SDUs would develop documentation to support the change. Most documentation is not attached to RFCs in ITIMS for review and therefore they may not be reviewed by Change Review Groups.

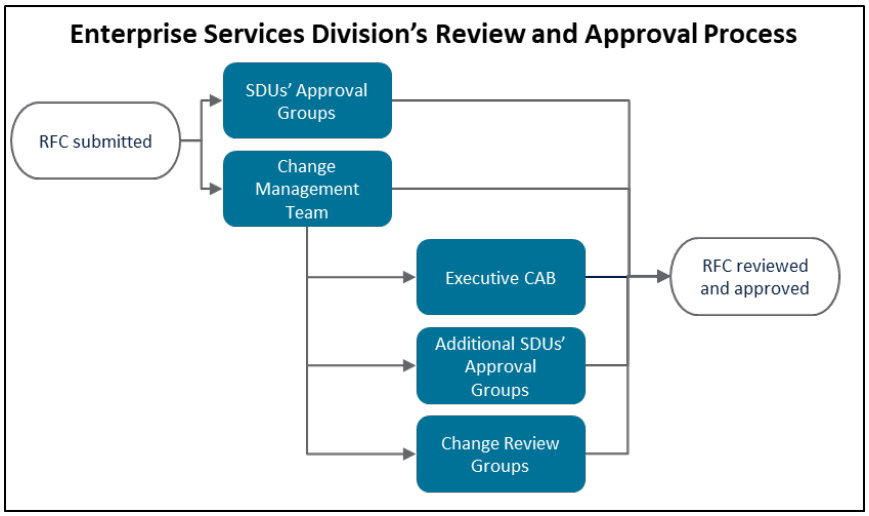
The Change Management Team and Change Review Groups expect SDUs to perform sufficient testing and planning for their changes. However, the Enterprise Services Procedures do not provide details on these requirements and SDUs' responsibilities. In early 2019, the Government experienced some significant outages on its shared IT infrastructure. To prevent further unexpected outages, the Service Management Branch cancelled all current significant changes and required SDUs to re-assess these changes. They communicated expectations for more robust planning to SDUs.

The Change Management Team has noticed improvements in the content of RFCs. Some SDUs provide extra information in significant RFCs. The Service Management Branch should clarify its expectations by providing guidance and defining requirements for planning and testing in the Enterprise Services Procedures. This includes SDUs' responsibilities, internal controls over changes, and documentation necessary to support RFC submissions.

Change Management Team's Review and Approval

Once an SDU submits an RFC, a notification is sent through ITIMS to the approval groups. By default, approval groups include the Change Management Team and various groups of SDUs' management and staff.

The following chart illustrates the review and approval process:



Source: IAAS, adapted from the Enterprise Services Division

The Change Management Team reviews the information contained in the RFCs. They assess the reasonableness of the request and SDUs' assessments. Change Managers may request further information from SDUs and adjust the change assessments. As described above, criteria to assess changes are not always consistently applied by SDUs; as a result, the Change Management Team plays a key role in detecting inconsistencies within RFC assessments.

Change Managers may also adjust the list of approvers for an RFC and require broader approval than the default approval groups, such as the Executive CAB. Change Managers may also consider that a technical review is not required due to the risk profile of the change (e.g. change impacting a single client). Removals of approvers are not automatically recorded by ITIMS. It is good practice to record these decisions to establish accountability in the IT change management process.

At the end of their review, Change Managers approve or reject RFCs in ITIMS. Reasons for rejection can include impracticability, risk considered too high, or lack of preparation. SDUs are also required to sign off their RFCs in ITIMS.

Change Review Groups

Every week, Change Review Groups meet to review the list of changes scheduled for the upcoming two weeks. Change Review Groups are generally not set as default approval groups in ITIMS.
The requirements for their review and approval vary between documents. Changes are reviewed; however, focus is given to unusual and high-risk RFCs as determined by the Change Managers. In addition, Change Review Groups' approvals are not clearly documented in minutes or in ITIMS. This resulted in lack of documentation to confirm whether RFCs received proper approvals prior to implementation.

Once changes are assessed against defined criteria, the Enterprise Services Division should define risk-based criteria that determine the reviews and approvals required for a specific RFC before its implementation. The level of review and approval can be based on the overall risk carried by the change. Any approval removals should be recorded.

Change Implementation Review

RFCs must receive all approvals in ITIMS before SDUs may implement changes. After implementation, the Enterprise Services Procedures require a post-implementation review to confirm that the change has met its objectives. The Enterprise Services Procedures provide limited requirements or guidelines to SDUs on how to conduct this review. Post-implementation reviews vary depending on the nature and exposure of the change. Therefore, SDUs determine how to conduct these reviews. In addition, Change Management Team relies on the limited notes left by implementers (e.g. "done", "change completed") in ITIMS to determine the final status of RFCs (e.g. successful change, change without approval).

In case of a significant event (e.g. incident triggered by a change), the Change Management Team may lead a review to find the root cause of the event and define recommendations. They track and report on the implementation of these recommendations. Criteria to initiate this review are not defined.

A post-implementation review is used to determine whether the change has met the expectations of its key stakeholders and to identify lessons learned. The Enterprise Services Division should clarify post-implementation review requirements in the Enterprise Services Procedures and define the criteria to determine when a significant event review is required.

Recommendations:

(2) **The Enterprise Services Division should review its assessment criteria and approval process and develop guidance to help SDUs assess their changes.**

(3) **The Enterprise Services Division should clarify SDUs' responsibilities and define requirements for SDUs' internal controls over changes, including the documentation necessary to support change planning and testing.**

(4) **The Enterprise Services Division should define risk-based criteria that determine the reviews and approvals required for a specific RFC.**

(5) **The Enterprise Services Division should clarify post-implementation review requirements in the Enterprise Services Procedures and define the criteria to determine when a significant event review is required.**

2.3 Application and Performance Monitoring

Technological resources can contribute to the performance of the IT change management processes. Change management applications can support change logging, assessment, review and approvals. They can also provide key information for the performance monitoring of the change management processes.

Change Management Application

The Enterprise Services Division uses ITIMS to administer RFCs from creation to closure. ITIMS is an IT service management application that is no longer supported by its vendor. This legacy application has several limitations that impact the performance of the IT change management process, including:

- Accessibility: ministries do not have access to ITIMS and some internal approvers prefer emailing their approvals. Manually, approval emails are attached to RFCs and Change Management Team enters the required approvals in ITIMS.

- Change assessment: ITIMS has limited configuration management capacity to allow the Enterprise Services Division to identify how a change on one system may impact other systems.

The Service Management Branch is implementing a new IT service management application, ServiceNow IT Service Management, to replace ITIMS. It plans to migrate the current change management process into the new system before deploying further capabilities. This module is planned to be operational in fiscal year 2020/21.

Envisioned capabilities for the new application include the ability for staff to more consistently assess and report on the impact and risks of proposed changes through assessment questionnaires and configuration management features. While these additional capabilities may help reduce manual processes for the Change Management Team, most of the current process challenges will not be resolved by implementing a new application without refining the process.

Moreover, the compatibility of some of the new configuration management capabilities with the existing IT systems is also uncertain as the Service Management Branch has not yet assessed it. It would be beneficial for the Enterprise Services Division to assess the compatibility of ServiceNow IT Service Management's further capabilities with existing IT systems.

Performance Monitoring

Monitoring activities should be established to assess the performance and maturity of ministry processes and typically involve evaluating a process against a set of performance targets. The results of monitoring activities should be reported and may be used to support decision-making, accountability and oversight.

The Enterprise Services Procedures include the following monitoring and reporting requirements:

- the Change Management Team must perform trend monitoring and delivers management reports; and

- the CAB must monitor performance targets, service availability and progress in the implementation of recommendations.

The Enterprise Services Procedures also define a list of service level indicators, which include the number of changes resulting in incidents and changes implemented without approval, but they do not define performance targets.

The Change Management Team oversees change activity and produces a monthly Executive Report for SDUs' Executive Directors. It provides the number of RFCs closed during the period by their final status. It also reports on the implementation of recommendations from significant event reviews. Change Review Groups do not receive these reports. These reports are reviewed by Service Management Branch and SDUs' Executive, and may result in follow-up actions.

Service Management Branch expects SDUs to monitor their own performance, including defining their own performance targets and conducting trend analysis. Some SDUs use the Change Management Team's reports to monitor the performance of their service providers on change management. They have also defined change management performance targets.

Opportunities exist for the Enterprise Services Division to strengthen its performance monitoring process. This monitoring process should define performance targets, frequency of reports, and who receives the reports. For instance, tracking the number of emergency changes and rolled-back changes over time would help management assess how the change management process is evolving, define performance targets that teams can work towards and determine corrective actions where necessary. Without monitoring process performance or defining performance targets for all areas, a risk exists that the IT change management processes do not meet expectations.

Recommendation:

(6) **The Enterprise Services Division should strengthen its performance monitoring and reporting process.**

3.0 Information Management Branch

IMB manages changes to many Ministry IT systems, including applications used by the CIRMO, the Real Property Division and Enterprise Services Division, as well as IMB's internal operations. Unlike changes managed by the Enterprise Services Division, which may potentially impact all ministries and Broader Public Sector, most changes managed by IMB would impact a smaller number of business areas.

IMB's IT change management processes and their related applications were designed to support specific business areas. Some processes have followed their business areas throughout the Government's successive reorganizations. These different IT change management processes have remained separate with various levels of maturity and dedicated application management teams.

3.1 Governance

Governance defines activities to evaluate changes and assigns roles with authority. Documented procedures enable to define objectives, determine how to achieve them consistently, and establish roles and responsibilities.

Procedures

IMB follows different processes for each business area it supports. A procedure has been documented for the Real Property Division that covers both the RFC process and the key technical stages of an IT change (i.e. planning, development, testing and implementation). However, IMB has not documented its procedures related to the other business areas and internal operations.

The lack of standardization and documented processes within IMB has resulted in the different teams following processes with various levels of maturity and lacking awareness of each others' processes. It would be beneficial for IMB to document its IT change management processes.

Roles & Responsibilities

Roles and responsibilities for IT change management vary according to the processes. IMB does not have a dedicated team to administer its change management processes and relies on its application managers to administer and manage IT changes within their respective scopes.

IMB's staff are members of CABs of various business areas. IMB chairs the CAB for the Real Property Division and attends other CABs if requested by the business area. These CABs serve a single application or a business area. Changes for IMB's internal operations are not overseen by a committee. There are no common practices between the various CABs in regard to terms of reference, agenda setting, documentation of minutes and decisions or change approval.

Without adequate oversight, changes may be implemented without stakeholders being fully aware. IMB should ensure all changes within its scope are reviewed by a committee of key stakeholders before implementation.

Recommendation:

(7) **The IMB should ensure that changes are reviewed and approved by a committee of key stakeholders before implementation.**

3.2 Processes

Real Property Division

As presented above, the Real Property Division has documented procedures for its change management process. IMB receives RFCs from the Real Property Division directly in its change management application or through the team's service desk.

According to its procedure, IMB reviews incoming service requests and identifies the higher priority RFCs based on business priorities set by the Real Property Division's CAB. Higher priority requests must go through assessment by IMB, including a technical and resource assessment and a business impact assessment. Other RFCs are either recorded in the backlog for later consideration or rejected. RFCs that may go ahead are presented to the CAB for approval.

Once RFCs are approved by the CAB, IMB must develop a project plan. Further technical planning and development tasks are then assigned to an IMB Business Analyst and/or a Developer. Technical tests performed by IMB and user acceptance test performed by the Real Property Division's staff must be done in the test environment.

Once the Real Property Division has signed off on the user acceptance test in the change management application, IMB Change Manager must ensure that other key activities have also been signed off before notifying the Release Manager to implement the change.

After implementation, the Real Property Division must close its RFCs in the change management application, which indicates that the change is considered successful by the business side. Post-implementation reviews are performed for significant changes.

Other Processes

For other areas supported by IMB, change management processes (i.e. assessments, change documentation, reviews and approvals) are not documented and vary according to:

- the area or IT system supported: factors such as the involvement of a service provider, the responsibilities of the CAB, and the change management application utilized structure IMB's processes differently. CIRMO's service provider uses its own change management process with limited oversight from IMB; and
- the nature of changes: factors such as the impact of the change, the involvement of stakeholders, the inclusion of the change within a project, define various expectations within a same process.

Integration with Enterprise Service Division

As some of the changes planned and developed by IMB also affect the Enterprise Services Division's managed IT environment (i.e. changes to the Enterprise Services Division's applications and some of IMB's internal operations regarding the Ministry's infrastructure), IMB must log its RFCs in ITIMS for review and approval by Change Management Team and Change Review Groups. Supporting information is stored in two different systems and there is not always a clear linkage between the information developed by IMB in its applications and the RFCs that IMB logs in ITIMS.

In addition, a few IMB teams advised that they were not entirely familiar with the requirements of the Enterprise Services Division's change management process. This has resulted in not all changes being logged in ITIMS and changes being implementing without IMB ensuring that they had received required approvals.

Using different processes creates a risk that IMB does not consistently apply appropriate change management practices across its service areas. There are opportunities for IMB to standardize its IT change management processes and leverage the Operations Security Standard. This will help IMB demonstrate its alignment with best practices and measure its process maturity.

Recommendation:

(8) **The IMB should standardize its IT change management processes in alignment with the Operations Security Standard, and document them in procedures.**

3.3 Applications and Performance Monitoring

IMB uses a variety of applications to support its IT change management processes, ranging from a dedicated change management application, a ticket tracking application, to emails. These applications were determined by the business areas. Some of these applications have limited capability and may not capture all necessary information in a consistent way. For instance, the compulsory information and the structure to report risk assessments are different amongst the applications. IMB should consider consolidating its IT change management applications to help with its process standardization and performance monitoring.

IMB does not monitor the performance of its IT change management processes and provides minimal oversight to the CIRMO's service provider. Without performance monitoring, management may not be aware of the risks carried by the various IT change management processes. Therefore, it would be beneficial for IMB to monitor the performance of its IT change management processes.

Recommendations:

(9) **The IMB should consolidate its IT change management applications and consider leveraging an existing application within the Ministry.**

(10) **The IMB should monitor the performance of its IT change management processes.**

Appendix 1 – Summary of Recommendations

1	The Enterprise Services Division should clarify and document the roles, responsibilities and processes associated with the Executive CAB, including emergency changes.
2	The Enterprise Services Division should review its assessment criteria and approval process and develop guidance to help SDUs assess their changes.
3	The Enterprise Services Division should clarify SDUs' responsibilities and define requirements for SDUs' internal controls over changes, including the documentation necessary to support change planning and testing.
4	The Enterprise Services Division should define risk-based criteria that determine the reviews and approvals required for a specific RFC.
5	The Enterprise Services Division should clarify post-implementation review requirements in the Enterprise Services Procedures and define the criteria to determine when a significant event review is required.
6	The Enterprise Services Division should strengthen its performance monitoring and reporting process.
7	The IMB should ensure that changes are reviewed and approved by a committee of key stakeholders before implementation.
8	The IMB should standardize its IT change management processes in alignment with the Operations Security Standard, and document them in procedures.
9	The IMB should consolidate its IT change management applications and consider leveraging an existing application within the Ministry.
10	The IMB should monitor the performance of its IT change management processes.

Appendix 2 – Abbreviations

CAB	Change Advisory Board
CIRMO	Corporate Information and Records Management Office
CITZ or Ministry	Ministry of Citizens' Services
Enterprise Services Procedures	Enterprise Services Division's Processes and Procedures
Government	Government of British Columbia
IMB	Information Management Branch, Ministry of Citizens' Services
IT	Information Technology
ITIMS	Enterprise Services Division's change management application
RFC	Request for Change
SDUs	Service Delivery Units