Audit of Information Technology General Controls Internal Audit Report

Project 2021-6B315
April 2022

Table of Contents

Introduction

Context

Fisheries and Oceans Canada (DFO) safeguards Canada's waters and manages its fisheries and oceans resources. Its mission is to provide Canadians with economically prosperous maritime and fisheries sectors, more sustainable aquatic ecosystems, and safe, secure, and navigable waters. The Canadian Coast Guard delivers a range of services to Canadians, including search and rescue, icebreaking operations, maritime security, and environmental response.

To deliver its mandate, the Department relies on an extensive network of information technology (IT) which together supports the delivery of national and region-specific programs and services. As a federal government department, DFO must adhere to and comply with IT requirements and expectations set out in government-wide legislation, policies and directives – specifically, the Treasury Board policy and directive on *Service and Digital*, *Policy on Government Security*, and the *Directive on Security Management*. These instruments govern how federal departments and agencies manage information and data, information technology, service delivery and cyber security. Within DFO, the Chief Information Officer (CIO), who reported to the Assistant Deputy Minister of Human Resources and Corporate Services (HRCS) over the course of the audit, is responsible for the Department's IT function and is accountable for all departmental IT projects, including those within the Canadian Coast Guard (Coast Guard).[1] [2] At the time of writing this report, a new Chief Digital Officer had just been appointed into a newly created assistant deputy minister position. Organizational changes resulting from this appointment, including those affecting IT functions, had yet to be announced.

The Department's IT portfolio consists of slightly more than 400 applications, 39 of which are identified as mission critical or essential to the continuity of departmental operations and services. The majority of applications are managed and supported by the Information Management and Technology Services (IM&TS) Directorate.[3] A key role of IM&TS is to ensure that adequate controls over IT are in place and are functioning effectively within the Department. IT general controls are essential to protect and preserve the integrity of information and data, and to ensure compliance with applicable policies and standards.

IT general controls are defined as controls, other than application controls, that relate to the environment within which computer-based application systems are developed, maintained and operated, and that are therefore applicable to all applications.[4] IT general controls include policies, procedures and practices designed to provide assurance over the development and operation of IT and are applicable to all systems, applications and processes, access and security management, application development, and data backup and recovery. By contrast, controls specific to an individual application or process, referred to as application controls, are not considered part of IT general controls.

IT expenditures within DFO have increased by 59% overall in the past three years. From FY 2018-2019 to 2019-2020, IT expenditures increased by 31% from $104.3M to $137.1M and by 21% from FY 2019-2020

[1] In 2011, DFO and other federal organizations' IT infrastructure services were centrally consolidated under Shared Services Canada (SSC). As such, SSC is responsible for managing and maintaining IT infrastructure, including servers, networks and data centres, that house many of DFO's IT systems and applications. Cyber and IT security responsibilities, however, are shared between SSC and DFO.
[2] The Canadian Coast Guard is a strategic operating agency of DFO and is responsible for the safety and protection of Canada's waterways and marine environment.
[3] The Coast Guard's operational and fleet networks are managed by its Electronics and Informatics (E&I) Branch.
[4] ISACA Control Objective for Information and Related Technologies (COBIT) 2019 framework.

to 2020-2021.[5] The increased funding over the three-year period was used to invest in network upgrades, Wi-Fi capabilities, human resources, a new departmental financial reporting system, and a new document management system.

DFO has also conducted other recent internal audits examining IT governance and planning, asset management, and security:

Audit of Information Management / Information Technology Governance and Integrated Planning (2020)

The audit examined whether the Department had put in place governance structures and processes to manage IM/IT projects and to integrate IM/IT into planning decisions. It concluded that the Department had implemented some elements of governance and some processes to manage IM/IT projects and to integrate IM/IT into planning decisions. However, the audit identified areas for improvement with regard to committee oversight practices and adherence to the Department's project management framework to better support IM/IT project monitoring, reporting and information decision-making.

Audit of Information Technology Asset Management (2019)

The audit examined whether the Department had put in place an effective IT asset management system for hardware devices that protects IT assets and information, complies with regulations, and supports program delivery. The audit concluded that an effective IT asset management system had not been put in place for hardware devices. It also identified opportunities to strengthen the inventory and protection of IT assets as well as the resourcing, coordination and disposal of such assets.

Audit of Information Technology Security (2016)

The audit examined whether the Department had an adequate and effective control framework in place to support IT security. It found that while governance structures did exist, IT security roles and responsibilities should have been better documented to ensure that the Department's IT security program was being adequately and effectively managed. It also concluded that there were opportunities to strengthen the Department's IT security program by implementing improvements to the account management and patch management processes, and to ensure that IT security threats and risks were being regularly assessed and monitored.

The audit was selected in accordance with the Department's 2020-2022 Risk-Based Audit Plan, which identified a need to assess the effectiveness of IT general controls.

Following a risk assessment during the planning phase of the audit, the audit identified five areas of higher risk that required further examination, namely:

- IT Service Desk
- Application Development – Security Design
- IT Continuity
- IT Security – Authority to Operate
- Cloud Adoption

Why this Audit is Important

IT plays a vital role in DFO's ability to deliver its programs and services to Canadians and achieve operational efficiencies. Essential to this is a well-functioning IT control environment to provide the necessary conditions for IT to operate as intended and in compliance with applicable policies.

[5] Figures do not include spending on information management (IM) services, with the exception of hardware and software expenditures to support IM services.

Audit Objective

The objective of this audit was to determine whether the Department's key general controls for information technology were in place and whether they are operating effectively.

Audit Scope and Approach

The scope of the audit was established based on the results of a detailed risk assessment carried out during the audit's planning phase and examined whether key controls were in place and operating effectively in areas determined to be of higher risk. These included IT service desk delivery, application development, IT continuity, IT security and cloud adoption. The audit did not examine other IT general controls, primarily on the basis of the risk assessment and recent coverage from prior audits. Of note, this the scope did not cover IT services managed by CCG. In addition, the audit scope excluded IT infrastructure and services under the jurisdiction of Shared Services Canada.

The audit covered the period from April 1, 2019 to August 31, 2021, but also considered information outside of this period for specific controls.

Audit work was carried out through:

- Consultation of applicable legislation, policies, and frameworks;
- Review of departmental IT plans, initiatives, tools, and records of decision;
- Interviews with selected personnel from IM&TS and the Coast Guard's Electronics & Informatics Branch;
- Walkthrough, mapping and analysis of key IT general controls; and
- Testing of security-related controls and practices.

Conclusion

Overall, the audit concluded that the Department had implemented IT general controls in the areas examined, and that they were generally working as intended. However, gaps existed in a number of areas:

- Timelines for completing remaining work to standardize IT Service Desk processes and procedures had not been defined or documented;
- Security design processes were not always fully followed and formal IT security training requirements for application developers were not implemented;
- A critical incident management process was in place but was missing a disaster recovery strategy and a plan for periodic testing;
- Security assessments were documented but security authorizations were generally not being maintained; and
- Two key components for cloud adoption were behind schedule with no clear timeline for their completion.

Statement of Conformance

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing as supported by the results of the Quality Assurance and Improvement Program of Fisheries and Ocean Canada's Internal Audit Directorate.

Audit Findings and Recommendations

This report presents findings organized around five lines of enquiry: IT service desk, application development, IT continuity, IT security and cloud adoption.

Appendix A outlines the supporting audit criteria, by line of enquiry, used to conclude on the audit objective.

IT Service Desk

DFO's IT Service Desk plays an integral function as it is the first point of contact for many of the Department's employees for receiving IT support and services. The standardization of processes and procedures are important to support Service Desk personnel to provide consistent and efficient services to its clients. In addition, service standards allow both the client and Service Desk personnel to clearly understand the level of service being provided so that expectations can be met. They also enable the prioritization of service requests and incident resolution.

With respect to IT service desk support and delivery, we expected the Department to have in place:

- Standardized processes and procedures to deliver IT services and resolve incidents; and
- Service standards for IT service delivery, with performance against those standards measured and reported.

Overall, we concluded that IM&TS had made good progress towards implementing standardized service desk processes and procedures and establishing service standards. Other work remained in progress but with no formal process in place to define priorities or completion timelines for outstanding items.

While progress had been made in implementing IT service desk improvements, timelines for the completion of remaining work had not been defined.

In 2017, IM&TS hired an external consulting firm to review its client service desk function and delivery of IT services. It led to seven main recommendations to improve service desk processes and technologies and improve the delivery of IT services. A second review was held in October 2019, led by the same consulting firm, to examine the progress made in implementing the earlier recommendations. This work culminated with the development of IM&TS' IT service support strategy.

On the basis of this strategy and other internal work done, which looked at further areas for improvement, IM&TS identified a number of action items that when implemented would result in the desired service desk improvements. Among these, we identified 29 that were related to the standardization of service desk processes and procedures and the establishment of client service standards. We then examined IM&TS' progress in implementing each item. However, we did not assess the action items as to their effectiveness in achieving intended service desk improvement outcomes nor associated internal controls to strengthen service desk processes or service standards. Overall, we found that IM&TS had made progress towards standardizing processes and operating procedures for service delivery and incident resolution, and establishing service standards.

Findings and Analysis

Standardized processes and procedures and service standards

Over half of the 29 action items we examined (15 of 29) had been completed, while eight items remained in progress, and six items had not yet started. Nine items that were scheduled to be completed by April 2021 had not yet been

completed. For example, a key process to perform backlog analysis and to reduce IT Service Desk queues on a regular basis had not been defined.

A new Innovation and Support team within IM&TS was created in January 2021 to lead the implementation of outstanding action items. However, the team reported slow progress in implementing changes, as members had been tasked with this new role in addition to their previous roles and responsibilities.

In addition, we found that there was no formal prioritization or defined completion timelines for action items that were in progress or not yet started. According to IT Service Desk management, items were completed on a best effort basis, with what were considered by management as easier tasks implemented first and more complex tasks completed once resources have been freed up from completion of easier tasks. Progress on the implementation of action items was being monitored and reported to senior management through monthly meetings.

Regarding service standards, we found that IM&TS had made some progress in this area as well, having developed performance indicators and work objectives for IT Service Desk personnel. It also implemented an initiative to analyse, track and report on the IT Service Desk's resource capacity over time.

Why this Matters

These findings matter because standardized processes and procedures as well as service standards enable the IT Service Desk to provide client support, incident resolution and other IT services in a consistent and timely manner. A clearer delineation of roles and responsibilities for personnel in implementing the remaining action items, as well as defined priorities and completion timelines for outstanding items, will better assist in planning and deployment of resources.

Application Development – Security Design

Security is an integral element in the design and development of information systems and applications. It refers to the safeguards that preserve the confidentiality, integrity, availability, and intended use of electronically stored, processed, or transmitted information.

In accordance with the Treasury Board *Directive on Security Management* and the Canadian Centre for Cyber Security's Information Technology Security Guidance, Publication 33 – *IT Security Risk Management: A Lifecycle Approach* (ITSG-33), we expected the Department to have in place:

- Security design processes that are integrated in the application development lifecycle; and
- IT security training requirements for application developers and monitoring of training progress.

Overall, we concluded that security design processes had been integrated during application development. However, some applications were being released to a production environment before required security controls could be fully implemented and prior to receiving security authorization from the appropriate authorities.[6] In addition, we concluded that formal IT training requirements for application developers had not been put in place.

[6] When an application is released or deployed to a production environment, it becomes a "live" application available for business use. In contrast, a development environment is a usually restricted environment where the application is developed and configured prior to being deployed to a production environment.

Security design processes were integrated in application development but the process was not always completed before applications were put in production.

We examined whether security design processes were integrated in application development. Before an application can be put in production, it must go through the Department's security assessment and authorization (SA&A) process to assess whether security controls and other security requirements have been met. It must receive formal security authorization from the appropriate authorities to operate in a production environment, including authorization from the CIO and the application owner.

The SA&A process is based on requirements from the Treasury Board *Directive on Security Management* and controls guidance from the Canadian Centre for Cyber Security's ITSG-33 publication. The purpose of the SA&A process is to identify and assess the key security risks to IT assets, and to ensure that security controls are implemented to mitigate risks that are deemed unacceptable. Overall, we found that security design processes were being carried out during application development. However, some applications we examined had not received the required security authorization before being put in production.

Findings and Analysis

The Treasury Board *Directive on Security Management* stipulates that measures should be in place to ensure that only authorized applications are released to production environments. Within the Department, authorization to release an application to production must be formally received from both the CIO and the application owner. Based on a sample of eight applications (out of 10) that were developed internally and that have been put in production since April 1, 2019, we found that:

- Four applications had gone through the entire SA&A process and received security authorization before being put in production.
- Four applications were put in production prior to completing the SA&A process and receiving security authorization. Since being put in production, two of these applications have received authorization, while the remaining two were still going through the SA&A process and had yet to receive authorization.

IM&TS management informed us that responsibility for releasing applications to production had been assigned to a single group within IM&TS. However, management acknowledged that this practice was not always followed and that a number of groups within the Directorate maintained access to the production environment, meaning that applications could potentially be released into production despite not having received the appropriate authorization.

Why this Matters

This finding matters because, without appropriate access controls, applications are at risk of being released to production without the appropriate authorization, exposing the Department to potential security risks beyond an acceptable level.

Recommendation

Recommendation 1: The Chief Digital Officer should ensure that only applications that have been approved by the designated authorities are released to production.

Formal IT security training requirements for application developers had not been implemented.

Under the Treasury Board *Directive on Security Management* and ITSG-33 guidance, security training is required for those having specific security responsibilities or who could affect the achievement of security objectives as part of their duties. In addition, training should be documented and monitored to ensure that it continues to meet the needs of the Department.

We examined whether IT security training requirements for application developers had been identified and implemented, and whether training progress was being monitored. Overall, we found that management had not formally identified IT security training requirements and had not identified gaps with respect to IT security-related skills and knowledge among application developers against departmental needs.

Findings and Analysis

Although a draft IT security training curriculum for application developers had initially been developed in 2016, formal IT security training requirements had not yet been defined for application developers. In addition, a gap analysis had not been performed to determine whether gaps existed in application developers' IT security-related skills and knowledge in relation to the specific security needs of the Department.

Managers confirmed that IT security training taken by application developers was determined on an individual basis between the developer and their supervisor. They further noted that offerings for applicable IT security training were hard to find and that identifying such training had not been a priority.

Managers of application development teams noted that IT security training would be useful for application developers, team leaders, technical advisors and managers – specifically, training that would provide a clearer understanding of security compliance expectations with respect to the SA&A process. They further noted instances where lack of clarity over specific security control expectations had contributed to delays in application production timelines.

Why this Matters

These findings matter because security design is integral to the application development process and this is dependent on resources with adequate training. IT security training for application developers helps mitigate potential security risks, such as preventing unauthorized access to an application or the compromise of information or data that is stored by the application. In addition, training can help clarify security compliance expectations within the SA&A process so that application production timelines can be better met.

Recommendation

Recommendation 2: The Chief Digital Officer should ensure that application developers possess IT security skills and knowledge required to meet application security requirements.

IT Continuity

IT plays a key role in DFO's ability to achieve its mandate. It is therefore important that plans, processes and procedures are in place that enable the continuity and recovery of mission critical applications, or applications that support mission critical programs and services, in the event of a disruption or disaster. The Treasury Board *Directive on Security Management* requires departments to have in place IT continuity management strategies, including for disaster recovery, to enable information systems to maintain or

return to their normal operating service levels quickly in the event of such occurrences. In accordance with Treasury Board requirements, we expected the Department to have in place:

- Defined recovery strategies and priorities to enable the continuous availability of mission critical applications and data in the event of a disruption or disaster; and
- IT continuity testing procedures that are performed periodically to ensure preparedness in the event of a disruption or disaster.

Overall, we found that the Department had developed a critical incident management process to manage critical incidents where there is no major damage to or complete failure of IT infrastructure, and where the recovery of applications and data could be performed on site. However, the process had not yet been formally approved or communicated to all stakeholders having a role in critical incident management. In addition, the process did not include a formal disaster recovery strategy to respond to major disasters such as flooding, fire or ransomware attacks, nor testing to validate the effectiveness of the IT continuity management process.

Certain elements of IT continuity management had been put in place but did not include a formal disaster recovery strategy.

We examined whether IT continuity management strategies and plans for the recovery of mission critical applications and data had been documented, approved, tested and communicated to those having a role in recovery. Overall, we found that the Department had put in place certain elements of IT continuity management in the form of a critical incident management process, but that it did not include a strategy to respond to potential major disasters or disruptions to IT assets.

Findings and Analysis

IT Continuity Management

IT continuity management consists of identifying applications that support mission critical programs and services, developing continuity strategies and mitigation measures, and ensuring that such applications can continue to operate in the event of a disruption or disaster. Key outputs of the IT continuity management process include:

- IT Continuity Plan: a plan describing the minimum acceptable recovery requirements and information needed to recover mission critical applications and data.
- Critical Applications Inventory: a list of applications that have been defined by the Department as critical or that support critical programs or services.

IT continuity management is a shared responsibility between departments and Shared Services Canada (SSC). The majority of infrastructure assets key to IT continuity management, including servers, networks and data centres, are managed and maintained by SSC. DFO is responsible for establishing and testing IT continuity plans, and for providing continuity requirements to SSC.

We found that the Department had developed certain elements of IT continuity management under its responsibility to enable the continuity of mission critical applications. These included a Critical Incident Management (CIM) process, which was launched in December 2018, and standard operating procedures to execute the CIM process. The CIM process was designed to respond to incidents in which

there is no significant physical damage or failure of IT infrastructure, and where the recovery of critical applications and data can be performed on site, such as incidents involving application crashes.

However, we found certain key limitations with the CIM process. Most notably, strategies to ensure the continuity of the Department's mission critical applications following a major disruption or disaster at an affected site were not defined or documented. This is significant in that if there was to be a major event that rendered a primary site inaccessible and inoperable, IT operations and services would need to be readily transferred to a secondary site to ensure the continuity of mission critical applications.

Although SSC is responsible for failure or damage to IT infrastructure affecting the Department, there was no formal arrangement in place between the two organizations to ensure the availability and continuity of mission critical applications and data during such events. Recovery has instead been carried out on a best effort basis, meaning that the Department and SSC would attempt to recover and restore applications to the extent that their resources allowed at the time. In addition, failover provisions that would allow critical applications to continue operating at secondary locations had not been established. The Department established a service agreement with SSC in April 2020, where SSC would provide 24/7 standby support of servers housing the majority of the Department's mission critical applications. Previously, SSC had provided this support only during normal operating hours.

Another significant risk to IT continuity management was emphasized in interviews with IM&TS management, who explained that a large number of the Department's mission critical applications are considered legacy. They were also uncertain to what extent the legacy applications could be recovered or restored in the event of a major disaster or complete failure, adding that such applications could not be easily put back into service and integrated with modern IT infrastructure and technologies.

IT Continuity Testing

The Treasury Board *Directive on Security Management* requires that departments test IT continuity management processes to ensure an acceptable state of preparedness as an integral element of overall departmental business continuity management. We found that testing was not integrated into the Department's CIM process, and that testing of mission critical applications against potential critical incident scenarios had not been performed. Periodic testing helps ensure that IT continuity processes will work in the event of an actual critical incident. It may also identify unanticipated challenges where lessons learned can be captured and incorporated in critical incident management processes and procedures.

Why this Matters

These findings matter because effective IT continuity management processes are key to ensuring the Department's programs and services can continue to operate as close to normal as possible in the event of a critical incident or major disaster. IT is the backbone of many programs and services the Department delivers to fulfil its mandate.

Recommendation

Recommendation 3: The Chief Digital Officer should ensure that mitigation strategies are developed for mission critical applications in response to potential major disasters, and that these applications are periodically tested against potential critical incident and disaster scenarios.

IT Security – Authority to Operate

The Department's IT security assessment and authorization (SA&A) process is a risk management control based on the Treasury Board *Directive on Security Management* and guidance in the Canadian Centre for Cyber Security's ITSG-33 publication. The purpose of the SA&A process, is to establish and maintain confidence in the security of information systems that are operating at DFO.

In accordance with the Treasury Board *Directive on Security Management* and guidance in the Canadian Centre for Cyber Security's ITSG-33 publication, we expected the Department to have processes in place to ensure that:

- Application security assessments and authorization decisions are documented, including the formal acceptance of residual risk;[7] and
- The security authorization of applications is periodically evaluated and maintained throughout their operational lifecycle.

Overall, we found that security assessments and authorization decisions, including the formal acceptance of residual risk, were documented for the applications we examined. However, authorizations were generally not being maintained, resulting in a large number of applications with expired security authorizations.

Authority for applications to operate in a production environment had not been periodically evaluated throughout their operational lifecycle.

We reviewed whether security assessments and authorization decisions, including the formal acceptance of residual risk, were documented. Furthermore, we examined whether the security authorization that allows an application to operate in a production environment had been periodically evaluated and maintained throughout its operational lifecycle. Overall, we found that although security assessments were documented and that the IT Security team had defined requirements to periodically evaluate the security authorization of an application, authorization was generally not being maintained, with a large number of applications having expired authorizations.

Findings and Analysis

Security Assessments and Authorizations

Based on the sample of eight applications examined earlier, we found that the security assessments, authorization decisions and the acceptance of residual risk for all eight applications were documented.

Evaluation and maintenance of security authorization

The Treasury Board *Directive on Security Management* requires that security authorization be maintained throughout a system or application's operational

[7] Given that all risks associated with IT systems and applications can never be entirely eliminated, there remains some residual risks associated with maintaining an application in a live production environment. Before an application can be released to production, residual risks must be identified and documented through the SA&A process. In addition, the risks must be acknowledged and accepted by both the CDO and the application owner.

lifecycle. We found that IT Security had established tools and practices to track the expiration of security authorizations for departmental applications. Based on a risk assessment of the security controls in place for an application, IT Security will recommend one of three levels of authorization: 1) Full Authority to Operate, 2) Interim Authority to Operate, or 3) Denial of Authorization. These are described in more detail in Appendix C.

In 2019, IT Security established a new practice whereby application owners are to be informed six months prior to expiration to begin the security re-authorization process. Additionally, IT Security is to follow up upon and following expiration of security authorizations if responses have not been received from application owners.

We reviewed whether security authorizations for departmental applications were in place or had expired. Based on an analysis of IT Security's tracking log as of July 27, 2021, we found that security authorizations were generally not being maintained throughout an application's operational lifecycle. Of the 133 applications that had received authority to operate, 77% (103) had expired authorizations. Broken down by level of authorization, this included:[8]

- 38 applications that had been granted Full Authority to Operate, of which 47% (18) had expired authorizations; and
- 92 applications that had been granted Interim Authority to Operate, of which 90% (83) had expired authorizations. Of those 83 applications, 83% (69) had been expired for longer than one year, with a median expiry of five years. For one of the applications, its authorization had been expired for approximately 10 years.

To understand why some applications had expired authorizations for several years, we followed up on a small sample of applications and found instances where the security authorization process was stalled awaiting response from the application owner and other instances where IT Security had not followed up. In interviews, resource capacity challenges – specifically, resource budgets and turnover of staff in IM&TS and in DFO programs and services – were often cited as the main reasons to explain prolonged expiration of security authorizations. We were also informed that applications have remained in production despite having expired authorizations and that there was no formal plan in place to clear the backlog.

Why this Matters

These findings matter because security authorizations ensure that departmental applications continue to maintain required security controls when operating in a production environment. With a large number of expired security authorizations, the Department may be assuming security risks beyond levels deemed acceptable.

Recommendation

Recommendation 4: The Chief Digital Officer should ensure that the process to assess and maintain the security authorization of departmental applications is reviewed to improve its efficiency while balancing security needs.

[8] For three of the 133 applications, the level of authorization was not indicated but two had expired authorization.

Cloud Adoption

DFO recently began a transition to cloud-based computing to modernize its services to Canadians. This shift is consistent with the Government of Canada's cloud-first adoption strategy, published in 2016, that mandates all departments and agencies to prioritize cloud-based applications, platforms, and infrastructure before initiating on-premise or SSC-based solutions. The cloud represents a new model for acquiring software, storage and computational resources. Consistent with the cloud-first strategy and the Treasury Board *Directive on Service and Digital*, we expected the Department to have:

- A structured governance approach in place to oversee cloud adoption; and
- A plan in place to implement cloud adoption, and that implementation progress is monitored.

Overall, we concluded that the Department had established a formal governance structure to oversee cloud adoption, and that regular progress monitoring and reporting were in place. However, despite having a strategy in place, there have been implementation delays to adoption, and two key components considered essential to achieving broader cloud adoption within the Department were behind schedule, with no clear timeline for their completion.

A governance structure for cloud adoption was put in place. However, roles and responsibilities had not been sufficiently defined or communicated to stakeholders.

We examined whether a governance structure was in place to oversee cloud adoption within the Department, and whether roles, responsibilities and accountabilities for cloud had been defined, communicated and understood. Overall, we found that a governance structure had been established to oversee cloud adoption within the Department. However, roles and responsibilities for cloud adoption, specifically for those at the operational level, had not yet been sufficiently defined or communicated.

Findings and Analysis

Governance

We found that a governance structure had been put in place to oversee cloud adoption within the Department, led by DFO's Cloud Program Steering Committee. It reported to the Department's National Digital Advisory Committee and its purpose was to provide DFO senior management with guidance and direction on cloud-bound initiatives and projects.

Roles and responsibilities

We found that although a matrix that mapped and outlined roles and responsibilities for cloud adoption had been drafted, there was no clearly defined timeline for its approval and communication to stakeholders within the Department. In a number of interviews, stakeholders indicated that roles and responsibilities – specifically for those at the operational level – for cloud adoption were not always clearly understood. Additionally, key functions for cloud asset management as well as incident and change management for cloud-bound systems and applications had not yet been defined.

Why this Matters

These findings matter because strong governance structures with clearly defined and communicated roles, responsibilities and accountabilities are foundational to successful cloud adoption within the Department. They enable effective decision-making, allocation and alignment of cloud resources, and mitigate delays or duplication of effort in adoption.

Timelines to implement two of the initiatives in the Department's cloud adoption strategy had not been defined.

We examined whether the Department had developed a plan to implement cloud adoption and whether it was monitoring its implementation. Overall, we found that the Department had developed a cloud adoption strategy and that implementation plans were in place and being monitored for two of the strategy's four initiatives. Although work on the remaining two initiatives had begun, implementation plans had not yet been developed to guide this work. In addition, we were told that two key components considered essential for the full implementation of the strategy were behind schedule, with no clear timeline established for their completion.

Findings and Analysis

We found that the Department had established a cloud adoption strategy, which was formally approved by DFO senior management in June 2020. The strategy consisted of four main initiatives:

1. Cloud environment and standard services
2. Workload migration to cloud
3. Cloud expertise and culture change
4. Cloud financial strategy

In addition, implementation plans had been developed for the first two initiatives under the cloud adoption strategy, with each having a scheduled implementation date of March 31, 2022. Management regularly monitored and reported progress on the two initiatives through monthly dashboards as well as through updates provided at project review committees and at the Department's National Digital Advisory Committee.

However, two key components considered essential by IM&TS management to implement the two initiatives, and to achieving broader cloud adoption within the Department, were behind schedule and at risk of not being completed by the scheduled March 31, 2022 deadline. The first required implementation of appropriate security controls on the cloud platform that will host applications storing protected information. The second component required implementation of the Secure Cloud Enablement and Defence (SCED) technology, which allows for the secure connection between DFO's information systems and the cloud. SSC is responsible for the deployment of this technology.

While work had begun on the remaining two initiatives, implementation plans had not yet been developed to guide this work.

Why this Matters

These findings matter because transition to the cloud to deliver IT services has been identified as a government-wide and departmental priority. Delays to the implementation of the strategy, particularly those related to ensuring secure cloud-hosting environments for applications storing protected information, risk delays to the onboarding of cloud-ready applications.

Appendix A: Lines of Enquiry and Audit Criteria

The audit criteria were developed from the following sources:

- Treasury Board *Policy on Service and Digital*
- Treasury Board *Directive on Service and Digital*
- Treasury Board *Policy on Government Security*
- Treasury Board *Directive on Security Management*
- Canadian Centre for Cyber Security Information Technology Security Guidance Publication 33 – IT Security Risk Management: A Lifecycle Approach (ITSG-33)
- ISACA Control Objective for Information and Related Technologies (COBIT) 2019 framework
- Government of Canada Cloud Adoption Strategy

Audit Criteria	Conclusion
Line of Enquiry 1 – IT Service Desk	
Criterion 1.1: The IT Service Desk has standardized processes and procedures in place to deliver IT services and resolve incidents, service standards are established and performance against standards is measured and reported.	Partially Met
Line of Enquiry 2 – Application Development	
Criterion 2.1: System security design processes are integrated in application development.	Partially Met
Criterion 2.2: IT security training requirements for application developers are identified and training progress is monitored.	Partially Met
Line of Enquiry 3 – IT Continuity	
Criterion 3.1: IT continuity management strategies and plans for the recovery of systems and data are documented, approved, tested and communicated to those having a role in disaster recovery.	Partially Met
Line of Enquiry 4 – IT Security	
Criterion 4.1: The security authorization of information systems to operate in a production environment is evaluated and maintained throughout the systems' operational lifecycle.	Partially Met
Criterion 4.2: Security assessments and authorization decisions are documented, including the formal acceptance of residual risk by an individual who has the required authority.	Partially Met
Line of Enquiry 5 – Cloud Adoption	
Criterion 5.1: Governance and functional roles, responsibilities and accountabilities for cloud are defined, communicated and understood.	Partially Met
Criterion 5.2: A plan to implement the Department's Cloud adoption strategy is in place and monitored.	Partially Met

Appendix B: Management Response and Action Plan

Recommendation	Action Plan	Responsible Manager(s)	Deliverables	Planned Completion Date
Recommendation 1: The Chief Digital Officer (CDO) should ensure that only applications that have been approved by the designated authorities are released to production. Management agrees with the recommendation.	a. Specify all the elements of the Authority to Operate (ATO) including the IT Security approval in the project or product charter.	Director, Project and Product Governance	a. Revised Project Charter. *Project / product charter includes all ATO elements.*	December 31, 2022
	b. Include Security Assessment and Authorization (SA&A) requirements in Project Management Framework (PMF) gating processes, and verify at each respective gate during the Gate Review Committee meeting.	Director, Project and Product Governance	b. Project Management Gating Checklist.	
	c. Review and update the release management process to include verification of the Interim Authority to Operate (IAO) or Authority to Operate (ATO) prior to any production release. Also plan to staff the IT Security team accordingly to meet the revised release plan.	Director General, Digital Innovation & Director, Cyber Security	c. Release management document is reviewed, updated and approved by Director General, Digital Innovation. HR plan to include the required staffing actions. Staffing actions are started and/or finalized.	

Recommendation	Action Plan	Responsible Manager(s)	Deliverables	Planned Completion Date
Recommendation 2: The Chief Digital Officer (CDO) should ensure that application developers possess IT security skills and knowledge required to meet application security requirements. Management agrees with the recommendation.	a. Develop a program for Information Technology (IT) Security trainings and/or certifications for developers.	Director General, Digital Innovation	a. Training is identified and/or developed.	December 31, 2022
	b. Develop a plan that would build and maintain a library of solutions for IT Security controls. Any project would then subscribe to this library to meet their IT Security requirements in a common manner.	Director, Cyber Security	b. Developed curriculum and DevSecOps body of knowledge.	
	c. Create a team that is assigned to projects to scan the code for vulnerability using designated tools, and provide reports and recommendations to the project team.	Director General, Digital Innovation	c. Under the new organizational chart, a new application development security team is created with a clear mandate to support the application development activity.	
Recommendation 3: The Chief Digital Officer (CDO) should ensure that mitigation strategies are developed for mission critical applications in response to potential major disasters, and that these applications are periodically tested against potential critical incident and disaster scenarios. Management agrees with the recommendation.	a. For new projects, ensure that they specify and implement all the elements of the Authority to Operate (ATO) including the required Service Level Agreement (SLA) and continuity plans in the project / product charter.	Senior Director, Strategic Planning	a. Confirm IT dependencies of DFO critical services. b. Document overarching Disaster Recovery Summary Plan and Governance. c. Document Disaster Recovery Plan for each mission critical application.	December 31, 2023

Recommendation	Action Plan	Responsible Manager(s)	Deliverables	Planned Completion Date
			d. Conduct Disaster Recovery Gap Assessment. e. Define and implement annual testing schedule. f. Recommendations for resolving Gap assessment consulted to National Digital Advisory Committee.	
Recommendation 4: The Chief Digital Officer (CDO) should ensure that the process to assess and maintain the security authorization of departmental applications is reviewed to improve its efficiency while balancing security needs. Management agrees with the recommendation.	a. Review the Security Assessment and Authorization (SA&A) process to: • align with the continuous integration continuous deployment (CICD) DevOps model; and • allow for a delta analysis / design from one project / product phase to another.	Director, Cyber Security	a. Refined Security Assessment and Authorization (SA&A) process with: • different processes per risk profile; and • guidelines for delta analysis.	March 31, 2023
	b. Establish a process to regularly review ATOs about to expire and engage application development teams early in renewal activities.	Director, Cyber Security	b. Inventory of systems with Confidentiality, Integrity, Availability (CIA) profile and ATO status with expiry dates. Process for continuous review of soon-to-expire ATOs.	

Appendix C: Levels of Security Authorization for Departmental Applications

The final step in the Security Assessment & Authorization process is the issuance of the Statement of Authorization (SOA). The SOA includes an assessment of any residual security risks associated with operating the application in a production environment. Based on this risk assessment, IT Security may recommend one of three levels of security authorization to the CIO and the application owner:

Full Authority to Operate – May be granted for a maximum of three years from the date on which the authorization was approved. Applications receive Full Authority to Operate if they comply with the applicable security control requirements.

Interim Authority to Operate – To balance the business needs of DFO programs and services, an Interim Authority to Operate may be granted for a one year period for applications that have not met all security compliance requirements, but where the outstanding security controls are considered not to exceed an acceptable level of risk.

For an application to receive Interim Authority to Operate, a plan to implement the outstanding security control recommendations must be prepared and show how the controls will be implemented within the interim period of operation. If they are not implemented within the one-year period, IT Security may extend the interim authority period or recommend the removal of the application from production.

Denial of Authorization – Should the security risk associated with an application be determined to exceed an acceptable level of risk, a denial of authorization may be issued and the application may not be permitted to operate in a production environment until appropriate safeguards are implemented that mitigate the risk to an acceptable level.