REPORT ON:

Management of Legacy Technology

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) relies on information technology (IT) to support the delivery of services to British Columbians. Government implemented some of its applications years ago with technologies that now present risks and challenges. These applications are generally referred to as legacy technology, and they are often essential to operations.

Internal Audit & Advisory Services (IAAS) conducted a survey to determine the extent of legacy technology across Government. Ministries self-assessed their application portfolio and identified about 40% of their business applications as legacy. To migrate from legacy technology, the Government will need to invest significant financial, technical and human resources over a sustained period of time. It will also have to balance the reduction of its legacy technology risks with its other competing priorities.

We also assessed how ministries manage legacy technology. We reviewed how three ministries[1] identify, monitor and plan for the modernization or replacement of their legacy applications. We found that selected ministries had taken steps to reduce their reliance on legacy technology. We also found that they were developing approaches to assess their applications and identify legacy technology. Further, these ministries were developing digital strategies to help them overcome legacy technology risks.

Modernizing or replacing legacy technology was a concern and focus for the three selected ministries. While these ministries had adopted a number of good practices, we found that not all of them had developed the processes necessary to demonstrate adequate management of legacy technology. Maturity varied between ministries, with some processes still in development. This review focused on three main processes necessary to manage legacy technology adequately:

- **Identifying Legacy Technology –** We reviewed whether selected ministries regularly assessed their application portfolio to identify the applications in need of modernization or replacement. Most ministries maintained an application inventory and had developed approaches to identify their legacy technology. We found room for improvement in these processes, such as regularly assessing applications, seeking input from program areas, and monitoring costs and risks identified. Without such improvements, ministries may not have a complete and accurate view of their application portfolio's health, and effectively track their legacy technology risks.

[1] Ministries of Health; Advanced Education and Skills Training; and Transportation and Infrastructure.

- **Defining Strategic Direction for Legacy Technology –** We assessed whether selected ministries had digital strategies that incorporated legacy technology risks, defined long-term investment goals and reflected government priorities. We found one ministry had a digital strategy meeting our criteria, while the other ministries' strategies were still in development. Without digital strategies, ministries may invest resources in initiatives that are not a high priority to achieve their strategic goals.

- **Prioritizing Legacy Technology Modernization** – We assessed whether selected ministries had a process to manage their digital investment portfolio that considered legacy technology risks and aligned with their digital strategies. Most selected ministries had developed such processes. We found opportunities to better formalize their steps. Ministries could strengthen the criteria used to evaluate and prioritize investment opportunities before executive approvals. Documenting key supporting information would strengthen how ministries make digital investment decisions.

While this review focused on selected ministries' processes, the good practices and the five recommendations within this report are relevant across Government. We encourage other government organizations to review their processes and consider the good practices and recommendations identified in this report.

Through this review, we identified several challenges ministries face when migrating from legacy technology, including the funding framework, IT policies and standards, and staffing. The Office of the Chief Information Officer (OCIO), which supports and oversees the Government's IT strategy, policies and standards, and the IT investment portfolio has initiatives to address these cross-government challenges. The OCIO is developing initiatives to train and hire IT staff, update policies and standards, and grow resources to help ministries adopt modern technologies. There are still opportunities for the OCIO to further help ministries develop their internal processes and adopt tools consistent across Government.

* * *

We would like to thank all government staff, who participated in and contributed to this review, for their cooperation and assistance.

Alex Kortum, CPA, CA
Executive Director
Internal Audit & Advisory Services
Ministry of Finance

Introduction

The Government of British Columbia (Government or Province) relies on information technology (IT) and information management (IM) to support the delivery of services to British Columbians. Government implemented some of its **IT systems**, including **business applications**, years ago with technologies (e.g., hardware, software, programming languages) and approaches in building IT systems that now present risks and challenges. These IT systems are generally referred to as legacy technology, and they are often essential for day-to-day operations.

An **IT system** is any equipment used to acquire, store, manipulate or share data. Systems include hardware, software and networks.

A **business application** is a collection of software and databases working together to perform a group of services or business processes.

The COVID-19 pandemic (pandemic) has highlighted the risk of legacy technology. Legacy technology does not often have the flexibility necessary to quickly adjust to changes. The pandemic resulted in the option for government staff to work from home, the introduction of new services and an increase in online access to public services. It required some ministries to review their priorities, accelerate the modernization of their services and adopt current industry practices for building and hosting IT systems.

Relying on legacy technology increases the risks of security breaches and disruptions, while it decreases overall service quality. There are also financial and technical burdens for ministries to maintain these aging IT systems. For example, it is challenging to source vendors to patch security vulnerabilities, meet new regulatory requirements and provide technical fixes.

The Office of the Chief Information Officer (OCIO) develops the IM/IT strategy, policies and standards, and manage the IM/IT investment portfolio for the Province. In 2020, the OCIO developed IM/IT principles to change the way Government manages its technology. It developed these principles to foster agility and sharing resources between ministries. The OCIO also published security standards and guidelines for aging systems.[2] These standards require that ministries develop plans to migrate from IT systems nearing the end of vendor support.

[2] *System Acquisition, Development and Maintenance Security Standard*, and *Information Security Guidelines for Aging Systems.*

Purpose, Scope and Approach

Internal Audit & Advisory Services (IAAS), Ministry of Finance, conducted this review to assess the adequacy of the processes in place to manage legacy technology risks across Government. This review also sought to identify ministry good practices, challenges with and subsequent strategies to migrate from legacy technology.

The objectives of this review were to:

- assess the extent of legacy technology risks across Government;[3]
- evaluate whether a selection of ministries have adequate processes to identify and monitor legacy technology; and
- evaluate whether a selection of ministries have plans to modernize and replace legacy technology.

For the first objective, we conducted a cross-government survey to assess the extent of legacy business applications and risks. For the last two objectives, we selected three ministries based on their business criticality and their risk profile:

- Ministry of Health;[4]
- Ministry of Transportation and Infrastructure; and
- Ministry of Advanced Education and Skills Training.

Our approach with the three selected ministries included:

- reviewing policies, standards and process-related documentation;
- conducting interviews with key management and staff;
- reviewing a selection of modernization or replacement initiatives in progress; and
- assessing ministries' practices against industry good practices.[5]

This review did not include Government's shared IT infrastructure (e.g., data centre facilities, network, enterprise architecture and security services) or enterprise systems (e.g., email and SharePoint) that the OCIO and its service providers manage.

[3] This review focused on core government entities, including ministries and the BC Public Service Agency.
[4] This review did not include regional health authorities.
[5] The primary good practice used for this review was the Information Systems Audit and Control Association's (ISACA) Control Objectives for Information Technologies (COBIT) 2019 framework

We completed our fieldwork in October 2021. We met with each selected ministry to discuss the findings of our work. This report consolidates those findings. We require the selected ministries to develop and submit an action plan in response to our recommendations, including their timeframe for implementation. We conduct an annual follow-up to assess ministries' progress in implementing their action plans.

While this review generally focused on selected ministries' processes, the recommendations within have relevance across Government. We therefore encourage other government organizations to review their processes and consider the recommendations identified in this report.

1.0 Legacy Technology Across Government

Legacy technology poses security, financial, technical and business risks across the Government. In our Report for the Ministry of Citizens' Services: IM/IT Capital Investment Management, published in June 2021, IAAS reported that the Province lacks consistent and complete information of existing government IT systems. Therefore, we assessed the extent of legacy technology across Government by surveying ministries.

1.1 Legacy Technology Survey

Based on our consultations with ministries and the OCIO, we selected four risk factors below as criteria for ministries to identify their legacy business applications:

- The application is at, or nearing (within 3 years), the end of support from vendors. Vendors provide important security patches and technical fixes to their clients.

- The application cannot meet current or planned business objectives or needs. Over time, systems cannot evolve enough to comply with new business requirements, such as legislative changes.

- The application is technically difficult and/or cost-prohibitive to maintain. This can lead ministries to delay the implementation of functional, technical or security updates. For example, if several applications use the same database, a ministry may postpone a complex upgrade to avoid unexpected consequences.

- Developers or vendors with the skills to support the application are scarce in the current marketplace. As ministry and vendor personnel retire, expertise to support aging technologies dwindles and becomes more expensive. Some ministries must source their vendor support internationally.

We found that the Government's reliance on legacy technology remains significant. Through their self-assessment, ministries reported having over 1,500 business applications, with approximately 40% meeting one or more legacy criteria. Ministries use these legacy applications to perform a broad scope of functions such as making payments, processing health claims, administering criminal justice and welfare cases. In addition, approximately:

- 30% of these legacy applications were key to their operations and most of them had a remediation strategy identified. A remediation strategy is a plan to either replace, modernize, retire legacy applications, or the informed decision to tolerate the applications and the risks they carry.

- 40% of their **Critical Systems** are legacy, and most of them have a remediation strategy identified.

Critical Systems are any IT service, system or infrastructure that is necessary to deliver a Mission Critical Service, i.e., services, that should they not be performed, could lead to loss of life, injury, cause personal hardship to citizens, major damage to the environment, or significant loss of revenue or assets.

To manage legacy technology risks, ministries will need to invest significant financial, technical and human resources over a sustained period of time to migrate their services from these applications. Ministries commented that as time passes, modernizing legacy applications becomes increasingly difficult. For instance, ministries noted that catching up with several application updates, and finding the knowledge needed to migrate from these legacy applications are challenging.

1.2 Legacy Technology Trends

Legacy technology risks have become more pronounced for the last few decades due to a number of trends. The OCIO has identified many of these trends and some of them are common to Government and the IM/IT industry. The main trends for the Government are as follows:

- **Citizens' Expectations** – Information and services are readily available through smartphones and tablets, fueling the public's expectation for digital and seamless interaction with Government. During the pandemic, ministries needed to quickly deliver financial support payments, and more virtual access to healthcare.

- **Application Growth** – Ministries have often addressed business needs by developing new applications without decommissioning old ones. They also often failed to collaborate between each other to leverage existing technology. The more applications ministries support, the more their resources and expertise stretch.

- **Monolithic Architecture** – Industry good practices used to favour large, stand-alone applications providing end-to-end services to their users. In addition to the redundancy of application components (e.g., identity management, payment processing) this architecture resulted in, these applications were often designed as single blocks. Current technologies favour modularity, through which each component and layer can be maintained independently.

- **Cloud –** Cloud is becoming the new industry standard, and as software companies move their key applications onto the cloud, they are scheduling to end the technical support to their applications' previous versions. Previous government privacy requirements limited ministries' ability to follow the trend towards cloud.[6]

> **Cloud** technologies encompass a broad range of on-demand resources (e.g., data centre, servers, storage) available over the Internet that ministries used to manage themselves and host in traditional data centres.

- **Vendor Lock-in** – The purchase of large applications has resulted in multi-year contracts with vendors. For ministries, such contracts have increased their IM/IT costs, created dependence on vendors and stifled innovation.

Based on these trends, it is important that Government identifies and manages its legacy technology. Effective management of Government's legacy technology risks would require ministries to identify and report on their legacy technology to the OCIO. This would help Government:

- apply security measures to protect legacy technology;
- develop corporate migration roadmaps before legacy technology risks impact service delivery; and
- forecast funding requirements for modernization or replacement initiatives.

The OCIO could increase the impact of our recommendations included in this report by promoting a consistent, government-wide approach that addresses legacy technology. The OCIO could also consider modern tools to help ministries better manage their legacy technology.

The OCIO has been working on a number of initiatives and programs to accelerate Government's digital transformation and address legacy technology risks. In Section 3.0 of this report, we summarize some of these initiatives.

[6] The data-residency provisions of the *Freedom of Information and Protection of Privacy Act* were updated in November 2021 to allow the use of cloud by ministries more broadly.

2.0 Identifying Legacy Technology

Managing applications over their lifetime requires maintaining a comprehensive inventory of existing applications. Ministries should also regularly assess their applications to monitor their applications' health, and identify actions to mitigate potential declines and optimize their value.

2.1 Maintaining an Application Inventory

Chapter 12 of the Government's Core Policy and Procedures Manual and the OCIO's Asset Management Security Standard require ministries to establish and update inventories of applications. Inventories must capture relevant and current information about the status, criticality and health of applications. Ministries failing to do so may not have an accurate view of the extent and health of their application portfolio.

We considered whether the selected ministries have an application inventory and a process to update it.[7] In doing so, we also considered how ministries update the Government's central asset registry.

We found that the maturity of application inventories was not consistent between ministries. Two selected ministries had established an inventory. Only one ministry had defined and documented procedures to update the inventory's information annually. Without formal review, inventory information may not remain current.

Ministries should develop an inventory that includes a description of applications, their functions to support service delivery, criticality, status (i.e., active, in development, retired), ownership and their expected useful life. They should also have processes, procedures and guidance available for the information to remain comprehensive, accurate and current. In doing so, ministries can better track and assess the health of their application portfolios.

The OCIO manages a central asset registry for the Province to capture information on ministry applications. In our Report for the Ministry of Citizens' Services: IM/IT Capital Investment Management, we found that the central registry was underutilized, and data was inconsistent. We found that most selected ministries update Government's central asset registry. Ministries noted, however, that this registry had limited value for their internal use. Ministries that do not rely on Government's central asset registry for their internal use should still consider maintaining it to enable analysis and planning for the Province as a whole.

[7] The Office of the Auditor General of British Columbia issued its report on IT Asset Management in B.C. Government in November 2020; business applications were not included in the scope of its audit.

Recommendation:

(1) Ministries should establish and annually update an application inventory that aligns with the OCIO's Asset Management Security Standard and includes information about applications' status, health and useful life.

2.2 Assessing an Application Portfolio

To support timely and strategic decisions about their busines applications, ministries should assess their applications, looking at both the **business value** and **technical fit.** Through regular and consistent assessment, ministries can identify trends and risks in their application portfolio, such as identifying technology that does not meet business needs or security requirements. In doing so, ministries can create roadmaps to migrate legacy technology before services to citizens are impacted.

Business Value is the importance an application has to achieve the organization's goals.

Technical Fit is the alignment of an application with the organization's IM/IT standards, risk appetite and service level objectives.

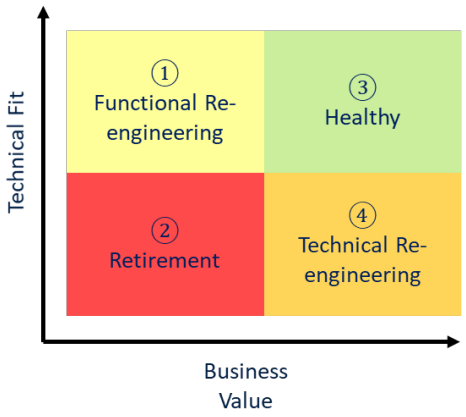
When assessing applications, ministries should regularly involve the program areas that rely on the applications to deliver ministry programs. Program areas should provide their input on business value and be informed of the technical risks they face when relying on legacy technology. Regular program area involvement can also help obtain their timely buy-in on modernization and replacement initiatives.

We assessed whether the three selected ministries regularly assess their applications' business value and technical fit, including risks and costs, and communicate those risks to their stakeholders.

Assessing Applications

We found that two selected ministries had developed approaches to assess their application portfolio. One ministry was developing an annual assessment process with its service provider, which was based on industry good practices. The ministry planned to identify roadmaps for its existing technology based on their business value and technical fit (see Figure 1). Another ministry identified the technical risks of its applications, including the lack of internal and vendor support, and security issues. The ministry recommended priorities for application remediation to its IT executives. We found that selected ministries did not always formalize their procedures to collect the information on applications' technical fit and risks, did not always look at the business value, or did not seek program areas or end-users' inputs.

Figure 1: Industry Good Practices – Assessment Tool



1. **Functional Re-engineering:** The ministry uses the application regularly and it does not cost much to maintain. The ministry can increase the application's business value by adding new processes.
2. **Retirement:** The application has a lot of downtime, which takes considerable time to resolve. The application is only used by a few staff or infrequently. The ministry can retire it to save resources.
3. **Healthy:** The application is stable and does not require significant support. The application is valuable to the ministry. Continual investment is worthwhile.
4. **Technical Re-engineering:** The ministry relies on the application and finds it valuable, but the technology is eroding. The ministry can look at modernizing the application; for instance, migrating it to a new platform.

Source: IAAS, adapted from ministry sources.

Tracking Application Costs

In addition, selected ministries did not actively track and monitor the direct costs of their applications. Costs, such as staff support and infrastructure (e.g., licensing, network and facilities), are a key indicator of legacy technology as the complexity of applications tend to increase over the years. Ministries noted that allocating some cost categories to specific applications is challenging, as applications regularly share resources, such as vendor support or server storage. There are also indirect costs to consider, such as the costs of potential security breaches, non-compliance, or missed opportunities of savings for program areas.

Ministries should track and monitor their applications' costs to their best efforts to ensure costs do not exceed their applications' business value and they can identify better alternatives timely. Tracking application costs can help ministries make better decisions and develop compelling business cases requesting the modernization or replacement of technology.

Communicating Risks to Stakeholders

From the two selected ministries with an application assessment, one had produced reports on its application portfolio's technical risks, limiting its audience to its IT executives. The other ministry had not yet developed such reporting. Selected ministries generally did not use their IT risk registers to record and report legacy technology risks to their IT executives because these registers focus on security and privacy risks. An IT risk register is an important tool to manage IT risks. In the absence of IT risk register, ministries may not appropriately track and manage their legacy technology risks.

Ministries should improve their processes by consistently and regularly assessing their applications' business value and technical fit. They should do so annually for critical and business priority applications, and every two years for other applications. Their processes should consider costs, and program areas' and end-users' input. When feasible, ministries can consider automated tools, such as vulnerability scans, to support their assessments.

In doing so, ministries should also identify high-level roadmaps for their applications. A roadmap would document for each application:

- the selected mitigation strategy (e.g., tolerate, invest, migrate, or eliminate) and the target environment (i.e., cloud or on premises);
- the selected mitigation strategy's estimated costs and benefits; and
- the timeline.

Ministries should also report significant risks to program areas, ministry executives and the OCIO. Such engagement will help ministries raise risk awareness and support future decisions.

The OCIO is conducting an initiative to build an overview of Government's application landscape. There is an opportunity for the OCIO to leverage ministries' application assessment methodologies to develop one methodology common to all ministries and embed it in its current initiative.

Recommendations:

(2) Ministries should develop a process to regularly assess their applications' business value and technical fit and define high-level modernization roadmaps. Ministries should engage with stakeholders to raise risk awareness and inform decision making.

(3) Ministries should record legacy technology risks, such as security, financial, business and technical risks, in a register to determine short-term mitigation actions and monitor risks.

3.0 Defining Strategic Direction for Legacy Technology

Replacing and modernizing legacy technology is complex. A digital strategy helps ministries align replacement and modernization initiatives with their overarching strategy, while also considering the costs and risks of legacy technology.

Through a digital strategy, ministries determine how their IM/IT environment will evolve to achieve their overarching strategy. To do so, ministries assess their IM/IT environment's current IM/IT capabilities, performance and digital maturity, and their envisioned states. Once ministries identify the gaps between the current and future states, they can determine the high-level roadmap to fill the gaps. Developing a digital strategy requires collaboration between the ministries' IT and program areas, ministry executives and IM/IT stakeholders (e.g., OCIO, service providers).

We assessed whether selected ministries have current digital strategies in place, which consider legacy technology risks and define their long-term investment goals. We found that one selected ministry had a current digital strategy which defined investment priorities and highlighted the need to upgrade existing technologies. The other selected ministries were developing such strategies.

It is essential that ministries finalize their digital strategies to align their modernization and replacement initiatives with their missions and strategic objectives. Ministries should support the implementation of their digital strategy by governance structures, such as a steering committee or working groups, and processes, such as regular status reporting and stakeholder feedback. Additionally, ministries should regularly consult with the OCIO on their digital strategies to ensure their strategic directions continuously align with Government's. It would also help the OCIO better understand ministries' investment priorities.

3.1 Digital Framework

Chapter 12 of the Government's Core Policy and Procedures Manual requires that the OCIO provides ministries with IM/IT strategic directions. In 2019, the Province launched the Digital Framework to set out a plan to harness technology and drive digital transformation across the Province.

As part of this framework, the OCIO established the Digital Principles as a strategic vision for moving towards a digital government. The 10 Digital Principles promote:

- **agile** project management approaches and the involvement of users in application development;
- the sharing of software codes and **common components,** across ministries; and
- the continuous improvement of applications over their lifetime.

Agile is an iterative project management approach emphasizing the early and continuous delivery of system capabilities over extensive planning.

Common Components are reusable services or products solving common problems across Government. Examples include identity management, payment processing and notification tools

We found that selected ministries generally support modern approaches, including agile methodology, common components and continuous improvement. However, they do not always document their alignment with the Government's 10 Digital Principles. It would be beneficial for ministries to affirm in their digital strategies their adoption of the OCIO's strategic directions, including the Digital Principles.

3.2 Cross-government Challenges

Throughout our review, we consulted with the IT executives of every ministry. Ministry IT executives expressed a need to migrate from legacy technology and adopt modern approaches. Executives also shared a number of challenges they face when they attempt to modernize or replace their legacy applications.

We found that the OCIO's Digital Framework identified most challenges raised by ministry executives. Many challenges were the result of the changes to the IM/IT environment and industry good practices over the past two decades. Under the Digital Framework, the OCIO had launched a number of cross-government initiatives to address these challenges. Some of these initiatives were still under development and may be subject to change.

Funding Framework

Government's funding framework requires that ministries define their application and project requirements up front. Ministries commented that this framework was not conducive to modern agile approaches, which deliver applications incrementally, encourage user feedback and expect to continuously improve applications over their lifetime.

Ministries also noted that the funding framework overlooked the operating funding necessary to develop, implement and maintain applications. The OCIO is defining plans to address these challenges and make decisions evidence-based, transparent, consistent and agile-friendly.

Staffing and Skills

Ministries also commented that staff turnover and reliance on service providers had resulted in a lack of modern digital skillsets and an erosion of internal expertise on legacy technology. The OCIO and the BC Public Service Agency are working on a common initiative to develop IM/IT training and modernize how Government hires, develops and retains its IM/IT staff.

Policies and Standards

Migrating from legacy technology and adopting modern ones, including cloud, is technically challenging. We found that the OCIO has developed high-level directions, such as the Digital Principles and strategies to instruct ministries on their modernization efforts. It has not yet finalized detailed guidance, such as a technology code of practice. In addition, some of these modern principles conflict with the OCIO's legacy standards. The OCIO has started to update IM/IT management policies, including the Chapter 12 of the Government's Core Policy and Procedures Manual, and is planning to retire many of its legacy standards.

Cloud Adoption

To help ministries on their modernization journeys, and adopt cloud technology, an OCIO team supports ministries on scope-limited projects. The OCIO team trains ministry staff on agile project management approaches and provides them with resources to develop custom-built applications using common components and cloud-compatible technology.

Ministries noted that they found the adoption of cloud technologies challenging partly due to compliance requirements. In early 2021, the OCIO launched a service to help ministries develop custom-built applications in public clouds. Its goals are to sign enterprise agreements with cloud service providers that comply with Government's privacy and security policies and provide ministries with technical directions when using these cloud services.

3.3 Approaches to Migrate from Legacy Technology

Migrating away from legacy technology is often a challenge. Industry good practices identify a number of approaches to do so. Each approach has different costs, risks and impacts. Selected ministries selected different approaches to modernize their applications and move away from legacy technology.

One approach consisted of replacing legacy applications with new, custom-built applications. This approach used Government's common components, cloud-ready technologies and agile delivery with the OCIO's support. This is relevant when no commercial application is available without customization. The new application that this approach aims to develop should be relatively simple as the project team needs to understand each business rule to re-build the application from scratch. By using this approach, ministries can build up and update their IM/IT expertise and reduce the number of technologies they support more quickly.

Rather than replacing a legacy application with a brand-new application, another approach consists of gradually introducing changes to the legacy application. This approach is relevant for complex applications. Complexity may be determined by the intricacy of the business problem and dependences (i.e., their number, whether they are documented), the data, or the database. This approach allows ministries to define their modernization strategy at the level of each application component. After separating and isolating the application components, ministries may decide to replace one component of their legacy application while modernizing another one. By doing so, ministries make incremental changes until the changes eventually replace the functionality of the legacy application. This approach provides value steadily, manages risks and frequent releases allow ministries to carefully monitor progress. However, it can take several years to fully replace a legacy application.

All approaches have benefits and risks. Ministries can determine the best approach by considering their complexity, and business, technical and financial circumstances, and their risk appetites.

Recommendation:

(4) Ministries should finalize and implement their digital strategies and document how they align with Government's IM/IT strategies (e.g., Digital Principles), and regularly consult with the OCIO to ensure alignment with Government's IM/IT strategies.

4.0 Prioritizing Legacy Technology Modernization

Ministries must often balance implementing new applications to meet new business needs and replacing or modernizing their legacy ones. A digital investment portfolio management process helps ministries evaluate and prioritize potential investment opportunities. The goal is to maximize the outcomes of multiple investments while optimizing risks and ministry resources.

An adequate digital investment portfolio management process starts with defining investment categories and setting a target allocation mix based on the investment strategies and priorities:

- Investment category – a collection of the investment opportunities that share similar purpose or benefit.

- Target allocation mix – a set of investment targets reflecting how a ministry will balance competing needs amongst limited resources.

A portfolio requires categories of investment with differing levels of complexity (e.g., project scope and size) and flexibility. Based on the established targets, ministries can categorize, prioritize and actively manage investments throughout their lifecycle. Ministries can then measure and evaluate periodically the portfolio results against the established targets and respond to changes in needs and priorities.

Part of the OCIO's responsibilities is to review and approve ministries' IM/IT capital investment requests. We assessed whether the selected ministries had developed a digital investment portfolio management process that considered legacy technology risks and aligns with their digital strategies. These procedures should occur internally, before ministries submit their IM/IT capital investment requests to the OCIO.

We found that two selected ministries had processes and governance structures in place to collect, review and approve investment opportunities before submitting them to the OCIO. Their IT executives and the ministry Executive Financial Officer made final decisions.

Some of the selected ministries' processes lacked documentation and formalization of their governance, which made it difficult for users to determine the path their investment opportunities must follow. In addition, selected ministries did not always define or document the criteria they used to evaluate and prioritize investment opportunities. This creates a risk that decision makers do not have the information necessary to make the most appropriate and informed decision. The third selected ministry generally reviewed and approved investment opportunities on an ad hoc basis. Selected ministries noted they plan to review or establish their processes.

Ministries should implement a digital investment portfolio management process in line with their digital strategies, the OCIO's capital investment framework and budget cycles. The decision-making processes should include key stakeholders, such as program areas and ministry executives. In doing so, ministries can prioritize their digital investments appropriately, maximize the expected outcomes in line with their digital strategy, and optimize internal resources.

Recommendation:

(5) Ministries should implement a process to document, review and approve their digital investments based on their alignment with their digital strategy.

Appendix A - Summary of Recommendations

1	Ministries should establish and annually update an application inventory that aligns with the OCIO's Asset Management Security Standard and includes information about applications' status, health and useful life.
2	Ministries should develop a process to regularly assess their applications' business value and technical fit and define high-level modernization roadmaps. Ministries should engage with stakeholders to raise risk awareness and inform decision making.
3	Ministries should record legacy technology risks, such as security, financial, business and technical risks, in a register to determine short-term mitigation actions and monitor risks.
4	Ministries should finalize and implement their digital strategies and document how they align with Government's IM/IT strategies (e.g., Digital Principles), and regularly consult with the OCIO to ensure alignment with Government's IM/IT strategies.
5	Ministries should implement a process to document, review and approve their digital investments based on their alignment with their digital strategy.

Appendix B - Abbreviations

IAAS	Internal Audit & Advisory Services
IM	Information Management
IT	Information Technology
OCIO	Office of the Chief Information Officer
Pandemic	COVID-19 pandemic
Province or Government	Government of British Columbia