© JORDAN YOUNGS

Report of the Information and Communication Technology (ICT) Division – Information Technology Security Audit

Fiscal Year (2014 – 2015)

Yukon
Executive Council Office
Government Internal Audit Services

June 24, 2015

Table of Contents

List of acronyms

ARCS – Administrative Records Classification System

AAF – Account Application Form

ERM – Enterprise Risk Management

GAM – General Administration Manual

GIAS – Government Internal Audit Services

HPW – Department of Highways and Public Works

ICT – Information and Communications Technology

IIA – The Institute of Internal Auditors

IRMC – Information Resources Management Committee

ISO/IEC – International Standards Organization / International Electrotechnical Commission

IT – Information Technology

PMD – Property Management Division

1.0 Executive Summary

1.1 Introduction

The Government of Yukon, like most large organizations, depends on the acquisition and analysis of information to achieve its core objectives. Over time, information holdings have grown in quantity and complexity. Likewise, the technology systems needed to manage information holdings have tended to increase in number, complexity and interconnectedness in an effort to find efficiencies. However, this has also led to a growth in the types and severity of potential damage due to information security risks. Awareness of these risks has prompted increased attention on the theme of information security in the management of operations.

The practise of 'information security' focuses on assuring the confidentiality, availability and integrity of information in support of an organization's needs, i.e. business objectives.

> *"Information security involves the application and management of appropriate security measures that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimising impacts of information security incidents."* [1]

Information security risks include the compromising of confidential personal or business information, and the interruption of routine and critical operations due to technical failures. Such risks may lead to loss of productivity, reputation and credibility, or occurrence of fraud.[2]

1.2 Why we completed this audit

The Government of Yukon's Information Technology Security Framework was created in response to the growing awareness of the importance of information technology (IT) security. In February 2014, the Audit Committee recognized the importance of performing an IT security audit. In the summer of 2014, the Audit Committee directed Government Internal Audit Services (GIAS) to focus the audit on the management of information security programs and the central leadership of the Information and Communications Technology (ICT) Division of the Department of Highways and Public Works (HPW) during the period of April 1, 2013 to May 31, 2014.

1.3 Objectives

The objective of this audit was to assess the compliance of existing IT security measures, implemented by the ICT Division, with the 2006 IT Security Framework. Measures include the appropriate governance of IT security and adequate IT security risk assessment as well as specific controls. In addition, the audit

[1] ISO/IEC 27000, section 3.2.3

[2] 2002 April Report of the Auditor General of Canada, Chapter 3 – Information Technology Security, paragraph 3.10

was designed to add value and relevance to the analysis by comparing the Framework to the current standard and guidance on information security published in 2013 by the International Standards Organization/International Electrotechnical Commission (ISO/IEC) in order to determine if any gaps exist.

1.4 Conclusion

Overall, the audit found that the Framework was designed according to a best practise standard that was current in 2006, although it had not been implemented as intended. Given that the standard itself has been updated since the Framework was approved, the Framework should be updated. The Yukon government continues to be exposed to risks as a result of shortfalls in the following areas: IT security governance, risk assessments, communications, network access, and measures to protect information and IT assets.

1.5 Summary of main findings

Governance of IT security and alignment with organizational needs

IT security governance is a foundational component in implementing and maintaining an effective IT security program. The audit expected that the Framework would clearly specify responsibilities for the oversight of IT security governance and implementation as well as principles for directing the selection and design of IT security measures that support organizational objectives.

While the Framework identifies roles and responsibilities for specific groups, the audit found that there was a lack of accountability and clarity on which group should direct and control the IT security function as well as the basis for designing a system of IT security measures.

Risk assessment

The Framework requires the ICT Division to develop high-level risk assessments. These risk assessments must be linked to corporate IT planning and IT management. Effective IT security risk management is critical to ensure that risks are appropriately identified, prioritized, and mitigated.

The audit expected to find a security plan that aligns IT planning with a comprehensive assessment of IT security risks. The audit found that there was no stated link between the Framework and the corporate Enterprise Risk Management (ERM) system or with any corporate IT planning process.

Existing IT security control measures

The audit examined four aspects of the implementation of IT security controls aimed at mitigating potential risks: security topics addressed, communication of IT security, management of access controls and protection of IT assets.

- The Framework was designed to support a set of IT security practices that was consistent with the ISO/IEC standard available in 2006, including a list of potential security topics that was expected to be covered in future policies and procedures.

The audit found that two important IT security control measures have been implemented, i.e. the Computer Use Guidelines and Password Management Policy. Other potential topics have not yet been clearly addressed through the implementation of approved measures.

- The Framework requires that all IT security policies and procedures be communicated to everyone who has access to Government information and IT assets. It also requires that individuals be informed and regularly reminded of their IT security responsibilities.

  Although the Framework is available in the General Administration Manual (GAM), it is not referenced in a number of policies and procedure documents related to IT security. This hinders efforts to raise awareness of the Framework and IT security in general.

- The Framework requires that appropriate controls be applied to ensure that only authorized users can access Yukon government IT systems. Access controls give the ability to manage, monitor and protect the integrity of the IT systems and confidentiality of the stored information, as well as prevent unauthorized access.

  The audit found that measures exist to control access to Yukon government networks through systems based on user accounts. However, user accounts have not consistently been updated in a coordinated and timely fashion. The audit found that responsibility for managing user accounts, or providing information necessary to manage them, was dispersed between different groups.

- The Framework requires a series of controls to ensure that IT equipment assets are protected from unauthorized access, theft, fire, flood and other hazards. Some measures were in place to protect facilities and equipment such as an inventory system and locked rooms for computer servers. The audit found that:

  a) improvements were needed to safeguard computer servers from risk of fire and water damages;

  b) there was an inability to accurately track IT assets; and

  c) key processes such as change management, secure disposal of IT assets, business continuity, and security incident monitoring process had not been formalized and documented.

1.6 ICT actions taken

Since June 2014 the ICT Division has concentrated its efforts in these key areas:

- Engaging an outside contract resource to review internal security architecture, identify immediate gaps or threats, and recommend changes.

- Working with the Property Management Division of HPW to begin the basic infrastructure upgrades required in the ICT Division’s Main Administration Building Data Centre to offer the protections necessary to ensure that essential information services for the Yukon government are maintained.

- Envisioning a fully trusted network consisting of fewer core devices within the ICT Division data centre’s fully-trusted network and establishing access for most network and user devices within a semi-trusted network or separate user networks. This is a reflection of the new reality around the ubiquity of access networks and the wide proliferation of additional devices in the burgeoning ‘internet of things’.
- Reviewing the overall IT security framework with HPW’s Policy & Communications unit in order to ensure that it reflects changes in the IT environment over the last 8+ years. The ICT Division has also developed a workplan of policies, standards, and educational guidelines that need to put in place by March 2016 as a baseline that all Yukon government departments must meet or exceed.

1.7 Recommendations, Management Response and Action Plan

Recommendation	Management Response /Action	Target Date	Position(s) Responsible
1. Address IT security risks in corporate IT strategic planning and implement a risk assessment process that accounts for both corporate and all departmental IT acquisitions.	Agree. ICT introduced a Privacy Impact Assessment tool (PIA) and mandatory request for any new systems development to be completed prior to a system going into production.	Q1 2015	Privacy Officer
	ICT is just piloting a new Security Threat & Risk Assessment tool (STRA).	Q2 2015	Mgr. TI
	ICT engaged a firm to conduct a security assessment of ICT's overall network infrastructure and to review the existing IT Security Framework and policies.	Q2 2015	CIO
2. **a)** Review and update IT Security Framework to ensure the design aligns with the most recent ISO/IEC standard, and mandatory implementation across the Yukon government . The framework must include:	Agree. A review of the Yukon government's GAM policy for the security framework is currently underway. It is a reflection of changes in the IT security environment over the last 8 years, the Government's current needs, and recognition that clarity around accountability is needed.		
• identification of corporate requirements;	• Identification of corporate requirements.	Q3 2015	DCIO
• a process for the selection and approval of controls as well as periodic review of their relevance and performance across the Government;	• A process for the selection and approval of controls as well as periodic review of their relevance and performance.	Q3 2015	ENT. ARCH. Mgr. TI
• awareness and communications strategies for Government employees and training for departmental IT staff ;	• Awareness and communications strategies, and training to IT staff.	Q4 2015	DCIO
• mandatory annual reporting on the implementation of the framework by all departments;	• ICT will collect annual reports from departments and prepare a report to be presented to the governance body regarding the compliance of the implementation of the IT Security Framework.	Q4 2017	DCIO
• coordination/monitoring of divided responsibilities such as user accounts;	• Coordination/monitoring of divided responsibilities such as user accounts.	Q4 2015	Dir. TIO
	• Documented change management	Q4 2015	ENT. ARCH.

• a documented change management process; • a documented business continuity plan and process to respond to security incidents; and • an IT asset tracking and disposal process that includes risk-based controls.	process. • Documented business continuity plan (BCP) and service that ICT can offer for BCP. Develop Individual BCP. • Develop Security Incident Response Plan. • IT asset tracking and disposal vision/process that includes risk-based controls.	Q1 2016 Q1 2016 Q1 2016	Mgr. TI and Dir. TIO Dir. TIO Mgr. TI Dir. TIO and Mgr. TI
b) Put in place clear governance roles and responsibilities to oversee the implementation and monitoring of the Framework and ensure accountability and compliance by all departments.	Agree. GAM policy update to clarify the ICT Division's role as accountable for setting minimum standards in the Information Technology space, as well as oversight responsibilities regarding the implementation and monitoring the compliance of all departments with this GAM policy.	Q3 2015	DCIO, Senior Planner
3. Address immediate shortcomings in the protection of physical assets, server facilities and equipment.	Agree. We are addressing immediate shortcomings. Renovation efforts are underway at the Main Administration Building (MAB) data centre which will alleviate the risk of flood damage and fire when complete as well as to provide a centralized and more reliable infrastructure for Government clients to utilize for their information-related systems and storage. Longer term solutions are pending Management Board approval.	Q4 2016	Dir. TIO

I approve the above Management Response and Action Plan
Signed by the Deputy Minister, Highways and Public Works

I recommend this Management Response and Action Plan for approval by the Audit Committee
Signed by the Director and Chief Audit Executive, Government Internal Audit Services

The Management Response and Action Plan for the Information and Communication Technology (ICT) Division – Information Technology Security Audit were approved by the Audit Committee on June 24, 2015.

2.0 Scope and methodology

The Audit Committee approved an IT security audit for completion in 2014-15 and directed that the audit examine the corporate governance and management of information security programs delivered by the ICT Division for the Yukon government during the review period of April 1, 2013 to May 31, 2014. The scope of the audit also included a review of sample IT projects in other Government departments within the previous five years.

The responsibility of GIAS was to add value by conducting an independent examination of IT security measures and to provide objective information, advice, and assurance to assist the Yukon government in its scrutiny of the Government's management of resources and programs.

The audit team reviewed documents and conducted interviews with all levels of staff within the ICT Division and a sample of other departments. The audit team conducted sampling and transaction testing. Two advisory papers on information security standards and best practices were also prepared for the benefit of the ICT Division.

All of the audit work in this report was conducted in accordance with the standards for internal audit published by the Institute of Internal Auditors (IIA) in the International Professional Practices Framework.

The results of this audit are presented in section 4.0 Observations and findings. The section is organized under three themes that correspond to the main components of the IT Security Framework and the related ISO/IEC standard. Audit recommendations appear in section 1.6.

3.0 Background

The Government of Yukon created an IT Security Framework in response to a growing awareness of the importance of IT security and concerns voiced by the Office of the Auditor General on the lack of a formal IT security policy. The design of the Framework was based on an ISO/IEC standard that was current at the time. The Framework was endorsed by the Information Resources Management Committee (IRMC) in February 2006.

The Framework describes how IT security measures are to be carried out according to:

- roles and responsibilities of the corporate lead group for information and communication technology (ICT Division), the interdepartmental management committee concerned with IT investments (IRMC), departments, corporations, employees and business partners;

- the types and frequency of security assessments and audits;

- access controls, security zones and equipment classification and protection for IT systems;

- management of IT security throughout the lifecycle of IT systems, including implementation, change management, disaster recovery, security incidents and disposal of equipment and information assets; and

- implementation of the Framework, including development of specific security policies, communication and training, and periodic review of IT security documents.

4.0 Observations and findings

4.1 Governance of IT security and alignment with organizational needs

While the Framework identifies roles and responsibilities for specific groups, the audit found that there was a lack of accountability and clarity on which group should direct and control the IT security function as well as the basis for designing a system of IT security measures.

The design of the Framework was based on an ISO/IEC standard on information security controls that was current in 2006 called 17799 Guidelines for Management of Information Technology Security. Since the publication of the Framework, ISO/IEC has updated the standard. The most recent version is called ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. The principle updates to the 2013 standard can be summarized as:

- an increased recognition of the leadership and oversight role of senior management;

- refinement of risk assessment concepts;

- additional requirements and details on the design and implementation of an information security management system, including consideration of the requirements of all interested parties and the process of selecting, communicating and evaluating information security control measures; and

- a series of additional guidance documents on specific IT security topics, such as governance practices.

The 2006 Framework currently identifies the IT security roles of six different groups or organizations in the Yukon government. The two groups with leading roles are:

- the ICT Division, responsible for all IT security measures in the Framework (unless the responsibility is transferred within the Framework) as well as the approval of any changes to IT infrastructure that affect IT security and the review of any Government security violations; and

- the Information Resource Management Committee (IRMC), responsible for directing a corporate approach to IT investments that is aligned with broad Government business needs. IRMC is named as being responsible for endorsing the Framework.

The Framework does not specify which group is ultimately responsible for governing IT security, i.e. directing, approving and reviewing the overall approach and ensuring compliance to IT security or the selection and performance of security measures suggested by the Framework.

While the Framework outlines a number of standard IT security measures and suggests a list of other possible measures to be developed, it does not specify the criteria for the selection and design of such measures or responsibility for their approval, implementation and periodic review. The ISO/IEC model of an information security management system requires information security systems to support the organization’s broad business objectives as well as legal and regulatory requirements. The model also includes the identification of any key external stakeholders and their requirements (e.g. the Legislature and the public) in the criteria for designing IT security measures. However, there is no mention in the Framework of any such broader organizational and stakeholder requirements or a process for determining them.

The audit found that reliance on an outdated standard, lack of clarity on governance authority for IT security and lack of criteria for the selection and design of security measures, as well as the decentralization of IT increase IT security challenges faced by the Yukon government in the management of its IT infrastructure. Without clear governance authority and all departments’ engagement, there is a greater potential for misalignment between IT investment decisions and IT security requirements and increase the risk of unintentional exposure to IT security vulnerabilities. Exposure to such risks could, in turn, impact the achievement of the Yukon government’s core business objectives.

See recommendations 2a) and 2b)

ICT Response

The ICT Division is currently working with the HPW Policy & Communications unit on revamping the GAM policies to provide clarity around leadership and accountabilities for Information governance in Yukon government. The intended outcome is to clarify the ICT Division’s role and accountabilities (under the authority of the Deputy Minister for HPW), IRMC’s role and accountabilities, and the corresponding role and accountabilities of the other departmental deputy ministers. Once completed and approved we will be able to move forward in providing leadership in this area for the Yukon government, including the production of the key underlying policies, standards, guidelines, and educational materials to provide a baseline to meet or exceed within the Yukon government.

4.2 Risk assessment

The audit expected to find a security plan that aligns IT planning with a comprehensive assessment of IT security risks. The audit found that there was no stated link between the Framework and the corporate Enterprise Risk Management (ERM) system or with any corporate IT planning process.

A fundamental objective of IT security is to address information risks in a way that reflects the business needs and risk tolerance of the whole organization. The audit did not find evidence of a broad risk management process being used to direct IT security planning. This lack of connection to a risk management process increases the likelihood that the IT security measures do not respond adequately to corporate risks. The existing Yukon government ERM process and team presents an opportunity to strengthen selection and design of IT security controls through the inclusion of IT security risk assessment.

Despite the absence of corporate risk assessment for IT security, the Framework requires that 'Threat and Risk Assessments' be conducted for each IT program, system or service. A 'Privacy Impact Assessment' is also recommended for new systems or enhancement that deals with the collection, storage, use or disclosure of personal information. The audit found no indication that such assessments on individual components of the IT infrastructure have been carried out.

The audit observed that the Framework gives the ICT Division the authority to approve or reject changes to Yukon government IT equipment, networks, systems, application or procedures that affect IT security. However, responsibility for approving the acquisition or upgrading of IT hardware and software applications is divided between the IRMC, which reviews proposals that draw on corporate funding, and individual departments that fund projects to meet their own specific needs. In addition, there is no specific link made in the Framework between IT security and corporate IT strategic planning overseen by the IRMC. As a result, there is no Government-wide oversight to ensure that risks posed by changes to IT infrastructure have been identified and mitigated. For example, the audit observed that there was a lack of integrated systems planning to ensure that IT hardware and software meet business needs within the capacity of the existing IT network infrastructure and can be effectively supported. Moreover, the audit found that legacy software applications were being maintained that are critical to Government operations but require specialist support or are no longer easily compatible with updated IT network hardware and software. These applications may be vulnerable to risks of malfunctioning and loss of data as compared to products that are more compatible with current IT infrastructure.

Overall, the audit findings highlight that the Yukon government may be unintentionally exposed to IT security risks due to the absence of a thorough use of ERM as well as a lack of both Threat and Risk Assessments and Privacy Impact Assessments. In addition, the divided responsibility for acquiring IT assets appears to be hampering integrated planning for IT systems that would acknowledge IT security requirements within a corporate IT investment strategy. For example, the presence of critical legacy applications appears to present an increased risk of systems malfunction and vulnerability.

See recommendation 1

ICT Response

The ICT Division has begun work on developing a Security Threat and Risk Assessment (STRA) template that will be a companion document to our existing Privacy Impact Assessment (PIA) tools.

Recently, the ICT Division, in conjunction with Department of Finance, worked with a third-party payment card industry Qualified Security Assessor firm to conduct a vulnerability and security assessment of two e-Services initiatives. The outcome of each assessment was summarized in a report detailing the security gaps that would need to be mitigated on each system prior to going live.

The ICT Division has engaged a firm to conduct a security assessment of our overall network infrastructure and to review our existing IT Security Framework and policies.

The ICT Division is working towards developing and implementing a framework, tools and risk assessment procedures that will contribute to the ERM process relating to IT activities and acquisitions.

4.3 Existing IT security control measures

4.3.1 IT security documents

The audit found that two important IT security control measures have been implemented. Other potential topics have not yet been clearly addressed through the implementation of approved measures.

The Framework identifies potential IT security topics that will be covered in policies, procedures, guidelines and standards to be developed by the ICT Division. Such documents are intended to provide more specific direction on how to address specific IT security issues. The audit observed that two policies have been developed to date: Computer Use Guidelines and a Password Management Policy. The Framework recognizes that the list of IT security topics should not be considered as a checklist. Rather, topics should be selected and developed in response to a comprehensive risk assessment and planning process as previously discussed in section 4.2.

ICT Response

The ICT Division developed a portfolio management document for planned policy, standard, guideline, and educational material work. This document provides a detailed work plan with a time frame for each project. It is being used to monitor progress and achievements with completion by March 2016.

4.3.2 Communicating IT security

The audit found that the policies and procedure documents related to IT security do not reference the IT Security Framework.

The Framework requires that all individuals with access to Government information and IT assets must be kept informed of IT security documents in order to be reminded of their IT security responsibilities. The audit noted that the Framework is referenced in the Password Management Policy. However, other key IT documents reviewed did not contain clear links to the Framework, e.g. the Computer Use Guidelines, service agreements, or vendor contracts for computer equipment and applications. In addition, the audit did not find any evidence of efforts to raise awareness about the Framework beyond its publication in the General Administration Manual (GAM) or mentions on the ICT Division intranet blog.

The Computer Use Guidelines were developed to inform all authorized users computers and networks of their responsibilities for safeguarding the IT infrastructure and the information stored on it. It also defines the roles of supervisors, the ICT Division, and Public Service Commission. Personnel are required to sign a form acknowledging that they have read the Guidelines when they sign the Account Application Form (AAF) prior to being granted user access. The Administrative Records Classification System (ARCS) requires that this form be stored in the employee's human resources file. The audit found that the AAF was not consistently filed.

Communicating the importance of IT security as well as engaging personnel in addressing risks is a vital part of managing an organization's efforts to achieve IT security objectives. The general lack of communication observed by the audit raises the risk that users accessing Government networks do not understand IT security risks and their responsibilities. The missing copies of the signed AAF indicate that some employees may not be aware of their IT security responsibilities. The absence of references to the Framework in a number of IT security core documents means that, at best, readers may not be aware of the link between them. At worst, such documents may not be aligned with the IT security objectives of the Framework and may unintentionally cause users to expose the Government to additional IT security risks.

See recommendation 2a)

ICT Response

The ICT Division is currently working with the HPW Policy & Communications unit to review, update, and essentially renew the overarching GAM policies on Information Governance, Security, etc. One of the primary drivers for doing so is to provide clarity around who is responsible for these things on behalf of the Yukon government (ICT) and what responsibilities departments will have by signing a memorandum of understanding (MOU) with the ICT Division. Once this clarity is in place and approved (anticipated by Q3 2015) many of the underlying, more detailed policy, guidelines, reporting and education materials can be executed. In conjunction with the production of these more formal documents, the ICT Division will work with the Policy & Communications unit on a communications plan in the near term and to sustain awareness on an ongoing basis. The Division is also looking to engage with the Public Service Commission on an employee onboarding and periodic refresher plan around key security and privacy information. The Division will be exploring tools and platforms that may allow it to post materials in a self-serve environment for employees that will test their knowledge after reading the material and record their success.

4.3.3 Control of user access

The audit found that measures exist to control access to Yukon government networks through systems based on user accounts. However, user accounts have not consistently been updated in a coordinated and timely fashion. The audit found that responsibility for managing user accounts, or providing information necessary to manage them, was dispersed between different groups.

It was observed that responsibilities for granting access to networks are divided between the ICT Division and the individual departmental IT groups. The ICT Division controls 'Active Directory' accounts required for all users to access any Government computer and network. Departmental IT groups permit access to the networked information systems (or ‘shared drives’) under their jurisdiction as well as any software applications that may be specific to an organization.

a) ICT Division controls

The ICT Division controls the creation of Active Directory accounts by requiring Government employees to complete an AAF in order to create an account, transfer it to another Department or to remove it. The audit noted that the ICT Division sends out an annual reminder to departmental IT groups to review accounts and update user account privileges as appropriate.

Three weaknesses were identified during testing of user access controls:

- there was no standard process to ensure Active Directory accounts are being disabled or deleted when individuals leave Government employment;

- administrator privileges granted to specific users responsible for maintaining networks were not being regularly reviewed to ensure they are still needed; and

- generic accounts, i.e. not tied to any specific employee, created for temporary, non-personal uses were not regularly reviewed to ensure that they were still needed.

The ICT Division’s help desk does receive requests for Active Directory account changes (creating, transferring, deleting) but it was noted that response times were not being tracked or monitored. This may increase the risk of unauthorized individuals having access to IT systems after termination or change in employment.

The audit also noted a specific issue related to access granted to vendors providing commercial IT services. The ICT Division has developed a Network and Information Access Agreement form to be signed by vendors. The audit found that vendor accounts have been created without verification that a form was signed. The audit was unable to determine how often the form was used and who was aware of it. It was also found that the ICT Division practice is to allow vendor accounts to expire at the end of each calendar year, but this practice was not documented.

b) Departmental controls

The audit observed that departmental IT groups grant access to the networked information systems within their organization to users assigned an Active Directory account by the ICT Division. The audit found that departmental human resources units were not routinely notifying those responsible for user access accounts at these different levels when an employee's access rights might need to be changed, i.e. when moving to a different department or termination of employment.

The audit noted that the ICT Division provides designated departmental IT representatives with an administrator password, i.e. in order to be able to install software applications on departmental computers. The audit found that these passwords have not been changed on a regular basis.

The audit also tested access controls for three specific software applications that are critical to departmental operations. The audit found that access to these applications is controlled with appropriate approvals, procedures and forms.

The division of responsibility for managing user access between the ICT Division and individual departments appears to be compromising the ability of the Government as a whole to process changes to user accounts in a timely manner. Accounts that are still functional beyond their supposed expiration increase the risk of unauthorized access to networks and information. The audit found no evidence that logons were routinely monitored to ensure that only authorized users are actually gaining access. That said, the audit observed that access to computer networks and certain critical applications are made more secure by requiring a password-protected logon linked to unique accounts for each user.

See recommendation 2a)

ICT Response

The ICT Division recognizes the lack of controls with respect to user accounts management and is endeavoring to resolve the issues with a number of efforts. The Division will be partnering with our clients to develop a framework for periodic verification of user access to various key systems.

4.3.4 Protecting information and assets

The audit noted that basic physical and environmental protection measures were in place for IT equipment. The audit found deficiencies in the protection of server facilities, the documentation of changes, and tracking disposal of IT assets.

a) Improvements needed to safeguard computer servers

The audit observed some physical threats to IT equipment during a visit of three computer server rooms, i.e.:

- there was no process in place to grant or revoke access to the server rooms for authorized personnel, and access permissions were not being updated on a regular, periodic basis; and
- there was a risk of an electrical fire that would likely cause damage to the servers as a result of water or flooding damage that had not been repaired after a storm in December of 2013.

Despite these issues, the audit confirmed that the ICT Division has been regularly saving back-up copies of the information stored on Government networks on a regular basis to enable recovery in the case of any IT equipment or software failure.

b) Inability to accurately track IT assets

The audit found that the ICT Division was keeping track of corporate IT assets, i.e. computers and software, and facilitated the ability of departmental IT units to track their assets by providing an inventory system. When the audit examined a list of IT assets provided by the HPW Supply Services Branch, the following issues were noted:

- there were approximately 1,300 IT-related items that appear to still be in service long past their scheduled replacement date;
- no process was found that would reconcile IT assets to inventory, so the audit was unable to verify if the asset list was accurate;
- location names were found to be inaccurate or incomplete, e.g. during a site visit, a significant number of servers were noted to be in a building that the location was not identified on the asset list;
- a comparison of duplicate inventories showed inconsistencies between records of the same assets;
- some assets were missing from inventories due to a corporate requirement (Management Board Directive #11/93) to only track assets worth more than $1000. In practice, this meant that some IT devices that could contain sensitive information, such as laptops and tablets worth less than $1000, were not being tracked.

c) No documented process to assure the secure disposal of IT assets

The audit found that once IT assets were identified for disposal, they were properly tracked and managed by the Supply Services Branch. As noted above, the audit was unable to confirm that all IT assets were being tracked and managed appropriately prior to disposal. Understanding that some assets were not being tracked, it would be impossible to ensure that all surplus IT assets are being disposed of appropriately, i.e. in a way that would ensure that data stored on these unknown assets is kept confidential. The audit found that the Government's Capital Asset Disposal Directive includes the asset disposal process but does not specify procedures for IT asset disposal.

d) No documented change management process, business continuity plan and security incidents as required by the Framework

The Framework requires the following processes to be formally documented and implemented: change management, disaster recovery and business continuity, and security incident monitoring. The audit was unable to find any documentation for these procedures, i.e.:

- an updated business continuity plan with details on technical procedures and the chain of communications to engage key personnel in a recovery effort;
- it was noted that, while the ICT Division does monitor and respond to IT security incidents, there was no process in place to document incidents and responses as well as assign responsibility for response as per the current Framework requirements.

A number of IT security risks to the Yukon government may result from the deficiencies noted above. The obsolete systems or equipment can be more vulnerable to technical failure or unauthorized access, or may be insufficient to support business or user needs. Without knowing which assets exist, where they are located, or if they have been disposed of appropriately, there is a risk of inappropriate access to data contained on the equipment or unauthorized access to Government networks. The lack of a documented business continuity plan exposes the Government to additional risks of loss of information, inaccessibility to critical information and inability to process critical transactions for extended periods were a significant system failure to occur. The lack of documentation of security incident monitoring impedes the ability of the Government to evaluate current measures in order to improve them.

ICT Response

The ICT Division has completed a number of tasks to address immediate shortcomings in the protection of physical assets, server facilities and equipment.

The ICT Division is currently working with the Property Management Division (PMD) in HPW on a seeking Management Board approval of renovations to the Main Administrative Building and Old Library space that will accommodate improvements to its primary data centre.

The Division recognizes the importance of information to our citizens and to the services government offers on their behalf and has begun discussions with various parties on the requirements for modifications to the 2nd data centre as a key piece of ICT's Business Continuity Plan for Information Security.

The Division has also started the development of a simple change-management process that will be refined and documented and will develop guidelines for the disposal of IT assets.

Security issues related to asset tracking are being addressed through Virtual Desktop, Mobile Device Management (AirWatch) and Sharepoint/OneNote capabilities that are part of our longer term vision to vastly reduce or mitigate the risks posed by users inappropriately or inadvertently putting our information at risk. All of these together provide an ecosystem in which information is more easily accessible to YG employees when they need it while, at the same time, remaining secure and under more centralized control independent of the location of the user's device. We are also leveraging these capabilities to support a Bring Your Own Device (BYOD) environment where requested. Ultimately this will mean that tracking and disposal of assets in the form of user devices will become a non-issue from a security of information standpoint.

5.0 Conclusion

Overall, the audit found that the Framework was designed according to a best practise standard that was current in 2006, although it has not been implemented as intended. Given that the standard itself has been updated since the Framework was approved, the Framework should be updated. The Yukon government continues to be exposed to risks as a result of shortfalls in the following areas: IT security governance, risk assessments, communications, network access, and measures to protect information and IT assets.

Appendix: table of audit criteria, sources and methodology used.

Criteria	Methodology
1. Roles and responsibilities of ICT, IRMC and departments 1.1 ICT has drafted government security policies, procedures, guidelines and standards for review by appropriate committees or groups. 1.2 High-level risk assessments and security awareness programs have been developed (within ICT branch); IT Branch communicates with national counterpart organizations regarding IT security issues and industry best practices. 1.3 ICT has the authority to approve or reject any changes in government IT equipment, networks, systems, applications or procedures that affect IT security. 1.4 ICT together with all department and corporations must work collaboratively to ensure that appropriate security measures are applied to all government IT activities. 1.5 IRMC is responsible for endorsing the IT Security Framework. 1.6 Corporations will adhere to the Framework through acceptance of terms and conditions of relevant service agreements. Corporations may initiate independent 3rd party IT security audits of shared government IT equipment, networks, systems and applications provided proper notices is given and any findings or reports are shared with ICT. 1.7 Employees are required to adhere to terms of the Framework and all government security policies, procedures, guidelines and standards. 1.8 Business partners (including but not limited to: individuals in private sector, agencies, NGOs) adhere to terms of the Framework and all government security policies, procedures, guidelines and standards.	Document review: IT service agreements, project documents, employee guides, committee proceedings, ICT Risk Assessment document & ICT Risk and Mitigation Strategy completed September 2014 Interviews
2. Conducting security assessments (threat and risk, privacy impact assessments) 2.1 Security risks to information and IT assets must be continuously assessed and managed throughout the life of programs and services (Threat & Risk Assessments; Privacy Impact Assessments; IT Security	Document review: project documents Interviews

Criteria	Methodology
Audits).	
3. Access controls and measures in place (monitoring, tracking and auditing) 3.1 Appropriate logical access controls must be in place for all IT systems. 3.2 Security zones: appropriate physical access controls must be in place for all IT systems. 3.3 Equipment classification and controls: an equipment database and inventory is maintained and kept up to date.	Document review: IT policies, IT service agreements, committee proceedings, HR files Testing and sampling Interviews
4. Operation management of IT Security 4.1 System planning and acceptance: an end-to-end IT security review must take place and any new system must meet all existing security policies, procedures, guidelines and standards. All systems must be tested and meet the documented IT security criteria prior to implementation. 4.2 System integrity: all essential software and information should be regularly backed up and only trusted and known sources of software should be used. 4.3 Change management: a formal change management and change control process has been implemented. 4.4 Disaster recovery and business continuity: a disaster recovery and business continuity plan is in place that is documented, tested and reviewed on a regular basis. 4.5 Security incidents: an effective security incident monitoring process is in place. 4.6 Security audit information and system logs: security log data is protected from modification or deletion. 4.7 Disposal of IT assets is handled appropriately.	Document review Interviews
5. Implementation of the Security Framework 5.1 Security Framework is implemented. 5.2 IT Security Document Completion Process is in place: communication of	Document review

Criteria	Methodology
security measures, training and awareness, and periodic review of IT security documents	

The Auditee reviewed and accepted the suitability of the criteria used in the audit.