Courts Administration Service (CAS)

Audit of Information Technology Security

____
MR. DANIEL GOSSELIN
CHIEF ADMINISTRATOR
COURTS ADMINISTRATION SERVICE

____September 2017___
DATE

TABLE of CONTENTS

1. EXECUTIVE SUMMARY

1.1 Background

Court Administration Services (CAS) was established in 2003 by the Courts Administration Service Act to support the four courts: Federal Court of Appeal; the Federal Court; the Court Martial Appeal Court of Canada; and the Tax Court of Canada (the Courts).

The Act specifies that the Chief Administrator is responsible for the effective and efficient management and administration of all court services while the Chief Justices are responsible for the judicial functions of their Courts. The Courts served by CAS are itinerant courts that sit and hear cases across Canada. Consequently, CAS must be able to support approximately 90 members of the Courts (judges and prothonotaries) in preparing files, conducting hearings and writing decisions "anywhere, anytime."

Support to the four Courts is provided through three programs: Judicial Services; Registry Services; and Internal Services. Judicial services include legal services and judicial administrative support to assist members of the four Courts in the discharge of their judicial functions. Registry Services process legal documents, provide information to litigants on court procedures, maintain court records, participate in court hearings, support and assist in the enforcement of court orders, and work closely with the offices of the four Chief Justices to ensure that matters are heard, and decisions are rendered in a timely manner. Internal Services include corporate services that apply across the organization and are essential to support the operation of the Courts. These include but are not limited to information technology (IT), information management (IM) and security.

The Courts and CAS were exempted from a 2011 Order in Council regarding the use of Shared Services Canada (SSC) email, data center and network services, as well as a 2015 Order in Council regarding procurement, data center and network services. CAS maintains its own data center and IT infrastructure.

CAS must meet high levels of IT security to protect judicial confidentiality, court information, commercial secrets, and personal privacy. The adjudication process must be protected from compromise that could result from unauthorized access to information. Security must be assured while members of the courts are working within CAS facilities and non-CAS facilities, as well as when they are traveling. Technical failures and security vulnerabilities could undermine the usefulness of IT systems and infrastructure. This would jeopardize the entire effort to modernize the court system, seriously limit the ability of the judiciary to conduct the work of the itinerant Courts, and lead to unreliable and insecure court operations. With this in mind, the CAS IM/IT plan has prioritized IT security to ensure adequate security of the Courts and CAS information and network.

Information and Technology Security Services (ITSS) works in collaboration with other areas of IM and IT Services, as well as programs and services, to protect the integrity of the courts and CAS sensitive and valuable information assets. ITSS includes promoting information and technology security, managing security incidents, and responding to client requests for information and assistance. ITS Services is also responsible for a range of activities to ensure sound and secure operations, including but not limited to: IT security monitoring on the network; responding to alerts from Shared Services Canada; vulnerability assessment of CAS infrastructure; risk assessment and security guidelines for new software and technology; and disposition of e-waste. ITS Services also actively contributes to security planning and reporting, such as the Business Continuity Plan and Departmental Security Plan, and to analysis such as Privacy Impact Assessments and Threat and Risk Assessments.

The ITSS is also responsible for day-to day security operations including the firewall, end point desktop security protection and all the other IT security services in between.This report presents the findings of the audit of CAS's control framework and practices associated with the Information Technology Security. The audit engagement was part of the multi-year Risk-Based Audit Plan (RBAP), adopted by CAS, for the period 2015-16 to 2019-20.

1.2 Audit Objective and Scope

The objectives of the audit were to determine the adequacy and effectiveness of:

1) The governance framework in place over IT security to protect the security of departmental information, and help to ensure compliance with related GoC Policies and Directives; and,
2) The selected control frameworks (security measures) in place to mitigate CAS IT security risks.

The scope of the audit included examination of:

- Governance & Policy framework
- Risk Management and Planning
- Key IT Security Measures & Controls, including incident management and security awareness
- Compliance

The scope included an examination of governance, risk management and key IT security controls/measures designed to protect the security of information and information assets, and to help ensure compliance with the Policy on Government Security and the Operational Security Standard: Management of Information Technology Security.

The audit also included specific testing of IT security controls implemented to protect information, applications and network folders. In order for observations and possible recommendations to be current and meaningful; audit examination of management activities and testing of IT security controls in place, covered the period from January 2016 to January 2017 with emphasis on more recent activities.

Audit activities were undertaken in the National Capital Region (NCR) only. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

1.3 Audit Findings and Recommendations

Overall, the audit found that there is a control framework in place for IT security that requires some improvements. The observed strengths and areas where opportunities for improvement were identified, including the related audit recommendations, are presented below. A more detailed discussion of audit findings is presented in Section 3 of this report.

1.4 Observed Strengths:

The following strengths were observed in the management control framework for IT Security:

- There is an organizational structure for IT Security consisting of four positions, 3 of which are currently staffed and reporting directly to the Chief Information Officer. IT Security has a functional reporting relationship with the Department Security Officer.
- There are some reporting mechanisms to provide management with appropriate information for oversight and decision-making. For example, the National Judges Committee on Information Management and Information Technology is responsible for collaborating on decisions pertaining to IMIT including IT Security.
- CAS uses an industry standard patch management tool for desktop machines and servers.
- Policies have been implemented to prevent, detect and remove malicious software.
- Vulnerability assessments have been conducted on the CAS infrastructure.
- IT Security has projects and tasks in progress.
- There is a documented incident management process in place which includes roles and responsibilities of different sections within CAS.

1.5 Opportunities for Improvement:

Governance and Policy Framework

The audit found that IT needs to identify the reporting relationships and authority of IT Security. This creates a risk that IT Security matters may not be escalated to the appropriate CAS authority and therefore may not get resolved. Audit recommends that the CIO modify and approve the IT Security Team Charter to identify the reporting relationships and authority of IT Security. (Refer to Finding # and Recommendation # in 3).

The audit found that the Terms of Reference for the Information Security Steering Committee needs to be developed. Without a Terms of Reference, there is a risk that the committee could deviate from its purpose and structure and therefore may not accomplish its goals. Audit recommends that the CIO develop, document and communicate an approved Terms of Reference for the Information Security Steering Committee.

Risk Management and Planning

The audit determined that CAS needs to identify in the system development process finite points at which IT Security is responsible for reviewing system design. This creates a risk that new applications may not include effective IT security specifications as expected. Audit recommends that the CIO build into the CAS system development process finite points at which IT Security is responsible for reviewing system designs and identifying required baseline controls.

The audit determined that the CIO should document an IT Security Strategy and Implementation Plan. Without such a documented strategy and plan, risks may not be mitigated, resources required to mitigate vulnerabilities may not be identified and options for mitigating risks may not be identified. Audit recommends that the CIO document an IT Security Strategy and Plan allowing for at a minimum, reporting on progress against the strategy and monitoring whether the plan is meeting its objectives.

IT Security Measures and Controls

The audit found that while IT Security does have some specific procedures for dealing with IT Security events related to end point protection software, there is not an overall framework (including policy and procedure).

Compliance

Audit determined that IT does not have a policy that defines requirements for reviewing audit logs and requirements for reviewing administrative privilege rules. This creates a risk that inappropriate access to the CAS infrastructure by staff may go undetected. Audit recommends that the CIO develop a policy that defines requirements for reviewing audit logs and staff administrative privilege rules.

1.6 Executive Summary of Management Response

Management agrees with the audit observations and the recommendations made in this report. Appropriate detailed action plans will be developed and implemented.

1.7 Conclusion

The audit found that the control framework in place for IT Security with respect to:

- Governance & Policy framework;
- Risk Management and Planning;
- Key IT Security Measures & Controls, including incident management and security awareness; and,
- Compliance.

is operating with key controls while improvements are required as identified in this report.

The audit found that there is opportunity for improvements regarding the design and the implementation of the IT security control framework related to organizational structure, planning, applications under development, and some monitoring activities.

The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

1.8 Statement of Conformance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The audit conclusion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The conclusion is applicable only to the entity examined. The evidence was gathered in compliance with Treasury Board policies, directives and standards on internal audit and conforms to the Internal Auditing Standards for the Government of Canada.

The evidence gathered was sufficient to provide senior management with proof of the conclusion derived from the internal audit.

André Bolduc CIA
Chief Audit Executive

2. INTRODUCTION

2.1 Background

CAS was established in 2003 by the Courts Administration Service Act to support the Federal Court of Appeal, the Federal Court, the Court Martial Appeal Court of Canada and the Tax Court of Canada (the Courts).

The Act specifies that the Chief Administrator is responsible for the effective and efficient management and administration of all court services while the Chief Justices are responsible for the judicial functions of their Courts. The Courts served by CAS are itinerant courts that sit and hear cases across Canada. Consequently, CAS must be able to support approximately 90 members of the Courts (judges and prothonotaries) in preparing files, conducting hearings and writing decisions "anywhere, anytime."

Support to the four Courts is provided through three programs: Judicial Services; Registry Services; and Internal Services. Judicial services include legal services and judicial administrative support to assist members of the four Courts in the discharge of their judicial functions. Registry Services process legal documents, provide information to litigants on court procedures, maintain court records, participate in court hearings, support and assist in the enforcement of court orders, and work closely with the offices of the four Chief Justices to ensure that matters are heard, and decisions are rendered in a timely manner. Internal Services include corporate services that apply across the organization and are essential to support the operation of the Courts. These include but are not limited to information technology, information management and security.

The Courts and CAS were exempted from a 2011 Order in Council regarding the use of Shared Services Canada (SSC) email, data center and network services, as well as a 2015 Order in Council regarding procurement, data center and network services. CAS maintains its own data center and IT infrastructure.

CAS must meet high levels of IT security to protect judicial confidentiality, court information, commercial secrets, and personal privacy. The adjudication process must be protected from compromise that could result from unauthorized access to information. Security must be assured while members of the courts are working within CAS facilities and non-CAS facilities, as well as when they are traveling. Technical failures and security vulnerabilities could undermine the usefulness of IT systems and infrastructure. This would jeopardize the entire effort to modernize the court system, seriously limit the ability of the judiciary to conduct the work of the itinerant Courts, and lead to unreliable and insecure court operations. With this in mind, the CAS IM/IT plan has prioritized IT security to ensure adequate security of the Courts and CAS information and network.

Information and Technology Security Services (ITSS) works in collaboration with other areas of IM and IT services, as well as programs and services, to protect the integrity of the courts and CAS sensitive and valuable information assets. ITSS includes promoting information and technology security, managing security incidents, and responding to client requests for information and assistance. ITS Services is also responsible for a range of activities to ensure sound and secure operations, including but not limited to: network monitoring; responding to alerts from CSE and Shared Services Canada; vulnerability assessment of CAS infrastructure; risk assessment and security guidelines for new software and technology; and disposition of e-waste. ITS Services also actively contributes to security planning and reporting, such as the Business Continuity Plan and Departmental Security Plan, and to analysis such as Privacy Impact Assessments and Threat and Risk Assessments.

The ITSS is also responsible for day-to day security operations including the firewall, end point desktop security protection and all the other IT security services in between.This report presents the findings of the audit of CAS's control framework and practices associated with the Information Technology Security. The audit engagement was part of the multi-year Risk-Based Audit Plan (RBAP), adopted by CAS, for the period 2015-16 to 2019-20.

2.2 Audit Objective

The objectives of the audit were to determine the adequacy and effectiveness of:

- the governance framework in place over IT security to protect the security of departmental information, and help to ensure compliance with related GoC Policies and Directives; and,
- the selected control frameworks (security measures) in place to mitigate CAS IT security risks.

The scope of the audit included examination of:

- Governance & Policy framework
- Risk Management and Planning
- Key IT Security Measures & Controls, including incident management and security awareness
- Compliance

The scope included an examination of governance, risk management and key IT security controls/measures designed to protect the security of information and information assets, and to help ensure compliance with the Policy on Government Security and the Operational Security Standard: Management of Information Technology Security.

The audit also included specific testing of IT security controls implemented to protect information, applications and network folders. In order for observations and possible recommendations to be current and meaningful, audit examination of management activities and testing of IT security controls in place, covered the period from January 2016 to January 2017 with emphasis on more recent activities; audit fieldwork was conducted at Headquarters.

Audit activities were undertaken in the National Capital Region (NCR) only.

2.3 Methodology

The audit engagement was conducted in accordance with *the Internal Auditing Standards for the Government of Canada* which incorporates *the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.* These professional standards require that the internal audit be planned and performed in such a way as to obtain reasonable assurance that audit objectives are achieved.

The audit team conducted a risk assessment during the planning phase of the audit. Key risks were identified and assessed using professional judgement and after considering facts/factors known to the audit team and/or identified during the planning phase of the audit. Audit determined whether a risk would be addressed by this audit based on the assessed risk after considering mitigation activities as discussed with CAS staff.

In addressing the audit objective, audit criteria were developed against which observations, assessments and conclusions were drawn. These audit criteria were derived primarily through the exercise of professional judgement, after consideration of the results of the risk assessment undertaken during the planning phase of the audit. Appendix A to this report presents a list of the criteria for the audit and the conclusion reached against each criterion.

An audit program was developed that addressed the audit criteria through the following approaches:

i. Interviews and discussions were conducted with staff directly involved with IT Security and Security. A list of interviewees is presented in Appendix B to this report;

ii. Review of relevant documentation including but not limited to: Policies, Procedures, NJC IMIT minutes, Plans, monitoring reports; and

iii. Detailed testing of key controls and management assertions.

   For purposes of the detailed testing, a sample of files was judgementally selected to test patch management and logical access controls.

2.4 Acknowledgement

The audit team acknowledges the collaboration and support received from interviewees within Information Management – Information Technology and the Security Services.

3. FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

3.1 Governance and Policy Framework

It was expected that an IT Security governance framework exists that defines and communicates roles and responsibilities, allows for effective management decision-making and oversight of IT security.

We conducted interviews with the 2 Managers within IT Security Services, Chief Information Officer and the Department Security Officer (DSO). We reviewed several documents including but not limited to The Information Security Management Framework.

The Information Security Management Framework describes the governance for information security at CAS. The governance structure includes an Information Security Steering Committee (ISSC) consisting of the Information Management Senior Officer (IMSO), Information System Security Officer (ISSO), IT Security Coordinator (ITSC) and the Technical Enterprise Architect (TEA). Audit has not found any Terms of Reference or description of the responsibility of the ISSC. Without a Terms of Reference, there is a risk that the ISSC could deviate from its purpose and structure and therefore may not accomplish its goals. In addition to the ISSC there is a National Judges Committee on Information Management and Information Technology (NJC IMIT) which is responsible for collaborating on decisions pertaining to IM and IT. Our review of the NJC IMIT minutes[1] shows that IT security items are being discussed with key stakeholders. The governance also includes the CAS Chief Justices Steering Committee and the CAS Executive Committee which provide direction on IT security strategies and are kept abreast of progress on IT security plans.

Organization Structure

The IT Management Plan identifies an IT Security organization with 4 approved positions devoted to IT Security. The current IT Security organization structure shows that the Director IT Security reports directly to the CIO with no formal functional relationship to the Department Security Officer (DSO). The Director of ITSS position is currently vacant.

IT Security is responsible for monitoring compliance with GoC security requirements, responding to IT security incidents, monitoring all IT security alerts, collecting IT performance logs and reviewing those logs to look for patterns and providing IT security training. The IT Security prime responsibility is to protect the integrity of the courts and CAS sensitive and valuable information assets[2].

A draft *IT Security Team Charter* states that the IT Security Team is responsible for all aspects of Information and Technology Security at the Courts Administration Service. The function coordinates and promotes the responsible use of systems in accordance with Government of Canada security policies, directives and best practices. The Charter also indicates that there is a Manager of IT Security Services. However, the charter does not describe any reporting relationships or authority. This creates a risk that IT Security matters may not be escalated to the appropriate CAS authority and therefore may not get resolved. In addition to the IT Security Team Charter there is an *IT Security Operations Team Charter*[3] which states that the Team is responsible to:

- Coordinate, promote the responsible use of, and provide CAS with perimeter security and an active defense strategy;
- Monitor and detect host based security issues.
- Respond to security issues; and
- To provide in-service support, and life cycle management of network security solutions.

According to the IT Security Operation Team Charter the IT Security Team is supposed to consist of a Manager and two Security Analysts. This draft team charter was developed in January 2016 and modified in November 2016

IT Security reports directly to the CIO and is responsible for monitoring alerts, collecting logs and reviewing those logs to look for patterns. In addition to IT Security, policy recommendation 3b of the *Blueprint for the Security of Judicial Information* states that every jurisdiction is supposed to ensure that a Judicial IT Security Officer (JITSO) is appointed. The JITSO is accountable to the judiciary and is appointed to oversee the management of court information technology security operations. The role of the JITSO is currently being filled by the CIO, who provides IT Security advice to the Judiciary related to judicial information, including to the Chief Justices, at the NJC IMIT where IT Security issues are routinely discussed, to various judicial committees and individual members of the courts. There are quarterly meetings of all JITSO's across the Canadian court jurisdictions that are attended by the CIO. The CIO is currently working on developing CAS specific functions for the JITSO[4]. It is expected that the proposed JITSO responsibilities will be assigned to the Director of ITSS with day to day IT responsibilities for IT Security with the Courts and CAS. It is expected that the JITSO will report to both the CIO and to the Judiciary. It is not yet clear what other roles and responsibilities will be part of the JITSO duties at CAS.

The reporting structure for Information Technology Security Services shows that ITSS reports directly to the CIO with no formal reporting relationship to the DSO. However, audit has been told by both the CIO and the DSO that IT Security Services does have a functional relationship with the DSO. Significant IT Security events are reported to the DSO.

Recommendation (Medium – medium enhancement to current processes and controls)

1. *The CIO should modify and approve the IT Security Team Charter to identify the reporting relationships and authority of IT Security. In addition, the CIO should develop, document and communicate an approved Terms of Reference for the ISSC.*

Management Response and Action Plan Recommendation #1

Agreed. While IT Security Services is a small organization within which the roles, responsibilities and relationships are known to the team members, it is prudent and timely to document its reporting relationships and authority as well as document and communicate the information and technology security governance.

Management Action Plan	Responsible Official	Target Completion Date
Revise and adopt the IT Security Team Charter for the IT Security Service. Document and communicate the governance structure for information and technology security.	CIO	September 2017

3.2 Risk Management and Planning

Risk Management Framework

It was expected that a documented risk management framework exists allowing for the continuous assessment of IT security risks and the certification of IT assets signifying that management has authorized the use of those assets and has accepted any residual risks.

To determine whether a Risk Management Framework exists, Audit reviewed several documents including the *Finance Information Technology General Controls (ITGC) Report*, the *Policy Framework for IT Management*, minutes of the NJCIMIT and the *DSP*. Audit found that an IT Risk Management Framework does exist. CAS uses governmental cyber defense monitoring services as well as its own tools to monitor IT security. The DSP states that a general purpose set of indicators to routinely monitor the overall changes in the Security environment is needed and that these indicators will be reported on a monthly basis. Although the IT Security Team Charters have not yet been implemented, they both state that teams will use a risk management process to document, track and monitor risks.

Audit found that risk assessments performed do clearly identify the risks and mitigation activities but monitoring activities are not effectively implemented. Management action plans were documented to mitigate the risks found.

Security Assessment and Authorization (SA&A) is the process by which federal departments examine their information technology infrastructure and develop supporting evidence necessary for security assurance accreditation. Although there are no accreditation certificates for existing business applications, CAS has conducted risk assessments on new software. However, Audit cannot determine whether the risks of the existing business IT assets fall within a risk tolerance for CAS.

Recommendation (High – significant enhancement to current processes and controls)

2. *The CIO should implement a complete SA&A process on existing key applications to ensure those applications fall within the risk tolerance of CAS.*

Management Response and Action Plan Recommendation #2

Agreed. Such exercise will ensure risks are appropriately assessed against CAS risk tolerance.

Management Action Plan	Responsible Official	Target Completion Date
Develop an overall plan for implementing SA&A for the key infrastructure components and for the key applications.	CIO	November 2017

IT Security Strategy and Plan

An IT Security Strategy is a blueprint or idea used to accomplish the CAS IT Security goals/objectives. An IT Security plan, on the other hand, is a specific list of projects/activities for achieving the IT Security goals/objectives outlined in the IT Security Strategy.

Audit expected that an overall IT security strategy and an IT Security Plan are documented and aligned with the DSP and the IT Plan and provides for integrating information technology security requirements into other processes. The IT Security Strategy and IT Security Plan should highlight among other things, resource requirements needed to achieve the strategy.

The CIO has highlighted general IMIT operational challenges related to staff turnover and balancing projects against daily operations. Some of these challenges are mitigated through the use of outsourced expertise to address specific needs. The *Department Security Plan* (DSP) for 2015-2019[5] identified a gap in staffing of the IM/IT Security Team and indicated that the gap was to have been actioned by March 2016.

In 2015, CAS received funding from government to enhance Physical and IT Security for the federal courts including two new IT Security staff which has been hired. In addition, the *IT Infrastructure Management Plan for 2016-17 to 2020-21,* supported by funding received in 2016, includes four additional FTE's in IT. One of those four FTE's is for the IT Security Services group.

There is an *Information Security – Projects and Tasks Summary* that identifies Security activities and daily operations. There is also an *ITS Master Task List* which identifies different IT Security tasks. Audit has not seen an IT Security Strategy, including resource requirements and timelines nor regular reporting against a strategy to monitor whether the strategy is on target.

Having multiple project/task lists creates a risk of double counting projects/tasks, having no authoritative source for official projects/tasks and having unclear resource requirements.

Recommendation (Medium – enhancement to current processes)

3. The CIO should develop one authoritative list of IT Security projects identifying estimated start/completion dates, financing required and resource requirements. Once this list is developed, the CIO should provide status reports against the project list to senior management on a regular basis.

<table>
<tr><td colspan="3"><i>Management Response and Action Plan Recommendation #3</i>

Agreed. Combining all IT security projects and initiatives into one authoritative list will be more efficient for tracking progress and allocating resources.</td></tr>
<tr><td>Management Action Plan

Consolidate all of the existing IT security project lists into a single list with dates and resource requirements and ensure a process for providing regular progress reports to</td><td>Responsible Official

CIO</td><td>Target Completion Date

September 2017</td></tr>
</table>

CAS senior management and appropriate governance committees.		

Recommendation (Medium – enhancement to current processes)

4. *The CIO should develop an IT Security resource plan to identify skills required and the process for identifying and selecting resources required in IT Security. This Plan should also set a reasonable timeline for hiring IT Security resources.*

<table>
<tr><td colspan="3"><i>Management Response and Action Plan Recommendation #4</i>
Agreed. Such plan will ensure specific skills are properly identified and timeline for hiring IT security resources are reasonable.</td></tr>
<tr><td>Management Action Plan
The Information and Technology Security Services Business Plan will identify the skills required to deliver the targeted services and the necessary resources to deliver those services, including the expected timeline for hiring the required staff.</td><td>Responsible Official
CIO</td><td>Target Completion Date
May 2017</td></tr>
</table>

The Government of Canada has identified baseline controls which represent best practices to protect the GC networks and to address current and potential cyber threats. CAS has fully implemented some of the controls while others are in various stages of implementation.

Audit determined that there is no strategy describing how CAS plans to implement the remaining controls and the risks to CAS for not having the remaining controls.

In 2014/2015 CAS engaged two Firms to conduct vulnerability assessments of the CAS IT infrastructure. The Firms identified opportunities for improvement. The CIO has provided ExCom and the NJC IMIT status reports. However, audit has not seen any IT Security Plan identifying timeframe, resources required and a risk management approach.

Recommendation (High – significant enhancement to current processes)

5. *The CIO should document an IT Security Strategy that allows for:*
   - *Formally establishing the scope and objectives of IT Security*
   - *schedule of measures required to implement IT security objectives*
   - *reporting on progress against the strategy,*
   - *monitoring whether the plan is meeting its timelines,*
   - *following up on outstanding items, and*
   - *providing for requirements of the NJC*

Management Response and Action Plan Recommendation #5

Agreed. An IT Security Strategy will articulate the overarching strategies and objectives and the plans to meet them, as well as the monitoring and reporting approach.

Management Action Plan	Responsible Official	Target Completion Date
The revised Team Charter (management response #1) will clarify the scope and objectives of IT Security Services. This combined with the Business Plan (management response #2) will track progress against IT Security projects and activities. Regular reporting to CAS senior management and NJC IMIT will be implemented.	CIO	September 2017

3.3 IT Security Measures and Control

Audit expected to see that the IT Security controls currently implemented are reasonably effective in preventing and detecting control breaches.

System Development

Audit has not found any documentation outlining a CAS System Development Life Cycle (SDLC) and therefore audit cannot conclude whether there are IT security requirements defined and communicated for new projects. CAS Information Technology does not have its own System Development Life Cycle (SDLC) but has a Project Management Framework that is consistent with the Treasury Board Secretariat Directive on the Management of Projects as well as following the Project Management Institute's Project Framework.

Audit was told that IT Security approves modified or new applications before installation. Audit was told that IT Security participates in the weekly (Wednesday) Change Management meeting, which includes Business Solutions to discuss the list of outstanding Change Requests.

Audit tested one project to determine whether IT Security is involved in the system development process. Audit found that valid IT security requirements or opportunities were identified.

However, the documentation does not identify who has authority to perform different key functions such as IT Security reviews.

Recommendation (Medium – enhancement to current processes and controls)

6. *The CIO should build into the CAS system development process finite points at which IT Security is responsible for reviewing system designs and allow for IT Security to identify required baseline controls for new systems.*

Management Response and Action Plan Recommendation #6

Agreed. IT Security reviews will be formally incorporated into the systems development process.		
Management Action Plan Incorporate into the PMF and SDLC, specific checkpoints that address the recommended IT security activities as specified by the Information Security Systems Implementation Process described in ITSG33.	Responsible Official CIO	Target Completion Date September 2017

Patch Management

Patches are additional pieces of code developed to address problems (commonly called "bugs") in software. Patches enable additional functionality or address security flaws within a program. Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within CAS.

The risk assessments previously performed recommended strengthening the patch management process but did not indicate whether there is an effective patch management framework for operating systems and business applications.

CAS reviewed its patch management process. The 2015-2019 DSP states that over the next three years, there will be a road map developed to continue to improve patching. The DSP also states that in 2016 routine and timely patching of software will be in place. The priorities included deploying patching software by March 2016.

Audit found that CAS now has a documented *Patch Management Strategy for End-User Computers* which describes the process to follow to distribute updates to desktop and laptop computers (end-user computers). Audit also found that CAS has taken action to patch CAS network servers.

CAS uses an industry standard patch management tool to provide patch management. However, there are insufficient licenses to use this software on all servers and therefore some servers have to be patched using a manual process rather than an automated process.

CAS also uses services to enable CAS system administrators to manage the distribution of updates and hotfixes[6]. In addition, CAS has recently acquired a set of web-based tools aimed at managing software and hardware including patch automation for some server-based software.

There are some outstanding server-based patches that are still not yet installed as a result of extensive testing required to determine their impact on the numerous applications in use at CAS.

CAS is addressing concerns around patch management

Logical Access

Audit determined that the Information Technology Security function has established policies and monitoring procedures that address: requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges. Roles and responsibilities for access control are clearly defined, documented and communicated.

Access control is granted to employees who need to work with specific applications and access information in specific folders or databases. Control is exercised by the manager requesting a user account for new or transferred-in employees. Procedures are noted in the *Request for CAS Employee Network Account or Move.*

The Director, Client Service and Infrastructure is responsible for establishing procedures for granting access to CAS' electronic network. According to the *Request for CAS Employee Network Account or Move* , Information and Technology Services Division (ITSD) accepts a "Request for CAS Employee Network Account or Move" Form to process a request for a new user account. ITSD sends a sealed envelope to the requisitioner containing the employee's network credentials and the *Acceptable Use of Electronic Networks Policy Acknowledgement of Receipt*, which is to be signed by the employee. The requisitioner returns the signed acknowledgement receipt to the Network Services Section. This is the same process used when an employee moves between teams.

The *CAS Exit Policy* states that the Manager is responsible for notifying IT that an employee is terminating or is seconded out of CAS. Whereas the *Network Account Procedures – Manager Responsibilities* describes the management process when an employee arrives or departs.

Audit tested the account process by obtaining a list of all users at CAS and selected a sample of 10 users. Audit determined that all 10 had proper authorization for obtaining user access. However, only one user had a signed acknowledgement Form which is required by CAS IT policy. Therefore CAS is at risk of not having documentation indicating that employee's acknowledge requirements for their use of the CAS network.

Recommendation (Medium – medium enhancement to current processes and controls)

7. The CIO should ensure that all employees sign the Network Use Policy form to acknowledge their responsibilities when using the CAS network.

Management Response and Action Plan Recommendation #7

Agreed. It is important to ensure that this process is consistently applied.

Management Action Plan	Responsible Official	Target Completion Date
The CAS Policy on Acceptable Network and Device Use (PANDU) for CAS employees will be refreshed and employees will be required to formally sign-off their acknowledgement. Employees will be reminded of the policy during log-on, and an employee awareness program will be launched to ensure employees are aware of the revised PANDU.	CIO	December 2017

According to the *Finance ITGC*, terminated employee access to FreeBalance, PBHC and the Trust Account System was not disabled/removed in a timely manner. As a follow-up to this key finding, Audit tested to determine if terminated employees had access to the CAS network after those employees left CAS.

With the exception of one remaining active account, audit determined that struck off strength individuals no longer have access to the CAS network. All accounts were disabled or removed within a short period of time. Having this one active account exposes CAS to the risk of someone using the account to gain unauthorized access to the CAS infrastructure.

The *Policy on Acceptable Use of Electronic Networks and Device Use* indicates that any violation of this policy will be subject to disciplinary action commensurate with the seriousness and circumstances of the incident. It also states that any violations of the policy will be dealt with in a fair and transparent manner. Suspected illegal activities will be reported to law enforcement authorities and may result in disciplinary measures even where a formal criminal charge or civil lawsuit is not pursued.

Employees are responsible for protecting their online personal identity and the Manager, Information Security is responsible for clarifying any questionable network usage. Employees email to the Help Desk the signed Remote Access Services Application and Authorization form to gain access remotely.

Identity management policies are enforced in that every new account or moved account follows the *Network Account Procedures* and *New Employee Procedure Account*. IT Security is currently reviewing the process and has recommended removing some accounts.

IT Security does produce an *IT Security Events Report* which identifies the number of different alerts generated, vulnerability notifications, security event details and outstanding events from previous months. The report also includes actions taken. Refer to recommendation #8 below regarding the monitoring of user accounts.

Network Monitoring

We expected to find that CAS regularly monitors its network for security events and user access.

We found that the CAS network is regularly monitored for IT security events. CAS Firewalls use a product which is a centralized management tool for all firewalls on the network. It has centralized logging of all firewalls and can do historical reporting. CAS uses a reporting tool that can identify key network security threats, issues and trends. It can monitor and gain critical and timely insights about network security, in real time, from anywhere and at any time.

A network monitoring system generally serves to keep track of the entire IT infrastructure with all devices and systems.

Recommendation (Medium – medium enhancement to current processes and controls)

#8. T*he CIO should develop a policy and procedure for regularly monitoring security events that occur on the CAS network. This should include monitoring the dates of last access for all user accounts as well as ensuring terminated employees and contractors have their accounts disabled.*

Management Response and Action Plan Recommendation #8

Agreed. A framework will ensure a more coordinated approach to monitoring of IT security, including identification of dormant accounts.

Management Action Plan	Responsible Official	Target Completion Date
Develop a policy outlining the routine monitoring of IT Security events and document the operational procedures used for the routine monitoring of those IT Security events.	CIO	September 2017
Develop improved processes to get timely information on employee and contractor departures, including reports to identify dormant accounts and detailed procedures to disable and remove them.	CIO	September 2017

Incident Management

We expected to find that CAS has an incident management process that provides for the classification of incidents, recording of incidents and reporting on incidents.

We found that CAS has an effective incident management process in place which includes the *IT and Cyber Security Incident Management Operational Guide* which identifies roles & responsibilities of different sections within CAS. The Guide defines and classifies incidents into low, medium or high impact[7]; outlines procedures for detecting incidents, responding to incidents, reporting on incidents and recovering from incidents. In addition, a CAS guideline produced to describe the deployment of anti-malware and anti-exploit software describes procedures for incident management when Malware is discovered on computers. CAS also has a procedure to deal with an event that was detected by either CSE or SSC and describes how CAS reacts to having a server compromised.

Audit reviewed an incident report from February 2017 (*IT Security Events Report)* and found that the incidents were classified, actions were documented and incidents were communicated to management through this *IT Security Events Report*.

Audit determined that the CAS security incident management process includes:

- Event detection and classification
- Correlation of events and evaluation of threat/incident
- Resolution of threat, or creation and escalation work order
- Criteria for initiating the organization's incident response process
- Who has authority to declare an incident
- Escalation procedures
- Verification and required levels of documentation of the resolution
- Post remediation analysis
- Work order/incident closure

Although incident processing follows the incident management plan, there are no timelines for resolving outstanding IT Security vulnerabilities.

<u>CAS is addressing concerns around incident management</u>

Password Management

We expected that CAS has a password policy identifying requirements for strong passwords, safeguarding passwords and changing passwords.

We found that identity management at CAS includes a *Password Protection Policy* which is a standard for creating strong passwords, protecting those passwords, and identifying the frequency of change.
The *CAS IT Security Best Practices* also includes instructions on creating a strong password (slide 3).

<u>CAS is addressing concerns around password management</u>

3.4 Compliance

It was expected that there is an IT security control framework that includes policies which are appropriate to ensure that Information Technology Security is adequately in place to mitigate CAS IT security risks.

Policies and Standards

Our review of the *Information Security Management Framework* (ISMF) version 6 shows that information Security Policy and Standards reflect a relevant aggregate of directives, rules, and practices that prescribes how CAS manages, protects and distributes information. The ISMF references specific GoC policies including but not limited to: *Policy on Government Security*, *Directive on Departmental Security Management*, *Directive on Information Management Roles and Responsibilities, Policy on Information Management, Privacy and Data Protection – Policies and Publications*. It also references the CAS departmental policies including; *Information Management Framework, Records Management Framework, Information, Records Management and Information Security Policy Suite*.

Audit determined that the existing CAS IT Security Management Framework includes relevant policies and procedures that are related to an ISMF such as:

- *The CAS IT Management Plan* which states that Network Services and Infrastructure supports a large range of applications and many security measures including access control;
- *The CAS IT Security Policy* which states that the ITSD Operations Personnel under the direction of the Director ITSD are responsible for managing access privileges and rights;
- *The CAS Policy on Remote Access* which states that one of the policy objectives is to Balance technology and controls with support to manage remote access and describes requirements for controlling remote access;
- *The CAS Policy on the Use of Electronic Networks and Devices* states that CAS will notify CAS's authorized individuals of its monitoring practices and that authorized users are

responsible for taking reasonable measures to control the use, strength and privacy of their password;

- *The CAS Password Policy* requires strong passwords which must be changed at least every 3 months.

Policies have been implemented to prevent, detect and remove malicious software. These policies include a malicious software prevention policy communicated throughout CAS. These policies are located on the CAS Intranet. Any violations of the above policies or procedures may be subject to appropriate disciplinary actions against the employee.

Audit finds that the CAS IT security framework provides for effective logical access controls but does not describe some rules and review requirements. This creates a risk that inappropriate access to the CAS infrastructure by staff may go undetected.

Recommendation (Medium – enhancement to current processes and controls)

9. *The CIO should develop a policy that defines*
    - *requirements for reviewing audit logs and*
    - *administrative privilege rules.*

Management Response and Action Plan Recommendation #9

Agreed. A policy will ensure requirements and responsibilities related to the operational practices are properly applied.

Management Action Plan	Responsible Official	Target Completion Date
Develop a perimeter protection policy. Develop a policy related to the management and monitoring of administrative privileges.	CIO	December 2017

APPENDIX A – AUDIT CRITERIA

C1	An IT Security governance framework exists that allows for effective management decision-making and oversight of IT security
C2	An overall IT security implementation plan is documented and aligns with the DSP and the IT Plan and provides for integrating information technology security requirements into other processes.
C3	A documented risk management framework exists allowing for the continuous assessment of IT security risks and the certification of IT assets signifying that management has authorized the use of those assets and has accepted the residual risks.
C4	An IT security control framework exists that includes policies which are appropriate to ensure that Information Technology Security is adequate
C5	The IT Security controls that are currently implemented are reasonably effective in preventing and detecting control breaches