Audit and Evaluation Division
June 2025

Audit of Cyber Security

Veterans Affairs Canada
Anciens Combattants Canada

Canada

Acknowledgements

The Audit team gratefully acknowledges Veterans Affairs Canada employees in the Information Technology, Information Management, Administration and Privacy Division. We also acknowledge employees at Shared Services Canada, Communications Security Establishment and the Canadian Centre for Cyber Security. Their contributions were essential to the success of this audit.

Table of Contents

Executive summary

Background and scope

The threat of cyber attacks presents a significant and growing risk to governments all over the world. These threats can challenge national security, economic stability and have the ability to damage public trust. Cyber threats have the potential to disrupt essential services and compromise sensitive data. As these types of attacks become more sophisticated, frequent and rapidly changing, it is essential that governments continually invest in cyber security measures in an effort to mitigate this increased risk.

The Department of Veterans Affairs Canada (VAC) has a responsibility to protect VAC from cyber security events and to protect against substantial damage to the Department's assets and reputation. VAC's current Cyber Security program seeks to "Identify, Protect, Detect, Respond and Recover." However, VAC does not carry this responsibility alone. Shared Services Canada (SSC) also has a role to play in facilitating some services for VAC to support their cyber security needs. It is important to note that the audit focuses only on VAC's role in cyber security management.

This is the first time that this topic has been subject to an audit at VAC. With this in mind, the engagement focused on governance, roles and responsibilities and policies and procedures. This approach is consistent with the Institute of Internal Auditors' (IIA) guidance on auditing cyber security programs. It is reasonable to suggest that a future, additional audit on cyber security could be beneficial which could focus on the more technical aspects of cyber security.

This audit sought to provide reasonable assurance that an adequate management control framework is in place. This is to ensure the Department has clearly defined cyber security goals and is prepared to manage cyber security in the digital era.

The scope included management control frameworks, policies, and procedures in place from January 1st, 2023, up to and including September 30th, 2024. However, the Audit team wanted to ensure the most updated and available information was analyzed and did consider some updated items that were completed by the Department.

Key findings

The information technology security team is a small but extremely knowledgeable group responsible for cyber security at VAC. This team carries considerable corporate knowledge and relies heavily on their competencies and experience to manage cyber security at VAC. There are, however, opportunities to improve the cyber security program at VAC.

The governance structure for cyber security at VAC lacks some clarity in terms of overall governance and defining roles and responsibilities. In addition, some policies and procedures are outdated and normally only updated in a reactionary manner.

VAC does not have a central reporting tool to properly document and record cyber threats and vulnerabilities. The Department relies on monitoring several different tools and the responsibility is shared amongst the team. This increases the risk of something being missed. It is also potentially a missed opportunity to effectively monitor, forecast and identify trends to proactively leverage their future stance on cyber security.

The Audit team found that a new course on cyber security became mandatory for all employees in January 2025. Through VAC's phishing campaign, employees are now increasingly recognizing phishing emails.

The Canadian Centre for Cyber Security (CCCS) is the single unified source of expert advice, guidance, services, and support on cyber security for Canadians. They offer a wide variety of services and tools. While VAC does use some of their services, the audit team found that VAC should consider leveraging more of these tools and services moving forward.

Conclusion

Overall, the Audit team determined that VAC has a strong reputation amongst other departments as it relates to cyber security, however, there are opportunities for further improvement.

Highlights of recommendations

The Audit team has recommended that the Department develop a formal governance framework which outlines roles and responsibilities for cyber security at VAC as well as identifying training that is required for employees. In addition, a recommendation has been made to ensure that the Department is leveraging new and existing tools to support its cyber security threat mitigation, particularly those offered by the CCCS. And finally, the Audit team also recommends that the recommendations from the mock cyber event exercise be implemented in a timely manner.

Chief Audit Executive's Signature
Lindy McQuillan, CPA, CMA
Chief Audit Executive
Veterans Affairs Canada

1.0 Background

The Communications Security Establishment's (CSE) defines Cyber Security as the body of technologies, processes, and practices designed to protect networks, devices, programs and data from attack, damage, or unauthorized access.

Cyber security is increasingly receiving the attention of management boards and committees as network connectivity continues to increase at an exponential rate, placing business outcomes at increasing risk. Consequently, there is increasing need for the audit function to provide cyber security-related compliance assessments, formal risk acceptance validation, internal control testing, and support for investigations and forensics.

Cyber Security events related to Government of Canada (GC) information systems can have a significant impact on the delivery of government programs and services to Canadians and, consequently, confidence in government. Government security and the continuity of GC programs and services rely upon the ability of departments and agencies, as well as government as a whole, to manage cyber security events. The ability to respond to cyber security events in a consistent, coordinated, and timely manner across the GC is essential to ensure the security and resilience of GC programs and service delivery.

Under the new guidance and standards set by the Institute of Internal Auditors (IIA) effective January 9, 2025, the audit followed the top-down industry approach for VAC's first engagement on cyber security. The Audit team attended the IIA's Cyber Security Conference on October 30, 2024, to learn more about this structure and focused on governance, incident response and appropriate policies/procedures.

When VAC identifies services needed to support cyber security initiatives, SSC's role is to support VAC by providing software, systems and resources for the task at hand. SSC collaborates with VAC's information technology security team to ensure that spam filters and protections are configured effectively and in line with security policies. SSC is also involved when major incidents arise to ensure current systems and software are at a sufficient level for mitigation and help acquire anything VAC may need to help with the resolution.

At VAC, there is a responsibility to protect VAC's network from cyber security events as it could cause substantial damage to the Department's assets and reputation. And, with the increasing global adoption and use of artificial intelligence (AI), the responsibility will

only get more challenging. VAC's Cyber Security program seeks to "Identify, Protect, Detect, Respond and Recover." With this in mind, VAC has not had a known "major" event within the Department.

2.0 Audit results

2.1 Governance structure

The governance structure for cyber security at VAC should be better defined and documented.

Why it's important

A well documented and understood governance structure is important because it sets clear guidelines for all VAC employees to ensure security compliance and resilience in the digital environment. It also ensures the Department is prepared for any potential cyber events and that risks are mitigated, reducing the potential for security breaches or data loss.

What we found

The Audit team found that VAC does not have a well-defined governance structure as it relates to cyber security decision making. Furthermore, internal policies and procedures are not well understood, documented or updated in a consistent manner and VAC does not currently identify any key performance indicators or conduct any performance measurement and monitoring.

Interviews with key informants indicated that policies and procedures are normally only updated in a reactionary manner when employees notice that documentation is outdated in their GCdocs repository. The responsibility for updating this documentation is shared amongst the members of the information technology security team. It was also noted that the information contained on VAC's intranet website is mostly outdated and/or obsolete.

The cyber security program at VAC has multiple players. Shared Services Canada (SSC) plays a role in supporting VAC's networks and systems as does the Department's Chief Security Officer in terms of reporting major incidents to the appropriate authorities. However, the vast majority of the program is led by a small but extremely knowledgeable information technology security team which is part of the Information Technology, Information Management, Administration and Privacy Division.

The information technology (IT) security team consists of six staff who each play a significant role in the department's cyber security posture. The team is made up of one IT Manager, one IT Technical Advisor, three IT Analysts and one IT Technician. There is a team lead role that exists but it is not funded and therefore the only supervisory position is the manager. This team has considerable experience and understands their

roles and responsibilities despite the fact that they are not always documented or updated. Interviews with key informants identified that roles and responsibilities as it relates to cyber security are not well understood outside of this team.

The Audit team found that VAC follows CCCS's guidelines, VAC's Cyber Security Event Management Plan (CSEMP) and Treasury Board Secretariat (TBS) policies related to cyber security. The Audit team acknowledges that this is a significant amount of information to process and manage and the information technology security team does so successfully despite the lack of overall governance structure.

At the time of this audit, VAC has not yet had a known "major" cyber event which is defined as any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and incidents. An experienced information technology security team, regular patching programs, software updates, awareness campaigns such as phishing email tests and accompanying training have played important role in the protection of the Department against cyber events.

What is the effect / impact?

Cyber events could have a significant impact on the Department, the integrity of client data and increase the risk of financial or reputational loss. With this in mind, it must be acknowledged that VAC will always be at risk of a cyber event especially with the global adoption of AI and other factors.

VAC must take steps to ensure that mitigation measures are in place to support all employees and to protect the Department. Despite the lack of a documented governance structure for cyber security, VAC successfully manages the requirements of various policies and guidelines. There is a risk, however, that if there is employee turnover, this would not be the case and having a strong governance structure would mitigate this risk.

2.2 Training

Training can play an integral role in employees understanding their roles and responsibilities as it relates to cyber security due to its technical nature and pace of change.

Information technology security employees may also require more specialised training to be able to adapt to the ever-evolving digital space as well as the increase in cyber threats, however, current responsibilities can make attending training a challenge.

Why it's important

As the information technology space and resulting cyber security threats continue to evolve at a fast pace, it is essential that all VAC employees are well informed and receive appropriate training on cyber security.

In addition, it is critical that information technology security employees stay updated on cyber security training because the threat landscape continues to evolve rapidly and there are many new vulnerabilities and attack methods that are emerging. Being adequately and appropriately trained is another important factor in VAC mitigating its cyber security risks.

What we found

The Audit team reviewed training as it relates to all VAC employees and then also as it relates to information technology security employees.

During the course of the audit, on January 22, 2025, VAC implemented its first mandatory cyber security course (Discover Cyber Security (DDN235)) for all VAC employees. The mandatory course was to be completed by March 31, 2025, with annual recertification thereafter. The course is offered by the Canada School of Public Service, and it was established by the Chief Information Officer of the Treasury Board Secretariat and offered in collaboration with the Canadian Centre for Cyber Security.

At the time of this audit, it is anticipated that completion will be tracked similar to other mandatory courses and the course will be reviewed and updated at least annually. These updates will be informed by the evolving cyber security threat landscape and by feedback received from learners. The Audit team took the relatively short course and felt that it had a significant impact on our knowledge of cyber security best practices.

VAC has also implemented a phishing email campaign that uses fictious emails to test and educate employees on cyber security best practices. In the event that an employee “fails” the phishing email test, they are notified of two courses related to cyber security that they must complete followed by a short quiz. If the employee does not attain 80% or higher, they must redo the quiz. Key informant interviews have suggested that this campaign has resulted in an improvement in VAC employees recognizing phishing emails and reporting them however, there is an opportunity to leverage this data further to identify trends and target future campaigns to address those trends. Additionally, there may be opportunity to tweak the quiz on subsequent attempts to ensure employees are actively learning the necessary information.

The Audit team identified that there is a variety of training available for VAC’s information technology security team. The information technology security team has access to free training provided by Microsoft, and some training is based on the team member’s role or interest. The team does not have a broad training curriculum, specific mandatory training, and it is not formally tracked in a central location. Employees reported that management encouraged training to help support the employee’s learning and development. However, interviews identified that training can often be delayed and/or cancelled due to competing priorities making it challenging to take as much training as required.

What is the effect / impact?

The Department has taken steps to improve the awareness and training available to VAC employees with the introduction of the first mandatory course on cybersecurity, however, the lack of consistently improving and updating cyber security training initiatives could have serious ramifications for the Department. Without appropriate training, employees, especially those in information technology security roles, may not be able to recognize or respond to a cyber security threat which could increase the risk to the Department. Information technology security employees need to remain up to date in a rapidly changing environment and this should be monitored to ensure required courses aren't being missed.

Recommendation 1

It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services develop an official governance framework for cyber security including, but not limited to:

- Roles and Responsibilities
- Mandatory and Other Training and Awareness

Management response

Management partially agrees with this recommendation.

Governance framework and roles and responsibilities for cyber security

The Information Technology, Information Management, Administration, and Privacy Division (ITIMAP) will formalize its Cyber Security Governance Framework including integration of roles and responsibilities. Current governance reports through the Digital Advisory Board in which we will establish additional further senior level reporting through that body, and we will also document formally key roles and responsibilities where TBS policy instruments do not provide sufficient guidance. This framework will align with the Treasury Board Secretariat's (TBS) *Policy on Government Security* and *Policy on Service and Digital*.

Training and awareness

As indicated, the department has implemented mandatory training for the department provided by the Canadian School of the Public Service which will be managed and updated by the school on an ongoing basis to align to Government of Canada needs. This will ensure imperative and updated training going forward.

In terms of employee training, the department will not provide a standardized training plan for IT security employees and allow the manager of the IT security unit to manage training in line with their needs and objectives. This approach will be taken due to the following factors:

1. Training for a small group of employees would be managed effectively by the manager directly with those employees
2. The security landscape moves quickly and training should pivot based on current security imperatives.

Individuals may have different focuses and training should be aligned to role and need.

2.3 Monitoring and reporting of cyber threats and vulnerabilities

There are different channels and tools currently in place that are used to evaluate, update and report on potential issues, however, there is no central reporting tool.

Why it's important

Accurate and efficient monitoring for reporting of potential cyber threats and vulnerabilities is important because it helps identify cyber events and trends. It also

provides an accurate picture to senior management on VAC's current cyber security posture. As cyber security continues to evolve with the increasing use of tools like artificial intelligence and our increased reliance on digital services, it is important that VAC integrates innovative tools to remain efficient and effective in the prevention, detection, and mitigation of risks.

What we found

The Audit found that VAC is taking steps to monitor and report on cyber threats and vulnerabilities although there are areas for important. For example, the Communications Security Establishment (CSE) has a "Top 10 IT Security Actions Placemat" that was created after an analysis of cyber threat trends affecting GC internet-connected networks. Essentially, there are ten things that a department should be doing to help mitigate cyber security threats. The Audit team confirmed that VAC is following all of these items and therefore taking important steps to protect its network and assets.

The Audit team was also able to observe the information technology security team walk through several different systems that they are required to monitor daily. The information technology security team collectively shares the responsibility, with no specific position clearly assigned to the task of monitoring these systems which could increase the risk of a threat being missed.

With the requirement to monitor several different systems, it is noted that the information technology security team does not have a central reporting tool. There are several repositories and tools being used to manage, monitor and report on cyber security threats. These threats and vulnerabilities are identified through several channels such as emails, Microsoft alerts, the CCCS and other internal dashboards. The information technology security team must manually pull data from various systems to report to senior management if required.

The CCCS offers many services to GoC departments, however, only two of them are currently mandatory. The mandatory services are the Cyber Centre's Sensor Program and the National Cyber Threat Notification Service (NCTNS). The Audit team found that VAC is subscribed to both of the mandatory services. The team also found that VAC is subscribed to most of the other tools CCCS offers, however, VAC does not have the resources available to be able to fully leverage these additional offerings as there are roughly 30 to consider.

For example, a non-mandatory service identified by CCCS is a dashboard called Howler that is designed to consolidate alerts from all sources and differentiate those that require triage or not. Detection engineers are expected to normalize the alerts, so that they can be looked up and compared with a common schema: Elastic Common Schema (ECS). By putting all the alerts in one place under one schema, it's much easier to find correlating events that warrant scrutiny from a triage analyst. For example, an analyst can easily find all alerts related to a given source IP with a single filter criterion regardless of the schema of the original telemetry. Similarly, there are other products such as Microsoft Sentinel which would provide a similar type of service.

What is the effect / impact?

Working with several tools can be challenging to manage, increases the risks of human error and risks preventing a cyber event from happening. In addition, when data and information is being pulled manually from various systems to report to senior management or others, there is a possibility that some of the data may be inadvertently missed. With no one specifically assigned to this responsibility, there is a risk of events being missed.

Also, by not having a centralized method to report on threats and vulnerabilities, there may be a missed opportunity to identify and monitor trends which could increase the Department's risk mitigation.

Recommendation 2

It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services ensure VAC's network is effectively protected and continuously monitored against potential threats by:

- Developing and implementing processes and procedures to adequately monitor the VAC network and connected devices and,
- Investigate the feasibility of integrating a central reporting tool and,
- Conducting an analysis of additional CCCS offerings and implementing those that are deemed beneficial to VAC.

Management response

Management agrees with this recommendation.

Environmental scan and tool feasibility

The IT security team will review and document the procedures and sources monitored for security related to the VAC network and connected devices to insure consistency and business continuity. The team will also review the sources to insure no duplication between VAC and security partners. Based on these results, the team will determine the go forward requirements and if a tool is required and feasible, and if so, implement that tool.

Evaluation of My Cyber Portal services

The IT Security team will evaluate the systems and services available through My Cyber Portal. If a service is deemed beneficial to the Department, and sufficient internal resources are available to support its use, IT Security will subscribe to the service.

2.4 VAC's Cyber Security Event Management

In March 2024, a third-party consulting firm was invited to assist in exercising VAC's Cyber Security Event Management Plan (CSEMP). From this exercise, ten recommendations were documented, however, no progress has been made on implementation of the recommendations.

Why it's important

The purpose of this exercise was to provide insight into the Department's preparedness for a possible cyber security compromise or event. VAC must be ready to respond, manage the impact and aftermath of the event and everyone involved needs to have a clear understanding of their role and responsibilities and the corresponding processes.

Conducting this type of exercise is a very important part of cyber security management. It is a way to build organizational resilience by ensuring that in the event of an actual breach, the Department's response is coordinated, efficient and effective. Ultimately, having a strong response, will reduce the risk of financial, operational and reputational damage.

What we found

In March 2024, VAC invited a third-party company to assist in exercising VAC's Cyber Security Event Management Plan (CSEMP). This exercise dealt with a possible cyber security compromise and ransom event to provide insight into VAC's preparedness for real threats and identify opportunities for improvement. The exercise involved participants at a senior management level (VAC, TBS, SSC, Veterans Review and Appeal Board (VRAB)) who would be involved in some manner with a cyber event within VAC.

As a result of this exercise, a report was completed, and ten recommendations were documented to help improve the information technology security team's cyber security posture. The top three recommendations from this exercise were:

1. Develop a matrix that outlines key roles and responsibilities for the participants (including third parties and partners) in a cyberattack response event and include it in the CSEMP.

2. Clearly identify who the right decision maker is at each stage of your response and ensure that they have the authority to act. **Important Note:** There was not enough clarity on escalation procedures and when to escalate an event up the chain during this exercise.

3. Update Plans: Continuously develop test and refine the overall CSEMP plan. Document cybersecurity scenario plans and refine IT system-specific playbooks

and ensure BCPs are updated accordingly.

The Audit team reviewed the documentation available related to this exercise and identified that no progress has been made to date on the implementation of these recommendations. The information technology security team stated this is due to multiple competing priorities and a lack of resources available to focus on the implementation Key informant interviews suggested that this exercise could become a regular occurrence as well to ensure VAC was well prepared for an incident. The audit found that there are currently no documented plans for a follow-up exercise.

What is the effect / impact?

Conducting this type of exercise provided valuable insight to all involved on their roles and responsibilities in the event of an actual cyber attack. It also helped participants assess their readiness, gain more experience and identify areas for improvement.

This exercise documented ten recommendations to help improve the Department's readiness. However, by not actioning the recommendations of the CSEMP exercise in a timely manner or not conducting this type of exercise at regular intervals, the Department may face a higher risk of not being prepared if a cyber event was to occur and losing the benefit of the valuable experience gained from such an exercise.

Recommendation 3

It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services take steps to mitigate cyber security risks to the Department by:

- Developing an action plan to implement the existing recommendations from the CSEMP exercise with accompanying timeline for implementation and,
- Developing a plan to conduct additional CSEMP exercises at regular intervals with a mechanism to ensure implementation of resulting recommendations in a timely manner.

Management Response

Management partially agrees with this recommendation.

CSEMP Recommendations:

The Cyber, Information Management and Data (CIMD) Directorate will implement recommendations 1, 2 and 4.

- Recommendation 1 and 2 will involve creating a roles and responsibility matrix outlining key decision makers
- Recommendation 4 outlines executing a CSEMP exercise every 2 years

The following recommendation will have no additional action taken:

- Recommendations 3 is related by keeping documentation up to date for the CSEMP and BCP's which will be done through bi-yearly exercises and BCP processes.
- Recommendation 5 outlines preparing advice on supports to clients for which the department would seek guidance and direction from CCCS and TBS. Therefore we would not craft our own procedures and advice for this item.
- Recommendation 6 related to risk appetite in general will continue to be high scrutiny and high response as flagged in the departmental risk framework and the current government of Canada position on cyber. Risk items will be discussed through governance updates as well as situational briefings which will occur though new governance and therefore we would not engage in a separate exercise.
- Recommendation 7 in regards to communications templates would not have sufficient benefits as communications will be very scenario dependent with many unique situations. Communications will be guided from CCCS and TBS for more complex scenarios, and for something infrequent will result in a high burden to keep material constantly updated for not a large benefit.
- Recommendation 8 in regards to internal vs external threats is something considered in all situations and part of standard security knowledge and practices.
- Recommendation 9 related to capturing records of incidents is outlined multiple times in the CSEMP templates and is integrated into the process. There is not a large benefit to providing specific training to individuals on capturing notes as it may be multiple people and a generally standard practice.
- Recommendation 10 is a noted consideration around containment vs disablement and would be part of standard considerations of a cyber analyst. This would not require any additional action.

2.5 Audit Opinion

Based on the findings above, the Audit team determined that the management of cyber security at VAC requires improvement. Although VAC is currently performing many tasks instrumental in mitigating cyber threats to the Department, improvements such as a formal governance framework which outlines roles and responsibilities as well as training requirements, leveraging new and existing tools and resources, conducting a regular mock cyber exercise and committing to implementing the resulting recommendations from the exercise will help ensure the Department is well positioned to meet the challenges associated with cyber security in the future.

In addition, given this was the first time that this topic has been audited at VAC, cyber security should be given consideration in future as part of risk-based audit planning for an additional audit, perhaps from a more technical perspective.

The audit conforms with the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing (the Standards), as supported by the results of the quality assurance and improvement program. The audit findings and conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with the Standards. The opinions expressed in this report are based on conditions as they existed at the time of the audit and apply only to the entity examined.

Appendix A – About the audit

Scope and Objectives

The scope of the audit included management control frameworks, policies, and procedures in place on January 1st, 2023, up to and including September 30th, 2024. It was very important to analyse the latest information available giving the rapidly changing and evolving landscape of cyber security. The scope excluded system access controls as a separate audit is in its final stages of completion.

The objectives of this audit were as follows:

1. VAC has an appropriate governance structure, policies, procedures, and monitoring in place to manage cyber security based on GC guidelines and best practices; and
2. VAC has the appropriate measures in place to prevent, respond to and learn from a cyber event.

Audit Criteria

Objective 1

VAC has an appropriate governance structure, policies, procedures, and monitoring in place to manage cyber security based on GC guidelines and best practices.

Criteria

a) The Department has implemented an effective governance framework and has bodies in place to ensure sufficient oversight of cyber security risks and initiatives.

b) The Department has clearly defined and communicated roles, responsibilities, policies, and procedures relating to cyber security including clearly defined roles and responsibilities with external partners such as Shared Service Canada and the Canadian Centre for Cyber Security.

c) The Department has a performance monitoring and reporting process in place to evaluate, update and report on cyber security activities.

d) The Department provides the necessary training and resources to support employees in performing their responsibilities relating to cyber security.

Objective 2

VAC has the appropriate measures in place to prevent, respond to and learn from a cyber event.

Criteria

a) The Department provides employees with the necessary training, tools, resources, and information to support them in discharging their responsibilities relating to cyber security.

b) The Department has the necessary processes and procedures in place for the prevention and response to a cyber security attack.

c) The Department has a performance monitoring and reporting process in place to evaluate, update and report on cyber security activities.

Methodology

Methodology	Purpose
Interviews	Inquired about interviewees roles and responsibilities as well as SSC and CCCS. Inquired about policies, directives, processes, guidelines, standards that are in place and whether they are up to date. Inquired about training for the information technology security team that is responsible for cyber security at VAC as well as all employees training. Inquired about tracking, monitoring, and reporting cyber security events, incidents, and trends. Inquired about the systems/software that are used to protect VAC's assets from cyber security events. Inquired about documentation being outdated on VACs @work today as well as their overall documentation process. Inquired whether mock cyber events are conducted as a learning experience and safety protocol.
Direct Observation	Audit team completed the Discover Cyber Security - DDN 235 course, mandatory for all employees. (came into effect January 2025) Audit team went through the phishing email process, passing and failing the quiz and what were the results. Observed several system processes that VAC's information technology security team uses.

Methodology	Purpose
Documentation Review	Reviewed GC and VAC's Cyber Security Event Management Plans. Reviewed information such as services, tools etc. on CCCS's website. Reviewed GC Enterprise Cyber Security Strategy. Reviewed information technology security information on VAC's intranet (@work). Reviewed media articles. Reviewed numerous policies, directives, processes, guidelines, standards and security plans (TBS, CCCS, VAC, GC). Reviewed previously completed and ongoing internal/external audits and horizontal evaluations. Reviewed the mock cyber security attack reporting DECKs.
File Review	N/A
Data Analysis	N/A
Survey/Questionnaire	N/A

Appendix B – Risk ranking of audit opinion

The following definitions are used to classify the ranking of the audit opinion presented in this report.

Well Controlled	Only few, insignificant weaknesses relating to the control objectives or sound management of the audited activity are identified.
Generally Acceptable	Identified weaknesses when taken individually or together are not significant or compensating mechanisms are in place. The control objectives or sound management of the audited activity are not compromised.
Requires Improvement	Identified weaknesses, when taken individually or together, are significant and may compromise the control objectives or sound management of the audited activity.

Appendix C – Recommendations and management response

Audit Recommendation	Management Response	Timeline for Completion
Recommendation # 1 It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services develop an official governance framework for cyber security including, but not limited to: • Roles and Responsibilities • Mandatory and Other Training and Awareness	**Management response** Management partially agrees with this recommendation. **Governance framework and roles and responsibilities for cyber security** The Information Technology, Information Management, Administration, and Privacy Division (ITIMAP) will formalize its Cyber Security Governance Framework including integration of roles and responsibilities. Current governance reports through the Digital Advisory Board in which we will establish additional further senior level reporting through that body, and we will also document formally key roles and responsibilities where TBS policy instruments do not provide sufficient guidance. This framework will align with the Treasury Board Secretariat's (TBS) *Policy on Government Security* and *Policy on Service and Digital*. **Training and awareness** As indicated, the department has implemented mandatory training for the department provided by the Canadian School of the Public Service which will be managed and updated by the school on an ongoing basis to align to Government of Canada needs. This will ensure imperative and updated training going forward. In terms of employee training, the department will not provide a standardized training plan for IT security employees and allow the manager of the IT security unit to manage training in line with their needs and objectives. This approach will be taken due to the following factors:	Full Completion by December 2026

	1. Training for a small group of employees would be managed effectively by the manager directly with those employees 2. The security landscape moves quickly and training should pivot based on current security imperatives. Individuals may have different focuses and training should be aligned to role and need.	
Recommendation # 2 It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services ensure VAC's network is effectively protected and continuously monitored against potential threats by: • Developing and implementing processes and procedures to adequately monitor the VAC network and connected devices and, • Investigate the feasibility of integrating a central reporting tool and, • Conducting an analysis of additional CCCS offerings and implementing those that are deemed beneficial to VAC.	**Management response** Management agrees with this recommendation. **Environmental scan and tool feasibility** The IT security team will review and document the procedures and sources monitored for security related to the VAC network and connected devices to insure consistency and business continuity. The team will also review the sources to insure no duplication between VAC and security partners. Based on these results, the team will determine the go forward requirements and if a tool is required and feasible, and if so, implement that tool. **Evaluation of My Cyber Portal services** The IT Security team will evaluate the systems and services available through My Cyber Portal. If a service is deemed beneficial to the Department, and sufficient internal resources are available to support its use, IT Security will subscribe to the service.	Full Completion by March 2027

Recommendation # 3 It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services take steps to mitigate cyber security risks to the Department by: • Developing an action plan to implement the existing recommendations from the CSEMP exercise with accompanying timeline for implementation and, • Developing a plan to conduct additional CSEMP exercises at regular intervals with a mechanism to ensure implementation of resulting recommendations in a timely manner.	**Management Response** Management partially agrees with this recommendation. **CSEMP Recommendations:** The Cyber, Information Management and Data (CIMD) Directorate will implement recommendations 1, 2 and 4. • Recommendation 1 and 2 will involve creating a roles and responsibility matrix outlining key decision makers • Recommendation 4 outlines executing a CSEMP exercise every 2 years **The following recommendation will have no additional action taken:** • Recommendations 3 is related by keeping documentation up to date for the CSEMP and BCP's which will be done through bi-yearly exercises and BCP processes. • Recommendation 5 outlines preparing advice on supports to clients for which the department would seek guidance and direction from CCCS and TBS. Therefore we would not craft our own procedures and advice for this item. • Recommendation 6 related to risk appetite in general will continue to be high scrutiny and high response as flagged in the departmental risk framework and the current government of Canada position on cyber. Risk items will be discussed through governance updates as well as situational briefings which will occur though new governance and therefore we would not engage in a separate exercise. • Recommendation 7 in regards to communications templates would not have sufficient benefits as communications will be very scenario dependent with many unique situations. Communications will be guided from CCCS and TBS for more complex scenarios, and for something	Full Completion by March 2026

	infrequent will result in a high burden to keep material constantly updated for not a large benefit. • Recommendation 8 in regards to internal vs external threats is something considered in all situations and part of standard security knowledge and practices. • Recommendation 9 related to capturing records of incidents is outlined multiple times in the CSEMP templates and is integrated into the process. There is not a large benefit to providing specific training to individuals on capturing notes as it may be multiple people and a generally standard practice. • Recommendation 10 is a noted consideration around containment vs disablement and would be part of standard considerations of a cyber analyst. This would not require any additional action.	