CANADIAN CENTRE FOR CYBER SECURITY

UNCLASSIFIED

CYBER SECURITY AUDIT GUIDE FOR THE GOVERNMENT OF CANADA

June 2020

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

Contents

Acronyms, Abbreviations and Definitions

Acronyms and Abbreviations

BIA	Business Impact Assessment
CIA	Confidentiality, Integrity and Availability
CSE	Communications Security Establishment
CSA	Control Self-Assessment
GC	Government of Canada
HIPS	Host-based Intrusion Protection System
DSO	Departmental Security Officer
DSP	Departmental Security Plan
GSP	*Government of Canada Security Policy*
IT	Information Technology
SA&A	Security Assessment & Authorization
TBS	Treasury Board of Canada Secretariat
TRA	Threat & Risk Assessment

Definitions

Cyber Security: The body of technologies, processes, and practices designed to protect networks, devices, programs and data from attack, damage or unauthorized access.

Administrative Privileges: Network, system or computer access rights provided to network or system administrators to carry out their duties managing and maintaining network and/or system operations.

Hardening: The disabling of all non-essential ports and services of a computer (i.e., normally a server) and removal of unnecessary accounts.

Host Level: A host is a computer that is accessible over a network. It can be a client, a server or any other type of computer (e.g., data server, e-mail server, workstation, laptop).

Host-based Intrusion Prevention System: A system or a program employed to protect critical computer systems -- against viruses and other Internet malware -- by placing sensors on any device that hosts data.

Patch Management: Updating software programs, with programming code changes, to correct recognized errors/weaknesses in the code that can result in negative outcomes.

Malicious Signatures: Recognized coding (e.g., a computer virus) -- that is like a fingerprint -- which can be detected and then isolated to protect the host e-mail, program or function where the signature code is located and/or what the malicious code is targeting.

Allowlisting: A list of items that are granted access to or through a specific device or system (e.g., transmissions from an acceptable IP address). When allowlisting is used, all entities are denied access except those included in the allowlist.

Cyber Security
Glossary of Terms: https://techterms.com/

CYBER SECURITY AUDIT GUIDE

Preface

This Audit Guide has been prepared to assist federal institutions in determining the extent to which cyber security governance, policy compliance, risk management, and protective measures are sufficiently planned and applied to minimize the risk of electronic intrusion.

The Audit Guide can be used in three ways:

- First, it presents the policy requirements, along with related information and key sources, for understanding the basics of establishing and auditing cyber security.
- Second, it provides background information to broaden the reader's understanding of the responsibilities of key stakeholders involved in establishing, assessing and auditing cyber security.
- Third, it proposes cyber security audit guidance, criteria and tests so that internal auditors may develop a customized audit program(s) using a risk-based audit approach.

The Communications Security Establishment (CSE) Internal Audit Group, with support from the CSE Canadian Centre for Cyber Security, has prepared this Audit Guide, an Audit Program and a Preliminary Survey Tool to promote an enhanced understanding of auditing cyber security in the federal government.

Section 1. Audit Guide Use and Organization

Guide Use

This Guide is intended as a reference tool for internal auditors in the Government of Canada but may also be of assistance to other federal employees who have not had exposure to cyber security. It was developed under guidance from the CSE Canadian Centre for Cyber Security.

The Guide has been structured to prepare internal auditors for the broad range of review activities that are inherent in cyber security. The Guide presents internal auditors with the opportunity to better inform management by tailoring their engagements to their department's areas of highest cyber security risk and management concern. Consequently, internal auditors will need to apply a risk-based approach and configure audit criteria and sub-criteria to address areas of substantial cyber security risk.

In this Guide, information is first given on the related Government of Canada policy framework, in order to communicate the environment and responsibilities in which various cyber security stakeholders build and maintain IT operations (i.e., that require ongoing vigil against a wide range of threats). The Guide then provides an audit approach, criteria and sub-criteria that address the soundness of the related management framework, compliance with policies and directives, and operational risk management and mitigation. Background information is given to supplement research.

Audit criteria and sub-criteria serve as suggestions for planning, scoping and preparing a cyber security audit program. For ease of reference, policy-compliant audit criteria are shaded in this Guide.

Guide Organization

The Audit Guide is organized into three parts:

Sections 1-5:	Requirements from the cyber security policy framework, and context for the Audit Guide, are provided in the body of the Guide.
Section 6:	The cyber security audit objective and audit criteria, which reflect the main operational responsibilities of institutions, are provided in Section 6 entitled Audit Elements.
Appendices:	Appendices cover cyber security accountabilities, and cyber security audit references & internet web sites.

Section 2. Scope of the Audit Guide

The Audit Guide is intended for use in all federal institutions. The Guide applies to some 150 departments, agencies and Crown corporations. The guide is intended to be an evergreen document and will be updated periodically.

The scope of this Guide is limited to cyber security governance, risk management, and preventive measures. Audit guidance in this document is focused on verifying that steps have been taken to build a sound management control framework for preventing cyber intrusion and protecting the institution's assets from attack.

It is recommended that Government of Canada internal auditors refer to the key policy framework requirements listed below, in order to learn more about how departments and agencies might organize their cyber security business practices.

Requirements
Policy on Government Security: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

Directive on Security Management: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611

Directive on Identity Management: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577

Guidance
CSE *TOP10 IT Security Actions*: https://cyber.gc.ca/en/top-10-it-security-actions

Section 3. Assumptions

In conducting an audit of cyber security, it is assumed that the internal auditor possesses both internal audit knowledge and fundamental cyber security skills and other competencies needed to perform the planning phase of the engagement, and an understanding of the risk-based audit methodology indicated in this Guide. Should the Internal Auditor or audit team not possess these competencies, it is assumed that such competencies would be acquired to support the audit engagement.

It is further assumed that cyber security audits will be completed in accordance with professional internal audit standards. For internal auditing standards followed by the Government of Canada, please refer to The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing (IPPF):

https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx

Section 4. Overview of a Cyber Security Audit

4.1 Does Internal Audit really need to become involved in cyber security?

Historically, the Chief Audit Executive - Internal Audit provides independent opinions on program operations, financial management, procurement, human resource management and information systems. Cyber security, however, 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.[1]

4.2 Where is cyber security in the 'Three Lines of Defence'?

Management is the First Line of cyber defence, followed by responsibility-based risk management as the Second Line, and internal audit as the Third Line of cyber defence:[2]

First Line – Management: Ensures regular management reviews; functional/technical testing; social/behavior testing; and Control Self-Assessments (CSA).

Second Line – Risk Management: Ensures identification of emerging risks; ID of threats, vulnerabilities and risks; Business Impact Assessments (BIA); and formal risk evaluations.

Third Line – Internal Audit: Undertakes cyber security compliance testing; internal controls examination; and examines formal risk tolerance and acceptance.

4.3 Is an audit necessary if key cyber protection assets are in place?

Even organizations that are low on the maturity scale have often implemented key controls that are necessary as a first line of defence. However, these organizations may not have planned their systems implementation(s) with comprehensive identification and installation of cyber defence according to a formal and recognized framework.

For example, they may have implemented a firewall, antivirus software, and some user education about cyber threats and making proper backups. Each of these practices, and related controls, serve an important purpose to protect information assets. However, the same organization may have not placed adequate attention to assuring that firewall rules are updated regularly, antivirus software may not be installed on all workstations or may not contain the latest malicious signatures (i.e., unique and identifiable program code), or end-users who are on leave may have missed security awareness training. Therefore, even though controls may appear to be in place, the organization must regularly conduct (independent) audits to ensure these processes are well-designed, are executing properly, and are meeting senior management and business needs.[3]

[1] *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, ISACA, 2017, 15 pages, pg. 8.
[2] Ibid, pg. 5.
[3] Ibid, pg. 4.

4.4 What should the auditor look for from management oversight of cyber security?

Cyber security responsibility should be formally and clearly delegated, from senior management, to various officers across the organization, in order to carry out appropriate testing activities such as functional and technical validation testing, control self-assessment (CSAs), attack and breach penetration testing, social/behavior testing, and management reviews. Each of these processes is part of the overall business process designed to identify control weaknesses or deficiencies in either the design or ongoing execution of business and system controls.[4]

4.5 Where should the internal auditor begin?

It is a common practice for internal auditors to begin the audit planning phase with a risk review in the area of compliance. Following compliance review, the internal auditor should review current and emerging cyber risks to the department, and then review the security controls that exist or are planned to be in place to protect the department's information assets.

The system(s) included in the audit risk review should have (i) a documented business purpose, (ii) technical specifications, and (iii) identified/documented controls that are currently operating. All the system assets involved should be formally recorded by the department. Also, understanding the security requirements of data in the system will help to frame the scope of the risk review (i.e., have the owners of business data clearly identified the levels of data confidentiality, integrity and availability that must be maintained?). Understanding these requirements will help frame the scope of the risk review. Failure to accurately scope data, and the systems that process data, can result in critical assets being excluded from needed security protections.[5]

4.6 What competencies are expected to conduct this type of audit?

An IT or systems auditor is not expected to plan and conduct the technical portions of this type of examination; the audit team will require a technical resource to advise and guide the audit team, whether he or she if from within the organization (i.e., an internal IT Branch advisor as part of the audit team), a contractor or a retiree. This resource will be needed to bridge the 'language divide', help with interviews, planning, data gathering and evidence assessment, and be a near to full-time part of the audit team for the Examination Phase of the audit.[6]

[4] Ibid, pg. 5.
[5] Ibid, pg. 6.
[6] Ibid, pg. 6.

Section 5. Understanding Cyber Security from a Management Perspective

In the process of conducting a cyber security audit, the internal auditor or CAE may be asked by senior management to answer high-level risk-related questions based on management concerns. For example, how well is the department adjusting to the requirements of the *Policy on Government Security*, the *Directive on Identity Management*, and the *Directive on Security Management*? Preparation for questions that could be asked by the audit committee or the deputy minister will support the presentation of audit findings and recommendations.

Other questions could be asked regarding overall implementation of the department's cyber security policy framework:

- Has awareness of cyber security risks, and the related policy framework, been raised sufficiently in the department?
- Are there instances where the department's introduction of a new, or significantly updated, IT service or application have been made without the corresponding completion of a Security Assessment & Authorization (SA&A)?
- Has the department fully understood the extent of its obligations within the cyber security policy framework (e.g., are cyber security responsibilities, risk identification and risk mitigation processes being verified only through template checking exercises)?

Other examples of management concern related to cyber security may include:

- Does it appear that the institution is obtaining and retaining the expertise required in the areas of IT operations, security, IT security, risk analysis, Threat and Risk Assessments (TRAs), and SA&A's?
- Are the costs of conducting an SA&A identified and integrated into the plan for a new IT function, service or application?
- Is the Level of Effort required from key stakeholders (i.e., appropriate officials from programs, IT operations, security, IT security, privacy and the information management areas) to complete an SA&As considered manageable?

Section 6. Audit Elements

Overall Audit Objective

To determine whether cyber security actions have been sufficiently planned and applied to minimize the risk of electronic intrusion.

Audit Program Organization

Criteria 1-10 – Internal Controls: To determine whether cyber security controls that could affect the reliability, accuracy and security of the enterprise infrastructure, data and resources are sufficiently understood, assessed, implemented and monitored.

1. **Internet Gateways**: The number of discrete external connections to the departmental network is minimized and centrally managed. (TOP10 #1)

2. **Patch Management**: Patch maintenance for operating systems and applications are implemented in a timely manner. (TOP10 #2)

3. **Administrative Privileges**: Access permissions are managed incorporating the principles of least privilege and separation of duties. (TOP10 #3)

4. **Harden Operating Systems (OS's)**: Operating Systems are hardened by customizing and selecting configuration settings, applying an enterprise approach. (TOP10 #4)

5. **Segment Information**: Information stores are categorized and segmented based on information sensitivity and privacy. (TOP10 #5)

6. **Awareness and Training**: A culture of security awareness is supported by tailored awareness and training. (TOP10 #6)

7. **Manage Devices**: Devices are managed at the enterprise level. (TOP10 #7)

8. **Host Level Protection**: A Host-based Intrusion Prevention System (HIPS) is deployed. (TOP10 #8)

9. **Web-facing Applications**: Web-facing applications are isolated. (TOP10 #9)

10. **Application Allowlisting**: Application allowlisting is implemented to control which applications can be installed or run. (TOP10 #10)

Criteria 11 - Governance: To determine whether a sufficient and effective management control framework is in place to support cyber security for the organization.

11.1 Policy Framework: The policies, practices and processes to manage and monitor the organization's regulatory, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.

11.2. Identifying Compliance: Departmental information technology (IT) security requirements and practices, including those for cyber security, are defined, documented and maintained.

11.3 Security Controls: Security controls are defined, documented, implemented and maintained to meet departmental IT security requirements, in accordance with departmental practices.

11.4 Systems Design: IT security is considered in key processes and design of new systems and projects.

11.5 Identify Assets: The data, devices, systems, and facilities that enable the organization to achieve business objectives are identified and managed.

Criteria 12 – Risk Management: To determine whether the organization understands its cybersecurity risks to operations, assets and individuals, and whether the organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.

12.1 Understanding Cyber Risk: The organization understands the cybersecurity risk to organizational operations (including mission, functions or reputation), organizational assets, and individuals.

12.2 Mitigating Risk: The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.

For easy identification, all mandatory / compliance criteria are shaded in the Audit Program.

APPENDIX A – Examples of Enumerated Cyber Security Accountabilities

Stakeholders	**Key Accountabilities** (from the *Policy on Government Security*)
Deputy Heads of Departments (*PGS* Section 4.1)	• Establish the department's security governance, including responsibilities for security controls and authorities for security risk-management decisions. (s. 4.1.2) • Identify security and identity management requirements for all departmental programs and services, considering potential impacts on internal and external stakeholders. (s. 4.1.4) • Approve a three-year Departmental Security Plan (DSP) that is reviewed annually, sets out strategies for meeting departmental security requirements reflective of and contributing to government-wide security priorities, and addresses the security controls described in Appendix A of the *Policy on Government Security*. (s. 4.1.5) • Review any residual security risk that exceeds established authorities for security risk management decisions. (s. 4.1.6) • Investigate and act when significant issues regarding policy compliance arise and ensure that appropriate remedial action is taken to address these issues. (s. 4.1.10)
Secretary of the Treasury Board (*PGS* Section 4.4)	• Liaise with Deputy Heads and other senior officials on security issues, including security events that have potential government-wide impacts. (s. 4.4.3) • Liaise with other lead security agencies on matters of national security and emergency management. (s. 4.4.4) • Establish measures that support the capacity and development of the security functional community. (s. 4.4.5)
Treasury Board of Canada Secretariat (*PGS* Section 5.12)	• Establish and oversee a whole-of-government approach to Security Management as a key component of all management activities by ensuring the conduct of periodic reviews of the effectiveness of security support services, to provide assurance that they continue to meet the needs of the government as a whole. (s. 5.12.1) • Provide policy leadership, advice and guidance for all matters related to government Security. (s. 5.12.2) • Provide strategic policy oversight and coordination for the management of security events that may affect the government as-a whole. (s. 5.12.3)

Stakeholders	**Key Accountabilities** (from the *Policy on Government Security*)
Lead Security Agencies and/or internal enterprise service organizations (*PGS* Sections 5.3 – 5.11)	• Canadian Security Intelligence Service (CSIS) ○ Provide government-wide security screening services. (s. 5.1.3.1) ○ Fulfill government-wide functions by investigating and analyzing threats to the security of Canada and by providing related reporting and advice to the Government of Canada. (s. 5.3.2) ○ Maintain a central registry for the retention of forms that designate persons permanently bound to secrecy under the Security of Information Act. (s. 5.3.3) • Communication Security Establishment (CSE) ○ Serve as the lead technical authority for information technology (IT) security, including the provision of leadership, advice, services and guidance for technical matters related to IT security. (s. 5.4.1) ○ Help to ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada. (s. 5.4.2) ○ Fulfill the following government-wide functions (s. 5.4.3) • Identify emerging cyber threats, • Defend government networks and systems, and • Protect against, and mitigating potential impacts of, cyber security events. ○ Lead the development of trusted sources of supply for government and critical infrastructure, and for mitigating the risk of untrusted equipment. (s. 5.4.4) ○ Serve as the national authority for communications security (COMSEC), including the procurement, distribution, control and use of cryptographic devices and encryption keying material for national security systems. (s. 5.4.5) ○ Serve as Canada's national authority for signals intelligence (SIGINT). (s. 5.4.6) • Department of National Defence (DND) ○ Fulfill government-wide functions for scientific and technological security research, defence intelligence, and investigation of security threats to military systems. (s. 5.5.1) ○ Provide support to departments in relation to the protection of Government of Canada officials outside Canada, cyber

Stakeholders	**Key Accountabilities** (from the *Policy on Government Security*)
	security, and the provision of other security-related services. (s. 5.5.2) o Serve as Canada's national authority for Talent-Keyhole (TK) information. (s. 5.5.3) • Privy Council Office (PCO) o Providing advice on recommendations from the Security Intelligence Review Committee (SIRC) regarding the security clearance of individuals. (s. 5.7.3) • Public Safety Canada (PSC) o Provide leadership, technical advice and guidance for matters related to business continuity management. (s. 5.8.1) o Provide operational leadership for the coordination, information sharing and situational awareness relating to security events involving multiple federal Departments or Agencies that may have government-wide, intergovernmental, critical infrastructure or national impacts. (s. 5.8.2) o Lead coordination and strategic policy-making on national security and national cyber security matters. (s. 5.8.4) ➢ Public Services and Procurement Canada (PSPC) o Provide emergency procurement and emergency accommodation and provide security services to help ensure the protection of sensitive information entrusted to Canadian and foreign industry. (s. 5.9.3) o Provide internal services for contract security, base building security for general-purpose office facilities under its custodial responsibility, and IT and IT security in support of providing and managing certain government-wide applications. (s. 5.9.4) ➢ Shared Services Canada (SSC) o Plan, design, build, operate and maintain effective, efficient and responsive enterprise IT security infrastructure services to secure federal data and systems under its responsibility. (s. 5.11.1)

APPENDIX B – Cyber Security Audit References & Internet Websites

Policy on Government Security
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

Directive on Security Management
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611

Directive on Identity Management
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577

Policy on Service and Digital (2020*)*
The Policy on Service and Digital will take effect on April 1, 2020. It will replace the Policy Framework on Information and Technology, the Policy on Management of Information Technology, the Policy on Information Management, the Policy on Service, and the Policy on Acceptable Network and Device Use.

The Policy Framework on Information and Technology, the Policy on Management of Information Technology, the Policy on Information Management, the Policy on Service, and the Policy on Acceptable Network and Device Use remain in effect until April 1, 2020.
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603

Guide to the Review of Management of Government Information Holdings (*MGIH*) (1995) – even though this Guide is based on the outdated *MGIH* Policy, it can be used to review the management of the information lifecycle. The Guide lists good practices in the establishment of limited collection processes.
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13602

Privacy Act and *Regulations* (1983; R.S. 1985) govern collection, use, disclosure and retention of personal information by federal government institutions listed in the Schedule to the *Privacy Act*.
https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

Policy on Privacy Protection (2018) provides direction to government institutions to ensure compliance with the Privacy Act regarding the collection, retention, use, disclosure and disposal of personal information.
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

ISACA Journal; Information Systems Audit Basics: *Auditing Cybersecurity*
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/is-audit-basics-auditing-cybersecurity

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework/framework

ISO/IEC 27001:2013: Continually Improving Information Security Management
https://www.iso.org/standard/54534.html

CSE *TOP10 IT Security Actions*
https://cyber.gc.ca/en/top-10-it-security-actions

CSE Information Technology Security Guidance – A System Lifecycle Approach (ITSG-33)
https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33

CSE Learning Hub – Canadian Centre for Cyber Security
https://cyber.gc.ca/en/learning-hub

APPENDIX C – List of Potential Cyber Security Audits

Selection of audits to be placed in departmental risk-based audit (& evaluation) plans should be the result of the assessment and determination of the overall need for the engagement based on risk, materiality and management concern. Notwithstanding, a potential ordering of cyber security engagements is presented below for consideration.

Potential Cyber Security (CS) Audits*	**Audit Criteria** **(refer to pages 10 & 11)**
Audit of Cyber Security Governance (L)	# 11
Audit of Cyber Security Risk Management (L)	# 12
Audit of Internet Gateways / TOP10 #1 (M)	# 1
Audit of CS Awareness & Training / TOP10 #6 (L)	# 6
Audit of Patch Management / TOP10 #2 (M)	# 2
Audit of Administrative Privileges / TOP10 #3 (H)	# 3
Audit of Secure Configuration / TOP10 #4 (H)	# 4
Audit of the Management of Cyber Devices / TOP10 #7 (M)	# 7
Audit of the Segmentation of Information Stores / TOP10 #5 & Audit of Isolating Web-facing Applications / TOP10 #9 (H)	# 5 & # 9
Audit of Host-level Protection / TOP10 #8 (H)	# 8
Audit of Application Allowlisting / TOP10 #10 (M)	# 10
* The level of IT security technical assistance anticipated: Low = L; Moderate = M; and High = H	