DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

May 2020

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Contents

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

INTRODUCTION

Purpose: To provide internal audit groups in federal departments and agencies with a cyber security audit program that can be adapted to address the risks and concerns particular to each organization.

This audit program provides the criteria, sub-criteria and audit tests that could be used for the development of a cyber security audit. The criteria and tests (found from 1 to 10) are based on CSE's *Top 10 IT Security Actions*. The governance and risk portion (11 and 12) outline the criteria, sub-criteria and audit tests for governance and risk management of a cyber security audit. The audit program is sourced from several authoritative references that are identified with each criterium. The governance and risk criteria include current policy framework requirements of the Government of Canada.

The audit program is intended to be used in conjunction with two other documents: The *Cyber Security Audit Guide* and the *Cyber Security Preliminary Survey Tool* (PST). The intended order of use is the guide (explains the rationale for cyber security audits), the PST (a tool for use in the preliminary survey stage of a cyber security audit), and then the audit program (from which audit criteria, sub-criteria and audit tests are selected to support the audit lines of inquiry determined by the audit team).

Evergreen Document: This audit program is presented as an evergreen document that is to be updated, periodically, on an ongoing basis. Updates to the audit program are to be obtained from a variety of common sources, including professional associations, academia, government directions and auditors like you. In this regard, any suggested changes to this audit program are appreciated.

Audit Program Confirmation: This audit program has been tested from a network audit perspective. The audit criteria, sub-criteria and tests presented are intended to be as general as possible and are provided as guidance to assist you in developing an audit program tailored for the environment that is the subject of your audit.

Selecting an Audit Approach: This audit program can be used in different ways to best meet the needs of the organization. The approach or focus of an audit can vary by engagement, and is often dependent upon business risks, audit timing, audit resourcing, auditor experience, previous audit findings, and/or management concerns at the time the audit is being planned. Therefore, depending on your circumstances, you may choose to focus your cyber security engagement on one or several of the following:

1. A governance and risk management focus (that addresses the whole enterprise).
2. Examining just one network, where a preliminary/audit risk review is conducted and the *Preliminary Survey Tool* (PST) is applied to determine which parts of the audit program should be used for your engagement.
3. Selecting one of the 'TOP10' criteria and applying it enterprise wide, such as examining the security of your internet gateway. The *Preliminary Survey Tool* (PST) is applied to help determine which parts of the audit program should be used for your engagement.
4. Compliance with the Treasury Board of Canada policy framework, either for one network or enterprise wide. To support this audit approach, Government of Canada compliance criteria are indicated in purple within the audit program.

1 USE SHARED SERVICES CANADA (SSC) INTERNET GATEWAYS

Reduce the number of discrete external connections to a departmental network by using the consolidated Internet gateways provided by SSC. Users will benefit from the protection provided by higher level cyber defences deployed at the enterprise level that monitors for, and can respond to, unauthorized entry, data exfiltration or other malicious activity.

Table 1: SSC Gateways

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
1.0 The number of discrete external connections to the departmental network is minimized* and centrally managed.	SSC Consolidated Networks 1.1 Consolidated internet gateways are provided by Shared Services Canada (SSC); which are used to reduce the number of discrete [i.e., distinct/separate] external connections to the departmental network.	1. Confirm that any internet connections that are not SSC gateways be justified, documented and approved by the appropriate level of management in the organization.			ITSB-89 *Mandatory based on the Directive on Security Management App B (B.2.3.6.2)
	Access Control 1.2 External access to the departmental network(s) is minimized and managed.	1. Identify all external connections via a network diagram. (added audit) 2. Determine whether policies and procedures related to external access capabilities are formally approved. Consider the following: a. External connections (e.g., employees, contractors, third parties) with access to critical systems are approved and documented. b. Remote connections are only opened as required. c. Remote connections are logged and monitored. d. Remote connections are encrypted. e. Strong authentication is in place (e.g., multifactor, strong password parameters). f. The ability to wipe data remotely on mobile devices when data are missing or stolen is enabled. g. Institution security controls (e.g., antivirus, patch management) are required on remote devices connecting to the network. 3. The information system implements sub-networks for publicly accessible system components that are physically/logically separated from internal organizational networks. 4. The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	APO13.01; DSS01.04; DSS05.03		ISO/IEC 27001:2013 A.6.2.2; A.13.1.1; A.13.2.1 ITSG-33 Security Control SC-7

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
	Maintenance 1.3 Maintenance to information systems and their components are authorized and recorded. *	1. Determine whether remote maintenance on servers, workstations and other systems is performed. Consider the following: a. Who is allowed to connect to systems (e.g. internal employees, third parties)? b. What software/version or service is used to connect? c. Whether end users have to take some action prior to allowing remote control of their workstation and/or whether access is logged and monitored? d. Adequacy of authentication requirements (e.g., multifactor authentication). 2. Maintenance performed conforms to departmental security practices.	DSS05.04		ISO/IEC 27001:2013 A.11.2.4; A.15.1.1; A.15.2.1 *Mandatory based on the Directive on Security Management App B (B.2.3.9.1)
	Monitoring 1.4 A monitoring system is in place on external network activity.	1. Obtain a list of the monitoring controls implemented by the organization at the following levels: a. Network (e.g., firewall, router, switch) 2. Determine if monitoring at each level includes detection of cybersecurity events (e.g., denial-of-service [DoS] attacks, unauthorized account access, unauthorized file/system access, privilege escalation attacks, SQL injection attacks). 3. The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	DSS05.07		ITSG-33 Security Control SC-7

2 PATCH OPERATING SYSTEMS (OSs) AND APPLICATIONS

Implement a timely patch maintenance policy for OSs and third-party applications to reduce departmental exposure to threats that could exploit known vulnerabilities. Use supported, up-to-date, and tested versions of applications. Moreover, the deployment of an unsupported OS or application, where updates are no longer available, will result in a significant risk of exposure to exploitation. Departmental tested and approved security patches need to be applied in a timely manner, ideally via an automatic patch management system.

Table 2: Patching

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards
2.0 Patch maintenance for operating systems and applications are implemented in a timely manner.	Policy 2.1 A patch management policy is in place.	1.The organization develops, documents, and disseminates: a. A system maintenance [incl. patch management] policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. 2. The organization reviews and updates the current policy and procedures [see 2.2 below] on a regular basis. Note: The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	APO11.06; DSS04.0		ITS G-33 Security Control SI-1
	Updated and Improved 2.2 Instructions and processes for patching OS's and applications are continuously updated.	1. Review the organization's policies and procedures related to continually improving protection processes. Consider the following: a. Ongoing audits, assessments and vulnerability scanning are conducted, reviewed and responded to. b. Plans, processes and policies are updated based on lessons learned from tests (e.g., business continuity, disaster recovery, incident response). c. Designated position and/or committee responsible for continuous evaluation of the organization's information security needs and posture d. Threat information gathering and responses to changes in the threat environment	APO11.06; DSS04.05		
	Vulnerabilities	1. Obtain the organization's vulnerability management plan and ensure it includes the following: a. Frequency of vulnerability scanning		APO04.03	ISO/IEC 27001:2013 A.12.6.1; A.18.2.2

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards
	2.3 Vulnerabilities in information systems and their components are identified, documented and reported. *	b. Method for measuring the impact of vulnerabilities identified (e.g., Common Vulnerability Scoring System [CVSS]) c. Incorporation of vulnerabilities identified in other security control assessments (e.g., external audits, penetration tests) d. Procedures for developing remediation of identified vulnerabilities 2. Obtain a copy of the organization's risk assessment to ensure vulnerabilities identified during the vulnerability management process are included. 3. Ensure system flaws are identified, reported (to the responsible security functional specialist and others, as defined in the department's security governance and security event management processes) and corrected.			ITS G-33 Security Control SI-2 B *Mandatory based on the Directive on Security Management App B (B.2.3.7.2)
	Actions 2.4 Impacts of identified vulnerabilities are analyzed, and corrective actions implemented. *	1. Review the organization's policies and procedures for patch management 2. Examine a sample of patches to determine if patches and updates are applied, in accordance with defined timelines and, as required, on an emergency basis.			*Mandatory based on the Directive on Security Management App B (B.2.3.7.3)
	Baseline Configuration 2.5 The organization develops, documents, and maintains (under configuration control) a current baseline configuration as a reference point for when IT configuration changes are made.	1. Baseline configurations for information systems and components are established including communications and connectivity-related aspects. 2. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items. 3. Baseline configurations serve as a basis for future builds, releases and/or changes to information systems. 4. Baseline configurations include information about information system components, such as standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices. 5. Baseline configuration reflect the current enterprise architecture and are continuously updated.			ITSG-33 Security Control CM-2
	Managed 2.6 Processes are in place for managing vulnerabilities in information systems with departmental and government-wide security event management processes. *	1. Applications and OS's are current, supported, maintained (timely) and tested for reliability 2. Third-party applications and OS's are updated based on a schedule. 3. Testing follows a defined process. 4. Information system components are replaced when support from the developer, vendor or manufacturer is no longer available.	BAI09.03	DSS03.05	ITS G-33 Security Control SA-22 and SI-2 B and D *Mandatory based on the

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards
		5. Justification and documentation of approval is required when the organization decides to continue to use unsupported system components. 6. Software and firmware updates are tested in a timely manner (including flaw remediation) for effectiveness and potential side effects. 7. Flaw remediation is incorporated into the organizational configuration management (automation, documentation, higher level script of what is happening, enforce compliance) process. 8. Review controlled maintenance processes. Consider the following: a. Maintenance activities are approved, scheduled and documented (e.g., date and time, name of individual(s) performing maintenance, description of maintenance performed, systems removed/replaced) b. Maintenance staff or vendors are approved, authorized and supervised (if required). c. Maintenance tools and media are approved and inspected for improper or unauthorized modifications prior to use. 9. Security-related software and firmware updates are installed a designated time period of the release of the updates.			Directive on Security Management App B (B.2.3.7.4) ISO/IEC 27001:2013 A.11.1.2; A.11.2.4; A.11.2.5 ITS G-33 Security Control SI-2 C

3 ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES

Minimize the number of users with administrative privileges and revalidate frequently the requirement for users to have a privileged account. Change administrative account passwords according to an established schedule or sooner, as required. Use two factor authentication (2FA) for accessing sensitive applications or for remote network access. Perform administrative functions on a dedicated workstation that does not have Internet or open e-mail access.

Table 3: Admin Privileges

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards
3.0 Access permissions are managed incorporating the principles of least privilege and separation of duties.	Policy 3.1 An access control policy is in place.	1.The organization develops, documents, and disseminates: a. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the access control policy and associated access controls. 2.The organization reviews and updates the current policy and procedures on a regular basis. **Note:** The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.			ITSG-33 AC-1; TBS Operational Security Standard
	Managed 3.2 Controls are in place to manage information system accounts (e.g. individual, group, system, application, guest, and temporary accounts).	1. Admin account passwords are changed according to an established schedule. 2. Network admin functions are performed on a dedicated workstation that do not have Internet or open mail access. 3. Information systems accounts are identified to support the organization's mission and business functions. 4. Managers are assigned to each account. 5. Conditions are applied to each group and role. 6. User access authorizations and other attributes are specified for each account. 7. Approvals are obtained for any new information system account. 8. Procedures are established for the creation, modification, disablement or removal of any information system account. 9. Accounts are monitored. 10. Account managers are notified of any changes to an account they are responsible for.			ITSG-33 Security Control AC-2

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards
		11. Access and reissuance of access is authorized based on need, intended use, other. 12. Compliance with account management requirements is reviewed.			
	Access Control 3.3 Access is given to users for specific duties and systems and is based on least privilege.	1. Review access rights and permissions for the network and any critical applications. 2. Determine if user access profiles are consistent with their job functions (based on least privilege). Compare a sample of users' access authority with their assigned duties and responsibilities. 3. Determine if access is granted for mission critical functions and information system support functions in order to reduce the risk of malevolent activity without collusion (e.g., critical processes require two people to perform the function). 4. Determine if users with local administrative privilege on workstations require this level of access. 5. Review how the organization restricts and/or monitors access to sensitive data by users with elevated network privilege. 6. Determine if role-based access controls are implemented (e.g., roles vs. users are assigned access rights). 7. Determine if there are regular reviews of access. 8. Accesses are clearly mapped to specific organizational missions and business functions. 9. This principle is also deployed to information system processes which ensures access is based on the accomplishment of a certain processes related to requirements. 10. Review where and when least privilege is being used and areas where it should potentially be used (development, implementation and operation of a system).		DSS05.04; DSS06.03	ISO/IEC 27001:2013 A.6.1.2; A.9.1.2; A.9.2.3; A.9.4.1; A.9.4.4 ITSG-33 Security Control AC-6
	Identification and Authorization 3.4 Systems uniquely identify and authenticate users and sources*.	1) Ensure unique identification also applies to group accounts 2) Test to ensure each employee including contractors, guests, etc. have a unique identifier recognized by the system. 3) Some information may require a combination of authentication - multifactor authentication (pass and password at the same time) 4) Access is defined as either local access (direct connections) or network access (network connections). 5) Two-factor authentication (2FA) is applied for accessing sensitive applications. 6) Two-factor authentication (2FA) is applied for remote network access. 7) Source authentication or other mechanisms are established where required, to ensure that information (for example, messages and financial transactions) can be attributed to an authorized individual.			ITSG-33 Security Control IA-2 *Mandatory based on the Directive on Security Management App B (B.2.3.7.6)

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/ Standards
	Isolation 3.5 Security functions are isolated from non-security functions.	1) Isolation boundaries are used (partitions and domains). 2) Security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.			ITSG-33 Security Control SC-3
	Monitoring 3.6 User activities can be audited to ensure accountability. *	1) Assess the department's ability to audit user activity. 2) Examine policies and procedures that outline this activity. 3) Ensure there is a mechanism to communicate to employees that their activities are being monitored. 4) Acceptable use of government information systems are monitored, regardless of location of access or system used, and reported through appropriate channels.			*Mandatory based on the Directive on Security Management App B (B.2.3.8.1 and 2)

4 HARDEN OPERATING SYSTEMS (OSs)

To prevent compromise of assets and infrastructures that are connected to the Internet, disable all non-essential ports and services, and remove unnecessary accounts. Both an enterprise-level auditing and anti-virus solution are key elements of any secure configuration. CSE has published ITSB-110, Microsoft Windows 7 Enterprise Edition Hardening Configuration Guidance, to support the deployment of this OS. Special consideration needs to be given to network architecture choices, security procedures. Further security controls should be applied to the OS when mitigating these risks; consult CSE's ITSG-33, IT Security Risk Management: A Lifecycle Approach, for more information on selecting and applying security controls.

Table 4: Harden OSs

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
4.0 Operating Systems are hardened by customizing and selecting configuration settings, applying an enterprise approach.	Policy 4.1 A system and information integrity policy is in place.	1.The organization develops, documents, and disseminates: a. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. 2.The organization reviews and updates the current policy and procedure on a regular basis. Note: The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.			ITSG-33 SI-1
	Monitoring and Corrective Actions 4.2 Enterprise-level risk assessments and monitoring of operating systems are conducted. *	1. An effective IT security posture is maintained through: a. Monitoring threats and vulnerabilities. b. Analyzing information system audit logs and records. c. Reviewing the results of system monitoring, security assessments, tests, and post-event analysis; and d. Taking pre-emptive, reactive and corrective actions to remediate deficiencies and ensure that IT security practices and controls continue to meet the needs of the department. 2. Regular risk assessments are conducted on the OS. 3. Threat and Risk Assessment (TRA) that takes into account departmental operational, business and security needs as well as the organization's security posture has been conducted. 4. Continuous monitoring is established to ensure the effectiveness of any implemented security controls			ITSB-110 ITSG-33 Security SI-4 *Mandatory based on the Directive on Security Management App B (B.2.7)

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
		5. The system is monitored to detect attacks (or indicators if attacks as determined by the organization) and unauthorized local, network and remote connections. 6. There is a process identified by the organization to identify unauthorized use of the system. 7. Monitoring devices are placed strategically within the system to collect essential information (determined by organization) and at ad-hoc locations within the system to track specific types of transactions of interest. 8. There is a process in place to protect the information obtained from the intrusion monitoring tools (from modification or deletion). 9. Monitoring is concentrated (increased) where there is higher risk (based on multiple sources and intelligence). 10. Legal opinions exist on monitoring activities (GC legislation and TB directions). 11. Information is provided to appropriate parties (decided by organization) on monitoring actives/results (as decided).			
	Configuration 4.3 Configuration settings are selected consistent with operational requirements and risk assessment activities.	1. The TRA is used to decide on which configuration guide will be used (for Microsoft OS see list in ITSB-110) 2. Configuration settings are established and documented for all products employed within the system. 3. The configuration settings are reflective of the most restrictive mode consistent with operations requirements. 4. the configuration settings are implemented. 5. Any deviation from the agreed upon configuration settings are identified, documented, approved (based on operational requirements) and monitored (based on organizational policies and procedures). 6. The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.			ITSB-110 ITSG-33 Security Control CM-6 and CM-2
	Change Management 4.4 Change management practices consider security impacts that may result from proposed changes. *	1. Determine if configuration change control processes for information systems are in place. Consider the following: a. Proposed changes are documented and approved. b. Changes are prohibited until designated approvals are received. c. Changes are tested and validated before implementation. d. Changes are documented and reported upon completion.	BAI06.01; BAI01.06		ISO/IEC 27001:2013 A.12.1.2; A.12.5.1; A.12.6.;, A.14.2.2; A.14.2.3; A.14.2.4 *Mandatory based on the Directive on Security

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
					Management App B (B.2.3.3.1)
	Access Controls 4.5 Systems are configured to only allow required capabilities. *	1. There is a process in place to ensure all non-essential ports and services are disabled, and unnecessary accounts removed. 2. Review information systems to determine if unnecessary and/or non-secure functions, ports, protocols and services are disabled. 3. Where feasible, the organization limits component functionality to a single function per device (e.g., dedicated email server). 4. Determine if the organization reviews functions and services provided by information systems or individual components of information systems to determine which functions and services are candidates for elimination. 5. The system is configured to provide only essential capabilities. 6. Pre-defined (by the organization) functions, ports, protocols and services are restricted.	DSS05.02	DSS06.03	ISO/IEC 27001:2013 A.9.1.2 ITSG-33 Security Control CM-7 *Mandatory based on the Directive on Security Management App B (B.2.3.3.2)
	Protection 4.6 Security features and tools (e.g. Configuration settings) are selected consistent with operational requirements and risk assessment activities. Anti-virus and malicious code measures are implemented* and are selected based on risk assessment activities, monitoring and configuration.	1. The OS is complimented with additional security features and controls (solely implementing "out-of-the-box" OS could compromise departmental IT Assets). 2. Based on the TRA and risk assessment activities and baseline configuration additional security features and tools are chosen and implemented (See ITSB-110 strategies for Microsoft OS's). 3. A process is in place to periodically assess the effectiveness of the anti-virus software. 4. Ensure malicious code protection mechanisms are located at the systems entry and exit points to detect and eradicate it. 5. Updates on the protection mechanism are done (when available) based on a configuration management policy or procedure. 6. The protection mechanism is configured to perform scans of the system when external files are opened/downloaded/executed in accordance with the security policy and respond to any malicious code detected (as decided by the organization). 7. False positives are dealt with depending on the impact it has on the availability of the system.			ITSB-110 ITSG-33 Security Control SI-3 *Mandatory based on the Directive on Security Management App B (B.2.3.7.5)
	Removable Media 4.7 Removable media is protected, and its use restricted according to policy.	1. Obtain a copy of the removable media policy. Review controls defined in the policy. Controls may include: a. User training b. Encryption of removable media	DSS05.02; APO13.01		ISO/IEC 27001:2013 A.8.2.2; A.8.2.3;

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
		c. Restricted access to removable media (e.g., USB restrictions) d. Sanitization procedures for decommissioned media 2. Perform spot-checks on systems with removable media restrictions to ensure restrictions are working as expected and comply with the organization's policy.			A.8.3.1; A.8.3.3; A.11.2.9

5 SEGMENT AND SEPARATE INFORMATION

Information stores should be categorized, taking into consideration information protection needs due to sensitivity or privacy. Networks should be zoned by segmenting infrastructure services into logical groupings that have the same communication security policies and information protection requirements. This logical design approach is used to control and restrict access and data communication flows. Further, monitor and enforce controls to maintain zone protection and integrity.

Table 5: Segment and Separate

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
5.0 Information stores are categorized and segmented based on information sensitivity and privacy.	Policy 5.1 A system and communications protection policy is in place.	1.The organization develops, documents, and disseminates: a. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. 2.The organization reviews and updates the current policy and procedures on a regular basis. **Note**: The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.			ITSG-33 SC-1
	Categorization 5.2 Information stores are categorized with consistent regard to information protection needs, data sensitivity and privacy.	1. There is a process in place to categorize information based on sensitivity and need. 2. Information stores/repositories are also categorized with appropriate information based on applicable GC legislation and TBS. 3. Categorization of information is documented, including supporting rationale, in the security plan for the system. 4. Categorization of information is reviewed and approved by the designated official.			ITSG-33 Security Control RA-2
	Security Zones 5.3 Networks are zoned by segmenting infrastructure services into logical groupings based on information protection requirements and communication security policies. * Network zoning results in physical and logical access controls that support information protection requirements	1. Review network diagrams and data flow diagrams. 2. Determine if high-value/critical systems are separated from high-risk systems (e.g., VLAN, DMZ, hard backups, air-gapping) where possible. 3. Evaluate controls related to communications to ensure the network is secure. Consider: a. Network perimeter defenses are in place (e.g., border router, firewall). b. Physical security controls are used to prevent unauthorized access to telecommunication systems, etc. c. Logical network access controls (e.g., VLAN) and technical controls (e.g., encrypting traffic) are in place to protect and/or segregate communications networks (e.g., wireless, WAN, LAN, VoIP).	DSS05.02; APO13.01	DSS05.02 DSS05.03	ISO/IEC 27001:2013 A.13.1.1; A.13.1.3; A.13.2.1 ITSG-33 Security SC-2 and SC-3 and SC-7 (B and C)

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
		4. Ensure the system separates user functionality (including user interface services) from information system management functionality (segregation of duties). 5. The system isolates security functions from non-security functions through partitions and domains. 6. The information system implements sub-networks for publicly accessible system components that are physically/logically separated from internal organizational networks. 7. The information system connects to external networks or information systems only through managed interfaces* (see bottom) consisting of boundary protection devices arranged in accordance with an organizational security architecture. 8. Information is partitions into organization-defined components residing in separate physical domains or environments based on circumstances.			and SC-32 *Mandatory based on the Directive on Security Management App B (B.2.3.6.1)
	Information Flow Protection 5.4 Information that flows within systems and between interconnected systems is protected* in accordance with applicable policy.	1. An information flow policy exists that clearly outlines the approved flow of information within and between interconnected systems. 2. Information flow restrictions include restricting information from going out (Internet) or coming in. 3. Information flow restrictions limits certain types of data based on structure, content and security domains. 4. Architectural solutions are used to enforce the flow restrictions. 5. Use encryption and network safeguards to protect the confidentiality of sensitive data transmitted across public networks, wireless networks or any other network where the data may be at risk of unauthorized access.			ITSG-33 Security Control AC-4 *Mandatory based on the Directive on Security Management App B (B.2.3.6.3)
	Data Storage 5.5 Measures are implemented to protect information on electronic media and electronic storage devices at rest and in transit. *	1. There is a process in place to protect information through appropriate sanitization or destruction before reuse or disposal of the equipment, commensurate with the sensitivity of the information and in accordance with departmental practices. 2. Secure electronic storage, transportation, transmittal, sanitization and destruction devices, methods and services are identified that are authorized for use in the department, including but not limited to portable storage devices; and 3. Appropriate safeguards are implemented where other devices, methods or services are used for operational purposes, subject to approval by an individual who has the required authority.			Directive on Security Management Appendix B - Security in IT Configuration Management (B.2.3.4)
	Monitoring 5.6 Zone protection and integrity is continually monitored.	1. Obtain a copy of processes and procedures designed to detect unauthorized access to the organization's facilities and systems (e.g., sign-in/out logs, video surveillance, break-in alarms, network port blocking, USB device restrictions on workstations and user devices, monitoring of excessive failed logins indicating a password-guessing attack). 2. Spot-check unauthorized access controls by accessing facilities and systems with permission to test, but not standard authorization. Request the organization provide the alert notifications generated by the simulated		DSS05.05	ITSG-33 Security Control SC-7 A

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
		unauthorized access. 3. The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system (SC-7 A).			
	Enforced 5.7 Zone protection and integrity controls are effectively enforced.	1. Controls are in place to protect the information according to their classification (access controls based on user identities and clearance levels). 2. Access is monitored based on risk (information with high classifications).			ITSG-7 (17 A) - Automated Enforcement of Protocol Formats

6 PROVIDE TAILORED AWARENESS AND TRAINING

Initiate regular awareness activities on current user-related vulnerabilities and proper user behaviours. IT security awareness programs and activities should be frequently reviewed, maintained and accessible to all users with access to departmental systems. Although system safeguards are expected to curtail suspected malicious activity on the networks, the human element will continue to provide an element of exposure. Current examples of spear phishing or the improper handling of removable media demonstrate the continued need to focus in this area. In addition, regular threat reporting to management on attempted or actual compromises will help to reinforce the behaviour changes required. Management involvement in information protection decisions is essential in choosing appropriate security controls.

Table 6: Awareness and Training

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
6.0 A culture of security awareness is supported by tailored awareness and training.	Policy 6.1 A security awareness and training policy is in place.	1.The organization develops, documents, and disseminates: a. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. 2.The organization reviews and updates the current policy and procedures on a regular basis. Note: The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.			ITSG-33 AT-1
	General Training 6.2 All departmental staff with access to systems receive periodic IT security awareness training.	1. Review acceptable use policy and/or training materials to ensure content is adequate. 2. Review user training reports and/or documentation to ensure users are trained in accordance with applicable policy, guidance, and/or requirement (e.g., annual cybersecurity training of all employees).	APO07.03; BAI05.07		ISO/IEC 27001:2013 A.7.2.2
	Content 6.3 IT security awareness training is based on current user-related vulnerabilities and proper user behaviours.	1. Available information (intelligence) on threats and incidents are used to inform the training plan. (Determine whether training materials are updated based on changes in cyber threat environment.) 2. This available information is also used to inform management of current threats so they are also aware of what controls should be in place and of what employees should be more aware of. 3. Employees must know their duties to report incidents, what to look for and when/how to report it. (IR-6) 4. Ensure rules, expected behaviour and responsibilities are communicated to employees who have access to the systems.	APO07.03; BAI05.07		ISO/IEC 27001:2013 A.7.2.2 ITSG-33 Security Control IR-6 and PL-4

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
	Current 6.4 IT security awareness training and activities are assessed and updated on a scheduled or as-needed basis.	1. Training given to all new employees and is updated on a prescribed schedule. 2. Did training change when an event occurred or a system changed?			ITSG-33 Security Control AT-2
	Specific Training 6.5 Security training is based on the employee's roles and responsibilities.	1. Determine if the organization has a process to identify privileged users. 2. Determine if privileged users' roles are well defined and if privileged users are trained based on their responsibilities. 3. Review training material and/or user agreements to ensure users with elevated privileges are taught security roles and responsibilities associated with elevated privileges.	APO07.02; DSS06.03	APO07.03	ITSG-33 Security Control AT-3 ISO/IEC 27001:2013 A.6.1.1; A.7.2.2
		1. Review applicable third-party contracts, customer agreements, and partner agreements to ensure security roles and responsibilities are clearly defined. 2. Review the organization's vendor management program to ensure third parties are complying with cybersecurity responsibilities defined in contracts and agreements.	APO07.03; APO10.04; APO10.05		ISO/IEC 27001:2013 A.6.1.1; A.7.2.2
		1. Review training and continuing education programs for senior executives. Consider the following: a. Cybersecurity knowledge and skill levels needed to perform their duties are defined. b. Specific role-based training is assigned based on cybersecurity roles and responsibilities. c. A method is in place to measure senior executives' cybersecurity knowledge and understanding against organization requirements. d. Training and education materials are updated to reflect changes in the threat environment.	APO07.03	EDM01.03	ISO/IEC 27001:2013 A.6.1.1; A.7.2.2
		1. Review training and continuing education programs for physical and information security personnel. Consider the following: a. Knowledge and skill levels needed to perform physical and information security duties are defined. b. Specific role-based training is assigned based on physical and information security roles and responsibilities. c. A method is in place to measure physical and information security personnel's cybersecurity knowledge and understanding against organization requirements. d. Training and education materials are updated to reflect changes in the threat environment.	APO07.03	DSS06.03	ISO/IEC 27001:2013 A.6.1.1; A.7.2.2

7 MANAGE DEVICES AT THE ENTERPRISE LEVEL

Use GC furnished equipment (GFE) within a device management framework and provide control over configuration change management. If a bring-your-own-device (BYOD) scheme is to be considered for a network with low expectations of confidentiality and integrity, a strict control policy must still be implemented as one element of the risk mitigation strategy.

Table 7: Manage Devices

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
7.0 Devices are managed at the enterprise level.	Inventory 7.1 The department maintains an inventory of all system components.	1. The organization has an inventory of system components that: a. accurately reflects the current system. b. includes all components in the boundary of the system. c. is at the level of detail necessary for tracking and reporting. d. includes enough information to achieve accountability. 2. The inventory is reviewed and updated on a specified basis.			ITSG-33 Security Control CM-8
	Authorized 7.2 Internet and network connected devices and their components are authorized. *	1. The organization authorizes the connection of mobile devices to organizational information systems. 2. Government of Canada Furnished Equipment (GFE) are used.			CSE ITSG - 33 Annex 3A - Security Control Catalogue: IT Security Risk Management: A Lifecycle Approach AC-19 ACCESS CONTROL FOR MOBILE DEVICES *Mandatory based on the Directive on Security Management App B (B.2.3.3.4)
	7.2.1 GFE is organized within a formal device management framework.	1. The organization establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.			CSE ITSG - 33 Annex 3A - Security Control Catalogue: IT Security Risk Management: A Lifecycle Approach AC-19 ACCESS CONTROL FOR MOBILE DEVICES

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
	7.2.2 GFE operates under a formal configuration change management system.	1. If the organization maintains a software development or testing environment, review network diagrams, database connections and applicable firewall/router configurations to determine sufficiency of separation between these environments and the production network.	BAI07.04		ISO/IEC 27001:2013 A.12.1.4 Directive on Security Management Appendix B - Security in IT Configuration Management
	BYOD - External Systems 7.3 The department has established terms and conditions for the use of external systems.	1. Terms and conditions exist for allowing authorized individuals to access information from external systems. 2. Terms and conditions exist for allowing authorized individuals to process, store or transmit organization-controlled information using external systems. 3. If the BYOD is permissible determine if there is a policy or framework in place to guide and inform employees on the management of these devices. a. ensure there is compliance monitoring of the policy/framework and of devices in use. **Note:** There are risks to using non-organizationally owned devices. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, it may be such that the use of non-organizationally owned devices is allowed but restricted in some way. Restrictions include, for example: (i) requiring the implementation of organization-approved security controls prior to authorizing such connections; (ii) limiting access to certain types of information, services, or applications; (iii) using virtualization techniques to limit processing and storage activities to servers or other system components provisioned by the organization; and (iv) agreeing to terms and conditions for usage. For personally owned devices, organizations should consult with Departmental Legal Services regarding legal issues associated with using such devices in operational environments, including, for example, requirements for conducting forensic analyses during investigations after an incident.			ITSG-33 Security Control AC-20 and (3)
	7.4 A strict control policy is implemented (as one element of the risk mitigation strategy) if a Bring-Your-Own-Devices (BYOD) arrangement is allowed in a department operating a network with low expectations of confidentiality and integrity.	1. The organization prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information *unless specifically permitted by the authorizing official*; and 2.The organization enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information: a. Connection of unclassified mobile devices to classified information systems is prohibited; b. Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official; c. Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited (i.e. turned off); and			ITSG-33 Security Control AC-19 (4)

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
		d. Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed. e. Restricts the connection of classified mobile devices to classified information systems in accordance with [Assignment: organization-defined security policies].			

8 APPLY PROTECTION AT THE HOST LEVEL

Deploy a Host-based Intrusion Prevention System (HIPS) solution to protect systems against both known and unknown malicious activity. HIPS can also take active measures by stopping an application or closing ports in the event of an intrusion. Monitoring HIPS alerts and logging information will provide early indications of intrusions.

Table 8: Protection at the Host Level

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
8.0 A Host-based Intrusion Prevention System (HIPS) is deployed.	HIPS Deployed 8.1 HIPS is deployed, or deployment is scheduled, as a boundary protection mechanism for servers, workstations and mobile devices, as needed.	1. Determine if the organization employs integrity verification tools (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) to detect unauthorized changes to software (e.g., middleware, applications and operating systems with key internal components such as kernels, drivers), firmware (e.g., Basic Input Output System [BIOS]), and information (e.g., metadata such as security attributes associated with information). 2. The organization implements a host-based boundary protection mechanism to specified components (deemed appropriate by the organization).		APO01.06	ISO/IEC 27001:2013 A.12.2.1; A.12.5.1; A.14.1.2; A.14.1.3 ITSG-33 Security SC-7 (12)
	Protect 8.2 Measures are implemented to protect systems against both known and unknown malicious activity.	1. Review risk assessments, information security meeting minutes and information security strategies to determine if the risk of data loss prevention or exfiltration of confidential data is being considered. 2. Ensure controls or tools (e.g., data loss prevention) are in place to detect or block potential unauthorized or unintentional transmission or removal of confidential data (e.g., email, FTP, USB devices, Telnet). 3. Ensure malicious code protection mechanisms are located at the systems entry *and exit points* to detect and eradicate it. 4. Updates on the protection mechanism are done (when available) based on a configuration management policy or procedure. 5. The protection mechanism is configured to perform scans of the system when external files are opened/downloaded/executed in accordance with the security policy and respond to any malicious code detected (as decided by the organization). 6. False positives are dealt with depending on the impact it has on the availability of the system. 7. Measures are used, reviewed and regularly updated to prevent, detect and eliminate malicious code (for example, viruses) in information systems and their components.	APO01.06	DSS05.06	ITSG-33 Security Control SI-3 ISO/IEC 27001:2013 A.6.1.2; A.7.1.1; A.7.1.2; A.7.3.1; A.8.2.2; A.8.2.3; A.9.1.1; A.9.1.2; A.9.2.3; A.9.4.1; A.9.4.4; A.9.4.5; A.13.1.3; A.13.2.1; A.13.2.3; A.13.2.4; A.14.1.2; A.14.1.3 *Mandatory

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework/Standards
					based on the Directive on Security Management App B (B.2.3.7.5)
	Monitoring 8.3 Departments monitor information systems (HIPS) to detect attacks and indicators of potential attacks; unauthorized local, network and remote connections; and unauthorized use of IT resources. *	1. The system is monitored to detect attacks (or indicators if attacks as determined by the organization) and unauthorized local, network and remote connections. 2. There is a process identified by the organization to identify unauthorized use of the system. 3. Monitoring devices are placed strategically within the system to collect essential information (determined by organization) and at ad-hoc locations within the system to track specific types of transactions of interest. 4. There is a process in place to protect the information obtained from the intrusion monitoring tools (from modification or deletion). 5. Monitoring is concentrated (increased) where there is higher risk (based on multiple sources and intelligence). 6. Legal opinions exist on monitoring activities (GC legislation and TB directions). 7. Information is provided to appropriate parties (decided by organization) on monitoring activities/results (as decided).			ITSG-33 Security SI-4 *Mandatory based on the Directive on Security Management App B (B.2.3.7.1)

9 ISOLATE WEB-FACING APPLICATIONS

Use virtualization to create an environment where web-facing applications can run in isolation. Internet browsers and e-mail clients are examples of applications that are susceptible to exploits that execute malware. Security exploits specific to such applications can be confined to this sandbox. Any malware that infects the virtualized environment cannot get out of the sandbox; therefore, the malware cannot infect the host or enterprise.

Table 9: Web-Facing Applications

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
9.0 Web-facing applications are isolated.	System Partitioning 9.1 Separate processing domains are provided for web-facing applications.	1. Is security categorization (process of identifying the potential injuries that could result from compromises) used to guide the selection of appropriate domain partitioning? 2. Do managed interfaces restrict or prohibit network access and information flow among partitioned information system components (hardware, software, database, network and people)?			ITSG-33 Security SC-32
	Least Privilege 9.2 Finer-grained allocation of user privileges are applied for web-facing applications.	1. Determine the admin privilege process. Determine if greater admin privilege controls are in place for web-facing applications. 2. Are virtualization techniques used to allow additional privileges within a virtual machine, while restricting privileges to other virtual machines to the actual machine? 3. Are hardware and/or software domain separation mechanisms being used?			ITSG-33 Security AC-6 (4)

10 IMPLEMENT APPLICTION ALLOWLISTING

Explicitly identify authorized applications and application components and deny all others by default to reduce the risk of executing zero-day malware. Application allowlisting technologies can control which applications are permitted to be installed or executed on a host. The allowlist can be defined by a selection of several file and folder attributes (e.g., file path, filename, file size, digital signature or publisher, or cryptographic hash). Application allowlisting policies should be defined and deployed across the organization using group policy management.

Table 10: Allowlisting

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
10.0 Application allowlisting is implemented (where feasible) to control which applications can be installed or run. *	Requirements Established 10.1 The requirement for application allowelisting has been assessed. An application allowlisting (deny-all, permit by exception) policy (documented process) is in place to allow the execution of only authorized software programs on the information system.	1. Collect evidence that the organization has assessed the need for application allowlisting. 2. Ensure other controls are in place to address the risk. "Organizations considering application allowlisting deployment in a typical managed environment should perform a risk assessment to determine whether the security benefits provided by application allowlisting outweigh its possible negative impact on operations." NIST 3. If allowlisting is being used, ensure there is a documented plan or policy that outlines which applications are allowed to run (deny-all, permit-by-exception) and who is allowed to run which applications. 4. Users are informed of the changes made because of allowlisting and how it will affect their work. They are also informed of the security reasons behind the change. Additionally, support staff are advised on how to address any issues.	NIST Application Allowlisting Guide		CSE Application Allowlisting guide ITSB-33 CM-7 (5) B (Policy) *Mandatory based on the Directive on Security Management App B (B.2.3.3.3)
	Identify 10.2 Authorized software programs are formally identified.	1. The organization identifies organization-defined software programs authorized to execute on the information system. 2. Allowlisted executables should be identified with something other than the file name or directory location to catch malware masquerading as legitimate software.			ITSB-33 CM-7 (5) A (Identify) CSE Application Allowelisting guide
	Implement 10.3 The list of authorized software programs is reviewed and updated on an organization-	1. Application allowlisting technologies already built into the host operating system are used. 2. Products that support more sophisticated application allowlisting attributes are used.	NIST.SP.800-167		CSE Application Allowelisting guide

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
	defined frequency.				
	Monitoring 10.4 Periodic monitoring and testing of the allowlisting process is applied to ensure it is working properly.	1. Updates occur frequently to the allowlisting information to ensure effectiveness as software updates are occurring all of the time. 2. Testing has been done to confirm that the application allowlisting is effective (can be done by testing in audit only mode). 3. The organization reviews and updates the list of authorized software programs on a regular basis.			CSE Application Allowlisting guide ITSB-33 CM-7 (5) A (Identify)

11 GOVERNANCE

Processes and structures are in place to inform, direct and monitor the organization's activities which inform the management of cybersecurity risk.

Table 11: Governance

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
11.1 The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	DSP 11.1.1 There is a three-year departmental security plan that is approved by the Deputy Head, 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.*	1. Obtain a copy of the DSP. 2. Determine if the plan is complete and includes the elements in Appendix A of the Policy on Government Security. 3. The DSP has been approved by the Deputy Head. 4. Determine if the policy is communicated and available to employees.	APO01.03; EDM01.01; EDM01.02		ISO/IEC 27001:2013 A.5.1.1 * Requirement *Policy on Government Security* (4.1.5)
	Roles and Responsibilities 11.1.2 Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. *	1. Determine if information security roles and responsibilities are defined. Roles and responsibilities may be defined in policies, job descriptions, agreements, RACI charts (Responsible, Accountable, Consulted, Informed), hierarchy charts and/or contracts. 2. Determine if there is sufficient independence within the information security roles in order to provide adequate separation of duties for critical functions. 3. Review contracts, nondisclosure agreements (NDAs) and service level agreements (SLAs) with critical vendors to determine if cybersecurity controls and incident notification are addressed appropriately (oversight, review and escalation). 4. A chief security officer has been established, designated by the Deputy Head, who is responsible to the deputy head or to the departmental executive committee to provide leadership, coordination and oversight for departmental security management activities.	APO13.12	APO01.02; DSS06.03	ISO/IEC 27001:2013 A.6.1.1; A.7.2.1* Requirements *Policy on Government Security* (4.1.1)
Compliance - Security practices and security controls are in place listed in Annex B of the Directive in Security Management.					
11.2 Departmental information technology (IT) security goals, requirements and practices are defined, documented and maintained.	Recovery 11.2.1 Pertinent physical security, business continuity, disaster recovery and information security requirements are identified for all	1. Review the process for documenting requirements for each system. 2. Does each system have identified requirements set out in department plans for physical security, business continuity, disaster recovery, etc. 3. Are documented goals identified for the Information System? Are the goals being met?			* Mandatory Directive on Security Management

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
	information systems that support departmental programs, services or activities.				Appendix B (B.2.2.1.1)
	Threats 11.2.2 Threats to information systems are identified and assessed regularly/as required.	1. Identify where threats to systems are being kept, monitored and reported on. 2. Are these threats assessed, managed, reported on and updated regularly?			* Mandatory Directive on Security Management Appendix B (B.2.2.1.2)
	Lifecycle 11.2.3 Requirements are defined and documented for ensuring the protection of departmental information systems throughout their life cycle.	1. Ensure security requirements and threats are identified for the information system for their lifecycle in accordance with applicable legislation, policies, contracts, agreements and memoranda of understanding			* Mandatory Directive on Security Management Appendix B (B.2.2.1.3)
	Controls 11.2.4 Departmental security practices are defined and documented for implementing and maintaining IT security controls, including practices for conducting IT security assessment and authorization, in accordance with departmental security requirements.	1. Ensure there are documented processes for security controls, including conducting Security Assessment and Authorizations (SA&A).			* Mandatory Directive on Security Management Appendix B (B.2.2.2)
11.3 Security controls are defined, documented, implemented and maintained to meet departmental IT security requirements, in accordance with departmental practices.	Identity and Access Management 11.3.1 An identification and authentication management process is in place that uniquely identifies and authenticates individuals and devices.	1. Measures are implemented to ensure that individuals and devices are uniquely identified and authenticated to an appropriate level of assurance before being granted access to information in information systems, in accordance with Appendix A: Standard on Identity and Credential Assurance of the Directive on Identity Management. Compliant with the *Directive on Identity Management*. 2. Measures are implemented to ensure that access to information (electronic data) and information systems is limited to authorized users who have been security-screened at the appropriate level and who have a need for access: a. Approval, notification, monitoring and operational requirements and procedures are established for the creation, activation, modification, periodic review, and disabling or deletion of information system accounts;			* Mandatory Directive on Security Management Appendix B Directive on Identity Management Policy on Government

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
		b. Access privileges are defined based on departmental security requirements and the principles of least privilege, segregation of duties, and acceptable use of government information systems; c. Authorized users are informed of expectations for acceptable use of government information systems, of monitoring practices being applied, and of the consequences for unacceptable use of those systems; d. Measures are established to control the use of accounts that have administrative privileges, including restricting the number of users who have administrative privileges, and restricting the information systems, networks and applications that can be accessed and the operations that can be performed using privileged accounts; e. Verify that individuals who are authorized to conduct privileged operations, such as setting or changing access privileges and implementing or maintaining other IT security controls, are not permitted to alter records of these operations and have been security-screened commensurate with their access level; and f. Access privileges are reviewed periodically, and access is removed when it is no longer required (for example, when an employee leaves or changes responsibilities). g. Ensuring that their authority to deny, revoke or suspend security clearances is not delegated from the Deputy Head (Policy on Government Security 4.1.3)			Security 4.1.3 and 4.1.4 (main criteria)
	Physical and Environmental 11.3.2 Information systems, their components, and the information processed are protected from physical and environmental threats, considering the sensitivity of the information.	1. Appropriate physical and environmental safeguards are implemented in facilities where information systems are developed, operated, maintained or stored; 2. Physical information system components are placed in appropriate physical security zones; and 3. Emanations security or other measures are used, as required, to protect information systems from information leakage owing to the emanation of electromagnetic signals.			* Mandatory Directive on Security Management Appendix B (B.2.3.5)
	Respond and Recover 11.3.3 Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) are in place, tested and managed.	1. Review incident response and business continuity plans to determine if the institution has documented how it will respond to a cyber incident. 2. Evaluate plans to determine how frequently they are tested, updated and approved. 3. Determine whether business continuity and incident response tests are performed according to policy and any applicable guidance. 4. There is a plan to enable information systems to maintain or return to defined service levels, as applicable. 5. Recovery strategies and restoration priorities are defined for data and information systems, in accordance with departmental business continuity requirements. 5. Measures are implemented to meet identified recovery strategies and restoration priorities. 6. IT continuity management mechanisms are tested to ensure an acceptable state of preparedness as an integral element of practices for departmental business continuity management. 7. Any direction, advice and information requests issued by the Treasury Board of Canada Secretariat and the Privy	DSS04.03	DSS04.04	ISO/IEC 27001:2013 A.16.1.1; A.17.1.1; A.17.1.2 A.17.1.3 * Mandatory Directive on Security Management Appendix B (B.2.2.1.1)

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
		Council Office regarding security events that require an immediate or coordinated government-wide action are responded to. (*Policy on Government Security* 4.1.8)			Also covers 4.1.7 in the Policy on Government Security
11.4 IT Security is considered in key processes and design of new systems and projects.	Project Management 11.4.1 IT Security is considered in all IT project management.	1. What is the process to ensure that IT Security considerations are integrated into all phases of IT project management? 2. IT security needs of programs and services are considered and addressed when developing, implementing or upgrading information systems.			* Mandatory Directive on Security Management Appendix B (B.2.4)
	IS Lifecycle 11.4.2 IT Security requirements, activities and gating requirements are identified and addressed throughout all stages of the information system life cycle, including definition, design, development and procurement, operations, maintenance and decommissioning.	1. System security engineering and security design processes are implemented at the appropriate stages of the system development lifecycle process; 2. Supply chain security measures are implemented to establish and maintain reasonable confidence in the security of sources of information systems and IT components, in accordance with applicable security requirements; 3. Risks are identified and addressed regarding transmission, processing or storage of data, both internal and external to Canada, when planning for an information system, including the complete life cycle of the system; and 4. For information systems managed for or by another organization, and for information systems shared or interconnected by two or more organizations, there is an established documented arrangement that defines applicable security requirements and respective security responsibilities.			* Mandatory Directive on Security Management Appendix B (B.5.2)
	SA&A 11.4.3 An IT security assessment and authorization processes is established to maintain confidence in the security of information systems that are used or managed by the department, while considering stakeholder security requirements.	1. Assess whether security controls are effective and whether applicable security requirements are met; 2. Risk mitigation measures are implemented and documented when security requirements cannot be fully met before putting an information system into operation, subject to approval by an individual who has the required authority; 3. All information systems are authorized before being put into operation through established IT security assessment and authorization processes; 4. Security assessments and authorization decisions are documented, including the formal acceptance of residual risk by an individual who has the required authority; and 5. The authorization is evaluated and maintained throughout the information system's operational life cycle.			* Mandatory Directive on Security Management Appendix B (B.2.6)

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
11.5 The data, devices, systems, and facilities that enable the organization to achieve business objectives are identified and managed.	11.5.1 Physical Devices and Systems Physical devices and systems within the organization are inventoried.	1. Obtain a copy of physical devices and systems inventory. Review the inventory considering the following: a. Scope of physical devices and systems is based on the organization's risk appetite (e.g. systems that contain sensitive information, allow access to the network, or are critical to business objectives) b. Completeness of inventory (e.g. sample location, asset number, owner) c. Inventory collection process ensures new devices are collected accurately and in a timely manner (e.g. automated software to detect and/or store the inventory) d. Frequency of inventory reviews	BAI09.01; BAI09.02		ISO/IEC 27001:2013 A.8.1.1; A.8.1.2
	11.5.2 Software and Applications Software platforms and applications within the organization are inventoried.	1. Obtain a copy of software inventory. Review the inventory considering the following: a. Scope of software inventory is based on the organization's risk appetite (e.g. software that processes, stores or accesses sensitive information or is critical to business objectives) b. Completeness of inventory (e.g. version, system, vendor, owner) c. Inventory collection process ensures new software is collected accurately and in a timely manner (e.g. automated software to detect and/or store the inventory) d. Frequency of inventory reviews	BAI09.01; BAI09.02; BAI09.05		ISO/IEC 27001:2013 A.8.1.1; A.8.1.2
	11.5.3 Data Flows Organizational communication and data flows are mapped.	1. Ensure the organization maintains accurate and current copies of data flow diagram(s) (DFD), logical network diagram(s) (LND), and/or other diagrams to show organizational communication and data flow.	DSS05.02	APO01.04	ISO/IEC 27001:2013 A.13.2.1
	11.5.4 External Systems External information systems are cataloged.	1. If the organization relies on information systems hosted by third parties, obtain a copy of the external systems inventory. Review the third-party inventory considering the following: a. Scope of external systems is based on the organization's risk appetite (e.g. systems that store, process or access sensitive information or are critical to business objectives). b. Completeness of inventory (e.g. location, third party, owner, etc.) c. Inventory collection process ensures new systems are collected accurately and in a timely manner (e.g. automated software to detect and/or store the inventory) d. Frequency of inventory reviews	APO02.02		ISO/IEC 27001:2013 A.11.2.6

12 RISK MANAGEMENT

The organization understands it's cybersecurity risks to operations, assets and individuals. The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Table 12: Risk Management

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
12.1 The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Asset Vulnerabilities 12.1.1 Asset vulnerabilities are identified and documented.	1. Determine if vulnerability testing is conducted and analyzed on critical organizational assets (e.g. assets important to business objectives and the organization's risk strategy).	APO12.01; APO12.02; APO12.03; APO12.04		ISO/IEC 27001:2013 A.12.6.1; A.18.2.3
	External Sources 12.1.2 Threat and vulnerability information is received from outside sources.	1. Determine if the organization is a member of or subscribes to a threat and vulnerability information sharing organization. 2. Determine if the organization has a formal process in place for disseminating threat and vulnerability information to individuals with the expertise to review the information and the authority to mitigate risk posed to the organization.		APO12.01; BAI08.04	ISO/IEC 27001:2013 A.6.1.4
	Threats 12.1.3 Threats, both internal and external, are identified and documented.	1. Review risk assessments to determine if internal and external threats are identified and documented. 2. Determine if the organization has developed processes to actively monitor and report potential threats.	APO12.01; APO12.02; APO12.03; APO12.04		
	Impacts and Likelihood 12.1.4 Potential business impacts and likelihoods are identified.	1. Review risk assessments and business impact analysis to determine if likelihood and potential impacts are identified and analyzed for threats.	DSS04.02	APO12.02; BAI04.02	
	Risk Determination 12.1.5 Threats, vulnerabilities, likelihoods and impacts are used to determine risk.	1. Determine if the risk assessment process identifies reasonably foreseeable internal and external threats and vulnerabilities, the likelihood and potential damage of those threats, and the sufficiency of controls to mitigate the risk associated with those threats.	APO12.02		ISO/IEC 27001:2013 A.12.6.1

DRAFT CYBER SECURITY AUDIT PROGRAM

BASED ON CSE'S TOP 10 CYBER SECURITY ACTIONS

Audit Criteria	Sub-Criteria	Potential Audit Tests	NIST Ref. to COBIT 5	Additional Ref. COBIT 5	Ref. Framework /Standards
	Risk Response 12.1.6 Risk responses are identified and prioritized.	1. Obtain the organization's risk management plan and/or other documentation showing the organization's response to risk levels identified in the risk assessment. Determine if the risk management plan is designed to accept or reduce risk level in accordance with the organization's risk appetite. 2. Obtain copies of management responses to recent cybersecurity-related audits and assessments to determine if exceptions noted in audits or assessments are identified and prioritized. 3. Reviewing any residual security risk that exceeds established authorities for security risk management decisions.	APO12.05; APO13.02		Requirement *Policy on Government Security* (4.1.6)
12.2 The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	RM Process 12.2.1 Risk management processes are established, managed and agreed to by organizational stakeholders.	1. Evaluate the framework or process used for risk management. Consider the following: a. Is the process formally documented? b. Is the process regularly updated? c. Is the process repeatable and measurable? d. Does the process have an owner? e. Are stakeholders involved or informed of the process?	APO12.04; APO12.05; APO13.02; BAI02.03; BAI04.02		
	Tolerance 12.2.2 Organizational risk tolerance is determined and clearly expressed.	1. Determine if the organization has defined and approved a cyber risk appetite statement. 2. Is the organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis?	APO12.06	APO12.03; EDM03.01 APO04.03	