Baseline Cyber Security Controls

For Small and Medium Organizations

Certification Body Handbook

V1.2

Foreword

The Certification Handbook is an UNCLASSIFIED publication developed by Innovation Science and Economic Development Canada, with guidance from the Canadian Centre for Cyber Security and Standards Council of Canada. This document is intended for organizations performing audits against the CAN/CIOSC 104:2021 National Standard – Baseline Cyber Security Controls for Small and Medium Organizations, as part of the Cyber Secure Canada cyber certification program.

Revision History

Revision	Amendments	Date
1	Initial internal release	Nov. 26, 2021
1.0	• Updated comments from team • Table formatting • Release to CBs and other departments	Dec. 7, 2021
1.1	• Incorporated comments • Editing • Added opening sections to document	March 1, 2022
1.2	• Incorporated additional comments • Editing • Removed references to levels	June 25, 2022
1.21	• Updated background section and grammar check	July 18, 2022

Table of Contents

Background 3
Introduction 4
4.1 Leadership 5
4.2 Accountability 6
4.3 Cyber Security Training 7
4.4 Cyber Security Risk Assessment 8
5.1 Incident Response Plan 9
5.2 Automatically Patch Operating Systems and Applications 10
5.3 Enable Security Software 11
5.4 Securely Configure Devices 12
5.5 Use Strong User Authentication 13
5.6 Backup and Encrypt Data 14
5.7 Establish Basic Perimeter Defenses 15
5.8 Implement Access Control and Authorization 16
6.1 Secure Mobility 17
6.2 Secure Cloud and Outsourced IT Services 19
6.3 Secure Websites 20
6.4 Secure Portable Media 21
6.5 Point of Sale (POS) and Financial Systems 22
6.6 Computer Security Log Management 23

Background

The CyberSecure Canada security certification program was announced in June 2018 for Canadian small and medium-sized organizations (SMO). As part of a renewed cyber security framework, Innovation, Science and Economic

Development Canada (ISED) and its partners were tasked to establish a voluntary, recognizable certification program intended to enable SMOs to demonstrate to customers—both businesses and consumers—that they follow a baseline set of security practices. A standardized certification will help participants position their cyber security practices for competitive advantage and will promote broader trust in the digital economy.

Program goals include:

- raising the cyber security baseline among Canadian SMOs;
- increasing consumer confidence in the digital economy;
- and better positioning SMOs to compete domestically and globally.

The CyberSecure Canada certification program is designed to be a "low-burden," cost effective and easy to implement solution for non-technical specialists. The CIO Strategy Council developed CAN/CIOSC 104:2021 National Standard – Baseline Cyber Security Controls for Small and Medium Organizations, this Standard specifies a minimum set of cyber security controls intended for small and medium organizations which typically have less than 500 employees.

Introduction

This document is intended as supplementary guidance for CyberSecure Canada auditors when evaluating the security controls present in the national standard: *CAN/CIOSC 104:2021 Baseline Cyber Security Controls for Small and Medium Business*. Each control has instructions outlining how auditors should evaluate conformity; what information to collect, how it can be collected, and corresponding evaluation guidance.

When reviewing information and evidence provided by organizations relating to the requirements outlined in the security controls, auditors shall ensure that provided information is accurate and recognizes the intended security objectives of the requirements outlined in the referenced standard.

Evidence comprises of verifiable documents, records, statements of fact or other information, such as customized questionnaires, relevant to audit criteria. Audit evidence may be qualitative or quantitative. It is expected that accredited conformity assessment bodies, or Certification Bodies, will each develop their own unique business process, procedures, and tools (e.g., templates/questionnaires) to facilitate the auditing process

A typical audit process consists of the following:

- Identification of sources of information
- Collecting the information by appropriate sampling and verifying, as necessary
- Establishing audit evidence from the information
- Evaluating the information and evidence against audit criteria
- Identifying audit findings
- Reviewing the audit findings and evidence
- Audit conclusion

Each section also includes an additional guidance sub-section. This guidance is intended to outline potential additional security best practices as well as providing contextual information for auditors. As such, this section and the guidance within is strictly informative and is not to be audited.

4.1 Leadership

4.1.2.1 Top management shall demonstrate their commitment to the cyber security program by:

a) ensuring the cyber security policy and objectives are established and are aligned with the strategic direction of the organization;
b) ensuring that the resources needed for the cyber security program are available and are aligned with the cyber security policy and objectives;
c) communicating the importance of effective cyber security and of conforming to the cyber security program requirements;
d) establishing cybersecurity program metrics and tracking progress; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
e) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility

Information to collect	Collection method	Criteria assessment

• Confirmation that top management is in support of the organization's commitment to implementing and maintaining the CyberSecure Canada security controls.	Provided information may include:
	• Documentation showing top management commitment to implementing and maintaining of security controls
	• Interview with auditor
	• Completed questionnaires
		Auditors shall evaluate that:
		• The provided information:
		  • Is rational
		  • Is logical
		  • Is appropriate for size of company/sensitivity of data

Additional Guidance

N/A

4.2 Accountability

4.2.3.1 Top management shall appoint a member of the senior-level leadership team to oversee and be accountable for the organization's IT security. Accountabilities of the member of the senior-level leadership team shall include the following:

a. developing and implementing a company-wide information cyber security program to meet baseline cyber security controls;
b. documenting and disseminating information security policies and procedures;
c. coordinating the development and implementation of a company-wide information security training and awareness program;
d. coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of the organization's data; and
e. identifying organizational risks and prioritizing risk treatment relative to likelihood and potential impact of cyber threats.

Information to collect	Collection method	Criteria assessment
• Name(s) and role(s) of the appointed member(s) of the senior-level leadership team to oversee and be accountable for the organization's IT security.	Provided information may include: • Name and role of appointed member • Interview with auditor • Confirmation from individual that accountabilities (a-e) from above are included in their role	No evaluation required. • Rationale for no evaluation – this controls essentially states that top management shall appoint a member to ensure the cyber security controls as outlined in the standard are properly implemented. A successful audit effectively proves the desired outcome is achieved.

Additional Guidance
N/A

4.3 Cyber Security Training

4.3.2.1 The organization shall train employees on basic security practices, including a focus on the following practical and easily implementable measures:

a. The use of effective password policies (see Subsection 5.5);
b. Identification of malicious emails and links;
c. Use of approved software;
d. Appropriate usage of the Internet; and
e. Safe use of social media;

4.3.3.1 The organization shall invest in regular and ongoing cyber security awareness and training for their employees.

Information to collect	Collection method	Criteria assessment
• Information on how the organization plans to provide employee security awareness training to all employees in the organization. • Content of training material that covers sections (a - e). • Information describing the organization's plan to invest in regular and ongoing cyber security awareness activities and training for their employees.	Provided information may include: • Documentation describing the provided training. This can include summary of organization's cyber security training plan, course outlines, frequency of training and sample training materials from the designed and implemented employee cyber security awareness training. • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: Employees are being trained on basic security practices, including at a minimum a) The use of effective password policies (see Subsection 5.5); b) Identification of malicious emails and links; c) Use of approved software; d) Appropriate usage of the Internet; and e) Safe use of social media; There is investment in regular and ongoing cyber security awareness and training.

Additional Guidance

- Standardize on a training format to deliver employee cyber security awareness and training (i.e., email, group meeting, etc.)
- Organizations consider how new employees are being onboarded to the organization and what channel of communication will be used to deliver their employee cyber security awareness training
- Organizations are Implementing a method of verification to ensure employees have completed necessary the employee cyber security awareness training
- The frequency of the training should be in accordance with size of company/sensitivity of data
- Organizations have a formal employee training plan

4.4 Cyber Security Risk Assessment

4.4.2.1 Complete the “Cyber Security Risk Assessment Questionnaire” found in Annex B
4.4.3.1 The member of the senior-level leadership team appointed to oversee the organization’s IT security shall conduct cyber security risk assessments and coordinate the implementation of cyber security controls to address potential cyber security risks.
4.4.3.2 The organization shall develop and maintain a list of their information systems and assets. For any information systems and assets not included in their implementation of the baseline cyber security controls, the organization shall document all instances where they make the business decision not to do so.
4.4.3.3 Cyber security risks accepted by the organization shall be documented and authorized by a senior official of the organization.
4.4.3.4 The organization shall identify their financial spending levels for IT and IT security investment (as raw numbers and as a percent of total expenditures).
4.4.3.5 The organization shall identify their internal staffing levels for IT and IT security (as raw numbers and as a percent of total staff).
4.4.3.6 The organization shall commit to progressive improvements to cyber security.
4.4.3.7 The organization shall determine triggers and thresholds to conduct a new or update an existing cyber security risk assessment.
4.4.3.8 Regardless of the outcomes from the cyber security risk assessment, the organization shall implement the foundational or baseline cyber security controls specified in Section 5, and as appropriate, Section 6 based on its business environment.
4.4.3.9 The organization shall periodically review and/or test cyber security controls to ensure effectiveness. Testing and/or review shall take place at a minimum annually, or if a major change occurs in their system.

Information to collect	Collection method	Criteria assessment
• Completed Questionnaire from Annex B. • Information relating to cyber risk assessment activities.	Provided information may include: • Documentation describing cyber risk assessment activities • Completed Questionnaire from Annex B (found in the National Standard) • Interview with auditor	Auditors shall evaluate that: • The organization provided information and details against each of the listed requirements. • The provided information is reasonable (i.e., not a blatant falsehood). • No further evaluation required.

Additional Guidance
N/A

5.1 Incident Response Plan

5.1.2.1 The organization shall have an incident response plan for how to respond to incidents of varying severity. If an organization is unable to manage some types of incidents on its own, the organization should have a plan for what it will do.
5.1.2.2 The incident response plan shall detail who is responsible for handling incidents including any relevant contact information for communicating to external parties, stakeholders and regulators. The organization shall have an up-to-date hard copy version of this plan available for situations where soft copies are not available.
5.1.2.3 The organization should consider purchasing a cyber security insurance policy that includes coverage for incident response and recovery activities or provide rationale for not purchasing one.
5.1.2.4 The organization may use the incident response plan template (see Annex A) as a measure of satisfying Requirements contained in Subsection 5.1.2.

Information to collect	Collection method	Criteria assessment
• A copy of the Incident Response Plan or information outlining the existence of an IRP and what is included. • Description of incident response plan for various level of severity. • If available, information regarding whether the company has purchased an insurance policy and possible rationale for not purchasing one.	Provided information may include: • Documentation describing Incident Response Plan • Completed IRP template from Annex A (found in the National Standard) • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: • An Incident Response Plan (IRP) exists and addresses incidents ranging from trivial to extremely severe, including incidents that cannot be handled directly by the organization. • The IRP outlines who is responsible for handling incidents including any relevant contact information for communicating to law enforcement, external parties, stakeholders and regulators. • An up-to-date hard copy version of the IRP is available • The organization considered purchasing or purchased a cyber security insurance policy. ○ Auditors to ask for rationale for not purchasing insurance, but do not need to evaluate.

Additional Guidance

- The plan should cover the following incidents at a minimum: Data breach, Ransomware, and Interruption of services due to connectivity loss (e.g., distributed denial of service [DDOS]). For incidents to which the organization is unable to respond, the plan should describe what the organization will do (e.g., Consultant company X has agreed to provide its services to respond to incident Y).
- The organization should have a method to contact internal and external parties in the case of an incident.

5.2 Automatically Patch Operating Systems and Applications

5.2.2.1 The organization shall have up-to-date security patches for all software and hardware installed to protect assets from known vulnerabilities.
5.2.2.2 The organization shall enable automatic patching for all software and hardware or document all instances where they make the business decision not to do so.
5.2.2.3 The organization shall perform a risk assessment whether to replace systems incapable of automatic patching.

Information to collect	Collection method	Criteria assessment
• The catalogue or list of all software/hardware installed/sanctioned by the organization (IT asset catalogue). The catalogue should contain information about the latest version available/installed and whether the patches are installed automatically or manually. • For instances where manual patching is being used, the company is to provide rationale for not using auto patching. • Information regarding any risk assessment activities performed on systems incapable of automatic patching.	Provided information may include: • IT Asset Catalogue • Documentation describing automatic patching activities • Interview with auditor • Random Sampling • Completed Questionnaires	Auditors shall evaluate that: • All hardware and software are up-to-date. • Where possible, automatic patching is enabled for all software and hardware. OR If manual patching is used there is a documented business decision and rational. • A risk assessment was performed for any systems incapable of automatic patching.

Additional Guidance

- A formal or informal business process to ensure regular manual updates exists

5.3 Enable Security Software

5.3.2.1 The organization shall enable anti-malware solutions that update automatically and prevent malware from executing without user intervention.		
Information to collect	**Collection method**	**Criteria assessment**
• Information describing organization-wide anti-malware solutions that are enabled on systems.	Provided information may include: • Documentation describing anti-malware solutions • Interview with auditor • Random Sampling of devices	Auditors shall evaluate that: • Where possible, anti-malware solutions are enabled, they are capable of automatic updates, and that they prevent malware from executing without user intervention.
Additional Guidance • Anti-malware solutions are configured to perform period scans		

5.4 Securely Configure Devices

5.4.2.1 The organization shall implement secure configurations for all their devices by:

a) changing all default passwords.

5.4.3.1 The organization shall implement secure configurations for all their devices unless it is impossible to do so on a specific device:

a) by turning off unnecessary features i.e., block unused ports, disable unused services, remove unused or obsolete software; and

b) by enabling all relevant security features.

Information to collect	Collection method	Criteria assessment
• Information describing organization efforts to change all default passwords. Information may include, but not limited to, the IT asset catalogue with indication of which devices/software allow for installation with default passwords, steps for changing of default passwords, or organizational password policy. • Information describing organization efforts to implement secure configurations for all their devices, including which devices from IT Asset catalogue were impacted.	Provided information may include: • Documentation describing secure configuration of devices • Interview with auditor • Random Sampling of devices	Auditors shall evaluate that: • The organization changes all default password • Provided information identifies the hardening guidelines used by the organization, the unnecessary features that were disabled from the devices, and the security features that were enabled on the devices.

Additional Guidance

N/A

5.5 Use Strong User Authentication

5.5.2.1 Organizations shall implement multi-factor authentication or document all instances where they cannot or make the business decision not to do so.
5.5.2.2 Organizations shall enforce password changes on suspicion or evidence of compromise.
5.5.2.3 Organizations shall have clear policies on password length and reuse, the use of password managers and if, when, and how users can physically write down and securely store a password.
NOTE: Organizations may use password selection guidance from the Communications Security Establishment's User Authentication Guidance for Information Technology Systems.
5.5.3.1 Organizations shall implement a password manager or document the business decision not to do so.
NOTE: Guidance document - Guidance documents as references to the Bibliography.
https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Information to collect	Collection method	Criteria assessment
• Evidence of the implementation of multi-factor authentication. Where multi-factor authentication is not being used, a rationale shall be provided. Evidence can include but is not limited to: company user authentication policy, a detailed description of how/where multi-factor authentication is being used, document outlining instances where multi-factor authentication is not being used with supporting reasoning. • Information describing password policies. Documentation can include: company user authentication policy (must include password policy) **OR** information outlining how/when password changes are enforced. • Information describing the use of a password manager or rationale for not using one.	Provided information may include: • Password policies • Documentation describing the implementation of multi-factor authentication • Interview with auditor • Random Sampling of accounts	Auditors shall evaluate that: • Multi-factor authentication is implemented, especially for the following accounts: ○ financial accounts, system administrators, cloud administrators, privileged users, and senior executives. • Rationale is provided for all instances where the organization decided not to use multi-factor authentication. • Password changes are enforced on suspicion or evidence of compromise, there is a clear policy on minimum password length, and if, when users can physically write down and/or securely storing a password. • A password manager is being used. In instances where one is not being used, a rationale is provided.

Additional Guidance

- The organization has clearly defined user policies to identify and capture requirements.
- Prohibition of password reuse for multiple systems and accounts
- Minimum password length for high value accounts, such as system administrators and financial controllers, is 14 characters.

5.6 Backup and Encrypt Data

5.6.2.1 Organizations shall determine on a case-by-case basis what business information and software (including but not limited to sensitive information) is essential to the functioning of the organization, and how frequently this information changes.
NOTE: As an example, critical workstations and servers may require daily incremental backups, whereas desktops may be recovered from one common image.
5.6.2.2 Organizations shall determine on a case-by-case basis what systems to back up and at what frequency since every system will have different back-up and recovery requirements.
5.6.2.3 Organizations shall backup systems that contain essential business information and ensure that recovery mechanisms effectively and efficiently restore these systems from backups.
5.6.2.4 Organizations shall store backups at a secure offsite location (either physically or via network separated cloud services) at regular intervals to provide diversity in the event of a disaster (fire, flood, earthquake or localized cyber security incident).
5.6.2.5 Organizations should consider the use of encrypted backups with securely stored and recoverable key material. Decryption keys and/or unencrypted backups should be stored securely and should be accessible only to authorized employees or officers.
5.6.3.1 Organizations shall use a sampling of backup data to test and verify recovery procedures at regular intervals to ensure the integrity of the end-to-end backup and restoration process.

Information to collect	Collection method	Criteria assessment
• Information describing what business information and software is essential and how often it changes. • Information describing what systems to back up and at what frequency. • Information describing that all systems with essential business information are being backed up and a recovery plan exists. • Information indicating the use of offsite backups. • Information indicating the use of encrypted backups using securely stored and recoverable key material. • Information regarding the testing and verification of recovery procedures.	Provided information may include: • Documentation describing backup and encryption processes • Documentation describing testing and recovery processes • Interview with auditor • Random Sampling of backups • Completed Questionnaires	Auditors shall evaluate that: • Essential business information and software is being identified and how frequently it changes. • The organization has evaluated their systems and identified the systems that need to be backed up and how frequently to back them up. • Essential business information is being backed up and that there are recovery mechanisms in place • Recovery mechanisms are being tested and verified to restore systems from backup. • Backups are being stored offsite.

Additional Guidance

- Essential information (including sensitive information) should always be backed up.
- The organization has a formal backup plan
- The frequency of updates is proportional to the rate at which the information is updated

5.7 Establish Basic Perimeter Defenses

5.7.3.1 The organization shall have a firewall placed between two perimeters that controls the amount and kinds of traffic that may pass between the two.
5.7.3.2 The organization should consider implementing a DNS firewall for outbound DNS requests to the Internet.
5.7.3.3 The organization shall activate any software firewalls included on devices within their networks or document the alternative measures in place instead of these firewalls.
5.7.3.4 The organization shall require encrypted connectivity to all corporate IT resources and require VPN connectivity with multi-factor authentication for all remote access into corporate networks.
5.7.3.5 The organization shall use secure Wi-Fi, at a minimum WPA2-AES, preferably WPA2-Enterprise or WPA3-Enterprise, following password requirements in section 5.5.
5.7.3.6 The organization should segment their networks to ensure networks provided to the public/customers are separated (and/or isolated) from the corporate networks.
5.7.3.7 The organization shall ensure the implementation of DMARC on all organization email services.
5.7.3.8 The organization shall ensure email filtering is implemented.

Information to collect	Collection method	Criteria assessment
• Information describing the use of firewalls within the organization's networks. • Information describing the use of a DNS firewall. • Information describing the activation of software firewalls on organizational devices or alternative methods in place. • Information describing the use of encryption/VPN. • Information describing the use of WiFi. • Information describing segmentation of networks. • The list of email domains used by the organization. Optionally, the DNS records indicating that DMARC [6] is implemented on all the organization's email services or a statement from an email provider indicating the implementation of DMARC. • Information describing the organization efforts to implement email filtering.	Provided information may include: • Network diagrams • Firewall rules/logs • Documentation describing the implementation of firewalls • Interview with auditor • Random Sampling of firewall rules • Completed Questionnaires	Auditors shall evaluate that: • That the firewalls are properly placed within the organizational networks and that firewalls are inspecting/filtering traffic adequately. • Provided documentation includes a list of the service ports that are open on the system(s) and the rationale or documentation describes the equivalent measures, such as network micro-segmentation. • Any and all software firewalls are activated or there are alternative documented solutions in place. • All site-to-site communications are encrypted (e.g., IPsec VPN tunnels), remote access communications are encrypted (e.g., L2TP/IPsec, OpenVPN) and use multi-factor authentication. • All Wi-Fi networks use WPA2 security protocol or better (e.g., WPA2-Enterprise, WPA3) and that password requirements are adequate. • DMARC is implemented for outgoing email. • The organization recognizes email as a security threat for ingress and egress traffic and has implemented adequate email filtering to address it.

Additional Guidance

- Organizations keep a list of all applications and service ports that must be open to the Internet with the rationale and a procedure/policy for verifying the ongoing business requirement for open firewall ports.
- DNS filtering is applied to all Internet DNS requests using one of the following three methods:
  - A DNS firewall bundled with the perimeter firewall, enabled and kept up to date.
  - A free DNS resolver that supports filtering/firewalling configured on all devices (e.g., 9.9.9.9 or Quad9 [4].
  - A DNS firewall implemented on premises and kept up-to-date (e.g., Pi-Hole).
- That the following DNS TXT records exist:
  - SPF record for each email domain.
  - DKIM record for each email domain.
  - DMARC record for each email domain.
- Email filtering schemes should include: malicious content filtering (signature-based, behaviour-based, inappropriate content, intellectual property, spam, and white/blacklisting).
- There is adequate network separation between public and corporate networks.

5.8 Implement Access Control and Authorization

5.8.3.1 The organization shall provision accounts with the minimum functionality necessary for tasks and shall restrict administrator privileges to an as-required basis.
5.8.3.2 The organization shall remove accounts and/or functionality when users no longer require these for their tasks.
5.8.3.3 The organization shall only permit administrator accounts to perform administrative activities (and not user-level activities such as accessing email or browsing the web).
5.8.3.4 The organization should consider the implementation of a centralized authorization control system.

Information to collect	Collection method	Criteria assessment
• Information describing the user account policies. • Information describing the updating of user account policies.	Provided information may include: • User account policies • Interview with auditor	Auditors shall evaluate that:

• Information describing policy for user accounts and how the organization limits administrator activities. • Information describing the implementation of a centralized authorization control system OR the rationale for not implementing a centralized authorization control system.	• Random Sampling of accounts • Completed Questionnaires	• That accounts are provisioned with minimum functionality necessary and that admin privileges are restricted to an as-required basis ○ Ideally the principle of least privilege access for task execution is applied on all accounts. • A process is in place to: disable accounts that are no longer required (e.g., departure of employees), promptly update account privileges/functionality, to review remote access privileges on a regular basis and remove/disable when no longer required. • Administrator accounts are limited to performing administrative activities (e.g., not used for web browsing and/or email access). Also, that only administrator accounts can perform administrative activities. • The organization implements a solution for access control (e.g., Active Directory, OpenLDAP) or, if not implemented, confirms due diligence and a rationale.

Additional Guidance

- Generally, users should not have administrator rights, including on their local devices. This includes, but is not limited to, the inability to disable or revert software updates, disable anti-malware or change the software settings. Only IT personnel should have administrator accounts, except in documented cases with the rationale. Only a small subset of IT personnel has domain administrator accounts (if applicable). Network share access is limited and controlled.

6.1 Secure Mobility

6.1.3.1 Organization using mobility (i.e., cellphones) shall decide on an ownership model for mobile devices and document the rationale and associated risks.

6.1.3.2 Organization using mobility (i.e., cellphones) shall:

a. Require separation between work and personal data on mobile devices with access to corporate IT resources and document the details of this separation;

b. Ensure that employees only download mobile device applications (i.e., apps) from the organization's list of trusted sources.

c. Require that all mobile devices store all sensitive information in a secure, encrypted state.

d. Consider the implementation of an enterprise mobility management solution for all mobile devices or document the risks assumed to the audit, management, and security functionality of mobile devices by not implementing such a solution.

e. Enforce or educate users to:

- disable automatic connections to open networks;
- avoid connecting to unknown Wi-Fi networks;
- limit the use of Bluetooth and NFC for the exchange of sensitive information ; and
- use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.

f. Consider using secure connectivity (VPN, Virtual Desktop etc.) when connecting to public Wi-Fi networks, or provide the rationale for not doing so.

Information to collect	Collection method	Criteria assessment
• Information on the ownership model for mobile devices, rationale and associated risks. • Description of the work-personal data separation on mobile devices with access to corporate IT resources. • Description of the list of trusted sources of applications available for download onto mobile devices. • Description of the sensitive information storage state on all mobile devices. • A description of the enforcement or education pertaining to mobile device use on the prescribed areas. • If provided by the organization, the auditor shall collect a description of the use of secure connectivity.	Provided information may include: • Description of the ownership model for mobile devices • Interview with auditor • Random Sampling of mobile devices • Completed Questionnaires	Auditors shall evaluate that: • An ownership model for mobile devices exists and that the risks associated with the ownership model have been identified. • The information provided demonstrates a requirement of the separation of work and personal data. • The provided description of trusted sources clearly identifies the organization's trusted sources and how the organization mandates employees to only use them as the source of applications for mobile devices. • The description of the sensitive information storage state identifies the use of an encryption technology. • The information provided demonstrates that the organization enforces or educates on the importance of no automatic connection to open/unknown wireless networks, the avoidance of connecting devices to unknown Wi-Fi networks, limiting the use of Bluetooth and NFC for the exchange of sensitive information and the use of corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.

Additional Guidance
N/A

6.2 Secure Cloud and Outsourced IT Services

6.2.2.1 Organization using cloud applications and/or outsourcing IT services shall evaluate their risk tolerance level with how their outsourced IT providers handle and access their sensitive information.

6.2.3.1 The organization using cloud applications and/or outsourcing IT services shall:

a. Require that all their cloud service providers share an AICPA SSAE 18 or equivalent report that states that they achieved Trust Service Principles compliance or provide a documented business case as why they chose not to;

NOTE: The organization determines equivalence to AICPA SSAE 18.

b. Evaluate their risk tolerance level with the legal jurisdictions where their outsourced providers store or use their sensitive information;

c. Ensure that their IT infrastructure and users communicate securely with all cloud services and applications; and

d. Ensure that administrative accounts for cloud services use multi-factor authentication and differ from internal administrator accounts.

Information to collect	Collection method	Criteria assessment
• Description of the types of information being shared, processed, stored or accessed by cloud service providers or outsourced IT services. • Description of the sensitivity of the information type being shared. • Overview of any risks being accepted (i.e., risk tolerance) by the applicant with respect to how outsources IT providers access an organizations sensitive information. • Description of the organization's due diligence and risk tolerance pertaining to legal jurisdictions where outsourced providers store or use sensitive information. • Description of the communications methods between the organization's IT infrastructure and cloud services • Description of the authentication methods for cloud services administrative accounts and how they differ from internal admin accounts.	Provided information may include: • Information regarding IT outsourcing activities • AICPA SSAE 18 reports or equivalent from all cloud service providers • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: • Any accepted risk is reasonable based on the information type and rationale provided. • The provided report is either AICPA SOC 2 or AICPA SOC 3, or an equivalent. • Due diligence is demonstrated (i.e., a risk assessment has been performed) with regard to the legal jurisdiction where outsources providers are storing or using sensitive information. • That communications between the organization's IT infrastructure and cloud services are secure. Secure communications include any of the following implementation, or combination thereof: TLS 1.3 encryption protocol, IPsec VPN tunnels, etc. • Authentication methods for all cloud administrative accounts use multi-factor authentication and differ from internal administrator accounts.

Additional Guidance

N/A

6.3 Secure Websites

6.3.3.1 Organizations deploying websites shall ensure that their websites address the OWASP top 10 vulnerabilities.
NOTE: For a comprehensive list of vulnerability scanning tools, please visit the "Vulnerability Scanning Tools" page on the OWASP website.
6.3.3.2 Organizations shall ensure that they understand the OWASP ASVS level they need to meet for each of their websites.

Information to collect	Collection method	Criteria assessment
• Information regarding the testing of the OWASP Top 10 Vulnerabilities. • Description of the organization's understanding of the OWASP ASVS levels required for each website.	Provided information may include: • OWASP Top 10 Vulnerability Scan report • Documentation describing their understanding of ASVS level for each company website • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: • That the test report attests that the organization's websites do not suffer from any of the OWASP top 10 vulnerabilities. OR If the automated test report contains vulnerabilities classified as low that are not easily rectified, the client must document a mitigation plan that outlines how the vulnerability will be monitored and logged and demonstrate an understanding of the accepted risk. • That the organization's description demonstrates an understanding of the ASVS levels and identifies the applicable level to their websites.

Additional Guidance
N/A

6.4 Secure Portable Media

6.4.2.1 Organizations using portable media shall mandate the sole use of organization-owned secure portable media.
6.4.3.1 Organizations using portable media shall:

a. Have strong asset controls for these devices;
b. Require the use of encryption on all of these devices; and
c. Have processes for the sanitization or destruction of portable media prior to disposal.

Information to collect	Collection method	Criteria assessment
• Description of how portable media is used and any policies or directives addressing it use within the organization. • Information regarding asset controls for all portable media devices. • Information regarding the use of encryption with portable media. • Information regarding the sanitation/destruction of portable media.	Provided information may include: • Portable media policy (if available) • Documentation regarding organizational portable media use • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: • The organization requires that only organization provided portable media can be used. • The organizations asset controls for portable media are identified and adequate (i.e., strong). • The organization requires the use of encryption on all portable media. • There is a process for the sanitization or destruction of portable media prior to disposal.

Additional Guidance
N/A

6.5 Point of Sale (POS) and Financial Systems

6.5.2.1 Organizations using point of sale terminals and financial systems shall follow the Payment Card Industry Data Security Standard (PCI DSS) and isolate these systems from the Internet.		
Information to collect	**Collection method**	**Criteria assessment**
• Description of the organization's point of sale terminals and financial systems isolation from the Internet. • Description of the organization's compliance to the Payment Card Industry Data Security Standard (PCI DSS).	Provided information may include: • Documentation on POS use and isolation from Internet • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: • The point of sale terminals and financial systems are isolated from the Internet.
Additional Guidance N/A		

6.6 Computer Security Log Management

6.6.3.1 Organizations shall ensure an appropriate understanding of their security logging capabilities and needs and ensure a corresponding log management policy is in place.
NOTE: NIST SP 800-92, “Guide to Computer Security Log Management” describes considerations for Security Log Management and includes examples. Understanding what data is available and what is missing is a key step in defining a good log management and incident.

Information to collect	Collection method	Criteria assessment
• Description of the organization’s understanding of security logging capabilities.	Provided information may include: • Log management policy • Documentation log management best practices • Interview with auditor • Completed Questionnaires	Auditors shall evaluate that: • There is a log management policy. • The policy and additional provided information demonstrate an appropriate understanding of the security logging capabilities including a description of log management, analysis and collection.

Additional Guidance

- The log management policy should address the following elements: user login events, file or data level accesses, device or user configuration status messages (e.g., installed software and version, firewall, intrusion detection system logs, etc.)