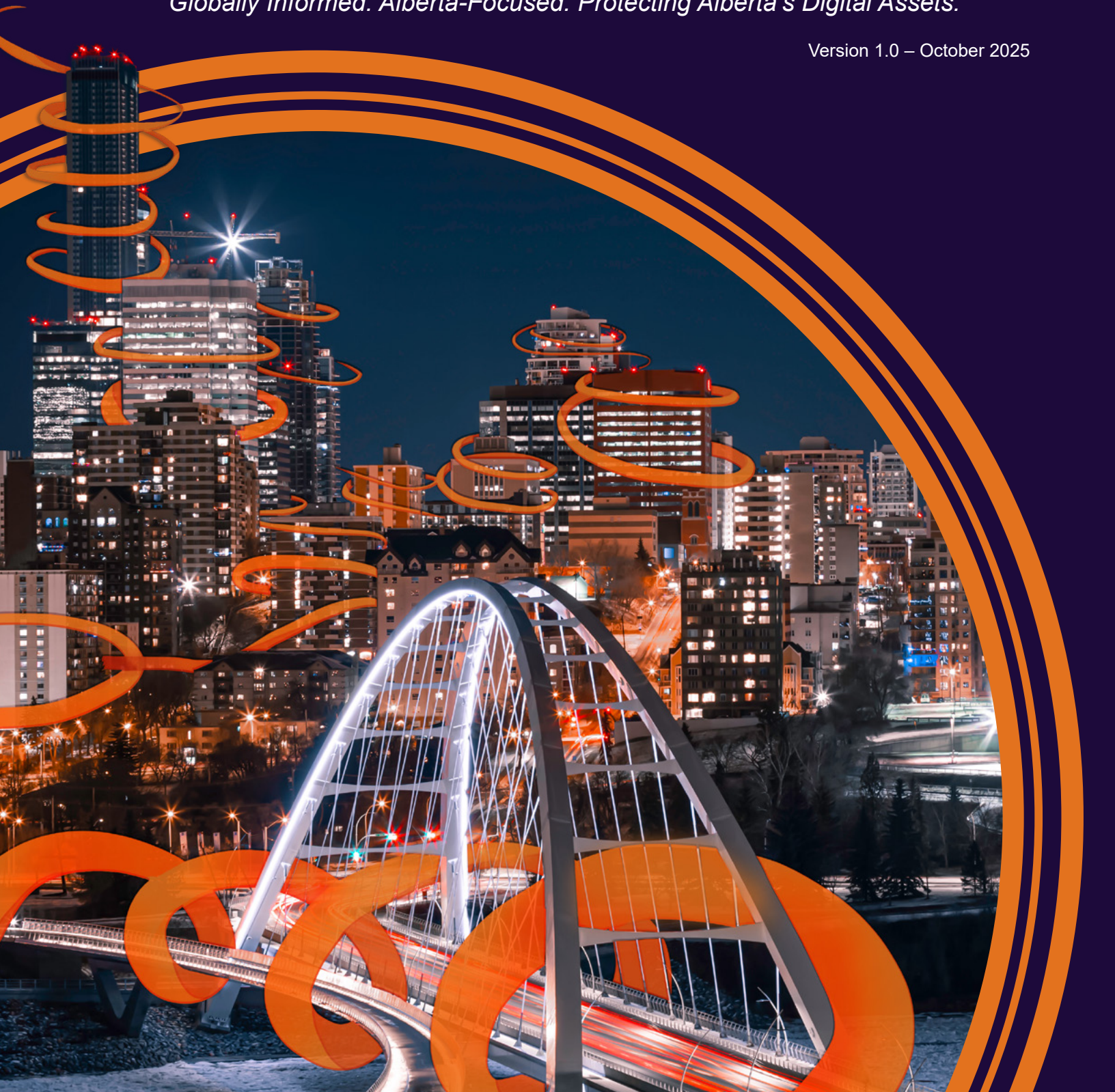
CYBER ALBERTA

Compliance Framework Assessment and Benchmarking Tool

Globally Informed. Alberta-Focused. Protecting Alberta's Digital Assets.

Version 1.0 – October 2025



Purpose

The purpose of the **CyberAlberta Compliance Framework Assessment and Benchmarking Tool** is to support Alberta businesses in understanding their cybersecurity posture and to build stronger cyber resilience.

Introduction

This framework is based on the six (6) core functions of cybersecurity: **Govern**, **Identify**, **Protect**, **Detect**, **Respond,** and **Recover** identified by the National Institute for Standards in Technology (NIST). Each function includes cyber readiness goals developed using the Canadian Centre for Cybersecurity's Cyber readiness goals (www.cyber.gc.ca) and tuned to the Alberta perspective. This includes consideration of privacy and cybersecurity laws within the province that may provide unique considerations for Alberta based businesses. Special thanks to the Canadian Centre for Cybersecurity's important work on this issue.

Building a strong and cyber resilient Alberta is key to CyberAlberta's mission and vision for Alberta's future.

This framework is provided in a PDF fillable form, allowing organizations to document their current cybersecurity posture and their progress over time. We invite organizations using this assessment for internal purposes to consider submitting an anonymous copy to **CyberAlbertaCompliance@gov.ab.ca**. Submissions are voluntary and will support provincial benchmarking and analysis. The assessment does not collect personal or identifying information. All submitted emails will be treated as transitory records, and the data will be used to help gauge Alberta's overall cybersecurity snapshot.

How to use this framework

This framework has been designed to simplify the process of determining an organization's cyber posture, to highlight areas of weakness and support provincial level benchmarking.

Cyber Implementation Overview

A strong cybersecurity posture is essential for securing an organization's systems and infrastructure. Understanding the organization's posture will help determine vulnerabilities and weaknesses and build compliance. The security posture includes security policies and procedures, training programs, specific security solutions, governance and other important considerations.

Completing this framework will help an organization look at its cyber risks and strengths as a whole, and measure how prepared the organization is to defend and respond to cyber threats.

This framework consist of six core functions and several goals within each function to assess the organization's maturity within that function.

Organizations should complete each goal within each core function, even if the assessment response is unidentified. Organizations should plan to review and reassess every one to two (1-2) years depending on changes to the environment and events such as cyber attacks or for any other reason identified by leadership.

Goals

Each goal consists of a title, outcome, recommended action, risks, an assessment level and references.

- Title refers to the name of the specific goal.
- Outcome is a single sentence that captures the overall objective of the goal.
- Recommended Action is a description of how to achieve the desired outcome of the goal.
- Risks are a listing of common risks identified with each goal, however organizations may have additional risks, depending on their work.
- Assessment Level is used by the organization to document their current level in relation to each goal. This section also includes the date on which the assessment was completed.
    - Unknown – should be used when the individual or team is unaware of their progress towards the desired outcome if any.
    - Not Started – should be used when the organization is aware of the need to reach the desired outcome but has not yet scoped or planned a path forward.
    - Scoped/Planned – the organization has a plan for the goal.
    - In Progress – the goal has been planned and work is progressing towards that goal.
    - Implemented – the organization has implemented the necessary steps to meet the desired outcome and it is reviewed regularly.
- References include related CyberAlberta documents, NIST Cybersecurity documents or other relevant materials that can assist the organization in understanding the specific goal.

Contents

Govern

The **Govern** function emphasizes executive-level oversight, strategy, and accountability. It ensures that cybersecurity priorities align with overall business goals and leadership remains actively involved in risk management decisions. The Govern function includes five key goals for building and assessing the organization's current measurement of cyber compliance cyber compliance.

Section Contents

Privacy Leadership

Outcome

A single leader or team is responsible and accountable for managing cyber-related privacy risk.

Risks

Risk of compliance to Alberta privacy laws.

Recommended Action

Identify a job title or role as responsible and accountable for the organization's privacy risk management program. The responsible person or team establishes policies and procedures that require the organization to:

- consider the full spectrum of cyber-related privacy risks and obligations, including the impact of applicable privacy legislation such as Alberta's Protection of Privacy Act (POPA).
- apply that analysis to support operational decisions that should reflect those privacy considerations.

The privacy risk management program could include maintaining a personal information inventory, as well as policies to limit collection and retention of personal information.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Intended for public bodies but useful for all organizations: Fact Sheet: Privacy Management Program.

Protection of Privacy Act.

Health Information Act.

Personal Information Protection Act.

Supply chain incident reporting process/policies

Outcome	Organizations rapidly learn about and respond to known incidents or breaches across vendors and service providers.
Risks	Supply Chain Compromise and risks to Industrial Control Systems.
Recommended Action	Ensure the organization's cybersecurity supply chain risk management program stipulates that vendors and/or service providers must notify the procuring customer of security incidents. This should be done within a specified time frame, as determined by the organization, and be documented in procurement documents and contracts, including service level agreements.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Threats to Home and Small Office Routers.

Protecting organizations from software supply chain threats.

Vendor/supplier cybersecurity requirements

Outcome	Risk is reduced by purchasing secure products and services from secure suppliers.
Risks	Risks include Supply Chain Compromise.
Recommended Action	Include cybersecurity requirements and questions in organizations' procurement documents and policies and procedures. Ensure responses are evaluated in vendor selection such that, given 2 offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred or, when possible, the more secure option is preferred even at higher cost.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Protecting organization from software supply chain threats.

Organizational and Operational Technology Cybersecurity Leadership

Outcome

A single individual in a leadership position is responsible and accountable for cybersecurity within an organization. If applicable to the organization, a single leader is responsible and accountable for operational technology-specific cybersecurity within an organization with OT assets. In some organizations, one individual may be responsible for both leaderships.

Risks

Lack of accountability, investment, or effectiveness in cybersecurity or operations technology cybersecurity programs.

Recommended Action

Identify a named role or title as responsible and accountable for planning, resourcing, and executing cybersecurity activities. This role may undertake activities, such as managing cybersecurity operations at the senior level, requesting, and securing budget resources, or leading strategy to inform future positioning. Additionally, identify a named role or title as responsible for resourcing, and executing operational technology-specific cybersecurity activities. In some organizations, both cybersecurity leadership and OT leadership can be the same position.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Executive Guide for Incident Management.

Identify

The **Identify** function is intended to help organizations understand their own unique environment including their systems, assets, data and risks to their environment. It is a key function that can be leveraged to determine an organizations current state of cybersecurity and shed a light on any gaps. This section can also help an organization to develop and prioritize a plan to address those gaps.

Section Contents

Asset Inventory and Network Topology

Outcome

Better identify known, unknown, and unmanaged assets, including web-facing assets for the cloud and data assets. The organization can then more rapidly detect and respond to new vulnerabilities and maintain service continuity.

Risks

Risks include Hardware Additions, Exploit Public-Facing Applications, and Internet Accessible Device.

Recommended Action

Maintain a regularly updated inventory of all assets within the organization's information technology and operational technology networks if applicable. Include in the inventory accurate documentation of network topology and identified data assets, in particular sensitive or classified information. Update this inventory on a regular basis for both information technology and operational technology, and immediately log in the existing inventory any new asset that is integrated into the organization's infrastructure.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Using information technology asset management to enhance cybersecurity.

Mitigating Known Vulnerabilities

Outcome

Reduce the likelihood that threat actors will exploit known vulnerabilities to breach organizational networks.

Risks

Organizations face risks such as Active and Vulnerability Scanning, Exploitation of Public-Facing Applications, Exploitation of Remote Services, Supply Chain Compromise, and unauthorized access through External Remote Services.

Recommended Action

Patch all known exploited vulnerabilities listed in the Cybersecurity and Infrastructure Agency: Known Exploited Vulnerabilities Catalog in Internet-facing systems within a risk-informed timespan, prioritizing more critical assets first. Identify security vulnerabilities in systems by conducting penetration tests and using automated vulnerability scanning tools, activities which are part of a comprehensive vulnerability management strategy.

For operational technology assets where patching is not possible or may substantially compromise availability or safety, apply and record compensating controls (for example, segmentation, monitoring). Sufficient controls either make the asset inaccessible from the public Internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.

Carefully select automated vulnerability detection tools as they can scan systems aggressively. These tools may cause devices to behave erratically, stop working, crash, or restart, or need manual intervention to revert to an operational state.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Top 10 IT Security actions: No. 2 patch operating systems and applications.

Top 10 IT security actions: No. 5 Segment and separate information.

How updates secure devices.

Baseline cybersecurity controls for small and medium organizations.

Known exploited vulnerabilities catalog.

Third-party Validation of Cybersecurity Control effectiveness

Outcome

Identify tactics, techniques, and procedures that lack proper defences and establish confidence in organizational cyber defences.

Risks

Reduce the risk of gaps in cyber defences or a false sense of security in existing protections.

Recommended Action

Third parties with demonstrated expertise in IT and/or OT cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defences. Conduct these exercises annually to include activities such as penetration tests, bug bounties, incident simulations, or table-top exercises, and include both unannounced and announced tests.

Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (for example, assume breach) to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems.

Mitigate in a timely manner high-impact findings from previous tests so these are not re-observed in future tests.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

CyberAlberta Governance, Risk and Compliance.

Incident Response Plans

Outcome

Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.

Risks

Inability to quickly and efficiently contain, mitigate, and communicate about cybersecurity incidents.

Recommended Action

Develop, maintain, update, and regularly test cybersecurity Incident Response Plans for both common and organization-specific (for example, by sector or locality) threat scenarios. Consider engaging with appropriate stakeholders to conduct tabletop exercises focused on artificial intelligence-enhanced attacks.

When tests or exercises are conducted, ensure they are as realistic as feasible and conform to the organization's acceptable levels of downtime. Conduct Incident Response Plan exercises at least annually and update within a risk-informed time frame following the lessons learned portion of any test.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

CyberAlberta Data Loss Playbook.

CyberAlberta Cyber Compromise Checklist.

Developing an Incident Response Plan.

Deploy security.txt files

Outcome

Allows security researchers to submit discovered weaknesses or vulnerabilities more quickly.

Risks

Organizations may be exposed to risks such as Active Scanning and Vulnerability Scanning, Exploitation of Public-Facing Applications and Remote Services, and Supply Chain Compromise.

Recommended Action

Ensure all public-facing web domains have a security.txt file that conforms to the recommendations in a recognized standard such as the NIST Publiation 800-53 Rev. 5.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Security.txt standard guide.

Vulnerability Reporting program.

Select a Trusted Cloud Service Provider

Outcome

If cloud is leveraged and a trusted relationship established with a mature and technically capable cloud service provider, organizations can confidently adopt cloud services, harnessing the benefits of scalability, flexibility, and cost effectiveness while safeguarding their sensitive assets.

Risks

Reduce risk of attacks and/or compromise due to immature Cloud Service Provider. Other risks include Supply Chain Compromise.

Recommended Action

Ensure that the selected Cloud Service Provider offers secure data storage, encryption, and access controls, and validate that the provider's cybersecurity capability and practices are compliant with relevant security standards and regulations. This can be accomplished by confirming a Cloud Service Provider's adherence to existing compliance regimes, which can vary depending on the organization's business requirements.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Top measures to enhance cybersecurity for small and medium organizations.

Baseline cybersecurity controls for small and medium organizations.

Protect

The **Protect** function is designed to develop and implement safeguards that ensure the delivery of critical services and limit the impact of potential cybersecurity events. This function plays a crucial role in strengthening an organization's cybersecurity posture by proactively preventing threats before they escalate.

Section Contents

Changing Default Passwords

Outcome

Prevent threat actors from using default passwords to achieve initial access to or move laterally in a network.

Risks

Risk include the use of Default Accounts with unchanged credentials and unauthorized access through Valid User Accounts.

Recommended Action

Develop and enforce an organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting them on any internal or external networks. This includes information technology assets for operational technology, such as operational technology administration web pages.

In instances where changing default passwords is not feasible (for example, a control system with a hard-coded password), implement and document appropriate compensating security controls such as access restrictions and network segmentation. Additionally, monitor logs for network traffic and login attempts on those devices.

While changing default passwords on an organization's existing operational technology requires significantly more work, enforce a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary tactics, techniques, and procedures change.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Learn how to protect digital identity.

Minimum Password Strength

Outcome

Organizational passwords are harder for threat actors to guess or crack.

Risks

Brute Force attacks include Password Guessing, Password Cracking, Password Spraying, and Credential Stuffing.

Recommended Action

Implement a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected information technology assets and for all operational technology assets where technically feasible.**

Consider leveraging passphrases of at least 4 words and 15 characters in length. Where suitable, use passphrases, as they are longer but easier to remember. In instances where minimum password lengths are not technically feasible, apply and record compensating controls, log all login attempts, and prioritize for upgrading or replacing those assets.

This goal is particularly important for organizations that:

• lack widespread implementation of multi-factor authentication and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks)

• are unable to adopt passwordless authentication methods.

Note:
* Modern attacker tools can crack 8-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations.
** Operational technology assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk operational technology assets that may not be technically feasible include those in remote locations, such as on offshore rigs or wind turbines.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Learn how to protect digital identity.

Best Practices for Passphrases and Passwords.

Unique Credentials

Outcome

Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between all networks.

Risks

Threat actors may use Stolen Credentials or Brute Force Password Guessing to access Valid Accounts.

Recommended Action

Provision unique and separate credentials for similar services and asset access on all networks. Ensure users do not (or cannot) reuse passwords for accounts, applications, services, etc. Require that service accounts/machine accounts have unique passwords from all member user accounts.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Top 10 IT security actions: No. 3 managing and controlling administrative privileges.

Revoking Credentials for Departing Employees

Outcome

Prevents unauthorized access to organizational accounts or resources by former employees, contractors, and other temporary staff.

Risks

Risk to Valid Accounts.

Recommended Action

Apply a defined and enforced administrative process to all departing employees, contractors, and other temporary staff by the day of their departure that:

- revokes and securely returns all physical badges, key cards, tokens, etc.
- disables all user accounts and access to organizational resources

Assessment

- ○ Unknown
- ○ Not Started
- ○ Scoped/Planned
- ○ In-Progress
- ○ Implemented

References

Top 10 IT security actions: No. 3 managing and controlling administrative privileges.

Separating User and Privileged Accounts

Outcome

Make it more difficult for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.

Risks

Risk to Valid Accounts.

Recommended Action

User accounts should not always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (for example, for business email, web browsing). Reevaluate privileges on a recurring basis to validate continued need for a given set of permissions.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Top 10 IT security actions: No. 3 managing and controlling administrative privileges.

Network Segmentation

Outcome

Reduce the likelihood that threat actors will access the operations technology network after compromising the information technology network.

Risks

Risks include Network Service Discovery, Trusted Relationship, Network Connection Enumeration, and Network Sniffing.

Recommended Action

All connections to the operational technology network are denied by default unless explicitly allowed (for example, by Internet Protocol address and port) for specific system functionality. Necessary communications paths between the information technology and operational technology networks must pass through an intermediary, such as a properly configured firewall, bastion host, jump box, or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Cybersecurity Top 10 Best Practices.

Top 10 IT security actions: No. 5 segment and separate information.

Detection of Unsuccessful (automated) Login Attempts

Outcome

Protect organizations from automated, credential-based attacks.

Risks

Brute Force methods include Password Guessing, Password Cracking, Password Spraying, and Credential Stuffing.

Recommended Action

Log all unsuccessful logins and send to the organization's security team or relevant logging system. Ensure security teams are notified (for example, by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (for example, 5 failed attempts over 2 minutes). Log and store these alerts in the relevant security or ticketing system for retroactive analysis.

For information technology assets, establish a system-enforced policy that prevents future logins for the suspicious account. For example, this could be for some minimum time or until the account is re-enabled by a privileged user. Enable this configuration when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins in a 10 minute period.

Assessment

- ○ Unknown
- ○ Not Started
- ○ Scoped/Planned
- ○ In-Progress
- ○ Implemented

References

Strategies for protecting web application systems against credential stuffing attacks.

OWASP's credential stuffing prevention cheat sheet.

Phishing-Resistant Multi-Factor Authentication

Outcome

Add a critical, additional layer of security to protect asset accounts whose credentials have been compromised.

Risks

Risks include Brute Force attacks, Remote Services such as Remote Desktop Protocol and Secure Shell (SSH), use of Valid Accounts, and External Remote Services.

Recommended Action

Implement multi-factor authentication for access to assets using the strongest available method for that asset (see below for scope).

Multi-factor authentication options ranked by strength, from high to low:

1. Hardware-based, phishing-resistant MFA (for example, Fast Identity Online (FIDO)/Web Authentication (WebAuthn) or public key infrastructure (PKI) based).

2. If such hardware-based multi-factor authentication is not available, then use mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys.

3. Only use multi-factor Authentication via text message/SMS or voice when no other options are possible.

Ensure all information technology accounts leverage multi-factor authentication. Prioritize accounts with highest risk, such as privileged administrative accounts. Within operational technology environments, enable multi-factor authentication on all accounts and systems that can be accessed remotely, including vendors/ maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

CyberAlberta's Compromise Checklist: A Guide for Alberta Businesses.

CyberAlberta's Ransomware Playbook.

CyberAlberta's Data Loss Playbook.

Alberta Government's Cybersecurity guidance: Multifactor Authentication.

Steps for effectively deploying multi-factor authentication.

Secure accounts and devices.

Basic and Operations Security Training

Outcome

Organizational users learn and perform more secure behaviours. If applicable, personnel responsible for securing operational technology assets receive specialized cybersecurity training focused on operational technology systems.

Risks

User awareness.

Recommended Action

Provide training that covers basic security and privacy concepts, such as phishing, business email compromise, basic operational security, password security, privacy breaches, etc., and foster an internal culture of security and cyber awareness. Provide training for all employees and contractors regularly. Require that new employees receive initial cybersecurity training during onboarding and recurring training regularly, and when required by system changes or following certain events.

Ensure security and privacy programs collaborate on developing awareness and training policy and procedures.

In addition to basic cybersecurity training, ensure that personnel who maintain or protect operational technology as part of their regular duties receive cybersecurity training specific to operational technology regularly.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Cybersecurity Awareness and Training materials.

Cybersecurity: Understanding malware.

Steps for effectively deploying multi-factor authentication.

Secure accounts and devices with multi-factor authentication.

Strong and Agile Encryption: Data in Transit

Outcome

Effective encryption deployed to maintain confidentiality of sensitive data and integrity of network traffic passing through information technology systems, operational technology systems, and cloud environments.

Risks

Risks include Adversary-in-the-middle, Automated Collection, Network Sniffing, Wireless Compromise, and Wireless Sniffing.

Recommended Action

Use a properly configured and up-to-date secure socket layer (a protocol that establishes encrypted links between networked computers) to protect data in transit, when technically feasible. Identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing implications of postquantum cryptography. Encrypt data in transit with appropriate and approved strength of encryption in accordance with the sensitivity of the data.

To minimize the impact to latency and availability, use encryption where feasible, usually for operational technology communications connecting with remote/external assets.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Using encryption to keep sensitive data secure.

Guidance on becoming cryptographically agile.

Preparing for the quantum threat.

Secure Sensitive Data: Data at Rest

Outcome

Protect sensitive information from unauthorized access.

Risks

Unsecured Credentials, Steal or Forge Kerberos Tickets, Operating System Credential Dumping, Data from Information Repositories, and Theft of Operational Information.

Recommended Action

Ensure sensitive data, including credentials, is not stored in plain text anywhere in the organization and that it can only be accessed by authenticated and authorized users. Store credentials in a secure manner, such as with a credential/password manager or vault or other privileged account management solution. Encrypt sensitive data at rest with appropriate and approved strength of encryption in accordance with the sensitivity of the data.

Assessment	References
○ Unknown	Password managers: Security Tips.
○ Not Started	
○ Scoped/Planned	
○ In-Progress	
○ Implemented	

Email Security

Outcome

Reduce risk from common email-based threats, such as spoofing, phishing, and interception.

Risks

Phishing and Business Email Compromise.

Recommended Action

Set encryption for email to an appropriate and approved level in accordance with the sensitivity. Turn on STARTTLS to make sure emails are encrypted, so they can't be easily read by hackers during delivery.

Set up Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to help verify that emails sent from the domain are genuine and not fake. Activate DMARC and configure it to "reject" fake emails, so fraudulent messages pretending to come from your domain are blocked. This helps protect your email system from being misused or hacked.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Implementation guidance: Email domain protection.

Disable Macros by Default

Outcome

Reduce the risk from embedded macros (scripts within documents that can execute code) and similar executive code, a common and highly effective threat actor tactic, technique, and procedure.

Risks

Risks include phishing attacks through Malicious Email Attachments and User Execution of harmful files that can compromise systems.

Recommended Action

Establish a system-enforced policy that disables Microsoft Office macros or similar embedded code by default on all devices. If macros must be enabled in specific circumstances, set a policy for authorized users to request that macros are enabled on specific assets.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

How to protect the organization from malicious macros.

Hardware and Software Approval Process

Outcome

Ensure visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.

Risks

Risks include Supply Chain Compromise, Hardware Additions, Browser Extensions, and Transient Cyber Asset.

Recommended Action

Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Maintain a risk-informed allow list of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For operational technology assets specifically, align these actions with defined change control and testing activities.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Application Allow List.

System Backups and Redundancy

Outcome

Organizations reduce the likelihood and duration of data loss of service delivery or operations.

Risks

Risks include Data Destruction, Data Encrypted for Impact, Disk Wipe, Inhibit System Recovery, Denial of Control, Denial/Loss of View, Loss of Availability, and Loss/Manipulation of Control.

Recommended Action

Regularly back up all systems that are necessary for operations. Determine on a case-by-case basis what systems to back up and the exact frequency since every system will have different backup and recovery requirements. Store backups separately from the source systems and test on a recurring basis, no less than once per year. Ensure stored information for OT assets includes at a minimum:

- configurations
- roles
- programmable controller (PLC) logic
- engineering drawings
- tools

Implement adequate redundancies (as determined by the organization) such as network components and data storage. Ensure that the redundant secondary system is not collocated with the primary system and can be activated without loss of information or disruption to operations.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Tips for backing up information.

Baseline Cybersecurity Controls for small and medium organizations.

Top measures to enhance cybersecurity for small and medium organizations.

Top 10 IT security actions: No. 7 protect information at enterprise level.

Security considerations for website.

Log Collection

Outcome

Achieve better visibility to detect and effectively respond to cyberattacks.

Risks

Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents. This limitation can Impair Defences and increase exposure to threats.

Recommended Action

Collect and store logs for use in both detection and IR activities (for example, forensics), including the following logs:

- Access- and security-focused (for example, intrusion detection systems/intrusion prevention systems
- firewalls
- data loss prevention
- virtual private networks

Notify security teams when a critical log source is disabled, such as Windows Event Logging.

For operational technology assets where logs are non-standard or not available, collect network traffic and communications between those assets and other assets.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Network security logging and monitoring.

Secure and Central Log Storage

Outcome

Organizations' security logs are protected from unauthorized access and tampering.

Risks

Risk of losing the integrity of forensic investigations, delaying breach detection, violating regulatory requirements, disrupting operations, and reputational damage.

Recommended Action

Ensure logs are stored in a central system, such as a security information and event management (SIEM) tool or central database, and can only be accessed or modified by authorized and authenticated users. Store logs for a duration informed by risk or pertinent regulatory guideline.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Network security logging and monitoring.

Prohibit Connection of Unauthorized Devices

Outcome

Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.

Risks

Hardware Additions and Replication Through Removable Media.

Recommended Action

Maintain policies and processes to ensure that unauthorized media and hardware are not connected to information technology and operational technology assets, such as by limiting use of USB devices and removable media or disabling AutoRun.

Establish procedures to remove, disable, or otherwise secure physical ports in operational technology environments to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Defending against data exfiltration threats.

Limit Operations Technology to Public Internet

Outcome

Reduce the risk of threat actors exploiting or interrupting operational technology assets connected to the public internet.

Risks

Risks include Active and Vulnerability Scanning, Exploit Public-Facing Application, Exploitation of Remote Service and External Remote Services.

Recommended Action

Ensure no operational technology assets are on the public Internet, unless explicitly required for operation. Require that exceptions be justified and documented and that excepted assets have additional protections in place to prevent and detect exploitation attempts (for example, logging, multi-factor authentication, mandatory access via proxy or other intermediary).

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Protect operational technology.

Security considerations for industrial control systems.

Document Device Configurations

Outcome

Efficiently and effectively manage, respond to, and recover from cyber attacks against the organization and maintain service continuity.

Risks

Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.

Recommended Action

Maintain accurate documentation describing the baseline and current configuration details of all critical information technology and operational technology assets to facilitate more effective vulnerability management and response and recovery activities. Perform and track periodic reviews and updates.

Assessment

- ○ Unknown
- ○ Not Started
- ○ Scoped/Planned
- ○ In-Progress
- ○ Implemented

References

Guide for security-focused configuration management of information systems.

No Exploitable Services on the Internet

Outcome

Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.

Risks

Risks include Active Scanning: Vulnerability Scanning, Exploitable Public-Facing Application, Exploitation of Remote Services and External Remote Services, and Remote Services: Remote Desktop Protocol.

Recommended Action

Ensure assets on the public Internet do not expose any exploitable services, such as remote desktop protocol. Where these services must be exposed, implement appropriate compensating controls to prevent common forms of abuse and exploitation. Disable all unnecessary operating systems applications and network protocols on Internet-facing assets.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Top 10 IT security actions to protect Internet connected networks and information.

Secure Administrator Workstation

Outcome

Limited-use dedicated Secure Administrator Workstations reduce cybersecurity risks from malware, phishing, and pass-the-hash attacks to allow administrators (for example, users with privileged access) to securely connect to the organization's network.

Risks

Risks include Credential Dumping, Use of Alternate Authentication Method, Exploitation for Privilege Escalation, Exploitation for Privilege Escalation, and unauthorized access through Valid Accounts and Remote Services. Other risks involve Command and Scripting Interpreter, Data from Local System, Exploitation for Defense Evasion, Account Discovery, and Network Sniffing.

Recommended Action

Organizations provide administrators with Secure Administrator Workstations to perform their administrative tasks. Create secure and hardened SAWs by:

- isolating SAWs from the public IT network, and when present, from the data plane
- deactivating capability to install other software
- restricting access to the Internet or email services

For cloud administration from this dedicated workstation, ensure it requires a VPN or allow lists to access the cloud tenancy.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Top 10 IT security actions: No. 3 managing and controlling administrative privileges.

Foundational cybersecurity actions for small organizations.

Detect

The **Detect** function has a focus on identifying and analysing potential cybersecurity incidents. This includes data collection, alert systems and event validation among other activities.

Section Contents

Detect Relevant Threats

Outcome

Organizations are aware of and able to detect relevant threats and tactics, techniques, and procedures in a timely manner.

Risks

Without knowledge of relevant threats and the ability to detect them, organizations risk that threat actors may exist undetected in their networks for long periods.

Recommended Action

Document a list of threats and cyber threat actor tactics, techniques, and procedures relevant to the organization (for example, based on industry, sectors, etc.), and ensure the ability to detect instances of those key threats (for example, through rules, alerting, or commercial prevention and detection systems).

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Best practices for setting up a security operations centre (SOC).

Network security logging and monitoring.

Respond

The **Respond** function considers an organization's actions once a cybersecurity event is detected. It includes activities such as containment and eradication and performing root cause analysis.

Section Contents

Incident Reporting

Outcome

Assist other organizations with detection and mitigation and to share in remediations strategies and tactics.

Risks

Without timely incident reporting, external support groups are less able to assist affected organizations and lack critical insight into the broader threat landscape (such as whether a broader attack is occurring against a specific sector).

Recommended Action

Maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities.

Report known incidents to relevant external parties within time frames directed by applicable regulatory guidance or, in the absence of guidance, as soon as capable of doing so safely.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Report a cyber incident.

Recover

The **Recover** function considers how an organization builds and maintains resilience as well as restoring any capabilities or services that were impacted by an incident. It helps organizations return to normal operations after an incident.

Section Contents

Incident Planning and Preparedness

Outcome

Organizations are capable of safely and effectively recovering from a cybersecurity incident.

Risks

Without timely incident reporting, external support groups are less able to assist affected organizations and lack critical insight into the broader threat landscape (such as whether a broader attack is occurring against a specific sector).

Recommended Action

Develop, maintain, and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cybersecurity incident.

If a cyber incident does occur, perform a post-incident lessons learned session to determine lessons learned and prevent future incidents. Integrate any lessons learned into improvements in governance processes and/or the incident response plan.

Assessment

- ○ **Unknown**
- ○ **Not Started**
- ○ **Scoped/Planned**
- ○ **In-Progress**
- ○ **Implemented**

References

Developing incident response plan.

Developing IT recovery plan.

Assessing Outcomes

This section helps organizations evaluate their current cybersecurity posture across all six functions. By scoring each measure based on implementation status, organizations can identify strengths, gaps, and opportunities for improvement.

Section Contents

How Implementation Status is Scored

Scoring Methodology

Each of the 35 measures receives a maturity score based on its implementation status.

Implementation Status	Score	Weight	Description
Unknown	0	0%	No awareness toward goal implementation
Not Started	0	0%	Awareness of the goal, but with no progress towards reaching it
Scoped/Planned	1	25%	Goal identified, planning initiated
In-Progress	2	50%	Active implementation underway
Implemented	4	100%	Goal fully achieved and operational

Assessment Score Table

The following table summarizes your organization's progress.

No.	Name	Function	Score
1	Privacy Leadership	GOVERN	0 ▪
2	Supply Chain Incident Reporting Process	GOVERN	0 ▪
3	Vendor/Supplier Cybersecurity Requirements	GOVERN	0 ▪
4	Organizational and Operational Technology Cybersecurity Leadership	GOVERN	0 ▪
5	Asset Inventory and Network Topology	IDENTIFY	0 ▪
6	Mitigating Known Vulnerabilities	IDENTIFY	0 ▪
7	Third-party Validation of Cybersecurity Controls	IDENTIFY	0 ▪
8	Incident Response Plans	IDENTIFY	0 ▪
9	Deploy Security.txt Files	IDENTIFY	0 ▪
10	Select a Trusted Cloud Provider	IDENTIFY	0 ▪
11	Changing Default Passwords	PROTECT	0 ▪
12	Minimum Password Length	PROTECT	0 ▪
13	Unique Credentials	PROTECT	0 ▪
14	Revoking Credentials for Departing Employees	PROTECT	0 ▪
15	Separating User and Privileged Accounts	PROTECT	0 ▪
16	Network Segmentation	PROTECT	0 ▪
17	Detection of Unsuccessful (automated) Login Attempts	PROTECT	0 ▪
18	Phishing-Resistant Multi-Factor Authentication	PROTECT	0 ▪
19	Basic and Operations Security Training	PROTECT	0 ▪
20	Strong and Agile Encryption: Data in Transit	PROTECT	0 ▪
21	Secure Sensitive Data: Data at Rest	PROTECT	0 ▪
22	Email Security	PROTECT	0 ▪
23	Disable Macros by Default	PROTECT	0 ▪
24	Hardware and Software Approval Process	PROTECT	0 ▪
25	System Backups and Redundancy	PROTECT	0 ▪
26	Log Collection	PROTECT	0 ▪
27	Secure and Central Log Storage	PROTECT	0 ▪
28	Prohibit Connection of Unauthorized Devices	PROTECT	0 ▪
29	Limit Operations Technology to Public Internet	PROTECT	0 ▪
30	Document Device Configurations	PROTECT	0 ▪
31	No Exploitable Services on the Internet	PROTECT	0 ▪
32	Secure Administrator Workstation	PROTECT	0 ▪
33	Detect Relevant Threats	DETECT	0 ▪
34	Incident Reporting	RESPOND	0 ▪
35	Incident Planning and Preparedness	RECOVER	0 ▪

Results by Function

Score Overview

Summary of total scores and percentage achieved, along with a scale to help interpret the level of implementation.

Function	Number of Measures	Total Score	Max Score	% Achieved	Level Achieved
GOVERN	4	0	16	0.00%	Level 1 – Minimal impleme
IDENTIFY	6	0	24	0.00%	Level 1 – Minimal impleme
PROTECT	22	0	88	0.00%	Level 1 – Minimal impleme
DETECT	1	0	4	0.00%	Level 1 – Minimal impleme
RESPOND	1	0	4	0.00%	Level 1 – Minimal impleme
RECOVER	1	0	4	0.00%	Level 1 – Minimal impleme
Grand Total	35	0	140	0.00%	Level 1 – Minimal impleme

% Achieved Scale

Match your score from the table above to the range below to understand your current level of implementation.

% Achieved Range	Level	Description
0-24%	Level 1 – Minimal implementation	Very limited implementation; most items are not yet known or addressed.
25%-49%	Level 2 – Limited Implementation	A few items are either planned or implemented; overall progress remains low.
50-69%	Level 3 – Moderate Implementation	Several items are scoped or implemented; progress is evident but incomplete.
70-89%	Level 4 – Substantial Implementation	Most items are implemented ot nearing completion.
90-100%	Level 5 –Full Implementation	Nearly all items are fully implemented.

Clear Form

Benchmarking & Maturity Tracking

Why Benchmarking Matters

Our Compliance Framework Assessment and Benchmarking Tool has 35 individual cybersecurity measures across six core functions. Each measure is score based on its implementation status.

Benchmarking these scores enables organizations to:

- Identify strengths and gaps
- Prioritize improvements
- Compare their maturity against similar peers across Alberta

Comparative Benchmarking Profile

Please complete the following to help us categorize your organization for benchmarking:

- **Number of Staff in Organization:**
- **Industry Sector:**
- **Region (North, Central, South):**
- **Organization Type (Public or Private Sector):**

Data and Privacy

By submitting this form, you agree that the information may be used for provincial benchmarking purposes. CyberAlberta will analyze the data to identify trends and support cybersecurity improvements across Alberta. This assessment does not collect personal or identifying information. Submitted data will be used only in anonymized, aggregated formats.

We encourage you to use your organization email address when submitting. CyberAlberta will treat all submitted emails as transitory records, retained only for the duration necessary to process the submission.

Please email your completed assessment to **CyberAlbertaCompliance@gov.ab.ca** or use the Submit button below.

Submit via Email

Benchmarking & Maturity Tracking

Use the table below to track your organization's scores and over time. This snapshot supports year-over-year benchmarking and helps visualize progress across all 35 goals.

No.	Name	Function	Year 1	Year 2	Year 3
1	Privacy Leadership	GOVERN	0		
2	Supply Chain Incident Reporting Process	GOVERN	0		
3	Vendor/Supplier Cybersecurity Requirements	GOVERN	0		
4	Organizational and Operational Technology Cybersecurity Leadership	GOVERN	0		
5	Asset Inventory and Network Topology	IDENTIFY	0		
6	Mitigating Known Vulnerabilities	IDENTIFY	0		
7	Third-party Validation of Cybersecurity Controls	IDENTIFY	0		
8	Incident Response Plans	IDENTIFY	0		
9	Deploy Security.txt Files	IDENTIFY	0		
10	Select a Trusted Cloud Provider	IDENTIFY	0		
11	Changing Default Passwords	PROTECT	0		
12	Minimum Password Length	PROTECT	0		
13	Unique Credentials	PROTECT	0		
14	Revoking Credentials for Departing Employees	PROTECT	0		
15	Separating User and Privileged Accounts	PROTECT	0		
16	Network Segmentation	PROTECT	0		
17	Detection of Unsuccessful (automated) Login Attempts	PROTECT	0		
18	Phishing-Resistant Multi-Factor Authentication	PROTECT	0		
19	Basic and Operations Security Training	PROTECT	0		
20	Strong and Agile Encryption: Data in Transit	PROTECT	0		
21	Secure Sensitive Data: Data at Rest	PROTECT	0		
22	Email Security	PROTECT	0		
23	Disable Macros by Default	PROTECT	0		
24	Hardware and Software Approval Process	PROTECT	0		
25	System Backups and Redundancy	PROTECT	0		
26	Log Collection	PROTECT	0		
27	Secure and Central Log Storage	PROTECT	0		
28	Prohibit Connection of Unauthorized Devices	PROTECT	0		
29	Limit Operations Technology to Public Internet	PROTECT	0		
30	Document Device Configurations	PROTECT	0		
31	No Exploitable Services on the Internet	PROTECT	0		
32	Secure Administrator Workstation	PROTECT	0		
33	Detect Relevant Threats	DETECT	0		
34	Incident Reporting	RESPOND	0		
35	Incident Planning and Preparedness	RECOVER	0		

Glossary

A-D

Account Manipulation
Changing account settings or permissions to gain unauthorized access or control.

Active Scanning
Automated tools used to probe systems or networks to find weaknesses.

Adversary-in-the-Middle
An attack where a threat actor intercepts and possibly alters communication between two parties without their knowledge.

Application Allow List
A security control that permits only approved software to run on systems, helping prevent unauthorized or malicious applications from executing.

Automated Collection
Tools or processes that gather data from systems without manual input, often used by attackers to collect sensitive information.

Browser Extensions
Add-ons installed in web browsers that can enhance functionality but may also pose security risks if malicious or poorly managed.

Brute Force Attack
A method where attackers try many password combinations to gain access.

Business Continuity
The ability of an organization to maintain essential functions during and after a cybersecurity incident.

Business Email Compromise
A type of cyberattack where attackers impersonate executives or vendors to trick employees into transferring money or sensitive data.

Cloud Tenancy
An isolated environment within a cloud service provider where an organization's data and applications are hosted. Proper configuration is essential to maintain security.

Command and Scripting Interpreter
Tools or environments used to execute commands or scripts, which can be exploited by attackers to automate malicious actions.

Credential Stuffing
Using stolen usernames and passwords to try and access accounts across different systems.

Cryptography
The science of securing information through mathematical techniques, including encryption and digital signatures.

Data Encryption for Impact
Using encryption to lock or make data inaccessible, often as part of a ransomware attack.

Data from Information Repositories
Sensitive data stored in databases or file systems that may be targeted by attackers.

Defacement
Altering the appearance or content of a website or system to spread messages or cause reputational harm.

Default Accounts
Preconfigured user accounts that come with hardware or software. These accounts often have known credentials and pose a security risk if not changed or disabled.

Demilitarized Zone (DMZ)
A network segment that separates internal systems from external-facing services, often used to add a layer of protection between public and private networks.

Domain-based Message Authentication, Reporting, and Conformance
A policy that tells email receivers how to handle messages that fail authentication checks, helping prevent email fraud.

DomainKeys Identified Mail
A method that uses cryptographic signatures to verify the authenticity of email messages.

Glossary

E-M

Embedded Macros
Scripts embedded in documents that can execute code. These are often used in attacks to run malicious software.

Encryption
The process of converting data into a coded format to prevent unauthorized access.

Exploit Public-Facing Applications
Attacks that target weaknesses in software or websites that are accessible from the internet.

Exploitation of Remote Services
Gaining unauthorized access through remote access tools like remote desktop or secure shell.

External Remote Services
Remote access systems that are reachable from outside the organization's network.

Exploitation for Defense Evasion
Techniques used by attackers to avoid detection by security systems.

Exploitation for Privilege Escalation
Gaining higher-level access within a system by exploiting vulnerabilities.

Fast Identity Online / Web Authentication
A method of authentication that uses cryptographic keys instead of passwords to verify identity, reducing the risk of phishing and credential theft.

Hardware Additions
Unapproved or unmanaged hardware connected to systems, which may introduce security risks.

Impair Defenses
Disabling or weakening security tools such as antivirus software, firewalls, or monitoring systems.

Incident Response Plans
Documented procedures that guide how an organization detects, responds to, and recovers from cybersecurity incidents. These plans help contain threats, reduce impact, and restore operations.

Indicator Removal on Host
Deleting or altering evidence on a system to hide malicious activity.

Industrial Control Systems
Systems used to monitor and control industrial processes, such as manufacturing, energy, or water treatment. These systems are often targeted in supply chain attacks due to their critical nature.

Internet Accessible Device
Any device connected to the internet that may be exposed to threats if not properly secured.

Kerberos Tickets
Digital credentials used in Kerberos authentication systems to verify identity and grant access to resources.

Malicious Code
Software designed to harm, exploit, or disrupt systems, including viruses, worms, and trojans.

Malicious Email Attachments
Files sent through email that contain harmful code or software.

Modify Authentication Process
Changing how users log in to systems, potentially to bypass security controls or create backdoors.

Modify Registry
Changing system registry settings to alter behavior, disable protections, or maintain persistence.

Multi-factor Authentication
A security method requiring more than one form of verification to access systems, such as a password and a physical token.

N-R

Network Connection Enumeration
Listing all active network connections to understand communication paths and identify potential vulnerabilities.

Network Denial of Service
Flooding a network with traffic to make systems or services unavailable.

Network Segmentation
Dividing a network into smaller, isolated sections to limit access and contain potential threats.

Network Service Discovery
Identifying active services running on devices within a network, often used by attackers to find targets.

Network Sniffing
Monitoring and capturing data packets traveling across a network, often used to intercept sensitive information.

Network Topology
A visual or documented layout showing how systems, devices, and connections are structured within an organization's network. It helps identify critical assets and potential vulnerabilities.

Operating System Credential Dumping
Extracting stored login credentials from a computer system.

Operational Technology
Technology used to monitor and control physical processes, devices, and infrastructure. Examples include control systems in manufacturing, utilities, and transportation.

Pass-the-Hash Attack
A technique where attackers use hashed credentials to authenticate without knowing the actual password.

Password Cracking
Recovering passwords by analyzing stored data or using software tools.

Password Guessing
Trying common or default passwords to gain access to systems.

Password Spraying
Trying a few common passwords across many accounts to find one that works.

Phishing
Sending deceptive messages to trick recipients into revealing sensitive information or installing malware.

Post-Quantum Cryptography
Encryption methods designed to be secure against future quantum computing threats, which could break current cryptographic algorithms.

Privileged Access Management
Processes and tools used to control and monitor access to accounts with elevated permissions, reducing the risk of misuse.

Public Key Infrastructure
A system that manages digital certificates and encryption keys to enable secure communication and authentication.

Remote Access Software
Programs that allow users to control systems from a distance, which can be misused if not properly secured.

Remote Desktop Protocol
A protocol that allows users to connect to and control a computer remotely. If not secured, it can be exploited for unauthorized access.

Replication Through Removable Media
Spreading malware or gaining access through USB drives or other portable devices.

Resource Hijacking
Using system resources without permission, often for cryptocurrency mining or other unauthorized tasks.

Root Cause Analysis
A method used to determine the underlying cause of a cybersecurity incident to prevent recurrence.

Glossary

S-Z

Secure Shell
A protocol used to securely access and manage remote systems. It encrypts communication to prevent interception.

Security Operations Centre (SOC)
A centralized team or facility responsible for monitoring, detecting, and responding to cybersecurity incidents.

Security.txt File
A standardized file placed on websites that provides contact information for the organization's security team. It allows security researchers or ethical hackers to report vulnerabilities or security issues they discover.

Sender Policy Framework
A method used to verify that an email is sent from an authorized server for a domain, helping prevent spoofing.

SIEM Tool (Security Information and Event Management)
A centralized system that collects, analyzes, and stores security logs from across the organization to support threat detection and incident response.

Spoofing
Falsifying the identity of a device or user to gain unauthorized access or deceive systems.

STARTTLS
A protocol command that upgrades an unencrypted email connection to a secure, encrypted one.

Supply Chain Compromise
Security breaches that occur through third-party vendors or service providers.

Trusted Relationship
A connection between systems or organizations that allows access based on established trust. If misused, it can be exploited for unauthorized access.

Unauthorized Access Through Valid Accounts
Using legitimate login credentials to access systems without permission.

Unsecured Credentials
Passwords or login details stored without proper protection.

User Execution
Convincing users to run malicious files or commands, often through deceptive prompts or instructions.

Valid (User) Accounts
Accounts with legitimate credentials that are used to gain unauthorized access.

Vulnerability Scanning
Using tools to find known weaknesses in systems or software.

Wireless Compromise
Unauthorized access or disruption of wireless networks, often through weak encryption or misconfigured settings.

Wireless Sniffing
Capturing data transmitted over wireless networks to gather information or identify vulnerabilities.