Carbide

SAMPLE REPORT

ISO/IEC 27001:2022

Current State Assessment

ORGANIZATION

Acme Corporation

ASSESSMENT DATE

April 28, 2026

ISMS SCOPE

ISMS covers all systems and personnel for Acme Corporation with infrastructure hosted in a Canadian cloud region

FRAMEWORK

ISO/IEC 27001:2022

CONTROLS ASSESSED

105

VERSION

1.0

Executive Summary

This Current State Assessment evaluates the information security posture of Acme Corporation against ISO/IEC 27001:2022 using a Q&A methodology. 68 practical questions were answered, with each answer automatically mapped to the relevant controls across all Mandatory Clauses (4–10) and the 93 Annex A controls.

77	22	5	1
Fully In Place	Partially In Place	Not In Place	Not Applicable

ISMS Scope: ISMS covers all systems and personnel for Acme Corporation with infrastructure hosted in a Canadian cloud region.

Compliance Summary by Domain

Domain	Total	Fully	Partial	Not In Place	N/A
Mandatory Clauses (4–10)	18	11	6	1	0
Theme 5 — Organizational	33	21	11	0	1
Theme 6 — People	8	7	1	0	0
Theme 7 — Physical	14	14	0	0	0
Theme 8 — Technological	32	24	4	4	0

Assessment Q&A; Findings

Governance & Leadership

Has top management formally approved, signed, and communicated an Information Security Policy to all staff? — Fully In Place

Controls: 5.1, 5.2, 4.4

Evidence / Notes: Staff signed Information Security policy

Are information security roles and responsibilities formally defined, documented, and assigned to named individuals? — Partially In Place

Controls: 5.3, 4.4, 5.2a

Evidence / Notes: C-level roles documented. Need to document roles for non C-level employees.

Has the organization formally defined and documented the scope and boundaries of its ISMS? — Fully In Place

Controls: 4.1, 4.2, 4.3

Evidence / Notes: Scope is all staff and systems related to the Acme Corporation SaaS platform.

Are information security objectives formally documented, measurable, tracked, and communicated to relevant staff? — Partially In Place

Controls: 6.2

Evidence / Notes: Document being developed but not complete.

Does top management participate in formal ISMS management reviews at least annually with documented decisions and action items? — Fully In Place

Controls: 9.3, 5.1

Evidence / Notes: Management part of regular security team meetings.

Are adequate resources (budget, staff, tools) formally allocated to the ISMS? — Not In Place

Controls: 7.1

Evidence / Notes: Need to create budget document for ISMS.

Risk Management

Is there a documented risk assessment process with defined criteria for identifying, analyzing, and evaluating information security risks? — Fully In Place

Controls: 6.1, 8.2

Has a risk assessment been performed and is a risk register maintained and reviewed at least annually?	Fully In Place

Controls: 8.2, 6.1

Has a risk treatment plan been implemented for risks that exceed the acceptance threshold?	Fully In Place

Controls: 8.3, 6.1

Evidence / Notes: Risk assessment, register, treatment plan all in place.

Is a Statement of Applicability (SoA) maintained showing which Annex A controls apply, their justification, and implementation status?	Fully In Place

Controls: 8.3

Evidence / Notes: SOA completed stating which Annex controls are being implemented.

Policies & Documentation

Are documented operating procedures in place for key IT and security processes (patch management, backups, access provisioning, incident response)?	Fully In Place

Controls: 5.37, 8.1

Is documented information (policies, procedures, records) controlled through version control, formal review, and approval?	Fully In Place

Controls: 7.5

Is there a formal information classification scheme, and is information labeled and handled according to its classification?	Partially In Place

Controls: 5.12, 5.13

Evidence / Notes: Need to review and finalize data classification.

Are policies governing the acceptable use of organizational assets documented, communicated, and enforced?	Fully In Place

Controls: 5.10

Evidence / Notes: Acceptable Use policy in place.

Are information transfer policies in place covering all transfer types (email, physical documents, electronic file transfer)?	Partially In Place

Controls: 5.14

Evidence / Notes: Need to review final info transfer policies.

Are all applicable legal, regulatory, and contractual information security requirements identified, documented, and reviewed?	Fully In Place

Controls: 5.31, 5.34

Are records retained per defined retention schedules and protected from unauthorized access, loss, or tampering?	Fully In Place

Controls: 5.33, 5.36

Is information security integrated into project management for all significant new initiatives?	Fully In Place

Controls: 5.8

Evidence / Notes: SDLC integrated security into dev cycle.

Access Control

Is there a documented access control policy covering least privilege, need-to-know, and role-based access?	Fully In Place

Controls: 5.15, 5.3a

Evidence / Notes: Access Control policy exists.

Are user accounts provisioned and deprovisioned through a formal, documented process with manager approval?	Partially In Place

Controls: 5.16, 5.18, 5.11, 6.5

Evidence / Notes: Need to review manager approval part of this.

Are user access rights reviewed regularly (at least annually) to verify they remain appropriate and least-privilege?	Fully In Place

Controls: 5.18, 5.15

Evidence / Notes: Twice a year vendor reviews happen.

Are privileged accounts (admin, root, service accounts) tightly managed, limited in number, and regularly reviewed?	Fully In Place

Controls: 8.2a, 5.18

Evidence / Notes: Twice a year vendor reviews happen.

Is multi-factor authentication (MFA) required for remote access, privileged accounts, and access to sensitive systems?	Fully In Place

Controls: 5.17, 8.5

Evidence / Notes: MFA in place anywhere it can be implemented.

Is there a formal password/authentication policy defining minimum complexity, rotation, and prohibition of reuse or sharing?	Fully In Place

Controls: 5.17, 8.5

Is access to systems restricted to what is necessary for the user's role, with access to source code tightly controlled?	Fully In Place

Controls: 8.3a, 8.4

Asset Management

Is there an up-to-date inventory of all information assets — hardware, software, and key data assets?	Fully In Place

Controls: 5.9

Evidence / Notes: Inventory stored offline.

Are procedures in place for secure disposal of equipment and media (data wiping, physical destruction, certificates)?	Fully In Place

Controls: 7.14, 8.10

Are removable media (USB, external drives) controlled, managed, and encrypted when containing sensitive data?	Fully In Place

Controls: 7.10

Are assets taken off-premises (laptops, mobiles) subject to formal controls including encryption and authorization?	Fully In Place

Controls: 7.9, 8.1a

HR & People

Are background checks (criminal record, employment history, qualifications) performed on all new employees and contractors?	Fully In Place

Controls: 6.1a

Evidence / Notes: HR handles all screening and background checks.

Do employment and contractor agreements include information security responsibilities and confidentiality obligations?	Fully In Place

Controls: 6.2a, 6.6

Evidence / Notes: Contracts and policies explain personal responsibility and confidentiality expectations.

Do all staff receive security awareness training on hire and at least annually, covering current threats and their responsibilities?	Fully In Place

Controls: 6.3, 7.3

Is there a formal disciplinary process for information security policy violations, and are staff aware of it?	Fully In Place

Controls: 6.4

Evidence / Notes: Contracts lay out discipline.

Is there a clear channel for employees to report security incidents and suspicious activity?	Fully In Place

Controls: 6.8, 5.25

Evidence / Notes: Company IM tool provides path for everyone to report incidents.

Are policies and controls in place for remote and home working to protect information off-site?	Fully In Place

Controls: 6.7

Physical Security

Are physical access controls (badge readers, keypads, security personnel) in place to restrict access to facilities and sensitive areas?	Fully In Place

Controls: 7.1a, 7.2a, 7.3a

Evidence / Notes: Badge swipe/FOB used for building entry.

Are facilities monitored by CCTV or alarm systems to detect and deter unauthorized physical access?	Fully In Place

Controls: 7.4

Are environmental protections (fire suppression, UPS/generators, HVAC) in place to protect IT equipment?	Fully In Place

Controls: 7.5, 7.11

Is there a clear desk and clear screen policy that is enforced?	Fully In Place

Controls: 7.7

Is IT equipment properly sited, protected, and maintained with documented maintenance records?	Fully In Place

Controls: 7.8, 7.12, 7.13

Are physical security procedures applied when working in secure or sensitive areas?	Fully In Place

Controls: 7.6

Operations & Change Management

Is there a formal change management process requiring documentation, risk assessment, testing, and approval before production changes?	Fully In Place

Controls: 8.32, 8.1

Evidence / Notes: Change management procedure documented.

Are development, testing, and production environments strictly separated to prevent unauthorized changes or data exposure?	Fully In Place

Controls: 8.31

Evidence / Notes: Segregation of environments in place.

Are event logs maintained for systems and user activities, protected from tampering, and retained for a defined period?	Fully In Place

Controls: 8.15, 8.16

Are systems and networks actively monitored for anomalies, intrusions, and security events with on-call alerting?	Fully In Place

Controls: 8.16, 5.7

Are system clocks synchronized to a reliable, authoritative time source (NTP)?	Fully In Place

Controls: 8.17

Is system capacity monitored and planned for, with redundancy in place for critical systems?	Partially In Place

Controls: 8.6, 8.14

Malware, Vulnerabilities & Patching

Is endpoint protection (anti-malware/EDR) deployed on all user devices and servers with definitions updated automatically?	Not In Place

Controls: 8.7

Evidence / Notes: Need to review potential MDM/RMM solutions.

Is there a vulnerability management process including regular scanning, risk-based prioritization, and defined SLAs for patching?	Fully In Place

Controls: 8.8

Is software installation on production systems controlled and restricted to authorized, approved software only?	Not In Place

Controls: 8.19, 8.18

Evidence / Notes: RMM/MDM will facilitate this.

Are system configurations documented and enforced using hardening standards, with deviations tracked and justified?	Not In Place

Controls: 8.9

Evidence / Notes: RMM/MDM will facilitate this.

Is web or DNS filtering in place to block access to known malicious or unauthorized websites?	Fully In Place

Controls: 8.23

Network & Communications

Are network firewalls in place at the perimeter and between segments, with documented and reviewed firewall rules?	Fully In Place

Controls: 8.20, 8.21

Are networks segmented (VLANs, DMZ) to isolate sensitive systems from general and guest networks?	Fully In Place

Controls: 8.22

Is all sensitive data encrypted in transit (TLS 1.2+ for external connections) and at rest (AES-256 or equivalent)?	Fully In Place

Controls: 8.24, 5.14

Are data loss prevention (DLP) controls in place to detect and prevent unauthorized exfiltration of sensitive data?	Fully In Place

Controls: 8.12

Development & Software Security

Are secure development practices applied throughout the SDLC — including security requirements, design reviews, coding standards, and code reviews?	Fully In Place
Controls: 8.25, 8.26, 8.27, 8.28	
Is security testing (SAST, DAST, penetration testing) performed during development and before releases go live?	Partially In Place
Controls: 8.29	
Is outsourced development governed by contracts requiring security standards, code review rights, and vulnerability disclosure?	Fully In Place
Controls: 8.30	
Is test data masked, anonymized, or synthetic — ensuring real production data is not used in test environments?	Fully In Place
Controls: 8.33	

Backups & Business Continuity

Are regular data backups performed, encrypted, stored off-site or in a separate region, and tested for restorability?	Partially In Place
Controls: 8.13	
Is there a business continuity and/or disaster recovery plan that is documented, approved, and tested at least annually?	Partially In Place
Controls: 5.29, 5.30, 8.14	

Incident Management

Is there a documented incident response plan with defined roles, severity classification, escalation, and communication procedures?	Fully In Place
Controls: 5.24, 5.25, 5.26	
Are post-incident reviews conducted with findings used to improve security controls and update procedures?	Partially In Place
Controls: 5.27	
Are forensic evidence collection and preservation procedures defined to support legal proceedings if required?	Fully In Place
Controls: 5.28	

Supplier & Third-Party Management

Are information security requirements included in all supplier and cloud provider contracts that involve access to organizational data?	Fully In Place
Controls: 5.19, 5.20, 5.23	
Are supplier security practices reviewed regularly through SOC 2 reports, questionnaires, or audit results?	Fully In Place
Controls: 5.21, 5.22	

Compliance & Audit

Are independent reviews (internal audits or external assessments) of the ISMS conducted at planned intervals, with findings addressed through corrective action?	Partially In Place
Controls: 5.35, 9.2, 9.1, 10.2	

Control Status — Full Reference

Mandatory Clauses (4–10)

Control	Title	Status
4.4	ISMS General Requirements	Partially In Place
5.1	Information Security Policies	Fully In Place
5.2	Information Security Roles and Responsibilities	Fully In Place
5.3	Organizational Roles, Responsibilities and Authorities	Partially In Place
6.1	Actions to Address Risks and Opportunities	Fully In Place
6.2	Information Security Objectives	Partially In Place
7.1	Resources	Not In Place
7.2	Competence	Fully In Place
7.3	Awareness	Fully In Place
7.4	Communication	Fully In Place
7.5	Documented Information	Fully In Place
8.1	Operational Planning and Control	Fully In Place
8.2	Information Security Risk Assessment	Fully In Place
8.3	Information Security Risk Treatment	Fully In Place
9.1	Monitoring, Measurement, Analysis and Evaluation	Partially In Place
9.2	Internal Audit	Partially In Place
9.3	Management Review	Fully In Place
10.2	Nonconformity and Corrective Action	Partially In Place

Theme 5 — Organizational Controls

Control	Title	Status
5.2a	Information Security Roles and Responsibilities	Partially In Place
5.3a	Segregation of Duties	Fully In Place
5.5	Contact with Authorities	Fully In Place
5.6	Contact with Special Interest Groups	Fully In Place

5.7	Threat Intelligence	Fully In Place
5.8	Information Security in Project Management	Fully In Place
5.9	Inventory of Information and Other Assets	Fully In Place
5.10	Acceptable Use of Information and Other Assets	Fully In Place
5.11	Return of Assets	Partially In Place
5.12	Classification of Information	Partially In Place
5.13	Labelling of Information	Partially In Place
5.14	Information Transfer	Partially In Place
5.15	Access Control	Fully In Place
5.16	Identity Management	Partially In Place
5.17	Authentication Information	Fully In Place
5.18	Access Rights	Partially In Place
5.19	Information Security in Supplier Relationships	Fully In Place
5.20	Addressing Security in Supplier Agreements	Fully In Place
5.21	Managing Information Security in ICT Supply Chain	Fully In Place
5.22	Monitoring, Review and Change Management of Supplier Services	Fully In Place
5.23	Information Security for Use of Cloud Services	Fully In Place
5.24	Information Security Incident Management	Fully In Place
5.25	Assessment and Decision on IS Events	Fully In Place
5.26	Response to Information Security Incidents	Fully In Place
5.27	Learning from Information Security Incidents	Partially In Place
5.28	Collection of Evidence	Fully In Place
5.29	Information Security During Disruption	Partially In Place
5.30	ICT Readiness for Business Continuity	Partially In Place
5.31	Legal, Statutory, Regulatory and Contractual Requirements	Fully In Place
5.33	Protection of Records	Fully In Place
5.34	Privacy and Protection of PII	Fully In Place
5.35	Independent Review of Information Security	Partially In Place
5.36	Compliance with Policies, Rules and Standards	Fully In Place

5.37	Documented Operating Procedures	Fully In Place

Theme 6 — People Controls

Control	Title	Status
6.1a	Screening	Fully In Place
6.2a	Terms and Conditions of Employment	Fully In Place
6.3	Information Security Awareness, Education and Training	Fully In Place
6.4	Disciplinary Process	Fully In Place
6.5	Responsibilities After Termination or Change	Partially In Place
6.6	Confidentiality or Non-Disclosure Agreements	Fully In Place
6.7	Remote Working	Fully In Place
6.8	Information Security Event Reporting	Fully In Place

Theme 7 — Physical Controls

Control	Title	Status
7.1a	Physical Security Perimeters	Fully In Place
7.2a	Physical Entry	Fully In Place
7.3a	Securing Offices, Rooms and Facilities	Fully In Place
7.4	Physical Security Monitoring	Fully In Place
7.5	Protecting Against Physical and Environmental Threats	Fully In Place
7.6	Working in Secure Areas	Fully In Place
7.7	Clear Desk and Clear Screen	Fully In Place
7.8	Equipment Siting and Protection	Fully In Place
7.9	Security of Assets Off-Premises	Fully In Place
7.10	Storage Media	Fully In Place
7.11	Supporting Utilities	Fully In Place
7.12	Cabling Security	Fully In Place
7.13	Equipment Maintenance	Fully In Place
7.14	Secure Disposal or Re-use of Equipment	Fully In Place

Theme 8 — Technological Controls

Control	Title	Status
8.1a	User Endpoint Devices	Fully In Place
8.2a	Privileged Access Rights	Fully In Place
8.3a	Information Access Restriction	Fully In Place
8.4	Access to Source Code	Fully In Place
8.5	Secure Authentication	Fully In Place
8.6	Capacity Management	Partially In Place
8.7	Protection Against Malware	Not In Place
8.8	Management of Technical Vulnerabilities	Fully In Place
8.9	Configuration Management	Not In Place
8.10	Information Deletion	Fully In Place
8.12	Data Leakage Prevention	Fully In Place
8.13	Information Backup	Partially In Place
8.14	Redundancy of Information Processing Facilities	Partially In Place
8.15	Logging	Fully In Place
8.16	Monitoring Activities	Fully In Place
8.17	Clock Synchronization	Fully In Place
8.18	Use of Privileged Utility Programs	Not In Place
8.19	Installation of Software on Operational Systems	Not In Place
8.20	Networks Security	Fully In Place
8.21	Security of Network Services	Fully In Place
8.22	Segregation of Networks	Fully In Place
8.23	Web Filtering	Fully In Place
8.24	Use of Cryptography	Fully In Place
8.25	Secure Development Life Cycle	Fully In Place
8.26	Application Security Requirements	Fully In Place
8.27	Secure System Architecture and Engineering Principles	Fully In Place
8.28	Secure Coding	Fully In Place

8.29	Security Testing in Development and Acceptance	**Partially In Place**
8.30	Outsourced Development	**Fully In Place**
8.31	Separation of Environments	**Fully In Place**
8.32	Change Management	**Fully In Place**
8.33	Test Information	**Fully In Place**

Recommendations

High Priority — Not In Place

7.1 — Resources — Allocate and formally document budget, headcount, and tooling for ISMS maintenance.

8.7 — Protection Against Malware — Deploy EDR/anti-malware on all devices with centralized management.

8.9 — Configuration Management — Document system configuration baselines and enforce via automated compliance scanning.

8.18 — Use of Privileged Utility Programs — Restrict use to authorized staff. Log and review all usage.

8.19 — Installation of Software on Operational Systems — Implement software installation controls (whitelist or MDM enforcement).

Medium Priority — Partially In Place

4.4 — ISMS General Requirements

5.3 — Organizational Roles, Responsibilities and Authorities

6.2 — Information Security Objectives

9.1 — Monitoring, Measurement, Analysis and Evaluation

9.2 — Internal Audit

10.2 — Nonconformity and Corrective Action

5.2a — Information Security Roles and Responsibilities

5.11 — Return of Assets

5.12 — Classification of Information

5.13 — Labelling of Information

5.14 — Information Transfer

5.16 — Identity Management

5.18 — Access Rights

5.27 — Learning from Information Security Incidents

5.29 — Information Security During Disruption

5.30 — ICT Readiness for Business Continuity

5.35 — Independent Review of Information Security

6.5 — Responsibilities After Termination or Change

8.6 — Capacity Management

8.13 — Information Backup

8.14 — Redundancy of Information Processing Facilities

8.29 — Security Testing in Development and Acceptance

Plan of Action

The following Plan of Action identifies specific remediation steps for all 27 controls that are Not In Place or Partially In Place. Actions are organized across four delivery phases based on priority, complexity, and interdependency. Address Phase 1 items first — they form the governance foundation for all subsequent phases.

1. Foundation & Quick Wins 0–30 days

4.4	ISMS General Requirements Formally establish the ISMS with documented policies, processes, and integrated procedures.
5.3	Organizational Roles, Responsibilities and Authorities Define information security roles. Assign a CISO or equivalent and publish accountability in the org chart.
6.2	Information Security Objectives Document measurable information security objectives with owners, timelines, and measurable KPIs.
7.1	Resources Allocate and formally document budget, headcount, and tooling for ISMS maintenance.
5.2a	Information Security Roles and Responsibilities Document security roles in job descriptions and assign accountability to named individuals across the organization.
5.12	Classification of Information Define an information classification scheme (e.g., Public, Internal, Confidential, Restricted) and publish guidance.
8.7	Protection Against Malware Deploy EDR/anti-malware on all devices with centralized management, automated definition updates, and scan reports.

2. Process & People Controls 30–60 days

9.1	Monitoring, Measurement, Analysis and Evaluation Define security KPIs and metrics. Implement scheduled monitoring, analysis, and reporting to management.
10.2	Nonconformity and Corrective Action Implement a formal nonconformity and corrective action process with root cause analysis and closure verification.
5.11	Return of Assets Add asset return and access revocation steps to the employee offboarding checklist and enforce within defined SLA.
5.13	Labelling of Information Implement labelling procedures for all classified information including documents, systems, and storage media.

5.14	Information Transfer Publish a data transfer policy covering approved tools, encryption requirements, and prohibitions on unencrypted transmission.
5.16	Identity Management Implement a formal identity lifecycle management process for all account types (users, service accounts, devices).
5.18	Access Rights Implement formal access provisioning and quarterly access reviews with manager approval and documented revocations.
5.27	Learning from Information Security Incidents Establish a post-incident review process and use lessons learned to update controls and procedures.
6.5	Responsibilities After Termination or Change Add information security obligations (access revocation, NDA enforcement, asset return) to the formal offboarding process.
8.13	Information Backup Implement automated, encrypted backups with off-site storage and a documented, tested restore process.
8.18	Use of Privileged Utility Programs Restrict privileged utility program use to authorized staff. Log and review all usage.
8.19	Installation of Software on Operational Systems Implement software installation controls (whitelist or MDM enforcement) on all production systems.

3. Technical Controls 60–90 days

9.2	Internal Audit Develop an internal audit program with qualified, independent auditors. Conduct the first audit cycle.
5.29	Information Security During Disruption Integrate information security continuity requirements into the Business Continuity Plan.
5.30	ICT Readiness for Business Continuity Implement and test ICT recovery procedures with defined RTO/RPO targets and annual recovery test evidence.
5.35	Independent Review of Information Security Schedule and conduct an independent review or third-party assessment of the ISMS at least annually.
8.6	Capacity Management Implement capacity monitoring with threshold alerting. Document capacity planning procedures.
8.9	Configuration Management Document system configuration baselines (CIS benchmarks). Enforce via automated compliance scanning.
8.14	Redundancy of Information Processing Facilities Implement redundancy for critical systems (HA/failover). Document RTO/RPO and test recovery annually.

8.29	Security Testing in Development and Acceptance Integrate SAST/DAST tools in CI/CD. Conduct annual penetration testing for critical and external-facing systems.

4. Advanced & Continuous Controls 90+ days

All	Ongoing Program Maintenance Maintain the ISMS through regular management reviews, continuous monitoring, and annual internal audits. Re-assess against ISO 27001:2022 annually or following significant changes to the organization, infrastructure, or threat landscape.

Statement of Accuracy

On behalf of Acme Corporation, I confirm that the information provided during this ISO/IEC 27001:2022 Current State Assessment has been, to the best of our knowledge, complete and accurate. We acknowledge the findings and commit to addressing identified gaps.

Name	[Authorised Signatory]
Title	[Title]
Organization	Acme Corporation
Signature	_____
Date	April 28, 2026

Carbide

This assessment was conducted using the Carbide Current State Assessment. For advisory support, Trust Audit™ services, and certification guidance, visit carbidesecure.com.