AUDIT READINESS REPORT

PREPARED FOR

Contoso Sample, Inc.

FRAMEWORK

SOC 2 Readiness Check

AICPA SOC 2 Trust Services Criteria

Audit Period	January 1, 2026 — December 31, 2026
Prepared For	Sample Audit Partners LLP
Generated	10/7/2026
Document ID	SOC2-20261007-f924a3

Generated client-side from live Microsoft Entra ID tenant configuration. No tenant data leaves the browser.

Audit preparation material only. EntraDocumentation.com is not a CPA firm and does not provide auditing, attestation, or assurance services. This document is not a SOC 2, ISO 27001, or other compliance report.

Auditor Cover Letter

To the auditor,

This readiness report documents the configuration of Microsoft Entra ID for the audit period stated on the cover page. It was generated directly from the tenant via the Microsoft Graph API in read-only mode and assembled client-side; no tenant data was transmitted to or stored by EntraDocumentation.com.

Every Common Criterion from CC1 through CC9 has its own section. Each section identifies the relevant SOC 2 criterion, summarises the evidence captured (or notes that none is available from Entra ID), and where applicable provides granular sub-findings with PASS / GAP / Not Applicable status. Gaps include recommended remediation.

Coverage depth varies by criterion: CC6, CC7, and CC9 receive the deepest coverage because they map directly to identity controls. CC2.3, CC4.1, CC5.2, and CC5.3 receive partial Entra-derived evidence that supplements — but does not replace — the organisational evidence those criteria require. The remaining criteria (CC1, parts of CC2, CC3, CC4.2, CC5.1, CC6.4–6.5, CC7.4–7.5, CC8.1) are marked Not Applicable; for each, the section explains exactly which other system holds the evidence (HR, GRC tool, policy repository, audit log, hosting provider SOC 2, etc.).

The cross-reference index at the end of the report maps each control to its page number for quick navigation. Configuration excerpts in this report reflect the live state of the tenant at the time of generation.

EntraDocumentation.com is not a CPA firm and does not provide auditing, attestation, or assurance services. This document is an audit-readiness report and does not constitute a SOC 2 report. Only a licensed CPA firm registered with the AICPA can perform a SOC 2 examination and issue the resulting report.

Generated by EntraDocumentation.com — SOC 2 Readiness Check

Scope Statement

This readiness report addresses every SOC 2 Common Criterion from CC1 through CC9. The deepest coverage is on CC6 (Logical and Physical Access), CC7 (System Operations), and CC9 (Risk Mitigation) as they relate to identity, where Microsoft Entra ID provides direct, configurable evidence. CC2.3, CC4.1, CC5.2, and CC5.3 receive partial Entra-derived evidence that supplements — but does not replace — the organisational evidence those criteria require. The remaining criteria (CC1.1–CC1.5, CC2.1–CC2.2, CC3.1–CC3.4, CC4.2, CC5.1, CC6.4–CC6.5, CC7.4–CC7.5, CC8.1) are marked Not Applicable with a specific pointer to the system or document where the evidence does live (HR, GRC tool, policy repository, audit log, hosting provider SOC 2, etc.). Together this gives the auditor a complete SOC 2 control checklist with the Entra-evidenced portions filled in and a clear hand-off list for everything else.

Auditor acknowledgement

Auditor name: _____

Firm: _____

Date: _____

Contents

Auditor Cover Letter 2

Scope Statement 2

Executive Summary 4

Control Status 4

External Evidence Matrix 6

CC2 — Communication and Information 8

CC2.3 — External Communication 9

CC4 — Monitoring Activities 10

CC4.1 — Ongoing and Separate Evaluations 11

CC5 — Control Activities 12

CC5.2 — Selects and Develops General Controls Over Technology 13

CC5.3 — Deploys Through Policies and Procedures 14

CC6 — Logical and Physical Access Controls 15

CC6.1 — Logical Access Controls 16

CC6.2 — User Access Provisioning 17

CC6.3 — Access Removal and Modification 18

CC6.6 — Multi-Factor Authentication 19

CC6.7 — Restriction of Privileged Access 20

CC6.8 — Application Access Controls 21

CC7 — System Operations 22

CC7.1 — Security Event Detection 23

CC7.2 — System Monitoring 24

CC7.3 — Incident Response Preparation 25

CC9 — Risk Mitigation 26

CC9.1 — Risk Mitigation 27

CC9.2 — Vendor and Business Partner Management 28

Cross-Reference Index 29

Executive Summary

This package evaluates 33 SOC 2 controls against the live Microsoft Entra ID configuration. 39 granular checks were executed across these controls.

PASS	Control evidenced directly from Entra configuration.
GAP	Control deficiency with recommended remediation.
N/A	Evidence lives outside Entra — see External Evidence Matrix.

Priority Gaps — address first

- **CC6.6 — Multi-Factor Authentication**
  • Device compliance enforced: For resources holding sensitive data, enforce device compliance via Conditional Access — pairs with Intune compliance policies.
- **CC6.7 — Restriction of Privileged Access**
  • Emergency access (break-glass) accounts: Provision 1–2 break-glass accounts (cloud-only, FIDO2-protected, monitored), grant them Global Administrator, and exclude them from every Conditional Access policy to ensure tenant recovery.
- **CC7.3 — Incident Response Preparation**
  • Automated response to risky activity: Add Conditional Access policies driven by sign-in or user risk so that suspicious activity is challenged or blocked automatically (Entra ID P2 …
- **CC6.8 — Application Access Controls**
  • Permission grant policies: Configure a custom permission grant policy that limits user consent to low-risk Microsoft Graph permissions on verified publisher apps. Disable user consent for non-verified apps.

9	6	18
Pass	Gaps	Not Applicable

Pass rate of in-scope controls: 60%

Entra coverage: 15 of 33 SOC 2 controls (45%) evidenced directly from tenant configuration. The remainder live outside Entra — see External Evidence Matrix.

Control Status

N/A	**CC1.1 — Commitment to Integrity and Ethical Values**
N/A	**CC1.2 — Board Independence and Oversight**
N/A	**CC1.3 — Organizational Structure, Reporting Lines, and Authority**
N/A	**CC1.4 — Commitment to Competence**
N/A	**CC1.5 — Accountability for Internal Control Responsibilities**
N/A	**CC2.1 — Quality of Information**
N/A	**CC2.2 — Internal Communication**
PASS	**CC2.3 — External Communication**
N/A	**CC3.1 — Specifies Suitable Objectives**
N/A	**CC3.2 — Identifies and Analyzes Risk**
N/A	**CC3.3 — Considers Potential for Fraud**
N/A	**CC3.4 — Identifies and Assesses Significant Changes**
PASS	**CC4.1 — Ongoing and Separate Evaluations**
N/A	**CC4.2 — Communicates Internal Control Deficiencies**

N/A	**CC5.1 — Selects and Develops Control Activities**
PASS	**CC5.2 — Selects and Develops General Controls Over Technology**
PASS	**CC5.3 — Deploys Through Policies and Procedures**
PASS	**CC6.1 — Logical Access Controls**
PASS	**CC6.2 — User Access Provisioning**
PASS	**CC6.3 — Access Removal and Modification**
N/A	**CC6.4 — Restricted Physical Access**
N/A	**CC6.5 — Asset Removal and Disposal**
GAP	**CC6.6 — Multi-Factor Authentication**
GAP	**CC6.7 — Restriction of Privileged Access**
GAP	**CC6.8 — Application Access Controls**
GAP	**CC7.1 — Security Event Detection**
PASS	**CC7.2 — System Monitoring**
GAP	**CC7.3 — Incident Response Preparation**
N/A	**CC7.4 — Incident Evaluation and Response**
N/A	**CC7.5 — Incident Recovery**
N/A	**CC8.1 — Change Management**
GAP	**CC9.1 — Risk Mitigation**
PASS	**CC9.2 — Vendor and Business Partner Management**

External Evidence Matrix

The following controls are marked N/A because their evidence lives outside Microsoft Entra ID. Each row identifies the owner / system where the auditor should source evidence and a concrete request to make.

Control	Title	Owner / System	What to request
CC1.1	Commitment to Integrity and Ethical Values	HR / Legal	Code of conduct, ethics policy, most recent acknowledgement campaign results, whistle-blower / ethics reporting records.
CC1.2	Board Independence and Oversight	Corporate Secretary / Board	Board minutes, audit committee charter, director independence attestations, oversight reporting from the audit period.
CC1.3	Organizational Structure, Reporting Lines, and Authority	HR / Operations	Org charts, reporting relationships, authority matrix, segregation-of-duties documentation. Entra directory roles (see CC6.7) supplement technical authority.
CC1.4	Commitment to Competence	HR / Learning & Development	Role-based training matrix, security awareness training completion records, role-based competence requirements.
CC1.5	Accountability for Internal Control Responsibilities	HR	Sample performance reviews where control responsibilities are evaluated; disciplinary procedure documentation.
CC2.1	Quality of Information	Data Governance / IT	Data governance policy, data classification standard, data quality monitoring reports.
CC2.2	Internal Communication	HR / Internal Comms	Policy communication samples, the internal control policy, training and onboarding materials.
CC3.1	Specifies Suitable Objectives	Executive / Risk	Documented strategic and operational objectives; risk appetite / tolerance statement.
CC3.2	Identifies and Analyzes Risk	GRC (Vanta / Drata / Hyperproof)	Export of the risk register covering the audit period; risk assessment methodology.
CC3.3	Considers Potential for Fraud	Risk / Finance	Fraud risk analysis, anti-fraud control documentation, segregation-of-duties analysis.

Control	Title	Owner / System	What to request
CC3.4	Identifies and Assesses Significant Changes	Risk / Engineering CAB	Minutes from change-review meetings; significant-change risk assessments performed during the audit period. (See CC8.1 for technical change management.)
CC4.2	Communicates Internal Control Deficiencies	GRC / Ticketing	Sample of identified deficiencies, remediation status, management / board communication evidence.
CC5.1	Selects and Develops Control Activities	GRC / Compliance	Control matrix mapping each risk in CC3.2 to at least one control activity.
CC6.4	Restricted Physical Access	Facilities / Hosting Provider	Badge-system logs, visitor logs, or (for cloud-only workloads) the hosting provider's SOC 2 report (Azure, AWS, GCP).
CC6.5	Asset Removal and Disposal	IT Asset Management / Hosting Provider	Hardware destruction certificates, media sanitization logs, or the hosting provider's SOC 2 for cloud-only workloads.
CC7.4	Incident Evaluation and Response	Security Operations	Incident response policy; sample of incident records (PagerDuty / Jira / Confluence) from the audit period.
CC7.5	Incident Recovery	IT / Business Continuity	DR / BCP plan with RTO/RPO targets; most recent recovery test report.
CC8.1	Change Management	Engineering CAB + Entra Audit Log	Representative sample of Entra audit-log entries (admin center → Monitoring → Audit logs); code-review / change-ticket approvals (GitHub PRs, Jira CRs).

SECTION

CC2 — Communication and Information

CC2.3 — External Communication

PASS

Control Description

The entity communicates with external parties regarding matters affecting the functioning of internal control.

Evidence Captured

1 Terms of Use agreements published to users; supplementary evidence — full external communications evidence lives outside Entra ID.

Captured 10/7/2026 from live tenant configuration.

Terms of Use agreement
Acceptable Use Policy v3

Detailed Findings

Passing checks

PASS

Terms of Use agreements published to users (supplementary evidence)

1 Terms of Use agreements published; users must accept them at sign-in via Conditional Access

Not applicable / out-of-scope

N/A

External communication evidence outside Entra ID

Customer and external communication artifacts (privacy notice, status page, security trust portal, contractual disclosures) are maintained in your marketing/legal systems and are out of scope here. Provide the published privacy notice URL, status page link, and any customer security disclosures.

Assessment

External communication partially evidenced via Entra Terms of Use; remaining evidence external to Entra.

SECTION

CC4 — Monitoring Activities

CC4.1 — Ongoing and Separate Evaluations

PASS

Control Description

The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Evidence Captured

2 access reviews + 1 report-only Conditional Access policies provide ongoing identity-control evaluation.

Captured 10/7/2026 from live tenant configuration.

Evaluation type	Name
Access review	Quarterly review of Global Administrators
Access review	Annual review of Engineering AWS Access
Report-only CA policy	Report-only: Risky sign-ins

Detailed Findings

Passing checks

PASS **Access reviews as ongoing evaluations**

2 recurring access reviews continuously re-evaluate whether identity access remains appropriate

PASS **Report-only Conditional Access as continuous monitoring**

1 CA policies in report-only mode generate ongoing telemetry that surfaces what would have been blocked

Not applicable / out-of-scope

N/A **Separate (independent) evaluations outside Entra ID**

Separate evaluations — internal audit, third-party penetration tests, control self-assessments — are performed outside Entra ID. Provide the latest internal audit report, penetration test report, and control self-assessment results.

Assessment

Ongoing identity-control evaluation evidenced; separate evaluations require external evidence.

SECTION

CC5 — Control Activities

CC5.2 — Selects and Develops General Controls Over Technology

PASS

Control Description

The entity also selects and develops general control activities over technology to support the achievement of objectives.

Evidence Captured

2 Conditional Access policies, 2 PIM eligible role assignments, 1 MFA-enforcing policies — Entra-implemented general technology controls.

Captured 10/7/2026 from live tenant configuration.

Entra general technology control	Count
Enforced Conditional Access policies	2
Report-only Conditional Access policies	1
Policies requiring MFA	1
PIM eligible role assignments	2
PIM eligible group assignments	0
Permanent privileged role assignments	0

Detailed Findings

Passing checks

PASS **Conditional Access as general technology control**
2 enforced Conditional Access policies act as general access controls over identity (see CC6.1 for full evaluation)

PASS **Privileged Identity Management as general technology control**
2 PIM eligible assignments implement just-in-time privileged access (see CC6.7 for full evaluation)

PASS **Multi-factor authentication as general technology control**
1 enforced policies require MFA (see CC6.6 for full evaluation)

Not applicable / out-of-scope

N/A **Non-identity general technology controls**
General technology controls outside identity (network controls, endpoint protection, vulnerability management, secure development) are evidenced from your network/EDR/SIEM/SDLC tooling. Provide network architecture diagrams, EDR coverage reports, vulnerability scan results, and SDLC documentation.

Assessment

Identity-layer general technology controls evidenced; broader technology controls require external evidence.

CC5.3 — Deploys Through Policies and Procedures

PASS

Control Description

The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Evidence Captured

2 enforced Conditional Access policies and 1 Terms of Use agreements deploy controls into the identity layer.

Captured 10/7/2026 from live tenant configuration.

Deployment mechanism	Name
Conditional Access (enforced)	Require MFA for all users
Conditional Access (enforced)	Block legacy authentication
Terms of Use	Acceptable Use Policy v3

Detailed Findings

Passing checks

PASS

Conditional Access deploys identity policy

2 Conditional Access policies are technical implementations of access policy in production

PASS

Terms of Use deploys user-facing policy

1 Terms of Use agreements deploy acceptable-use and data-handling policies to users at sign-in

Not applicable / out-of-scope

N/A

Written policy library outside Entra ID

The written policy library (security policy, access control policy, data classification policy, incident response policy) lives in your policy management system. Provide the current versions of all relevant policies and evidence of management approval.

Assessment

Identity-layer policy deployment evidenced via CA and ToU; written policy library external.

SECTION

CC6 — Logical and Physical Access Controls

CC6.1 — Logical Access Controls

PASS

Control Description

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events.

Evidence Captured

2 enforced and 1 report-only Conditional Access policies (3 total). 2 directory roles defined.

Captured 10/7/2026 from live tenant configuration.

Policy	State	Users	Apps	Grant
Require MFA for all users	Enforced	All users	All cloud apps	MFA
Block legacy authentication	Enforced	All users	—	Block
Report-only: Risky sign-ins	Report-only	—	—	MFA

Detailed Findings

Passing checks

PASS **Conditional Access enforced**
2 enabled Conditional Access policies

PASS **Tenant-wide user coverage**
2 enforced policies target the "All users" group

PASS **Tenant-wide application coverage**
1 enforced policies target "All cloud apps"

Assessment

Logical access controls assessed across enforcement, user coverage, and application coverage.

CC6.2 — User Access Provisioning

PASS

Control Description

Prior to issuing system credentials and granting access, the entity registers and authorizes new internal and external users whose access is administered by the entity.

Evidence Captured

2 entitlement management access packages across 1 catalogs.

Captured 10/7/2026 from live tenant configuration.

Governance object	Name
Catalog	Engineering Catalog
Access package	Engineering AWS Access
Access package	Sales CRM Access

Detailed Findings

Passing checks

PASS **Access packages configured**

2 access packages governing user provisioning

PASS **Catalogs separating resource ownership**

1 catalogs in use

Assessment

User access provisioning assessed via Entitlement Management.

CC6.3 — Access Removal and Modification

PASS

Control Description

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design.

Evidence Captured

2 access reviews configured.

Captured 10/7/2026 from live tenant configuration.

Access review
Quarterly review of Global Administrators
Annual review of Engineering AWS Access

Detailed Findings

Passing checks

PASS **Access reviews scheduled**

2 access reviews configured

PASS **Reviews target privileged access**

1 access reviews appear to target privileged or administrative access

CC6.6 — Multi-Factor Authentication

GAP

Control Description

The entity implements logical access security measures to protect against threats from sources outside its system boundaries, including multi-factor authentication for remote access.

Evidence Captured

1/2 enforced policies require MFA. 1 block legacy authentication. 0 require compliant device.

Captured 10/7/2026 from live tenant configuration.

Control	Policy	Users
MFA required	Require MFA for all users	All users
Blocks legacy auth	Block legacy authentication	All users

Detailed Findings

Gaps requiring remediation

GAP **Device compliance enforced**

No policy requires compliant or domain-joined devices

Target: At least one policy enforcing device compliance for sensitive resources

Remediation: For resources holding sensitive data, enforce device compliance via Conditional Access — pairs with Intune compliance policies.

Passing checks

PASS **MFA required by Conditional Access**

1 enforced policies require MFA

PASS **Legacy authentication blocked**

1 enforced policies block legacy authentication clients

Assessment

Authentication security assessed: MFA, legacy auth blocking, and device compliance.

Recommended Remediation

• Device compliance enforced: For resources holding sensitive data, enforce device compliance via Conditional Access — pairs with Intune compliance policies.

CC6.7 — Restriction of Privileged Access

GAP

Control Description

The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal.

Evidence Captured

2 Global Administrators, 3 total members across 2 high-privilege roles. PIM eligible: 2 role + 0 group.

Captured 10/7/2026 from live tenant configuration.

High-privilege role	Member (UPN)
Global Administrator	alex.lee@contoso.example
Global Administrator	jamie.park@contoso.example
Security Administrator	sam.rivera@contoso.example

Detailed Findings

Gaps requiring remediation

GAP

Emergency access (break-glass) accounts

No enforced Conditional Access policies exclude any users

Target: At least 1–2 dedicated emergency access accounts excluded from all CA policies

Remediation: Provision 1–2 break-glass accounts (cloud-only, FIDO2-protected, monitored), grant them Global Administrator, and exclude them from every Conditional Access policy to ensure tenant recovery.

Passing checks

PASS

Global Administrator count

2 Global Administrators

Target: Microsoft recommends 2–4

PASS

Just-in-time privileged access

2 role and 0 group PIM eligible assignments configured against 3 permanent privileged assignments

PASS

MFA coverage of privileged accounts

1 MFA-requiring policies and 3 privileged members — verify policy scope includes administrative roles

Assessment

Privileged access restriction assessed: GA count, PIM, break-glass, and MFA coverage.

Recommended Remediation

• Emergency access (break-glass) accounts: Provision 1–2 break-glass accounts (cloud-only, FIDO2-protected, monitored), grant them Global Administrator, and exclude them from every Conditional Access policy to ensure tenant recovery.

CC6.8 — Application Access Controls

GAP

Control Description

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Evidence Captured

2 app registrations and 2 service principals. 1 admin consent policies, 0 permission grant policies.

Captured 10/7/2026 from live tenant configuration.

Application artefact	Name
App registration	Contoso Internal Tools
App registration	Contoso Customer Portal
Service principal	Salesforce
Service principal	GitHub Enterprise
Admin consent policy	Default admin consent workflow

Detailed Findings

Gaps requiring remediation

GAP

Permission grant policies

No permission grant policies configured beyond defaults

Target: A permission grant policy restricting user consent to low-risk, verified apps only

Remediation: Configure a custom permission grant policy that limits user consent to low-risk Microsoft Graph permissions on verified publisher apps. Disable user consent for non-verified apps.

Passing checks

PASS

Admin consent workflow

1 admin consent policies enforce centralized governance over high-privilege app permissions

Not applicable / out-of-scope

N/A

Token lifetime policies

No custom token lifetime policies configured (Microsoft defaults apply)

Target: Optional — Microsoft default lifetimes are acceptable for most workloads

Assessment

Application access governance assessed across consent workflow, permission grants, and token lifetimes.

Recommended Remediation

• Permission grant policies: Configure a custom permission grant policy that limits user consent to low-risk Microsoft Graph permissions on verified publisher apps. Disable user consent for non-verified apps.

SECTION

CC7 — System Operations

CC7.1 — Security Event Detection

GAP

Control Description

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Evidence Captured

0 CA policies trigger on user risk, 0 on sign-in risk.

Captured 10/7/2026 from live tenant configuration.

No risk-aware Conditional Access policies captured.

Detailed Findings

Gaps requiring remediation

GAP

User-risk-driven Conditional Access

No enforced policy reacts to Identity Protection user risk

Target: A policy requiring password change or block when user risk is high

Remediation: Create a Conditional Access policy with user risk condition (high) requiring secure password change. Requires an Entra ID P2 license.

GAP

Sign-in-risk-driven Conditional Access

No enforced policy reacts to sign-in risk

Target: A policy requiring MFA when sign-in risk is medium or high

Remediation: Create a Conditional Access policy that requires MFA when sign-in risk is medium or high — catches anomalous sign-ins automatically. Requires Entra ID P2.

Assessment

Detection of identity-related security events assessed via risk-based Conditional Access.

Recommended Remediation

• User-risk-driven Conditional Access: Create a Conditional Access policy with user risk condition (high) requiring secure password change. Requires an Entra ID P2 license.
• Sign-in-risk-driven Conditional Access: Create a Conditional Access policy that requires MFA when sign-in risk is medium or high — catches anomalous sign-ins automatically. Requires Entra ID P2.

CC7.2 — System Monitoring

PASS

Control Description

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives.

Evidence Captured

1 Conditional Access policies in report-only mode for monitoring.

Captured 10/7/2026 from live tenant configuration.

Mode	Policy
Report-only	Report-only: Risky sign-ins
Enforced (log source)	Require MFA for all users
Enforced (log source)	Block legacy authentication

Detailed Findings

Passing checks

PASS **Report-only Conditional Access policies**

1 policies in report-only mode provide visibility into would-be enforcement decisions

PASS **Conditional Access telemetry generated**

3 Conditional Access policies generate sign-in log entries available in the Entra audit and sign-in logs

Assessment

Monitoring posture assessed via Conditional Access telemetry.

CC7.3 — Incident Response Preparation

GAP

Control Description

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Evidence Captured

0 risk-aware CA policies, 0 policies with user exclusions (consistent with break-glass).

Captured 10/7/2026 from live tenant configuration.

No risk-response or exclusion policies captured.

Detailed Findings

Gaps requiring remediation

GAP

Automated response to risky activity

No risk-aware Conditional Access policies; response is fully manual

Target: Risk-based CA policies that automate first-line response

Remediation: Add Conditional Access policies driven by sign-in or user risk so that suspicious activity is challenged or blocked automatically (Entra ID P2 required).

GAP

Recovery path preserved during incident response

No emergency access pattern detected; aggressive blocking could lock all admins out

Target: Break-glass account excluded from CA policies (see CC6.7)

Remediation: Configure 1–2 break-glass accounts (cloud-only, FIDO2, monitored) and exclude them from every Conditional Access policy.

Assessment

Incident response preparation assessed via risk-based response and emergency access continuity.

Recommended Remediation

• Automated response to risky activity: Add Conditional Access policies driven by sign-in or user risk so that suspicious activity is challenged or blocked automatically (Entra ID P2 required).
• Recovery path preserved during incident response: Configure 1–2 break-glass accounts (cloud-only, FIDO2, monitored) and exclude them from every Conditional Access policy.

SECTION

CC9 — Risk Mitigation

CC9.1 — Risk Mitigation

GAP

Control Description

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Evidence Captured

1 Terms of Use agreements registered. 0 risk-aware Conditional Access policies.

Captured 10/7/2026 from live tenant configuration.

Mitigation mechanism	Name
Terms of Use	Acceptable Use Policy v3

Detailed Findings

Gaps requiring remediation

GAP

Risk-aware access controls

No risk-aware Conditional Access policies

Target: CA policies reacting to sign-in or user risk

Remediation: Add risk-driven Conditional Access policies (Entra ID P2) so Identity Protection signals translate into automated access decisions.

Passing checks

PASS

Terms of Use acceptance enforced

1 Terms of Use agreements registered; can be enforced via Conditional Access

Assessment

Risk mitigation assessed via Terms of Use acceptance and risk-aware access controls.

Recommended Remediation

• Risk-aware access controls: Add risk-driven Conditional Access policies (Entra ID P2) so Identity Protection signals translate into automated access decisions.

CC9.2 — Vendor and Business Partner Management

PASS

Control Description

The entity assesses and manages risks associated with vendors and business partners.

Evidence Captured

1 connected organisations registered for B2B partner identity. 2 service principals installed in the tenant.

Captured 10/7/2026 from live tenant configuration.

Vendor / partner	Name
Connected organisation	Acme Partner Inc.
Service principal (third-party app)	Salesforce
Service principal (third-party app)	GitHub Enterprise

Detailed Findings

Passing checks

PASS **B2B partner organisations registered**

1 connected organisations formally registered

PASS **Service principal (third-party app) inventory**

2 service principals catalogued (includes Microsoft first-party apps); review periodically for unused or excessive-permission applications

Assessment

Vendor risk assessed via B2B partner registration and third-party application inventory.

Cross-Reference Index

Each control mapped to its page number in this report.

CC2.3 — External Communication 9
CC4.1 — Ongoing and Separate Evaluations 11
CC5.2 — Selects and Develops General Controls Over Technology 13
CC5.3 — Deploys Through Policies and Procedures 14
CC6.1 — Logical Access Controls 16
CC6.2 — User Access Provisioning 17
CC6.3 — Access Removal and Modification 18
CC6.6 — Multi-Factor Authentication 19
CC6.7 — Restriction of Privileged Access 20
CC6.8 — Application Access Controls 21
CC7.1 — Security Event Detection 23
CC7.2 — System Monitoring 24
CC7.3 — Incident Response Preparation 25
CC9.1 — Risk Mitigation 27
CC9.2 — Vendor and Business Partner Management 28