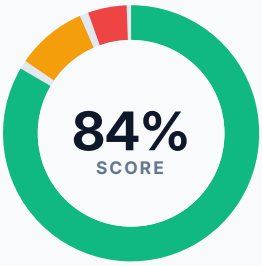
Cloud Security Posture Blueprint

Automated SOC 2 & CIS Benchmark Evaluation for **Contoso Cloud Technologies**

CIS AZURE V3.0 | SOC 2 TYPE II | AZURE RM + GRAPH | CONTINUOUS AUDIT

TARGET TENANT: 72f988bf-86f1-41af-91ab-2d7cd011db47 RUN ID: run_azp_984128_prod



Executive Posture & Audit Readiness

Azure environment meets baseline SOC 2 controls with 3 critical remediation items required prior to auditor review.

25	4	3	32/32
PASSED	WARNINGS	FAILURES	EVALUATED

Cloud Domain Compliance Matrix

Identity & Entra ID	90%	(9/10)
Key Vault & Encryption	75%	(6/8)
Compute & Workloads	80%	(4/5)
Database & Storage	83%	(5/6)
Network & Perimeter	100%	(3/3)

Priority Remediation Action Queue

Immediate engineering runbooks for high-risk findings

CRITICAL **KV1.4 — Key Vault Network Isolation Disabled** SOC 2 CC6.6 • CIS Azure 8.4

Key Vault 'kv-contoso-prod-east' allows traffic from all public networks without private endpoint restriction or firewall IP rules.

```
# Disable public network access & set firewall default action to Deny:
$ az keyvault update --name kv-contoso-prod-east --resource-group rg-prod --default-action Deny
```

1. Action: Navigate to Key Vault > 'kv-contoso-prod-east' > Networking in the Azure Portal.

SAFETY / IMPACT: Ensure private DNS zone 'privatelink.vaultcore.azure.net' is linked before disabling public access to avoid application downtime.

HIGH **CC6.1a — MFA Conditional Access Policy Gap** SOC 2 CC6.1 • CIS Azure 1.1

3 privileged administrative accounts do not have enforced phishing-resistant MFA under Conditional Access policy 'CA-Admins-MFA'.

```
# Update Entra ID Conditional Access policy to enforce MFA for all directory admins:
$ az ad policy update --id 'CA-Admins-MFA' --set conditions.users.include=['All']
```

1. Action: Open Microsoft Entra ID admin center > Protection > Conditional Access.

SAFETY / IMPACT: Verify break-glass emergency accounts are excluded with dedicated monitoring before saving.

Detailed Findings & Step-by-Step Remediation

Step-by-step resolution guides to satisfy SOC 2 Trust Services Criteria and CIS Benchmarks.

CRITICAL

KV1.4: Key Vault Network Isolation Disabled

SOC 2 CC6.6 • CIS Azure 8.4

Key Vault 'kv-contoso-prod-east' allows traffic from all public networks without private endpoint restriction or firewall IP rules.

TARGET ASSET: `/subscriptions/sub-001/resourceGroups/rg-prod/providers/Microsoft.KeyVault/vaults/kv-contoso-prod-east`

```
# Disable public network access & set firewall default action to Deny:
$ az keyvault update --name kv-contoso-prod-east --resource-group rg-prod --default-action Deny
```

ENGINEERING REMEDIATION WORKFLOW:

1. Navigate to Key Vault > 'kv-contoso-prod-east' > Networking in the Azure Portal.
2. Set 'Public network access' to 'Disabled' or 'Enabled from selected virtual networks and IP addresses'.
3. Provision an Azure Private Endpoint inside your production virtual network subnet.
4. Add authorized corporate egress IPs to the firewall exception list.

BLAST RADIUS & SAFETY: Ensure private DNS zone 'privatelink.vaultcore.azure.net' is linked before disabling public access to avoid application downtime.

HIGH

CC6.1a: MFA Conditional Access Policy Gap

SOC 2 CC6.1 • CIS Azure 1.1

3 privileged administrative accounts do not have enforced phishing-resistant MFA under Conditional Access policy 'CA-Admins-MFA'.

TARGET ASSET: `user: sec-admin@contoso.com`

```
# Update Entra ID Conditional Access policy to enforce MFA for all directory admins:
$ az ad policy update --id 'CA-Admins-MFA' --set conditions.users.include=['All']
```

ENGINEERING REMEDIATION WORKFLOW:

1. Open Microsoft Entra ID admin center > Protection > Conditional Access.
2. Select policy 'CA-Admins-MFA' and navigate to Users and groups.
3. Ensure 'All Users' or directory roles 'Global Administrator' are included in the scope.
4. Set Grant control to 'Require multifactor authentication' or 'Require authentication strength'.

BLAST RADIUS & SAFETY: Verify break-glass emergency accounts are excluded with dedicated monitoring before saving.

MEDIUM

CC6.6a: Storage Account Public Blob Anonymous Access

SOC 2 CC6.6 • CIS Azure 3.5

Storage account 'stcontosobackups' has allowBlobPublicAccess set to true, permitting container-level anonymous reads.

TARGET ASSET: `/subscriptions/sub-001/resourceGroups/rg-storage/providers/Microsoft.Storage/storageAccounts/stcontosobackups`

```
# Disable anonymous public blob read access on storage account:
$ az storage account update --name stcontosobackups --resource-group rg-storage --allow-blob-public-access false
```

ENGINEERING REMEDIATION WORKFLOW:

1. In Azure portal, select Storage Account 'stcontosobackups' > Configuration.
2. Set 'Allow Blob public access' to 'Disabled'.
3. Review storage audit logs to ensure no public CDN endpoints rely on anonymous reads.

BLAST RADIUS & SAFETY: Check if public assets are served directly; migrate to CDN with SAS tokens if necessary.

Complete Controls Evaluation Telemetry Register

Automated compliance evaluation records for all evaluated Microsoft Azure security controls.

CONTROL ID	DOMAIN	CONTROL OBJECTIVE & SCOPE	STATUS	TECHNICAL VERIFICATION RESULT
CC6.1a	IDENTITY	MFA Conditional Access for Privileged Roles	[FAIL]	3 admin accounts lacking enforced MFA policy
CC6.1b	IDENTITY	Block Legacy Authentication Protocols	[PASS]	Legacy auth blocked across all client apps
CC6.1c	IDENTITY	Global Administrator Account Limit	[PASS]	3 Global Admins active (limit <= 5)
CC6.1d	IDENTITY	Privileged Identity Management (PIM)	[PASS]	PIM eligible roles enabled with approval workflow
CC6.6a	STORAGE	Storage Account Public Blob Access	[WARN]	1 storage account allows anonymous container access
CC6.6b	DATABASE	Azure SQL Transparent Data Encryption (TDE)	[PASS]	TDE enabled on all 4 production SQL databases
CC6.6c	COMPUTE	Managed Disks Encryption at Rest	[PASS]	100% of OS and data disks encrypted with ADE/PMK
CC6.6d	DATABASE	PostgreSQL Flexible Server SSL/TLS Enforcement	[PASS]	TLS 1.2+ enforced, public access disabled
KV1.1	SECURITY	Key Vault Soft Delete & Purge Protection	[PASS]	Purge protection and 90-day retention active
KV1.4	SECURITY	Key Vault Network Isolation & Firewall	[FAIL]	DefaultAction is Allow on production vault
CC6.8	SECURITY	Microsoft Defender for Cloud Standard Tier	[PASS]	Defender plans active on Servers, Storage & DBs
CC7.1a	GOVERN	Activity Log Alert for Role Assignment Changes	[PASS]	Alert rule configured sending to SecOps webhook
CC7.2c	GOVERN	Diagnostic Settings Coverage for Key Services	[PASS]	Diagnostic logs stream to central Log Analytics
CC8.1a	GOVERN	Management Lock on Core Resource Groups	[PASS]	CanNotDelete locks enabled on production state

CRYPTOGRAPHICALLY SEALED EVIDENCE ARTIFACT

SHA-256 Digest: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Verified via AzureProof Compliance Engine v2026.8 • Preserved in Immutable Evidence Ledger