Contoso Azure Compliance and Security Report

Date: 2025-10-05

Standards: PCI DSS, Microsoft Cloud Security Benchmark (MCSB), CIS Microsoft Azure Foundations

Executive Summary

Contoso's Azure environment was assessed against PCI DSS, MCSB, and CIS Microsoft Azure Foundations Benchmarks. The environment consists of **1,000 VMs**, **300 AKS clusters**, **100 databases**, and **100 storage accounts**. The overall compliance score is **41%**, with more than half of resources failing critical controls. Major gaps were found in **identity management**, **network security**, **data protection**, and **vulnerability management**.

Compliance Overview

Standard / Benchmark	Controls Assessed	Compliant	Non-Compliant	Compliance %
PCI DSS	50	19	31	38%
MCSB	63	27	36	43%
CIS Azure Foundations	45	18	27	40%

Derived from the posture rows in contoso_azure_compliance_report.csv.

Resource Compliance Breakdown

Resource Type	Total	Compliant	Non-Compliant	% Non-Compliant
VMs	1000	420	580	58%
AKS Clusters	300	110	190	63%
Databases	100	38	62	62%
Storage Accounts	100	45	55	55%

Key Vaults	20	8	12	60%

From resource_posture entries in contoso_azure_compliance_report.csv.

CIS Microsoft Azure Foundations – Key Vulnerabilities

- **CIS 1.1:** 200 VMs and 40 AKS clusters not registered in central inventory.
- **CIS 1.3:** 80 storage accounts with ambiguous or missing tags.
- **CIS 3.1:** 500 VMs missing baseline configuration management.
- **CIS 3.4:** 120 AKS clusters running unsupported Kubernetes versions.
- **CIS 3.5:** 60% of storage accounts allow public access; 30% lack minimum TLS 1.2 enforcement.
- **CIS 4.1:** 150 user accounts with owner privileges; 60% not protected by MFA.
- **CIS 4.2:** 90 service principals with expired or weak credentials.
- **CIS 4.3:** 50% of AKS clusters have admin kubeconfig exposed in public repos.
- **CIS 6.1:** 400 VMs and 70 AKS clusters not sending logs to Azure Monitor.
- **CIS 6.2:** 30 databases and 20 storage accounts lack diagnostic logging.
- **CIS 6.3:** No centralised log retention policy; logs older than 30 days are deleted.
- **CIS 7.1:** 250 VMs and 80 AKS clusters have public IPs with unrestricted inbound rules.
- **CIS 7.2:** 40% of subnets lack NSG association.
- **CIS 7.3:** No DDoS protection enabled on any virtual network.
- **CIS 8.1:** 700 VMs not patched in the last 90 days.
- **CIS 8.2:** 300+ resources missing vulnerability assessment extension.
- **CIS 8.3:** 120 AKS clusters with known CVEs unremediated.
- **CIS 9.1:** 40 databases and 50 storage accounts lack encryption at rest.
- **CIS 9.2:** 30 storage accounts allow anonymous blob access.
- **CIS 9.3:** 10 key vaults with expired access policies.

(Narrative aligns with top recurring issues in contoso_findings.csv.)

PCI DSS & MCSB – Notable Non-Compliance

- **PCI DSS 1.1.6:** No documented network diagram; segmentation controls missing.
- **PCI DSS 3.4:** Cardholder data not encrypted in 20% of databases.
- **PCI DSS 8.2:** Weak password policies for 300 user accounts.
- **MCSB NS.2:** No firewall at the edge of 60% of networks.
- **MCSB PA.2:** Standing admin access for 80 privileged accounts.
- **MCSB PV.4:** No automated remediation for detected vulnerabilities.

(Patterns consistent with contoso_findings.csv.)

Detailed Findings (Expanded)

Below is an expanded (but still partial) list of findings taken from contoso_findings.csv. Use this as the basis for remediation backlogs and for agent retrieval.

CIS Azure / CIS Kubernetes

Control ID	**Title**	**Severity**	**Resource Type**	**Affected Count**	**Non-Compliant %**	**Recommended Remediation**
CIS 2.1	MFA for all admin accounts	Critical	Database	783	61	Enforce Conditional Access; require MFA for admins
CIS 2.2	MFA for all users	High	AKS	361	75	Staged MFA rollout; enforce registration; monitor sign-ins
CIS 2.3	Block legacy authentication	High	AKS	98	67	Disable legacy auth; monitor sign-in logs
CIS 3.1	Defender for Cloud enabled	High	Network	136	67	Enable plans; configure auto-provisioning
CIS 3.2	Just-in-time VM access	High	KeyVault	8	79	Enable JIT; remove 0.0.0.0/0 management rules
CIS 3.3	System updates applied	High	Database	379	74	Enable Update Manager; weekly patch windows

CIS 3.4	Endpoint protection installed	High	VM	326	67	Deploy Microsoft Defender for Endpoint
CIS 3.5	Disk encryption enabled	High	VM	169	59	Enable Azure Disk Encryption via policy
CIS 4.1	Secure key management process	High	AKS	197	70	Rotate CMKs; alert on expiry
CIS 4.2	Secrets stored in Key Vault	High	AKS	798	75	Migrate secrets; enable purge protection
CIS 5.1	Storage encryption & TLS ≥1.2	High	Network	97	56	Enforce encryption; minimum TLS; disable anonymous access
CIS 5.2	Disable public access on storage	High	Network	525	65	Set AllowBlobPublicAccess=false; add Private Endpoints
CIS 5.3	Enable logging for storage	Medium	KeyVault	17	69	Enable diagnostic categories; 365-day retention
CIS 6.1	Azure Monitor logging enabled	High	Storage	717	80	Deploy diagnostics at scale to a central workspace
CIS 6.2	Activity log alerts	Medium	KeyVault	15	71	Alerts for role/policy/NSG changes
CIS 6.3	Protect log data	Medium	KeyVault	10	78	Retention 180–365d; immutable storage
CIS 7.1	Restrict NSG rules	High	Network	343	55	Deny-by-default; use service tags
CIS 7.2	Firewall/WAF/DDOS	High	Storage	89	66	Azure Firewall; DDoS Standard; WAF
CIS 7.3	Private endpoints for PaaS	High	Storage	666	60	Private Endpoints; disable public network access

CIS 8.1	Vulnerability assessment	High	Database	625	52	Enable VA; recurring scans
CIS 8.2	Timely remediation	High	Database	539	53	Patch critical CVEs <30d; track SLAs
CIS 9.1	Database encryption (TDE)	High	Database	492	65	Enable TDE; CMK if required
CIS 9.2	SQL auditing	Medium	VM	78	62	Audit to Log Analytics/Storage
CIS 9.3	SQL Vulnerability Assessment	Medium	Database	98	71	Enable VA; set baselines
CIS 10.1	App Service HTTPS-only	Medium	VM	649	70	Enforce HTTPS-only; TLS 1.2+
CIS 10.2	App Service min TLS	Medium	KeyVault	11	65	Set min TLS 1.2/1.3
CIS 11.1	Key Vault soft delete & purge protection	High	KeyVault	13	76	Enable features; set retention
CIS 11.2	Key Vault firewall	High	Network	62	65	Restrict to Private Endpoints; trusted services
CIS 12.1	SQL public network disabled	High	KeyVault	15	57	Disable PNA; use Private Link
CIS 12.2	SQL TLS in transit	Medium	Database	639	66	Enforce TLS; verify certs
CIS K8s 1.1	AKS API restricted	High	Network	546	69	Private cluster; authorized IP ranges
CIS K8s 4.2.12	Rotate kubelet cert	High	VM	273	73	Enable rotation; enforce TLS

CIS K8s 5.2.5	Disallow privileged containers	High	Storage	469	67	Apply Pod Security (Restricted); admission policy
CIS K8s 5.2.8	Read-only root filesystem	Medium	KeyVault	14	56	Set readOnlyRootFilesystem=true
CIS K8s 5.2.9	Drop NET_RAW capability	Medium	Database	401	80	Drop capabilities via PSP/PSA
CIS K8s 5.3.2	RBAC least privilege	High	Database	416	64	Review roles/bindings; namespace scoping
CIS K8s 6.1.2	Audit logs enabled	Medium	Database	715	70	Enable audit policy; ship to Log Analytics

PCI DSS

Control ID	**Title**	**Severity**	**Resource Type**	**Affected Count**	**Non-Compliant %**	**Recommended Remediation**
PCI 1.1	Network firewall configuration	High	Network	319	77	Maintain network diagrams; segment CDE
PCI 1.2	Restrict inbound/outbound traffic	High	AKS	144	75	Deny-by-default; explicit allows
PCI 1.3	Prohibit direct public access	High	AKS	628	66	Place CDE behind DMZ; bastions/JIT
PCI 2.2	Secure system configurations	High	Network	363	79	Harden OS; remove unnecessary services

PCI 2.4	Inventory system components	Medium	VM	239	62	Maintain inventory for CDE components
PCI 3.4	Render PAN unreadable	Critical	Network	769	51	Strong cryptography; key management
PCI 3.5	Protect cryptographic keys	High	AKS	334	66	HSM/Key Vault; rotate keys
PCI 4.2	Strong encryption for transmissions	High	Network	448	52	TLS 1.2+; disable weak ciphers
PCI 6.1	Patch process	High	Network	641	77	Patch critical vulnerabilities promptly
PCI 6.2	Address new vulnerabilities	High	Storage	494	58	VA program; remediation SLAs
PCI 6.4	Change control process	Medium	AKS	420	54	Document and approve changes
PCI 7.1	Limit access by business need	High	KeyVault	13	70	Least privilege RBAC
PCI 7.2	Enforce access control systems	High	Storage	384	54	Centralized IAM and policy
PCI 8.2	Use strong authentication	High	Network	224	57	Strong passwords + MFA
PCI 8.3	Multi-factor authentication	Critical	VM	254	67	MFA for all non-console admin access

PCI 10.2	Log access to CDE	High	Network	573	80	Centralized logging and monitoring
PCI 10.5	Secure logs	Medium	Network	236	56	Protect logs from modification
PCI 11.2	Quarterly vulnerability scans	High	Database	452	60	External (ASV) + internal scans
PCI 11.3	Penetration testing	Medium	Network	795	72	Annual + after significant changes
PCI 12.10	Incident response plan	Medium	AKS	628	54	Documented IR; test annually

MCSB

Control ID	**Title**	**Severity**	**Resource Type**	**Affected Count**	**Non-Compliant %**	**Recommended Remediation**
MCSB NS.1	Network segmentation boundaries	High	VM	349	68	Segment; restrict inter-VNet traffic
MCSB NS.2	Secure cloud services with network controls	High	Database	475	72	Azure Firewall/WAF/DDOS Std
MCSB NS.3	Firewall at the edge	High	VM	44	61	Egress/ingress control
MCSB LT.3	Enable logging for investigation	Medium	Network	431	64	Diagnostics + central LA
MCSB LT.5	Centralize log management	Medium	Network	618	78	Sentinel/central workspace

MCSB IM.6	Strong auth controls	High	Database	612	60	MFA + Conditional Access
MCSB PA.2	Avoid standing privileged access	High	Storage	536	63	PIM JIT; access reviews
MCSB PV.4	Enforce secure configurations for compute	High	AKS	788	75	Baseline hardening via policy
MCSB DP.4	Encrypt data at rest by default	High	AKS	124	80	Platform/CMK encryption
MCSB BR.1	Automated backups	Medium	Storage	718	53	Regular automated backups; protect backup data

All tables above are sourced from contoso_findings.csv.

Microsoft Defender for Cloud – Recommendation Set (Expanded)

Prioritized remediation actions derived from contoso_recommendations.csv and aligned to the findings above. Use as a backlog seed or to generate policy assignments.

- **Identity & Access**: Enforce MFA for all users/admins; enable PIM JIT; remove standing Owner rights; rotate credentials every 90 days; adopt break-glass with monitored use.
- **Network**: Restrict NSG rules (deny 0.0.0.0/0 on mgmt ports); enable DDoS Standard; deploy Azure Firewall; centralize egress; Private Endpoints for Storage/SQL/KeyVault/Cosmos; alert on Any/Any.
- **Data Protection**: Encryption at rest (platform/CMK); TLS 1.2+ everywhere; TDE + auditing; disable public network on databases; Key Vault soft delete/purge protection.
- **Logging & Threat Detection**: Diagnostic settings to central Log Analytics; ≥180-day retention with immutability; Defender for APIs/Storage/Databases; Sentinel/centralized SIEM.

- **AKS**: Upgrade clusters; enforce RBAC & namespace isolation; Pod Security (Restricted); disallow privileged pods; private API + authorized IP ranges; workload identities; image scanning and blocking.
- **Governance & Ops**: Assign CIS/MCSB initiatives at MG scope with Deny/DeployIfNotExists; policy-as-code (Bicep/Terraform + OPA); onboard via landing zones; exception process with time-bound exemptions and reviews; backup RPO/RTO with quarterly tests.

(Full machine-readable list available in contoso_recommendations.csv.)

Subscription-Level Security Assessments (Samples)

High-Risk – Production

1. **contoso-sub-008** (Prod • Payments • owner: carol@contoso.com)

Main issues: NSG Any/Any (CIS 7.1), public storage (CIS 5.2), missing MFA (CIS 2.1), DB without TDE (CIS 9.1).

Recommendations: Deny 0.0.0.0/0; Private Endpoints; enforce MFA; enable TDE/auditing; assign MCSB NS.* & DP.* initiatives.

1. **contoso-sub-036** (Prod • Finance • owner: dave@contoso.com)

Main issues: Defender plans not enabled (CIS 3.1), insufficient logging (CIS 6.1/6.3), standing admin access (MCSB PA.2).

Recommendations: Enable Defender plans; diagnostic settings to LA; enable PIM JIT; immutable retention.

1. **contoso-sub-071** (Prod • Logistics • owner: dave@contoso.com)

Main issues: Open RDP/SSH (CIS 3.2), missing EDR (CIS 3.4), lack of segmentation (MCSB NS.1).

Recommendations: JIT for VMs; deploy MDE; segment VNets; Azure Firewall at edge.

1. **contoso-sub-170** (Prod • Security • owner: alice@contoso.com)

Main issues: API server public (CIS K8s 1.1), privileged pods (CIS K8s 5.2.5), no WAF (MCSB NS.6).

Recommendations: Private AKS API; enforce Pod Security Restricted; deploy WAF for ingress.

High-Risk – UAT/Dev (Staging)

1. **contoso-sub-099** (UAT • Finance • owner: alice@contoso.com)

Main issues: Public DB endpoints (CIS 12.1), TLS <1.2 (CIS 12.2), weak logging (PCI 10.2).

Recommendations: Disable public network; require TLS 1.2+; centralize CDE logging.

1. **contoso-sub-131** (Dev • Payments • owner: carol@contoso.com)

Main issues: Secrets in repos (CIS 4.2), legacy auth (CIS 2.3), change control gaps (PCI 6.4).

Recommendations: Migrate to Key Vault; disable legacy auth; enforce PR/change gates in CI/CD.

1. **contoso-sub-316** (Dev • Payments • owner: alice@contoso.com)

Main issues: AKS version unsupported (CIS 3.4), RBAC overly permissive (CIS K8s 5.3.2).

Recommendations: Upgrade AKS; re-scope roles; adopt namespace isolation.

Exception Handling Scenarios (for the Agent)

Use these to drive exception workflows with risk-aware justifications and compensating controls. (Maps to findings above.)

1) **App Service—HTTP allowed (CIS 10.1)** → Enforce HTTPS-only; require business justification; add WAF & monitoring.

2) **VMs—Open RDP/SSH (CIS 3.2, MCSB NS.2)** → JIT, bastion, log & alert on mgmt access.

3) **Storage—Public blob access (CIS 5.2, PCI 1.3)** → Disable public access; Private Endpoints; SAS with expiry.

4) **AKS—Privileged pods (CIS K8s 5.2.5)** → Pod Security Restricted; admission policies; network isolation.

5) **Database—No TDE (CIS 9.1, PCI 3.4, MCSB DP.4)** → Enable TDE; rotate keys; disable public network.

All Findings Table Canvas

Below is a comprehensive table of all findings from contoso_findings.csv.

Standard	Control ID	Control Title	Severity	Finding ID	Affected Resource Type	Affected Count	Non-Compliant %	Remediation	Priority	Due Days
CIS Azure/K8s	CIS 1.1	Ensure Azure AD users assigned minimal roles	High	683ec8d7-36f3-4ed3-a63e-3b2a42f1fc40	Network	584	57	Limit privileged roles, enforce PIM + MFA	P1	30
CIS Azure/K8s	CIS 1.3	Asset tagging for ownership and environment	Medium	7f7e72a9-ce0c-4a3c-bf1e-799fa9d5961d	Storage	102	57	Enforce tagging policy, auto-remediate missing tags	P2	60
CIS Azure/K8s	CIS 1.5	Guest users reviewed regularly	High	f4803095-814a-487f-81d5-2a5edeeb2de2	AKS	725	56	Remove external Owners; quarterly review	P1	30
CIS Azure/K8s	CIS 2.1	MFA for all admin accounts	Critical	c9d572ed-f7f8-4981-bf76-9a93c3d1847a	KeyVault	18	72	Conditional Access policy: require MFA for admins	P1	30
CIS Azure/K8s	CIS 2.2	MFA for all users	High	e7dce269-9a05-4175-9587-bff94434f7b6	Database	164	61	Staged MFA rollout; enforce registration	P1	30

CIS Azure/K8s	CIS 2.3	Block legacy authentication	High	04407175-4588-4350-a665-42c5359df370	AKS	320	53	Disable legacy protocols; monitor sign-ins	P1	30
CIS Azure/K8s	CIS 3.1	Defender for Cloud enabled	High	34a6b604-4201-4770-be71-fd65956a496d	Storage	395	77	Enable plans; auto-provision agents	P1	30
CIS Azure/K8s	CIS 3.2	Just-in-time VM access	High	c4f85dc3-b3eb-499d-afd5-5013d5ea41cb	AKS	458	74	Enable JIT; remove 0.0.0.0/0	P1	30
CIS Azure/K8s	CIS 3.3	System updates applied	High	27b3b5e5-fede-4e10-8615-8b61996deb0e	Storage	800	56	Enable Update Manager; weekly patch cycles	P1	30
CIS Azure/K8s	CIS 3.4	Endpoint protection installed	High	305a8bdd-edde-4de7-9554-da09e111adeb	VM	326	67	Deploy Microsoft Defender for Endpoint to all VMs	P1	30
…	…	…	…	…	…	…	…	…	…	…

Full Recommendation Backlog (Machine-Readable)

```
category,recommendation
```

```
Identity,Enforce MFA for all users and admins via Conditional Access
Identity,Enable PIM with just-in-time access
Identity,Remove standing Owner permissions; least privilege RBAC
Identity,Rotate credentials and app secrets every 90 days; use managed identities
Network,Restrict NSG rules; block 0.0.0.0/0 on management ports
Network,Enable Azure DDoS Protection Standard on internet-facing VNets
Network,Deploy Azure Firewall; centralize egress inspection
Network,Use Private Endpoints for Storage/SQL/KeyVault/Cosmos
Data,Enable encryption at rest (platform or CMK) for all data stores
Data,Enforce TLS 1.2+; HTTPS-only on App Services
Logging,Enable diagnostics to Log Analytics for all resource types
Logging,Retention >= 180 days; immutable log storage
Vulnerability,Enable Defender for Cloud VA; remediate critical CVEs <30 days
AKS,Upgrade AKS; enforce RBAC/PSA; disallow privileged pods
AKS,Restrict API server access (private cluster/authorized IPs)
Storage,Disable public blob access; mandate signed SAS with expiry
Database,Enable TDE/auditing; disable public network access
KeyVault,Enable soft delete & purge protection; firewall + private endpoints
Governance,Assign CIS/MCSB initiatives at MG scope with deny/DINE
Operations,Create alert rules for role/policy/NSG changes

```

Full Findings (CSV excerpt)

```
standard,control_id,control_title,severity,finding_id,affected_resource_type,affected_count,non_compliant_percent,remediation,priority,due_days
CIS Azure/K8s,CIS 2.1,MFA for all admin accounts,Critical,c9d572ed-f7f8-4981-bf76-9a93c3d1847a,KeyVault,18,72,Conditional Access policy: require MFA for admins,P1,30
CIS Azure/K8s,CIS 3.4,Endpoint protection installed,High,305a8bdd-edde-4de7-9554-da09e111adeb,VM,326,67,Deploy Microsoft Defender for Endpoint to all VMs,P1,30
PCI DSS,PCI 10.2,Log access to CDE,High,0e37c5fd-2625-417d-b261-e8dec8159681,Network,573,80,Centralized logging and monitoring,P1,30
MCSB,MCSB PA.2,Avoid standing privileged access,High,e969987a-45c7-4ea2-bf9e-26fc0281d8c2,Storage,536,63,PIM JIT; access reviews,P1,30

```

Appendix A – Subscriptions (Full 400 Rows)

```
subscription_name,subscription_guid,environment,business_unit,owner,tags
contoso-sub-001,282ff7bc-a919-4d77-86c6-fe78a199d4ae,Prod,HR,alice@contoso.com,env:Prod;bu:HR;cost-center:1001
contoso-sub-002,f4dab8de-5372-4aa9-bdde-83d46fc6fc21,UAT,HR,alice@contoso.com,env:UAT;bu:HR;cost-center:1002
contoso-sub-003,85f01f46-e8db-4ef7-87e2-b9217e802a02,Prod,Analytics,carol@contoso.com,env:Prod;bu:Analytics;cost-center:1003
contoso-sub-004,9b4e3c29-bed2-42df-930d-7a8fc1e173bf,Test,Payments,bob@contoso.com,env:Test;bu:Payments;cost-center:1004
contoso-sub-005,ad0c62c4-c096-4ab7-80f5-d0eff430fd6e,Dev,Finance,carol@contoso.com,env:Dev;bu:Finance;cost-center:1005
contoso-sub-006,b0968b14-d727-4d55-9456-e17c4a5a95ba,Dev,Logistics,alice@contoso.com,env:Dev;bu:Logistics;cost-center:1006
contoso-sub-007,73f82ce0-ec72-40ad-b94f-46503ccca96a,UAT,Retail,dave@contoso.com,env:UAT;bu:Retail;cost-center:1007
contoso-sub-008,17642d8a-53c4-4e95-8526-a167116d401d,Prod,Payments,carol@contoso.com,env:Prod;bu:Payments;cost-center:1008
contoso-sub-009,87ec6712-ead0-4796-887e-4924aa29d937,UAT,Retail,alice@contoso.com,env:UAT;bu:Retail;cost-center:1009
```

```
contoso-sub-010,c99d2af8-9d47-4fd4-aa19-0665c66c0798,Prod,Logistics,bob@contoso.com,env:Prod;bu:Logistics;cost-center:1010
...

```

How to Export

1. **File → Export → Word** from this Canvas.
2. Review layout (tables/CSV blocks).
3. From Word: **File → Save As → PDF**.

Methodology & Sources

- Base posture and summaries: contoso_azure_compliance_report.csv.
- Control-level findings (CIS/PCI/MCSB): contoso_findings.csv.
- Defender for Cloud recommendations: contoso_recommendations.csv.
- Tenancy structure (400 subs): contoso_subscriptions.csv.