

CONFIDENTIAL — SAMPLE REPORT

IT Security Audit Report

Comprehensive Security Posture Assessment

PREPARED FOR	[Client Organisation]
PREPARED BY	AMS Services — Security Practice
REPORT ID	AMS-AUDIT-2025-SAMPLE
DATE	May 2025
CLASSIFICATION	Confidential

TABLE OF CONTENTS

Report Structure

01

Executive Summary

02

Audit Scope & Methodology

03

Organisation & Environment Profile

04

Overall Security Posture Score

05

Key Findings — Endpoint & Email Security

06

Key Findings — Identity, Access & Cloud

07

Key Findings — Compliance & Governance

08

VAPT Summary

09

Risk Register

10

Prioritised Recommendations & Roadmap

11

About AMS Services & Next Steps

This report gives your leadership team a clear, actionable view of your current IT security posture — from high-level risk scoring through to a prioritised remediation roadmap.

SECTION 01

Executive Summary

This IT Security Audit was conducted by AMS Services across the full IT environment of [Client Organisation]. The assessment covered endpoint security, email, network, identity & access, cloud infrastructure, and regulatory compliance. Findings are prioritised by severity to enable immediate action by IT leadership and the board.

Critical	High	Medium	Low / Info
2	5	6	4

Figure 1 — Findings by severity

Key Observations

- **No MDM or centralised device management** — remote and BYOD devices operate without policy enforcement or compliance monitoring.
- **Email is the highest-risk attack vector** — no advanced email gateway; phishing simulation shows 34% click-through rate.
- **MFA not enforced organisation-wide** — including administrator accounts, creating critical credential compromise risk.
- **No SIEM / security monitoring** — threats and anomalies across cloud and network go undetected in real time.
- **Azure tenant misconfigured** — overly permissive service principals and public storage access identified.
- **Below compliance threshold** — organisation is not currently audit-ready for DPDP Act or ISO 27001.

The overall security posture is rated **High Risk**. Without immediate remediation of critical findings, probability of a successful cyberattack within 12 months is elevated. This report provides a prioritised 90-day roadmap.

SECTION 02

Audit Scope & Methodology

What Was Assessed

- Endpoint security — managed and unmanaged devices
- Email infrastructure and security controls (Microsoft 365)
- Network security — perimeter, segmentation, firewall configuration
- Identity & Access Management — Active Directory, Azure AD, MFA, Conditional Access
- Cloud environment — Microsoft Azure tenant, storage, VMs, service principals
- Regulatory compliance — DPDP Act, ISO 27001, MAS TRM
- Security monitoring capability — SIEM, logging, alerting
- Vulnerability Assessment & Penetration Testing (VAPT) — external and internal

Methodology

This audit follows NIST Cybersecurity Framework (CSF), CIS Controls v8, and ISO/IEC 27001:2022. The engagement ran over 5 business days across four phases:

PHASE	ACTIVITY	TIMING
1 — Discovery	Stakeholder interviews, environment inventory, documentation review	Day 1
2 — Assessment	Technical controls review, configuration audit, VAPT scanning	Days 2–3
3 — Analysis	Risk rating, gap analysis against compliance frameworks	Day 4
4 — Reporting	Findings documentation, roadmap, executive walkthrough	Day 5

Risk Rating Scale

RATING	CVSS	MEANING	RESPONSE SLA
CRITICAL	9.0–10.0	Exploitation likely; immediate business impact	Remediate within 48 hours
HIGH	7.0–8.9	High probability; significant operational impact	Remediate within 7 days
MEDIUM	4.0–6.9	Moderate risk under certain conditions	Remediate within 30 days
LOW	0.1–3.9	Limited impact if exploited	Remediate within 90 days
INFO	—	Best-practice observation; no direct risk	Next planning cycle

SECTION 03

Organisation & Environment Profile

The environment profile below is documented during the discovery phase. It provides the context required to interpret all findings accurately.

Organisation	[Client Organisation]
Industry / Sector	[e.g. Financial Services / BFSI]
Users & Locations	[e.g. 650 users across 4 locations — Mumbai, Pune, Singapore]
Primary Environment	Microsoft 365 / Azure hybrid
Identity Platform	On-premises AD + Azure AD (partial hybrid join)
Email Platform	Microsoft Exchange Online
Endpoint Mix	Windows 10/11 (primary) · macOS · Android · iOS
Cloud Platforms	Microsoft Azure (primary) · limited AWS workloads
Current Security	[e.g. Third-party AV, basic firewall — no EDR, no SIEM]
Compliance Scope	DPDP Act (India) · ISO 27001 (target) · MAS TRM (Singapore)
Last Audit	[e.g. None in prior 24 months]

SECTION 04

Overall Security Posture Score

Scores are calculated per domain based on control effectiveness, configuration compliance, and risk exposure. A score ≥70 indicates acceptable baseline. Below 50 requires immediate action.

DOMAIN	SCORE	RISK	SCORE INDICATOR
Endpoint Security	32/100	HIGH	32/100
Email & Communication	28/100	HIGH	28/100
Identity & Access Management	38/100	MEDIUM	38/100
Network Security	45/100	MEDIUM	45/100
Cloud Infrastructure	41/100	MEDIUM	41/100
Compliance & Governance	22/100	CRITICAL	22/100

OVERALL SECURITY POSTURE SCORE

34 / 100

■ HIGH RISK — ACTION REQUIRED

A score of 34/100 places the organisation in the **High Risk** band. AMS Services recommends a structured 90-day remediation programme.

SECTION 05

Key Findings — Endpoint & Email Security

EP-001	No Mobile Device Management (MDM)		CRITICAL
Finding	Devices operate independently with no policy enforcement, remote wipe, or compliance monitoring.		
Recommendation	Deploy Microsoft Intune MDM/MAM. Enforce Conditional Access requiring device compliance before granting M365 access.		
EP-002	No EDR/XDR — outdated endpoint protection		HIGH
Finding	Basic signature-based AV only. No behavioural detection or post-compromise visibility.		
Recommendation	Deploy Microsoft Defender for Endpoint or Kaspersky EDR. Integrate with SIEM for centralised alerting.		
EM-001	No advanced email security — 34% phishing click rate		HIGH
Finding	Only basic Exchange Online Protection in place. Safe Links and Safe Attachments not enabled. Simulated phishing yielded a 34% click-through rate.		
Recommendation	Enable Microsoft Defender for Office 365 (Safe Links, Safe Attachments). Configure DMARC, DKIM, SPF. Run phishing awareness training.		

SECTION 06

Key Findings — Identity, Cloud & Compliance

IAM-001	MFA not enforced — including admin accounts		CRITICAL
Finding	MFA active on <15% of accounts. No Conditional Access policies. Global Admin accounts have no MFA.		
Recommendation	Enable MFA via Azure AD Conditional Access immediately, prioritising admin accounts. Use Microsoft Authenticator. Enable SSPR.		
CL-001	Azure misconfiguration — overly permissive access		HIGH
Finding	Service principals have Owner-level permissions at subscription scope. Public blob access enabled on multiple storage accounts.		
Recommendation	Apply least-privilege to all service principals. Disable public blob access. Enable Microsoft Defender for Cloud. Implement CIS Azure Benchmark.		
NW-001	Flat network — unrestricted lateral movement		MEDIUM
Finding	No segmentation between user workstations, servers, and finance systems. A single compromised device can reach all others.		
Recommendation	Implement VLAN segmentation. Deploy inter-VLAN firewall rules on default-deny posture.		

SECTION 07

Key Findings — Compliance & Governance

CG-001	Not audit-ready — DPDP Act & ISO 27001		CRITICAL
Finding	No data classification policy. No documented incident response plan. Access to personal data not logged. No retention/deletion policy.		
Recommendation	Conduct formal DPDP gap assessment. Implement Microsoft Purview DLP. Document and test incident response plan. Target ISO 27001 within 12 months.		
SIEM-01	No SIEM — zero real-time threat visibility		HIGH
Finding	No centralised security monitoring. Threats, anomalies, and incidents across cloud and on-premises environments go undetected.		
Recommendation	Deploy Microsoft Sentinel. Connect all data sources. Configure baseline alert rules and automated incident response playbooks.		

SECTION 08

VAPT Summary

Vulnerability Assessment & Penetration Testing was conducted against the external perimeter and selected internal systems using Nmap, Burp Suite, and SQLMap. Top findings:

REF	TARGET	VULNERABILITY	CVSS	SEVERITY
V-01	External perimeter	RDP (3389) exposed to internet	9.8	CRITICAL
V-02	Internal network	Default credentials on network device	9.1	CRITICAL
V-03	Web application	SQL injection in login parameter	8.6	HIGH
V-04	Active Directory	Kerberoastable accounts with weak passwords	7.5	HIGH
V-05	Internal network	SMBv1 enabled — EternalBlue exposure	8.1	HIGH
V-06	Azure storage	Public blob container with PII data exposed	7.8	HIGH
V-07	Web application	Cross-Site Scripting (XSS) — reflected	6.1	MEDIUM
V-08	Microsoft 365	Legacy authentication (IMAP/POP3) enabled	5.3	MEDIUM
V-09	Email (phish test)	34% of staff clicked simulated phishing link	—	HIGH

SECTION 09

Risk Register

Top risks consolidated for board and leadership reporting. Risk Score = Likelihood (1–5) × Impact (1–5). Maximum score = 25.

REF	RISK	LIKE.	IMPACT	SCORE	RATING	OWNER
EP-001	No MDM — uncontrolled device access	5	5	25	CRITICAL	IT Director
IAM-001	MFA not enforced — credential theft risk	5	5	25	CRITICAL	IT Director
CG-001	DPDP non-compliance — regulatory penalty	4	5	20	CRITICAL	CISO
V-01	Internet-exposed RDP — remote exploitation	4	4	16	HIGH	IT Director
EP-002	No EDR — ransomware goes undetected	4	5	20	HIGH	IT Team
EM-001	No email gateway — high phishing susceptibility	5	4	20	HIGH	IT Team
SIEM-01	No SIEM — threats undetected in real time	3	5	15	HIGH	CISO
CL-001	Azure misconfiguration — data exposure risk	3	5	15	HIGH	Cloud Team
NW-001	Flat network — unrestricted lateral movement	3	4	12	MEDIUM	Network
V-03	SQL injection in web application	3	4	12	MEDIUM	Dev Team

SECTION 10

Prioritised Recommendations & Roadmap

Recommendations are grouped by urgency. The 90-day roadmap below provides a structured programme. AMS Services can act as your implementation partner across all phases.

PHASE 1 — IMMEDIATE (0–14 DAYS)	
IAM-001	Enable MFA for all admin and privileged accounts via Conditional Access
V-01	Close internet-exposed RDP port (3389) via firewall rule
V-02	Change default credentials on all network management interfaces
CL-001	Disable public blob access on all Azure storage accounts
EM-001	Enable Defender for Office 365 — Safe Links & Safe Attachments
PHASE 2 — SHORT TERM (15–45 DAYS)	
EP-002	Deploy Microsoft Defender for Endpoint across all managed devices
EP-001	Deploy Microsoft Intune MDM/MAM for all device types
IAM-001	Roll out MFA to all users (phased by role risk)
V-04/05	Disable SMBv1; remediate Kerberoastable AD accounts
SIEM-01	Deploy Microsoft Sentinel — connect data sources, configure alerting
PHASE 3 — STRATEGIC (46–90 DAYS)	
CG-001	Initiate DPDP Act compliance programme; implement Microsoft Purview DLP
NW-001	Design and implement network segmentation (VLAN architecture)
CG-001	Develop and tabletop-test Incident Response Plan
CG-001	Initiate ISO 27001 certification programme
V-03/07	Remediate remaining web application vulnerabilities

SECTION 11

About AMS Services & Next Steps

This report is a sample of the deliverable provided as part of AMS Services' Free IT Security Audit programme. Findings, scores, and recommendations shown are illustrative examples based on vulnerabilities commonly identified across our BFSI, Manufacturing, and Professional Services client base.

Who We Are

AMS Services is a managed IT, cloud, and cybersecurity company headquartered in Pune, India, with offices in Singapore and expanding into the UAE. We are authorised implementation partners for Microsoft, Kaspersky, and Trellix.

100+ clients served	400+ projects completed	150+ yrs collective expertise	3 authorised OEM partnerships	99% uptime SLA guarantee
---------------------	-------------------------	-------------------------------	-------------------------------	--------------------------

Our Services

- Cybersecurity — Endpoint, Email, Network, VAPT, SIEM, SOAR, Digital Forensics & Incident Response
- Cloud & Migration — Microsoft Azure, M365, hybrid environments, DC migration
- Managed IT Services — 24x7x365 monitoring, SLA-backed support, infrastructure management
- Compliance Advisory — DPDP Act, ISO 27001, MAS TRM, HIPAA readiness
- Resource Augmentation — certified cloud and security engineers on-demand

Get Your Free IT Security Audit

The full IT Security Audit — as shown in this sample — is available at no cost for qualifying organisations. Our engineers conduct a 2-hour assessment and deliver a written report within 5 business days. No sales pitch. No generic slide deck.

INDIA	SINGAPORE	WEB
sales@amsservices.in +91 98502 17757	sam@amsinfra.sg +65 97861000	www.amsservices.in

DISCLAIMER: This is a sample report for demonstration purposes only. All findings, scores, and data shown are illustrative and do not represent any specific organisation's actual security posture. Actual audit reports are confidential and delivered directly to the client. © 2025 AMS Services. All rights reserved.