Strictly Confidential

IAR 04-2026

OSOTSPA PUBLIC COMPANY LIMITED

Internal Audit Report

Cloud and Cybersecurity Management

(Governance, Infrastructure, Network, Application and Cloud)

3 August 2026

1. Executive Summary

Background

According to the 2026 Audit Plan of Osotspa Public Company Limited ("OSP" or "the Company"), as approved by the Audit Committee, the Company engaged an independent external service provider with specialized expertise, namely Mayaseven, to conduct a Cloud and Cybersecurity audit.

As the Company continues to expand its adoption of cloud technologies and digital platforms, effective Cloud and Cybersecurity has become increasingly critical to protecting business operations, information assets, and customer trust. The evolving threat landscape, combined with the complexity of cloud environments and the shared responsibility model, requires organizations to implement robust governance, secure configuration management, identity and access controls, continuous monitoring, and timely incident response capabilities.

Given the increasing sophistication of cyber threats and the technical complexity of cloud security, the Audit Committee considered an independent assessment by external specialists essential to provide deeper technical insights, benchmark the Company's security practices against recognized industry standards and best practices, and identify opportunities to further strengthen the Company's overall cyber resilience.

The audit was conducted to evaluate the adequacy and effectiveness of the Company's cloud and Cybersecurity controls, identify key risk areas, and support management in strengthening the Company's overall Cybersecurity posture.

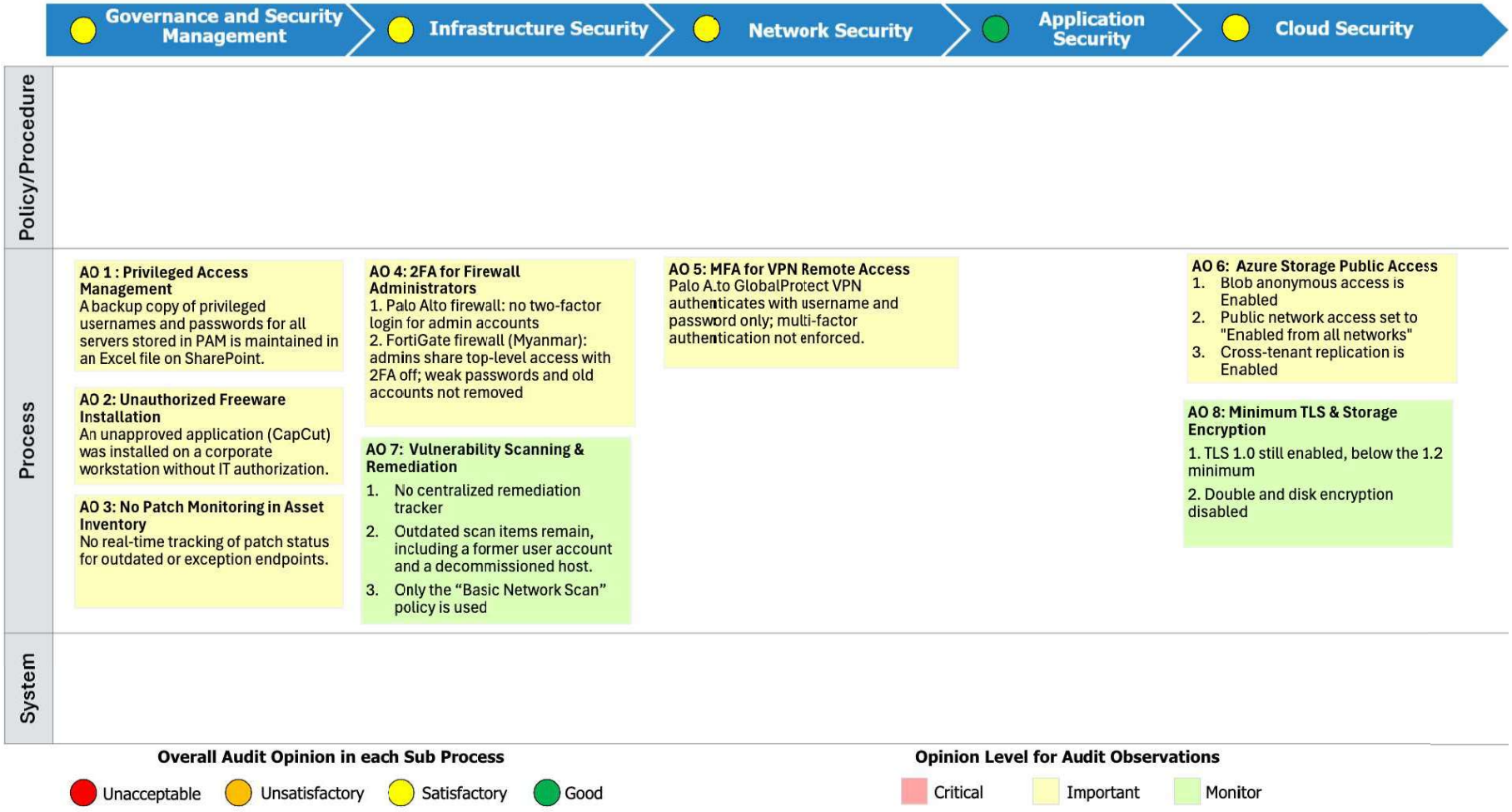
Overall Conclusion

We greatly appreciate the cooperation and support of the Digital Technology team and all parties involved, which were instrumental in completing this engagement. Based on our review, the overall opinion for this audit is assessed as "Satisfactory". The company has established a generally mature security posture and operation supported by a managed Security Operations Centre (Cybertron), an XDR/Zero-Trust platform (Trend Vision One), enterprise vulnerability management (Tenable), and immutable cloud backup (AWS Vault in Compliance Mode). Nevertheless, our fieldwork identified a number of observations that should be addressed to further strengthen the control environment. The most significant of these are rated "Important" and should be prioritized for management action.

The overall opinion for each business process is summarized below:

Business Process	Opinion Level
Overall Opinion	**Satisfactory**
1. Governance and Security Management	**Satisfactory**
2. Infrastructure Security	**Satisfactory**
3. Network Security	**Satisfactory**
4. Application Security	**Good**
5. Cloud Security	**Satisfactory**

Overall Audit Result: The overall opinion for this audit project is rated as "Satisfactory."



Summary of Audit Observations by Risk Ranking

There are 8 observations which 6 are defined "**Important**" and 2 are defined "**Monitor**" with details as follows:

No.	Observation	Audit Opinion (Target Date)	Ref No
1	Privileged Access Management backup storage, evidence and review should be strengthened	**Important** (31 August 2026)	3.1
2	Unauthorized installation of non-business freeware on employee workstation	**Important** (31 August 2026)	3.2
3	Lack of OS/software patch monitoring in asset inventory	**Important** (31 August 2026)	3.3
4	Two-factor authentication for firewall administrators should be enforced and hardening policy	**Important** (31 August 2026)	3.4
5	Multi-factor authentication for VPN remote access should be enforced	**Important** (30 September 2026)	3.5
6	Public and anonymous access to the Azure Storage Account should be restricted	**Important** (30 September 2026)	3.6
7	Vulnerability scanning policy and remediation tracking should be strengthened	**Monitor** (30 September 2026)	3.7
8	Minimum TLS version and storage encryption should be strengthened	**Monitor** (30 September 2026)	3.8

2. Objectives, Scope, and Approaches

Objectives

The objectives of this audit are to obtain assurance that management has established adequate and effective risk management, internal control, and governance over cybersecurity and cloud security, and that the related controls comply with applicable standards and regulations and safeguard the confidentiality, integrity and availability of the Company's systems and data.

Scope

This audit covers the end-to-end cybersecurity and cloud security controls of Osotspa across five domains: The audit period is 1 Mar 2025 to 31 May 2026.

Key policies, procedures and work instructions within the scope of this audit include:

Formal policies, procedures and work instructions

- M-HM-ITD-001 Information Security Policy (also the basis for data classification, firewall / security-policy approval and anti-malware requirements)
- P-HM-ITD-003 Secure Software Development Life Cycle (SDLC)
- P-HM-ITD-006 Cybersecurity Incident Response Plan (Rev 03), together with the updated Cybersecurity Incident Response Plan (CSIRP, Thai draft)
- P-HM-ITD-010 Guideline for Using Generative AI (EN / TH)
- W-HM-ITD-003 Data Backup and Restore (v2, eff. 2 December 2024) also reviewed as logging and retention evidence
- W-HM-ITD-006 IT BCP and IT DR Plan (v7, eff. 7 August 2024)
- W-HM-ITD-008 IT Outsource (Supplier) Management
- W-HM-ITD-010 Change Management (v5, eff. 1 April 2025)
- W-HM-ITD-012 Data Sanitization (data deletion and retention)
- Vulnerability Management Policy (Tenable)
- IP_SEC_Parameter Settings - Cryptography and Key Management for VPN and network traffic
- BYOD Guideline - acceptable use of personal computers for work purposes
- Digital Technology organizational chart (effective 1 April 2026)

Approaches

Timeline

Entrance meeting	2 April 2026
Audit fieldwork	2 April – 27 May 2026
Wrap-up and exit meeting	23 July 2026
Final audit report	3 August 2026

Report Distribution

Management responsible persons:

[redacted] Head of Digital Technology

[redacted] Head of Infrastructure & Operations

Auditor Team

[redacted]

[redacted] Project-Lead IT Audit

[redacted] IT Audit

Project Oversight & Coordination (Osotspa Internal Audit)

[redacted] Audit Champion

[redacted] Audit Champion