

ISO 27001:2022

INTERNAL AUDIT REPORT

Information Security Management System

Organization:	EMIRATES FACE RECOGNITION
Trade License No:	CN-1895744
Audit Date:	June 26, 2026
Report Date:	June 28, 2026
Classification:	CONFIDENTIAL

Table of Contents

1. Executive Summary	4
1.1 Audit Conclusion	4
2. Organization Profile	4
2.1 Company Information	4
2.2 Business Activities	4
3. Audit Details	5
3.1 Audit Objective	5
3.2 Audit Scope	5
3.3 Audit Team	5
3.4 Audit Methodology	5
4. Audit Criteria and Rating	6
4.1 Rating Methodology	6
5. Key Observations	6
5.1 Positive Observations	6
5.2 non-conformities	6
5.3 Opportunities for Improvement	6
6. Detailed Audit Findings	7
6.1 Organizational Controls (Clause 5)	7
6.2 People Controls (Clause 6)	8
6.3 Physical Controls (Clause 7)	8
6.4 Technological Controls (Clause 8)	9
7. Compliance Summary	10
7.1 Control Domain Summary	10
8. Conclusion and Recommendations	10
8.1 Audit Conclusion	10
8.2 Recommendations	10
9. Approval and Sign-Off	11

Document Control

Document Information

Item	Details
Document Title	ISO 27001:2022 Internal Audit Report
Version	1.0
Status	Final
Classification	Confidential
Author	Internal Audit Team
Reviewed By	Mr. Ayham- Senior Technical Coordinator

Version History

Version	Date	Author	Description
1.0	28/06/2026	Internal Audit Team	Initial Release

Distribution List

Name	Role
Mr. Ayham	Senior Technical Coordinator
Mr. Manoj Prabhakaran	Internal Auditor

1. Executive Summary

This Internal Audit Report presents the findings of the ISO 27001:2022 Information Security Management System (ISMS) audit conducted for Emirates Face Recognition. The audit was performed to assess the organization's compliance with ISO/IEC 27001:2022 standard requirements and the effectiveness of implemented information security controls.

1.1 Audit Conclusion

Based on the comprehensive assessment of all 93 controls specified in ISO 27001:2022 Annex A, Emirates Face Recognition, with the standard requirements. One Minor non-conformity was identified during this audit.

2. Organization Profile

2.1 Company Information

Item	Details
Company Name	EMIRATES FACE RECOGNITION
License Number	CN-1895744
Expiry Date	28/01/2027
Headquarters	Abu Dhabi, United Arab Emirates
Website	https://facerecognition.ae/

2.2 Business Activities

Emirates Face Recognition (EFR) is a UAE-based pioneer in biometrics and facial recognition technology, built on principles of privacy, trust, and security.

Amongst the first to introduce this technology in the UAE, EFR supports the nation's digital vision by delivering inclusive and accurate AI solutions across sectors.

. The organization offers the following services:

- ARTIFICIAL INTELLIGENCE SOFTWARE DEVELOPMENT AND SERVICES
- AI-POWERED FACE RECOGNITION, TRACKING, AND LOOKOUT SYSTEM
- BIOMETRIC IDENTIFICATION, VERIFICATION, AND VISION-BASED ANALYTICS SOLUTIONS
- SOFTWARE, MOBILE, AND WEB APPLICATION DEVELOPMENT
- COMPUTER INFRASTRUCTURE ESTABLISHMENT AND MAINTENANCE
- DATABASE DESIGN, DEVELOPMENT, AND ADMINISTRATION
- SYSTEM INTEGRATION, TESTING, AND QUALITY ASSURANCE SERVICES
- IT CONSULTANCY, TECHNICAL SUPPORT, AND MAINTENANCE
- DATA STORING AND RECOVERING
- DATA COLLECTION FROM ONE OR MORE SOURCES
- DATA CLASSIFICATION & ANALYSIS SERVICES
- COMPUTER SYSTEMS AND SOFTWARE DESIGNING
- ONSHORE AND OFFSHORE OIL AND GAS FIELDS AND FACILITIES SERVICES

3. Audit Details

3.1 Audit Objective

The primary objective of this internal audit was to evaluate the effectiveness and compliance of Emirates Face Recognition Information Security Management System (ISMS) against

ISO/IEC 27001:2022 requirements and to verify that information security controls are properly implemented and maintained.

3.2 Audit Scope

The audit scope included the following areas:

1. Information Security Program Governance
2. Identity and Access Management
3. Computer Operations, Network Monitoring and Security
4. Business Continuity Management & IT Disaster Recovery
5. System and Data Backup Management
6. Change Management & Configuration Management
7. Technical Vulnerability Management
8. Information Security Incident Management
9. Supplier Relationship Management
10. Physical & Environmental Security
11. Human Resource Security
12. Cloud Security & Threat Intelligence
13. 1 Data Protection & Privacy Controls

3.3 Audit Team

Name	Role
Mr. Manoj Prabhakaran	Lead Auditor
Ms. Jayasri Duraipandi	Report Preparation

3.4 Audit Methodology

The audit was conducted using a risk-based methodology covering People, Process, and Technology domains. The methodology included:

- Document review and policy assessment
- Interviews with key personnel
- Technical control verification
- Evidence collection and analysis
- Control effectiveness testing

4. Audit Criteria and Rating

4.1 Rating Methodology

The following rating scale was used to assess compliance with ISO 27001:2022 controls:

Rating	Status	Description
GREEN	Compliant	The controls fully complied with the requirements as mandated.
YELLOW	Partially Compliant	Conditions exist that can lead to non-compliance if not addressed.
RED	Non-Compliant	Control is not implemented. Significant adverse impact if not addressed.
GRAY	Not Applicable	The control is not applicable based on business requirements.

5. Key Observations

5.1 Positive Observations

During the internal audit, the following positive observations were noted:

- **Penetration Testing:** Regular penetration testing of applications is conducted through third-party vendors, with vendors rotated annually for independent assessment.
- **Data Disposal:** Proper data disposal procedures are in place. Annual data disposal is conducted through certified third-party vendors. All data is encrypted before destruction.
- **24/7 SOC Monitoring:** The organization maintains a 24/7 Security Operations Center monitoring with regular report generation and alerts.
- **Data Backup:** Data is maintained in different locations, ensuring redundancy and business continuity.
- **Restoration Testing:** Regular restoration testing is practiced. No data loss incidents have been recorded.
- **Endpoint Protection:** Microsoft Defender is deployed across endpoints with proper threat management procedures.

5.2 Non-conformities

No major and Observations were found; however, one minor non-conformity was identified during this audit:

- During the audit, it was observed that although the organization had implemented the information security controls in accordance with Annex A of ISO/IEC 27001:2022, the documented information supporting the implementation and operation of certain controls was not available for verification. In addition, several documented procedures and records were found to be outdated and had not been reviewed or revised to reflect current practices. As a result, the organization was unable to consistently demonstrate effective control implementation and maintenance through properly controlled documented information, as required by ISO/IEC 27001:2022 Clause 7.5.

5.3 Opportunities for Improvement

No significant opportunities for improvement were identified. The organization demonstrates mature information security practices across all domain

6. Detailed Audit Findings

The following section presents the detailed assessment of all 93 controls as per ISO 27001:2022 Annex A. All controls have been evaluated and found compliant.

6.1 Organizational Controls (Clause 5)

Total Controls: 37 | Compliant: 37 | non-compliant: 0

Ref.	Control	Status
5.1	Policies for information security	✓
5.2	Information security roles and responsibilities	✓
5.3	Segregation of duties	✓
5.4	Management responsibilities	✓
5.5	Contact with authorities	✓
5.6	Contact with special interest groups	✓
5.7	Threat intelligence	✓
5.8	Information security in project management	✓
5.9	Inventory of information and other associated assets	✓
5.10	Acceptable use of information and other associated assets	✓
5.11	Return of assets	✓
5.12	Classification of information	✓
5.13	Labelling of information	✓
5.14	Information transfer	✓
5.15	Access control	✓
5.16	Identity management	✓
5.17	Authentication information	✓
5.18	Access rights	✓
5.19	Information security in supplier relationships	✓
5.20	Addressing information security within supplier agreements	✓
5.21	Managing information security in the ICT supply chain	✓
5.22	Monitoring, review and change management of supplier services	✓
5.23	Information security for use of cloud services	✓
5.24	Information security incident management planning and preparation	✓
5.25	Assessment and decision on information security events	✓
5.26	Response to information security incidents	✓
5.27	Learning from information security incidents	✓
5.28	Collection of evidence	✓
5.29	Information security during disruption	✓
5.30	ICT readiness for business continuity	✓
5.31	Legal, statutory, regulatory and contractual requirements	✓
5.32	Intellectual property rights	✓
5.33	Protection of records	✓
5.34	Privacy and protection of PII	✓
5.35	Independent review of information security	✓
5.36	Compliance with policies, rules and standards	✓

5.37	Documented operating procedures	✓
------	---------------------------------	---

6.2 People Controls (Clause 6)

Total Controls: 8 | Compliant: 8 | non-compliant: 0

Ref.	Control	Status
6.1	Screening	✓
6.2	Terms and conditions of employment	✓
6.3	Information security awareness, education, and training	✓
6.4	Disciplinary process	✓
6.5	Responsibilities after termination or change of employment	✓
6.6	Confidentiality or non-disclosure agreements	✓
6.7	Remote working	✓
6.8	Information security event reporting	✓

6.3 Physical Controls (Clause 7)

Total Controls: 14 | Compliant: 14 | non-compliant: 0

Ref.	Control	Status
7.1	Physical security perimeters	✓
7.2	Physical entry	✓
7.3	Securing offices, rooms and facilities	✓
7.4	Physical security monitoring	✓
7.5	Protecting against physical and environmental threats	✓
7.6	Working in secure areas	✓
7.7	Clear desk and clear screen	✓
7.8	Equipment siting and protection	✓
7.9	Security of assets off-premises	✓
7.10	Storage media	✓
7.11	Supporting utilities	✓
7.12	Cabling security	✓
7.13	Equipment maintenance	✓
7.14	Secure disposal or re-use of equipment	✓

6.4 Technological Controls (Clause 8)

Total Controls: 34 | Compliant: 34 | non-compliant: 0

Ref.	Control	Status
8.1	User endpoint devices	✓
8.2	Privileged access rights	✓
8.3	Information access restriction	✓
8.4	Access to source code	✓
8.5	Secure authentication	✓
8.6	Capacity management	✓
8.7	Protection against malware	✓
8.8	Management of technical vulnerabilities	✓
8.9	Configuration management	✓
8.10	Information deletion	✓
8.11	Data masking	✓
8.12	Data leakage prevention	✓
8.13	Information backup	✓
8.14	Redundancy of information processing facilities	✓
8.15	Logging	✓
8.16	Monitoring activities	✓
8.17	Clock synchronization	✓
8.18	Use of privileged utility programs	✓
8.19	Installation of software on operational systems	✓
8.20	Networks security	✓
8.21	Security of network services	✓
8.22	Segregation in networks	✓
8.23	Web filtering	✓
8.24	Use of cryptography	✓
8.25	Secure development lifecycle	✓
8.26	Application security requirements	✓
8.27	Secure system architecture and engineering principles	✓
8.28	Secure coding	✓
8.29	Security testing in development and acceptance	✓
8.30	Outsourced development	✓
8.31	Separation of development, test and production environments	✓
8.32	Change management	✓
8.33	Test information	✓
8.34	Protection of information systems during audit testing	✓

7. Compliance Summary

7.1 Control Domain Summary

Domain	Total	Compliant	Non-Compliant	Score
Organizational Controls (5)	37	37	0	100%
People Controls (6)	8	8	0	100%
Physical Controls (7)	14	14	0	100%
Technological Controls (8)	34	34	0	100%
TOTAL	93	93	0	100%

8. Conclusion and Recommendations

8.1 Audit Conclusion

Based on the comprehensive internal audit conducted, Emirates Face Recognition demonstrates full compliance with ISO/IEC 27001:2022 requirements. The organization has established, implemented, and maintained an effective Information Security Management System (ISMS) that appropriately addresses information security risks and meets stakeholder requirements.

The audit team concludes that:

- All 93 controls specified in ISO 27001:2022 Annex A are properly implemented and maintained.
- Information security policies and procedures are well-documented, communicated, and followed.
- Security controls are operating effectively across all domains (Organizational, People, Physical, Technological).
- The organization demonstrates a mature security culture with appropriate management commitment.
- Risk management processes are well-established and continuously monitored.

8.2 Recommendations

While the organization maintains full compliance, the following recommendations are provided to ensure continued excellence:

- Continue regular internal audits to maintain compliance levels and identify emerging risks.
- Stay updated with the evolving threat landscape and adjust security controls accordingly.
- Maintain documentation of all security processes and ensure timely updates.
- Continue employee security awareness training programs.
- Regularly review and test business continuity and disaster recovery plans.

9. Approval and Sign-Off

Prepared By	Approved By
Ms. Jayasri Duraipandi	
Internal Audit Team	Mr. Ayham
Date: <u>28.06.2026</u>	Date: _____