AiVRIC

ISMS Continuous Monitoring Guide

Purpose

This guide outlines how continuous monitoring within an Information Security Management System (ISMS) is operationalized using Aivric to maintain ISO 27001 compliance, reduce risk, and ensure controls remain effective throughout the lifecycle of the ISMS.

---

1. Introduction to ISMS Continuous Monitoring

Continuous Monitoring (ConMon) is a core requirement of ISO 27001's ongoing performance evaluation and operational control obligations. The objective is to ensure security controls function as intended, remain effective, and adapt to environmental or organizational changes.

An effective ConMon program:

- Identifies control failures early
- Monitors risk indicators and threat exposure
- Ensures evidence is continuously collected for audits
- Aligns with Annex A controls and clauses 9 & 10 of ISO 27001
- Reduces manual governance fatigue

Aivric enables organizations to automate this continuous oversight across technical, administrative, and operational layers.

---

2. Continuous Monitoring Requirements (ISO 27001)

ISO 27001 requires ongoing performance evaluation through:

2.1 Clause 9 – Performance Evaluation

- **9.1 Monitoring, measurement, analysis, and evaluation**

- **9.2 Internal Audit requirements**
- **9.3 Management Review inputs and outputs**

2.2 Clause 10 – Improvement

- Addressing nonconformities
- Corrective action tracking
- Continual improvement

2.3 Annex A Control Families Supporting ConMon

- **A.5 Organizational Controls** – policies, governance, and oversight
- **A.8 Technological Controls** – protection, detection, and response
- **A.12 Operations Security** – logging, change management, vulnerability mgmt.
- **A.16 Information Security Incident Management**
- **A.18 Compliance Controls**

Aivric directly supports continuous monitoring across significantly all technical Annex A controls.

---

3. Aivric Continuous Monitoring Capabilities

Aivric enables a modernized, automated ConMon program through:

3.1 Control State Monitoring

- Hardening checks (CIS, NIST, cloud baseline)
- IAM configuration and privilege drift detection
- Endpoint & workload security posture
- Network segmentation & boundary control verification

3.2 Evidence Automation

- Auto-collection of logs, screenshots, configurations, and security data
- Time-stamped evidence mapped to ISO 27001 controls
- Evidence library for audit cycles and surveillance audits

3.3 Automated Reporting

- Monthly, quarterly, and on-demand ISMS performance reports
- Risk heatmaps and trending
- Control maturity scoring

3.4 Vulnerability & Threat Monitoring

- Continuous vulnerability scanning across cloud & endpoint assets
- Patch-status evaluations
- External exposure checks
- Correlation with threat intelligence for prioritization

3.5 Nonconformance & Corrective Action Tracking

- Automated generation of CAPA/NC findings
- Control-level POA&M items
- Integration into ISMS corrective action workflows

---

4. ISMS Continuous Monitoring Operating Model

4.1 Weekly Activities (Automated via Aivric)

- Scan cloud and identity control posture
- Validate critical Annex A controls
- Identify new misconfigurations or privilege drift
- Update vulnerability inventory

4.2 Monthly Activities

- Review automated ISMS performance dashboards
- Validate control evidence freshness (30–90 day cadence)
- Review new risks and update risk register entries

4.3 Quarterly Activities

- Full control effectiveness evaluation
- Consolidated ConMon report for Management Review inputs
- Documentation of nonconformities and planned corrective actions

4.4 Annual Activities

- Support internal audits with consolidated evidence volumes
- Support external audits & surveillance reviews
- Evaluate improvements and update ISMS scope, SoA, and risk treatments

---

5. ISMS KPIs & Metrics Powered by Aivric

Aivric supports measurement of:

- **Control Effectiveness Scores**
- **Compliance Coverage** (% of controls with current evidence)
- **Patch & Vulnerability Metrics**
- **IAM Metrics** (MFA coverage, privilege levels, inactive accounts)
- **Configuration Drift Count**
- **Incident & Alert Volume**
- **MTTD / MTTR indicators** (detect/respond timing)

These measurements feed the ISO-required evaluation cycles.

---

6. Evidence Requirements & Aivric Alignment

Evidence types supported:

- Configuration exports
- System logs
- Identity & access data
- Ticketing and remediation artifacts
- User activity summaries
- Asset inventories

Evidence automatically maps to ISO 27001 Annex A controls including:

- A.5, A.6, A.8, A.12, A.14, A.16, A.18

---

7. ConMon Roles & Responsibilities

Role	Responsibility
ISMS Manager	Ensures monitoring aligns with policy and risk management requirements
Security Operations	Responds to alerts, vulnerabilities, misconfigurations
System Owners	Implement corrective actions and maintain systems
Aivric Platform	Provides automated monitoring, evidence, and reporting

8. Output Artifacts

Common output deliverables include:

- Continuous Monitoring Dashboard
- Monthly ISMS Status Report
- Quarterly Posture Review
- Corrective Action/Nonconformity Logs
- Audit-Ready Evidence Exports

9. Continuous Improvement Loop

Aivric supports an iterative process:

1. **Monitor** controls and system posture continuously
2. **Detect** failures, misconfigurations, or risks
3. **Evaluate** control impact and root cause
4. **Correct** through POA&M/CAPA workflows
5. **Improve** ISMS documentation and security architecture

10. Summary

This guide provides a structured, repeatable framework for operating Continuous Monitoring within an ISMS using the Aivric platform. By automating evidence, maintaining control visibility, and reducing operational burden, organizations can demonstrate stronger compliance, improved risk management, and ongoing security assurance.