ShopSecure

INFORMATION SECURITY POLICY

Code: IS-P-001

Version: 0.1

Date of version: July 20, 2025

Author: Khuong Nguyen

Approver: ShopSecure Board Members

Confidentiality level: Internal

Change History

Date	Revision	Created by	Description of change
July 20, 2025	0.1	Khuong Nguyen	Customized for ShopSecure GRC framework

Table of Contents

1. Purpose, Scope and Users

The aim of this Policy is to establish ShopSecure's Governance, Risk, and Compliance (GRC) framework, ensuring secure operations for its AWS-based e-commerce platform with 50 employees. It applies to the entire Information Security Management System (ISMS), covering AWS S3 for customer data, EC2 for web hosting, as defined in the ISMS Scope Document. Users include all employees and external parties (e.g., AWS administrators). The policy addresses risks identified in risk_analysis.xlsx, such as MFA absence and public S3 buckets, aligning with COBIT, ISO 27001, and NIST CSF.

2. Reference Materials

The reference materials consist of the following:

- ISMS Scope Document
- ISO/IEC 27001:2022
- COBIT 2019 Framework (APO01, DSS05)
- NIST Cybersecurity Framework (CSF)
- Risk Analysis (risk_analysis.xlsx)
- MITTRE ATT&CK Framework

The materials can either be found online or are being attached.

3. Managing Information security

3.1 Objectives and Measurement

Objectives:

- Reduce security incidents by 20% within 12 months via proactive investigating (Prowler, Nessus).
- Achieve 100% compliance with ISO 27001 and NIST CSF within 6 months, addressing risks in risk_analysis.xlsx.

The Chief Information Security Officer (CISO) reviews objectives annually. Department heads propose control-specific objectives (e.g., 100% MFA adoption), approved by the CISO.

Measurements:

The CISO defines methods (e.g. Nessus patch compliance). Monthly measurements, reported quarterly to the CEO in the Measurement Report.

Key Performance Indicators (KPIs) (from risk_analysis.xlsx):

KPI	Target	COBIT	ISO 27001	NIST CSF	MITRE ATT&CK
MFA Adoption	100%	DSS05.01	A.5.17	PR.AA-05	T1078.004
S3 Block Public Access	100%	DSS05.01	A.5.15	PR.IR-01	T1133
CloudTrail Logging	100%	DSS05.07	A.8.15	DE.CM-03	T1562.002

- 100% MFA adoption for IAM users (A.5.17, PR.AA-05, mitigates T1078.004, T1110.002).
- 100% S3 bucket Block Public Access (A.5.15, PR.IR-01, mitigates T1133).
- 100% CloudTrail logging enabled (A.8.15, DE.CM-03, mitigates T1562.002).
- 95% high/medium Nessus vulnerabilities (e.g., SSL certificates) patched in 30 days (A.8.24, PR.AA-04).

3.2 Information Security Requirements

The ISMS complies with data protection laws, AWS agreements, and contractual obligations, as listed in the List of Legal, Regulatory and Contractual Obligations, ensuring risks like T1133 (public S3 access) are addressed.

3.3 Information Security Controls

Controls are selected per the Risk Assessment and Risk Treatment Methodology, documented in the Statement of Applicability, and informed by risk_analysis.xlsx. Key controls and mitigations:

- MFA for root/cli-security-audit accounts (A.5.17, PR.AA-05, T1078.004, T1110.002): Reduces ALE from €5.5M–€552M to €552K–€828M (cost: €1,000).
- S3 Block Public Access (A.5.15, PR.IR-01, T1133): Reduces ALE from €27.6M–€51.5B to €2.76M–€4.5B (cost: €2,000).
- Multi-region CloudTrail logging (A.8.15, DE.CM-03, T1562.002): Reduces ALE from €448K–€504M to €5.6K–€16.8M (cost: €1,000).
- Valid SSL certificates (A.8.24, PR.AA-04, T1040): Reduces ALE from €662K–€1.1B to €221K–€331M (cost: €500).
- IAM password policy (lowercase, expiration) (A.5.17, PR.AA-05, T1110.002, T1003.005): Reduces ALE to €22K–€88M (cost: €500 each).

3.4 Responsibilities

As for the responsiblities, the followings apply:

- CISO: Oversees Splunk SIEM, reviews Prowler/Nessus scans monthly, ensures ISO 27001 compliance (A.5.1.1), reports to CEO quarterly (APO01.02).

- IT Team: Runs Prowler (DSS05.01) and Nessus scans (DSS05.02), implements mitigations (e.g., MFA, S3 Block Public Access, CloudTrail logging) by 12/31/2025.
- CEO: Approves Policy, reviews quarterly risk reports (APO01.02).
- Security Analyst: Configures monitoring rules (e.g., failed logins >10), maintains logging/monitoring system (DSS05.07).

3.5 Process

- Monthly Risk Reviews (APO01.03): CISO/IT team analyze Prowler/Nessus findings, update risk_analysis.xlsx, prioritize mitigations (e.g., S3 Block Public Access, Critical, ALE €51.5B).
- Continuous Monitoring (DSS05.07): Logging system detects threats (e.g., T1078.004, T1133).
- Incident Response (DSS05.06): Alerts from monitoring system resolved within 24 hours.
- Quarterly Reporting (APO01.02): CISO reports risks/compliance to CEO.

3.6 MITRE ATT&CK Alignment

- T1078.004, T1110.002 (Valid Accounts): MFA, Logging system.
- T1133 (External Remote Services): S3 Block Public Access.
- T1562.002 (Impair Defenses): CloudTrail logging.
- T1040 (Network Sniffing): Valid SSL certificates.

4. Support for ISMS Implementation

- ShopSecure supports the ISMS by: Training employees on AWS security, Splunk, and mitigations (e.g., MFA setup).
- Allocating resources for Prowler, Nessus, Splunk.
- Aligning with COBIT (APO01, DSS05), ISO 27001 (A.5.1.1, A.5.15, A.5.17, A.8.15, A.8.24), NIST CSF (PR.AA-04, PR.AA-05, PR.IR-01, DE.CM-03).

5. Validity and Document Management

This Policy is valid upon CEO approval and reviewed annually or upon AWS/regulatory changes. The CISO manages updates, with version history recorded above.