Aberrant Open-ISM™

# ENTERPRISE RISK POLICY

| Property | Description |
|---|---|
| Document Version | 1.0 |
| Status | DRAFT |
| Last Update | 2022-03-25 |
| Document Owner | Risk Management |
| Next Scheduled Review | |

**PROPRIETARY**

| Document Approvals | | |
|---|---|---|
| **Approver Name** | **Title** | **Date** |
| ??? | ??? | ??? |

| Revision History | | | |
|---|---|---|---|
| **Version** | **Date** | **Description of Changes** | **Revised by** |
| 1.0 | 2022-03-25 | DRAFT | Aberrant |

# TABLE OF CONTENTS

# 1 OVERVIEW

Enterprise Risk Management Policy helps to identify vulnerabilities that pose a material risk to the company. Risks that are identified can be avoided, transferred, accepted, or mitigated. Once vulnerabilities are identified management can establish objectives and assign ownership to address issues.

The Enterprise Risk Policy is comprised of two parts:

- Risk Management that addresses vulnerabilities that have the potential to become material—it's in essence a counter-factual view of vulnerabilities that potentially threaten the enterprise.
- Corrective Actions, which address vulnerabilities, system issues, or process gaps that have been actualized and require action.

# 2 PURPOSE

The ultimate aim of this policy is to ensure effective reporting and compliance with applicable laws and regulations, and helps avoid damage to the company's reputation and helps to attenuate, or mitigate associated consequences. This is accomplished by:

- Aligning risk appetite and strategy: Management should consider the company's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- Establishing a readiness posture to minimize damage: The capability to identify potential events and establish responses, reduces surprises and associated losses to the company.
- Identifying opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities. Security done well can be a strategic asset for the company.
- Efficient allocation of capital – Obtaining risk information allows management to effectively assess overall capital requirements and prioritize effectively to align security priorities with budget realities.
- Continuous Improvement.

# 3 SCOPE

The scope of this document is related to how the organization identifies vulnerabilities and their associated impact to the company. This document should be considered supplemental to the Incident Response Procedure.

# 4 RISK MANAGEMENT

## 4.1 ENTERPRISE RISK ASSESSMENT AND PLANNING

A formal enterprise risk assessment is performed at least annually by senior management in order to identify internal and external threats and vulnerabilities that could potentially impair system commitments and requirements—an assessment should also be performed if a substantial change is made to company operations. <<Company Name>> assesses risks to information assets qualitatively by estimating the impact and likelihood of information security events within the organization.

### 4.1.1 FORMAL RISK ASSESSMENT

The formal risk assessment by management evaluates:

- the effectiveness of existing internal controls;
- vulnerabilities that could impair system commitments and requirements;
- the use of technology in business processes;
- internal and external threats and vulnerabilities that could impact security, availability, and confidentiality;
- types of fraud that could impact their business and operations, including risks such as unauthorized access; and,
- potential threats and vulnerabilities arising from its vendors and third parties.

Additional, changes to the enterprise are also evaluated during the annual assessment, namely:

- Changes to compliance and contractual requirements are considered and evaluated as part of the annual comprehensive risk assessment.
- Changes in job roles are considered and evaluated as part of the annual comprehensive risk assessment.
- Changes to, or outdating of, the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.
- Comparison to the previous Enterprise Risk Assessment.

Identified risks should be assessed against a matrix that evaluates the potential severity of each vulnerability and the probability of the vulnerability materializing. The ultimate aim is to assign a specified CVSS risk rank to each identified risk and to identify an owner: see Appendix A.

### 4.1.2 INDEPENDENT THIRD-PARTY RISK ASSESSMENT

A third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. The assessment is reviewed by management.

Issues that require corrective action are logged, assigned an owner, and prioritized for remediation.

### 4.1.3 TRIAGE

Once a risk has been identified management should evaluate the best way to approach the risk.

- Avoid the risk, identify was to alter the business model to avoid the risk entirely.
- Mitigate the risk, the current status quo is deemed inadequate and requires improvement.
- Transfer the risk, acquire a third party to address the risk.
- Accept the risk, the current status quo in conjunction with other controls is deemed adequate.

The annual Enterprise Risk Assessment is used to establish a posture based on an inventory of operational and security threats to the business, and serves as a justification for inclusions, or for exclusions of controls from Annex A of the ISO/IEC 27001:2013 standard. This information is also used in establishing Information Security objectives, planning, and budgeting.

## 4.2 INFORMATION SECURITY OBJECTIVES

Executive management uses information security objectives to align the goals of the organization with the ISMS program. The benefit of the creating security objectives is to consolidate known vulnerabilities in one location to facilitate transparency.

The Enterprise Risk Assessment is instrumental in identifying potential system or process gaps that could leave the company vulnerable to external and internal threats. As a result, management must use the annual risk assessment to identify opportunities to improve existing security and operational controls—and in some case identify controls that are wholly missing and need to be added. Security Objectives should be recorded in the company's Issues Queue. Documented objectives should be specific, measurable, attainable, relevant and time-bound (SMART).

**The 'SMART Goals' methodology.**

| | |
|---|---|
| **[S]pecific** | Objectives should be documented concisely and assigned an owner. |
| **[M]easurable** | Objectives should have a clear definition of success. Additionally, progress and outcomes should be quantifiable. All objectives should be assigned a CVSS score. |
| **[A]chievable** | Objective should be actionable and achievable within a reasonable timeframe. |
| **[R]elevant** | Objectives should be based on problem that impacts the business. |
| **[T]ime-bound** | Objectives must have a target date of resolution. |

## 4.3 CYBER-INSURANCE

In the event that management believes that a particular identified risk poses a substantial material hazard to <<Company Name>>, management may opt to purchase cyber-insurance to offset the financial loss that could result if the risk manifests itself as an incident.

# 5 CORRECTIVE ACTIONS

Vulnerabilities, system issues, or process gaps that have been identified and that pose an imminent threat to the business are required to be recorded in a centralized issue queue where they are triaged and assigned a corrective action plan. Process owners and management have a responsibility to investigate and troubleshoot control failures.

## 5.1 IDENTIFYING ISSUES

Management must consider the following sources to identify vulnerabilities, deviations and control gaps within the company's ISM documentation:

- Customer complaints.
- Internally or externally identified errors, or deviations from normal process.
- Changes in the business environment.
- Changes in the legal and regulatory environment.
- Assessment of external threats.
- The Enterprise Risk Assessment.
- Control effectiveness and maturity measurements.
- Internal and external audit results from compliance, control, and risk assessments.
- After action reviews of operational exceptions and root cause analysis.

Known vulnerabilities, or gaps in processes (henceforth referred to as 'issues') should be stored in a centralized reporting system, e.g. Issue Queue.

## 5.2 REPORTING FAILURES, ERRORS, AND ISSUES

Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the company's intranet. Notification of resolution should be event based.

## 5.3 CENTRALIZED LOCATION FOR DOCUMENTED ISSUES

Management shall document the entire process of corrective action via a centralized reporting system that is specifically designed to store and disseminate non-conformities. The system should incorporate a mechanism for identifying parties responsible for implementing corrective actions. The system should also disseminate information regarding non-conformities to ensure that the corrective action plans are followed in a timely manner. Documentation will be subject to the ISMS Document and Records Control Standard.

## 5.4 CVSS ASSIGNMENT

Issues should be evaluated, and assigned a specified CVSS risk rank: see Appendix A for more information. The assessment matrix evaluates the potential severity of each vulnerability and the probability of the vulnerability materializing. The issue can be assigned a CVSS ranking by the person who reported the issue, but it is the CISO that ultimately manages the 'Issue Queue' and who gets the final decision on the appropriate risk score for any issue. In the event that an issue is predicated on multiple controls with different CVSS risk rankings, the issue should be assigned a risk ranking from the control with the most risk.

## 5.5 ISSUE TRIAGE

Once the issue has been entered into the system a determination of what to do can be decided. Management has the option of addressing issues in one of four ways:

- Avoid the risk
- Mitigate the risk
- Transfer the risk
- Accept the risk

Decisions should be based on opportunity cost and ROI.

## 5.6 ISSUES THAT REQUIRE REMEDIATION

Issues that require remediation must be assigned an owner, a required date of completion, and a status. The issue queue should provide optional event notification when issues are remediated. Management should periodically review issues to ensure that issues are completed before their required date of completion. Additionally, an annual comprehensive review of risk assessment results must be reviewed and approved by appropriate levels of management. Vulnerabilities that have been identified and that require remediation must be remediated within the following timeline.

- Vulnerabilities which are ranked critical on the internal risk assessment will be remediated with seven (15) calendar days.
- Vulnerabilities which are ranked high on the internal risk assessment will be remediated with seven (30) calendar days.
- Vulnerabilities that are ranked medium on the internal risk assessment will be remediated within fourteen (45) days.
- Vulnerabilities that are ranked low should be remediated at the discretion of management as resource permit.

### 5.6.1 VULNERABILITIES THAT CANNOT BE REMEDIATED WITHIN THE RECOMMENDED TIMEFRAMES

In some cases it's not possible to remediated an issue within the recommended timeframe. In such cases, executive management can extend a corrective action to account for technical constraints or additional scope.

## 5.7 ROOT CAUSE ANALYSIS (RCA)

The purpose of a root cause analysis is to identify and memorialize the source of issues to identify patterns and implement corrective actions.
RCAs are an important component of continuous improvement. An RCA can be used to justify modification of Information Security Objectives, update policies and procedures in the control standard, or even change the scope of the program. Please see Appendix C which includes an RCA Corrective Action template.

## 5.8 AFTER ACTION REVIEW

Within a reasonable period after completing an RCA management should revisit the completed RCA to ensure that the continuous improvement recommendations included in the RCA have be operationalized.

## 6 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

## 7 DOCUMENT RACI

| | | |
|---|---|---|
| **Responsible** | Assigned to do the work | Security Program Manager |
| **Accountable** | Final decision, ultimately answerable | ISM Governance Committee |
| **Consulted** | Consulted BEFORE an action or decision is taken (proactive) | Executive Management |
| **Informed** | Informed AFTER a decision or action has been taken (reactive) | Named Participants in this document<br>Other parties affected by the change |

# 8 LICENSE INFORMATION

## APPENDIX A: RISK ASSESSMENT METHODOLOGY

<<Company Name>> uses the Common Vulnerability Scoring System (CVSS) methodology in order to align with the National Vulnerability Database (NVD) maintained by NIST to risk rank Common Vulnerabilities and Exposures (CVE)—this system is maintained by MITRE. <<Company Name>> CVSS uses an enumeration of five values: None, Low, Medium, High, and Critical. The CVSS score can also be represented by an integer that ranges from zero to ten where zero represents no risk and ten represents critical risk.

**CVSS Qualitative severity rating scale**

| Rating | CVSS Score |
|---|---|
| NONE | 0 |
| LOW | 0.1 - 3.9 |
| MEDIUM | 4.0 - 6.9 |
| HIGH | 7.0 - 8.9 |
| CRITICAL | 9.0 - 10.0 |

The risk matrix juxtaposes the significance of a potential incident versus the probability of the incident occurring.

**CVSS Rating: Incident Probability (P) versus Impact Significance (S)**

| | | | | | |
|---|---|---|---|---|---|
| **Near Certain (> 81%)** | MED (5,1) | MED (5,2) | HIGH (5,3) | CRITICAL (5,4) | CRITICAL (5,5) |
| **Likely (26-80%)** | LOW (4,1) | MED (4,2) | MED (4,3) | HIGH (4,4) | CRITICAL (4,5) |
| **Possible (6-25%)** | LOW (3,1) | MED (3,2) | MED (3,3) | MED (3,4) | HIGH (3,5) |
| **Unlikely (1-5%)** | LOW (2,1) | LOW (2,2) | MED (2,3) | MED (2,4) | MED (2,5) |
| **Remote (< 1%)** | NONE (1,1) | LOW (1,2) | LOW (1,3) | MED (1,4) | MED (1,5) |
| | **Insignificant** | **Minor** | **Moderate** | **Major** | **Extreme** |

Incident Significance should be evaluated from the perspective of the impact of the worst case scenario with existing operational controls in-place where the damage assessment falls within two standard deviations of a large number of sample of instances. An example, unmitigated a credential stuffing attack can have a severe impact on an organization, but with an operational 2FA control in place the significance should be considered 'insignificant'—especially when you limit the impact of extreme outliers: e.g. 2FA not working correctly.
Incident Significance descriptions:

**Insignificant**: Internal disruption; minor impact to normal operations.

**Minor**: Disruption visible to clients; impact to normal operations.

**Moderate**: Disruption visible to clients; substantial impact to operations; loss of revenue; possible brand damage.

**Major**: Disruption visible to clients; substantial impact to operations; loss of revenue; violation of internal RTO / RPO; loss of customers; impact on personnel; brand damage.

**Extreme**: Disruption visible to clients; substantial impact to operations; loss of revenue; violation of SLA; legal liability; damage to the brand; impact on sales; loss of customers; reputational damage with clients and vendors; impact on personnel.

## APPENDIX B: ENTERPRISE RISK TEMPLATE

| Identified Risk | Risk Owner | Probability | Significance | CVSS Rating | Trend | Action |
|---|---|---|---|---|---|---|
| Malware injected into Opensource | ISMS Manager | Near Certain | Major | Critical | ↑ | Mitigate |
| Undetected OWASP code vulnerabilities | ISMS Manager | Possible | Major | High | ↑ | Accept |
| External actor breach with PII exfiltration | ISMS Manager | Possible | Extreme | High | ↔ | Mitigate |
| Zero Day CVE | ISMS Manager | Near Certain | Moderate | High | ↔ | Accept |
| Compromised B2B Customer Credentials | ISMS Manager | Possible | Moderate | Medium | ↑ | Accept |
| Compromised Security Consultancy Credentials | ISMS Manager | Possible | Moderate | Medium | ↑ | Accept |
| Loss of PII as a result of regression bug | ISMS Manager | Possible | Major | Medium | ↑ | Accept |
| Multi-tenant SaaS customer PII leakage | ISMS Manager | Unlikely | Major | Medium | ↑ | Accept |
| System Misconfiguration | ISMS Manager | Near Certain | Minor | Medium | ↑ | Accept |
| Compromised Client Machine | ISMS Manager | Possible | Major | Medium | ↔ | Accept |
| Credential Stuffing Attack | ISMS Manager | Near Certain | Insignificant | Medium | ↔ | Accept |
| Domain Hijacking | ISMS Manager | Unlikely | Moderate | Medium | ↔ | Accept |

| | | | | | | |
|---|---|---|---|---|---|---|
| Encryption obsolescence / compromise | ISMS Manager | Remote | Major | Medium | ↔ | Accept |
| Internal actor breach incident with PII exfiltration | ISMS Manager | Unlikely | Major | Medium | ↔ | Accept |
| Loss of encryption key for KMS | ISMS Manager | Remote | Major | Medium | ↔ | Accept |
| Ransomware | ISMS Manager | Unlikely | Major | Medium | ↔ | Mitigate |
| Replay Attack | ISMS Manager | Near Certain | Insignificant | Medium | ↔ | Mitigate |
| SQL Injection | ISMS Manager | Near Certain | Insignificant | Medium | ↔ | Mitigate |
| Successful Phishing Attack | ISMS Manager | Unlikely | Moderate | Medium | ↔ | Mitigate |
| Theft of personal device | ISMS Manager | Possible | Extreme | Medium | ↔ | Mitigate |
| Trojan attack | ISMS Manager | Unlikely | Major | Medium | ↔ | Mitigate |
| Compromised artifacts | ISMS Manager | Unlikely | Major | Medium | ↓ | Mitigate |
| System inoperable from regression issue | ISMS Manager | Likely | Minor | Low | ↑ | Mitigate |
| Account takeover of admin account | ISMS Manager | Remote | Moderate | Low | ↔ | Accept |
| Cloud provider failure / SLA violation | ISMS Manager | Unlikely | Minor | Low | ↔ | Accept |
| DDOS | ISMS Manager | Near Certain | Minor | Low | ↔ | Transfer |

| | | | | | | |
|---|---|---|---|---|---|---|
| DNS Server Compromised | ISMS Manager | Unlikely | Low | Low | ↔ | Accept |
| Expired Cert | ISMS Manager | Likely | Minor | Low | ↔ | Transfer |
| Instance compromised with core dump | ISMS Manager | Unlikely | Minor | Low | ↔ | Mitigate |
| Invoice Fraud | ISMS Manager | Unlikely | Minor | Low | ↔ | Accept |
| LDAP Injection | ISMS Manager | Possible | Insignificant | Low | ↔ | Accept |
| Wire Fraud | ISMS Manager | Remote | Moderate | Low | ↔ | Accept |
| Spectre Attack | ISMS Manager | Remote | Insignificant | None | ↓ | Accept |

## APPENDIX C: INFORMATION SECURITY OBJECTIVES TEMPLATE

| # | Objective | Task | Results | Owner | Assigned To | Cost Center | Eval Criteria | Action Items | Next review | Evidence |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Demonstrate management commitment to, and support for, information security | Continual participation in Management Review of the ISMS on an semi-annual basis. | ISMS Steering Committee attendance and meeting minutes | ISMS Manager | ISMS Manager and ISMS Steering Committee | n/a | Completion of Meetings and Attendance Tracking , revision history of ISMS Documentation | Meetings held at least semi-annually | YYYY-MM-DD | Information Security Policy Statement; Information Security Manual; ISMS Steering Committee Meeting Minutes; |
| 2 | Establish directives and principles for action in regard to information security | Enforcement of the Information Security Manual and Information Security Policy through training and awareness, incident tracking and ISMS metrics. | Information Security Awareness training, incidents tracked, Technical Management Meeting (with meeting minutes). | ISMS Manager | ISMS Manager and ISMS Steering Committee | n/a | Completion of Training and number of incidents and review | 90% of all employees have completed annual training<br>90% of reported incidents have been fully documented and closed | YYYY-MM-DD | Vision and Traction; ISMS Steering Committee Meeting Minutes; |

## APPENDIX D: RCA CORRECTIVE ACTION

**Root Cause Analysis (RCA) Report**

| | | |
|---|---|---|
| **Issue ID** | | |
| **Owner** | | |
| **Issue Type** | | ['Operations Exception', 'Overdue Task', 'Incident Response'] |
| **Status** | | ['Not-Started', 'In-Process', 'Complete', 'Closed'] |
| **Affected Control(s)** | | |
| **CVSS Rating** | | |
| **Event Date** | | |
| **Event Duration** | | |
| **Event Description** | | |
| **Consequences** | | |

**Event Timeline**

| Date | Time | Duration | Person | Action |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

**Remediation Plan**

| Action Item | Link to Issue Tracking Ticket | Owner | Date of Completion |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Continuous Improvement**

| | | |
|---|---|---|
| **Resolution** | | |
| **Lessons Learned** | | |