INSERT LOGO

METRICS & REPORTING PLAN

Classification: **Internal**

This document may not be shared externally without written approval from the document owner.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Introduction

This document outlines the approach to metrics and reporting within the Information Security Management System (ISMS) to comply with ISO 27001 requirements.

This approach ensures that information security performance is effectively monitored, measured, analyzed, and evaluated to support continual improvement.

Objectives

- To establish a clear framework for defining, collecting, and analyzing metrics related to information security.
- To ensure regular reporting and review of ISMS performance.
- To identify areas for improvement and ensure timely corrective actions.
- To demonstrate compliance with ISO 27001 requirements.

Metrics and KPIs

The following metrics and key performance indicators (KPIs) have been identified to measure the effectiveness of the ISMS:

Metric	Description	Measurement Method	Frequency	Responsible Party
Number of Security Incidents	Total number of reported security incidents	Incident Management System	Monthly	IT Security Team
Time to Resolve Incidents	Average time taken to resolve security incidents	Incident Management System	Monthly	IT Security Team
Percentage of Employees Trained	Percentage of employees who have completed security awareness training	Training Management System	Quarterly	HR Department
Compliance Rate with Security Policies	Percentage of compliance with established security policies and procedures	Internal Audits	Quarterly	Internal Auditor
Number of Identified Vulnerabilities	Total number of vulnerabilities identified through regular scans and assessments	Vulnerability Scanning Tools	Monthly	IT Security Team
Risk Assessment Completion Rate	Percentage of planned risk assessments completed	Risk Management System	Quarterly	Risk Management Team
Audit Findings	Number of findings from internal audits	Internal Audit Reports	Quarterly	Internal Auditor
Corrective Actions Implemented	Percentage of corrective actions implemented within the agreed timeframe	Corrective Action Log	Quarterly	ISMS Manager

Measurement Methods

Each metric will be measured using the following methods:

- **Incident Management System** - Automated tools and manual logging of security incidents.
- **Training Management System** - Tracking completion rates of security awareness training programs.
- **Internal Audits** - Regular internal audits to assess compliance with security policies.
- **Vulnerability Scanning Tools** - Regular scans to identify vulnerabilities.
- **Risk Management System** - Documentation and tracking of risk assessments.
- **Corrective Action Log** - Logging and tracking corrective actions and their implementation status.

Reporting Schedule

Regular reporting will be conducted as follows:

- **Monthly Reports**: Metrics such as the number of security incidents, time to resolve incidents, and identified vulnerabilities will be reported monthly.
- **Quarterly Reports**: Metrics such as the percentage of employees trained, compliance rate with security policies, audit findings, and corrective actions implemented will be reported quarterly.
- **Annual Reports**: A comprehensive annual report summarising all metrics and KPIs for the year, including trends and recommendations for improvement.

Reporting Template

A standard reporting template will be used to ensure consistency:

Monthly Information Security Metrics Report

Metric	Current Period	Previous Period	Year-to-Date	Target	Status
Number of Security Incidents	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]
Time to Resolve Incidents (days)	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]
Percentage of Employees Trained	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]

Compliance Rate with Security Policies	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]
Number of Identified Vulnerabilities	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]
Risk Assessment Completion Rate	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]
Audit Findings	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]
Corrective Actions Implemented	[Current Value]	[Previous Value]	[YTD Value]	[Target]	[Status]

Summary and Analysis:

- **Key Trends**: [Describe key trends observed]
- **Anomalies**: [Describe any anomalies detected]
- **Actions Taken**: [Detail any corrective actions implemented]
- **Recommendations**: [Provide recommendations for improvement]

Prepared By: [Name, Role]
Date: [Date]
Reviewed By: [Name, Role]

Management Review

The results of the metrics and analysis will be presented to top management during regular management review meetings.

The reporting will ensure that management is aware of the ISMS performance and can make informed decisions on improvements and resource allocation.

Continual Improvement

The ISMS will be continuously reviewed and improved based on the metrics and reporting.

Corrective and preventive actions will be taken to address any identified issues, and opportunities for improvement will be implemented.