METRICS AND MEASUREMENT METHODOLOGY

Document Revision History

Version	Document No:	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/MMM/POL/026	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/MMM/POL/026	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/MMM/POL/026	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/MMM/POL/026	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/MMM/POL/026	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/MMM/POL/026	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/MMM/POL/026	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 INTRODUCTION

<Company Overview>

2 ABOUT METRICS AND MEASUREMENT

ISO 27004 International Standard that address the specification of an privacy information management system(PIMS) This particular standard provides guidance and advice in support of the monitoring and measurement requirements for ISMS as specified in ISO 27001.

This International Standard is also applicable to any organization that has an information security and privacy information management. Programme and that wishes to make measurements concerning information security and privacy information management. The use of this standard will allow organizations to answer the question how effective and efficient the information security and privacy information management programme is and what degree of implementation and maturity has been achieved. Use of measurements will allow comparison of achieved information security and privacy outcomes over a period of time and between similar business areas in the organization as part of continuous improvement.

3 DEFINITIONS

- Measure

  Variable to which a value is assigned as the result of measurement [ISO/IEC 15939:2002]

- Measurement

  The action or set of actions that make it possible to obtain the value of a measurement for the attribute of an entity using a form of measurement

- Metric

  Derived through analysis applied to measurements

  Provide quantitative data about a target process or asset in order to achieve an explicit purpose

  Truly useful metrics provide the incite needed to make better decisions

  Defines what, where, and how risk is occurring

- Object

  A business object is a business process, business unit, system or location. E.g. Antivirus

- Attribute

  Property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means [ISO/IEC 15939:2002]. E.g. Antivirus installation, Signature updation.

4 WHAT DOES THE ISO 27004 STANDARD SAYS?

The purpose of the information security and privacy information management measurements development and implementation process, defined in ISO 27004 is to create a base for organization to collect, analyse and communicate data related to ISMS processes. This data is ultimately to be used to base ISMS-related decisions and to improve implementation of an ISMS.

This International Standard supports the requirements of the ISMS Plan – Do – Check – Act (PDCA) cycle. Measures are used mainly for the measurement of the of the "Do" components of an ISMS (Implement and operate the ISMS) as input to the "Check" (monitor and review) components of an ISMS, with the goal of providing a means for taking decisions at the "ACT" (maintain and improve the ISMS) stage, leading to continuous improvement of the ISMS cycle.

Measurements should be integrated into the management cycle of the organization and used to effect improvement of security-related processes and outcomes within the project or organization.

OBJECTIVES

- Evaluate security controls implementation effectiveness.
- Evaluate the information security and privacy information management system effectiveness including continuous improvement.
- Provide security status to guide management review, facilitate security improvements, and provide input for security audits.
- Communicate value of security to the organization.
- Serve as an input into risk assessment and risk treatment plan

PLAN

1. Identify and list the possible Technical and Process control objects and attributes for measurement from

    - Risk Assessment – Risk Treatment Plan (RA RTP)
    - ISO 27001 Control Objectives
    - ISMS Policies and Procedures
    - IT Operational Procedures

2. Select Technical and Process control objects, attributes for Measurement on the following criteria

    - Analyze and check for availability of data sources
    - Analyze Measures for feasibility of periodical measurement and trend analysis

DO

Define Metrics for selected attributes of the objects

- Each attribute metric must be defined with the following metric types
    - Implementation Metric
    - Effectiveness metric
    - Impact Metric
- Mention Clauses, Control objectives and control reference to ISO 27001
- Mention related records reference (like RARTP, Policies and Procedures)
- Mention data source location
- Identify Frequency of data collection
- Identify person responsible to ensure data availability, collection and measurement

Develop metrics Dashboard for Overall view of Metrics and Measurements

- Create a Dashboard to show summary of all departmental metrics. Dashboard should consists of the following
    - Input for departmental Summary page
    - Display of Departmental and Overall summary of the organization
    - Graphical representation of Metrics and its Trends
    - Map Metrics effectiveness to ISO 27001 Controls

Create Policy and Procedures for Metrics, which should include

- Metrics Development, Review and approval procedure

Development Stage

- For each department, a person should be identified for Metrics & Measurements Activities
- Metrics will be identified by the consultant with the help of identified person.
- Consultant will gather all information related to each metric of the department.
- Final Metrics developed by consultant for each department.

Review

- Developed Metrics must be Reviewed by each department Head
- Then Review will be done by COO.

Approval

- The Identified and reviewed Metrics shall be discussed and approved by the Information Security and Privacy Steering Committee(ISPSC)

- Roles and Responsibilities for Data availability, collection and measurement

  COO

- Final Reviewer of Metrics and recommends for ISPSC Approval
- Reviewer and Co-ordinator of entire Metrics and Measurements Process
- Reviewer of their departmental Metrics
- Ensures data availability and reports measurements at periodical intervals as per schedule.

  Member

- Procedures for Data collection, Analysis and reporting
- Management Review, Corrective and Preventive Action

Create a schedule for data collection

CHECK

1. Collect Data as per the schedule
2. Enter collected data into the metrics
3. Feed collected metrics to the metrics dashboard
4. Prepare report on the results arrived with recommendations to mitigate any deviations

ACT

1. Take Action to improve effectiveness of the weak controls
2. Create Corrective and Preventive Action (CAPA) report
3. Conduct Periodical Management review Meeting
4. Record MoM

5 BENEFITS OF MEASURING SECURITY

Eases process of monitoring the effectiveness of the ISMS (e.g. less labor intensive, for example, if using tools, and provides a means of self-checking)

Proactive tools to measure can prevent problems arising at a later date (e.g. network bottlenecks, disk clutter, development of poor human practices)

Reduction of incidents

Motivates staff when senior management set targets

Tangible evidence to auditors, and assurance to senior management that you are in control – i.e. Corporate Information Assurance (Corporate Governance), and top down approach to Information Assurance.

6 ASSOCIATED DOCUMENT

- Metrics process document

7 DOCUMENT MAINTENANCE

- Chief Operating Officer shall be responsible for document control and any changes.
- Updates shall be discussed in the ISMF under the guidance of COO.
- COO shall forward the document to Chairperson of the ISPSC for approval, after review.

End of Document