CORE SYSTEM
CONSULTANT

Defining Information Security Objectives / Metrices for ISO 27001:2022 Information Security Management System

In establishing an information security management system based on ISO 27001:2022, defining and implementing practical information security objectives is a key requirement and vital for protecting sensitive data and maintaining organizational integrity. Tracking key performance indicators (KPIs) such as security incidents, detection and response times, and user training completion rates helps assess and improve your Information Security Management System (ISMS). Regularly monitoring these metrics, patch management, phishing simulation results, and NCR rates provide insights into the effectiveness of security measures. This approach protects your organization from threats and promotes continual improvement and resilience against evolving cyber risks.

Below are some sample ISMS objectives/measurement metrics (with examples) that can be selected and used:

1. Number of Vulnerabilities Identified

Definition: The total number of vulnerabilities found in systems and applications.

Purpose: Indicates the effectiveness of vulnerability management and scanning processes.

Example:

Monthly vulnerability scans detect 50 vulnerabilities in January, 40 in February, and 30 March. A decreasing trend in identified vulnerabilities shows an improved security posture.

2. Number of Security Incidents

Definition: The total count of security incidents within a specific period.

Purpose: Measures the overall effectiveness of the ISMS in preventing incidents.

Example:

January: 5 incidents

February: 3 incidents

March: 7 incidents

If the number of incidents decreases over time, the ISMS is becoming more effective. An increase may indicate the need for more robust controls or additional training.

Note1: the number of incidents can be further categorized as high/medium/low-level incidents, and each category can be further elaborated

Note 2: the number of incidents can also be categorized as Data breaches, Access control violations (logical/physical), Application failures, Server/s downtime, Connectivity issues etc.

The above categorization helps in directing the efforts for specific resolutions, corrective actions and monitoring

3. Mean Time to Respond (MTTR)

Definition: The average time to respond and mitigate a security incident.

Purpose: Assesses the responsiveness and effectiveness of incident response procedures.

Example:

Incident 1: Responded to in 3 hours

Incident 2: Responded to in 5 hours

Incident 3: Responded to in 4 hours

MTTR = (3 + 5 + 4) / 3 = 4 hours

A lower MTTR suggests an efficient response process, minimizing potential impact.

Note: MTTR can also be used for the tickets opened and closed at the help desk.

4. Mean Time to Detect (MTTD)

Definition: The average time taken to identify a security threat or incident.

Purpose: Evaluate the efficiency of monitoring and detection processes.

Example:

Incident 1: Detected in 4 hours

Incident 2: Detected in 6 hours

Incident 3: Detected in 2 hours

MTTD = (4 + 6 + 2) / 3 = 4 hours

A lower MTTD indicates a quicker detection time, crucial for minimizing damage.

Note: the MTTD can again be categorized as related to high/medium/low-level incidents

5. Incident Resolution Rate

Definition: The percentage of security incidents resolved within a defined timeframe.

Purpose: Evaluate the efficiency of incident management processes.

Example:

20 incidents occurred; 18 were resolved within the SLA.

Resolution Rate = (18/20) 100 = 90%

A higher resolution rate signifies efficient incident management.

Note: this can be further categorized as per the nature of the incidents as defined in no

6. User Awareness Training Completion Rate

Definition: The percentage of employees who have completed information security awareness training.

Purpose: Reflects the organization's commitment to educating employees about security practices.

Example:

200 employees in the company, 180 completed the training.

Training Completion Rate = (180/200) 100 = 90%

High completion rates correlate with better overall security awareness.

Note: this can be further enhanced by adding a quiz at the end of the training, and based on the total scores acquired by the employee, an 'employee Information Security awareness index' can also be established and monitored

7. Phishing Simulation Results

Definition: The percentage of employees who successfully identify and report phishing attempts during simulations.

Purpose: Assesses the effectiveness of user training programs and awareness.

Example:

100 employees are tested; 80 identify and report the phishing attempt.

Success Rate = (80/100) 100 = 80%

Higher success rates indicate better training effectiveness.

8. Backup and Recovery Success Rate

Definition: The percentage of successful data backups and recoveries.

Purpose: Evaluate the effectiveness of data backup and disaster recovery processes.

Example:

100 backups attempted; 95 successful.

Backup Success Rate = (95/100) 100 = 95%

A higher rate indicates a reliable backup and recovery process.

9. Conformity Rate

Definition: The percentage of systems and processes conforming to ISO 27001 requirements and internal security standards.

Purpose: Measures the organization's adherence to standards and the company's requirements.

Example:

20 systems audited; 15 are conforming.

Conformity Rate = (15/20) 100 = 75%

Higher conformity rates reflect better alignment with requirements.

10. Third-party Compliance

Definition: The number of third-party vendors assessed and their compliance status.

Purpose: Assesses the security posture of third-party vendors and partners.

Example:

10 vendors were assessed; 8 found compliant.

Compliance Rate = (8/10) 100 = 80%

High compliance rates among vendors ensure better overall security.

Conclusion

Tracking these KPIs provides a comprehensive view of the effectiveness of an ISMS. By regularly reviewing and analyzing these KPIs/metrics, organizations can improve their security posture, ensuring they are well-protected against potential threats and conforming to standard requirements.

Syed Arshad Hashmi
Director & Principal Consultant/Trainer/Auditor
Cell: +1 832 3736812