ISMS Risk Assessment Methodology

Purpose

This document defines the methodology used to identify, evaluate, and treat information security risks within the scope of the ISMS. It ensures consistent, repeatable, and auditable risk assessment aligned with ISO/IEC 27001:2022.

Scope

Applies to all information assets, systems, processes, and departments within the defined ISMS scope of Technet Solutions (including software development, QA, support, and IT infrastructure).

Risk Assessment Objectives

- Identify threats and vulnerabilities affecting information assets.
- Determine the likelihood and impact of identified risks.
- Prioritize risks for treatment based on their severity.
- Ensure risk acceptance decisions are justified and documented.

Risk Assessment Criteria

Risk = Likelihood × Impact

Likelihood Levels:

1. Rare - May occur in exceptional circumstances
2. Unlikely - Could happen but not expected
3. Possible - Might happen occasionally
4. Likely - Expected to happen
5. Certain - Will occur frequently

Impact Levels:

1. Insignificant - Minimal effect on operations or data
2. Minor - Limited disruption or small financial loss
3. Moderate - Noticeable disruption or financial/legal concern
4. Major - Significant disruption or legal violation
5. Critical - Severe business impact or breach of critical data

Risk Classification Matrix

ISMS Risk Assessment Methodology

Risk Matrix (Simplified):

L = Low, M = Medium, H = High, C = Critical

Higher values of likelihood and impact lead to more severe risks.

Risk Treatment Options

- Treat: Implement controls to reduce the risk.
- Tolerate (Accept): Accept the risk if within tolerance level.
- Transfer: Outsource or insure against the risk.
- Terminate: Discontinue the process causing the risk.

Risk Acceptance Criteria

- Low risks: May be accepted with minimal review.
- Medium risks: Require management approval and monitoring.
- High/Critical risks: Must be treated or formally accepted by senior management.

Documentation Requirements

- Risk Register: All identified risks, likelihood, impact, and status.
- Risk Treatment Plan (RTP): Describes how each risk will be managed.
- Statement of Applicability (SoA): Justifies control selection based on risk results.

Review and Updates

Risk assessments shall be reviewed annually or upon major changes (e.g., new systems, mergers). The methodology is reviewed annually and updated as needed.

References

- ISO/IEC 27001:2022 - Clause 6.1.2 and 6.1.3
- ISO/IEC 27005:2018 - Information Security Risk Management