NimbusTech Solutions, Inc.

Risk Assessment & Treatment Methodology

ISO 27001:2022

Table of contents

1. Document Control

Document ID: NT-ISMS-RM-001
Version: 1.0
Date: August 15, 2025
Owner: Laura Chen, ISMS Manager
Approved By: Rajesh Patel, CISO

2. Purpose

The purpose of this document is to define NimbusTech's methodology for identifying, analyzing, evaluating and treating information security risks in accordance with ISO/IEC 27001:2022 Clauses 6.1.2 and 6.1.3.

3. Scope

This methodology applies to all information assets, business processes, supporting IT systems, and third-party services within the scope of NimbusTech's ISMS.

4. Risk Assessment Methodology

4.1. Risk Identification

Risks will be identified through:

- Asset inventory reviews.
- Threat and vulnerability analysis.
- Incident reports and audits.
- Legal, regulatory and contractual requirements.

Roles & Responsibilities:

- **ISMS Manager** - Facilitates the risk assessment process.
- **Asset Owners** - Provide input on risks related to their systems and processes.
- **CISO** - Provides oversight and approves risk assessment results.

4.2 Risk Analysis

Each Identified risk will be analyzed based on:

- **Likelihood Scale** (1-5):
  - 1 = Rare, 5 = Almost Certain
- **Impact Scale** (1-5):
  - 1 = Negligible, 5 = Critical (e.g. major financial loss, regulatory fines)
- **Risk Rating :** Likelihood * Impact = Risk Score (1-25)

4.3 Risk Evaluation

- Risks are plotted on a Risk Matrix (Low, Medium, High, Critical).
- Risks above the defined risk appetite (≥12) must be treated.
- Risk scoring thresholds:
  - 1-8 : Acceptable
  - 9-11 : Requires management review.
  - ≥12 : Unacceptable, must be treated.

4.4 Risk Treatment

For risks above the acceptance threshold, NimbusTech will apply one of the following:

- Avoid - discontinue risky activity.
- Mitigate - apply controls to reduce likelihood/impact.
- Transfer - outsource or insure against the risk.
- Accept - acknowledge the risk with management approval.

Treatment decisions must be documented in the Risk Register and linked to the SoA.

4.5 Risk Acceptance Criteria

- Risks with residual score ≤ 8 are considered acceptable.
- Risks with a residual score 9-11 require review and approval by the CISO and Executive Management.
- All risk acceptance decisions must be formally documented and signed off by the CISO.

4.6 Risk Review & Monitoring

- Risk Assessment will be conducted:
  - Annually.
  - Following major incidents.
  - After significant organizational or technical changes.
- Results will be reported in Management Reviews.

5. Documentation & Records

The following records will be maintained:

- **Risk Register** - full list of risks, scores, and treatments.
- **Statement of Applicability (SoA)** - mapping of controls to risks.
- **Risk Treatment Plan** - actions, owners, deadlines.

6. Review & Approval

This Risk Methodology will be reviewed annually and updated as necessary.

Approved By:
Rajesh Patel - CISO
Date: August 15, 2025