Risk Assessment Policy

Doorway

SOC 2 Criteria: CC3.1, CC1.2, CC2.1, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Keywords: Risk assessment, Threat impact, Threat likelihood, Risk score, Risk remediation

---

Purpose

The purpose of this policy is to define the methodology for the assessment and treatment of information security risks within Doorway, and to define the acceptable level of risk as set by Doorway's leadership.

Scope

Risk assessment and risk treatment are applied to the entire scope of Doorway's information security program, and to all assets which are used within Doorway or which could have an impact on information security within it. This policy applies to all employees of Doorway who take part in risk assessment and risk treatment.

Background

A key element of Doorway's information security program is a holistic and systematic approach to risk management. This policy defines the requirements and processes for Doorway to identify information security risks. The process consists of four parts: identification of Doorway's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

Policy

Risk Assessment

- The risk assessment process includes the identification of threats and vulnerabilities having to do with company assets.

- The first step in the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets which may affect the confidentiality, integrity, and/or availability of information in the organization. Assets may include documents in paper or electronic form, applications, databases, information technology equipment, infrastructure, and external/outsourced services and processes. For each asset, an owner must be identified.
- The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities must be listed in a risk assessment table. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities.
- For each risk, an owner must be identified. The risk owner and the asset owner may be the same individual.
- Once risk owners are identified, they must assess:
    - Impact for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.
    - Likelihood of occurrence of such a risk (i.e. the probability that a threat will exploit the vulnerability of the respective asset).
    - Criteria for determining impact and likelihood are defined in the tables below.
- The risk level is calculated by multiplying the impact score and the likelihood score.

Description of Impact Levels and Criteria:

Impact (Score)	**Definition**
Incidental (1.0)	• Minimal financial loss • Local media attention quickly remedied • Not reportable to regulator • Isolated staff dissatisfaction
Minor (2.0)	• Minor financial loss • Local reputational damage • Reportable incident to regulator, no follow up • General staff morale problems and increase in turnover
Moderate (3.0)	• Moderate financial loss • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Widespread staff morale problems and high turnover
Major (4.0)	• Significant financial loss • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
Extreme (5.0)	• Massive financial loss • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Multiple senior leaders leave

Description of Likelihood Levels and Criteria:

Likelihood (Weight Factor)	**Definition**
Rare (1.0)	Once in 100 years or less (<10% chance of occurrence over the life of the company)
Unlikely (2.0)	Once in 50 to 100 years (10% to 35% chance of occurrence over the

	life of the company)
Possible (3.0)	Once in 25 to 50 years (35% to 65% chance of occurrence over the life of the company)
Likely (4.0)	Once in 2 to 25 years (65% to 90% chance of occurrence over the life of the company)
Almost Certain (5.0)	Up to once in 2 years or more (90% or greater chance of occurrence over the life of the company)

Risk Rating Criteria:

Risk Rating:
Low Risk: Less than or equal to 4.0
Medium Risk: Greater than 4.0 but less than or equal to 9.0
High Risk: Greater than 9.0 but less than or equal to 16.0
Critical Risk: Greater than 16.0

Risk Rating Matrix:

RISK SCORE MATRIX						
		Impact				
		INCIDENTAL (1.0)	**MINOR (2.0)**	**MODERATE (3.0)**	**MAJOR (4.0)**	**EXTREME (5.0)**
Likelihood	**RARE (1.0)**	**LOW** 1.0 x 1.0 = 1.0	**LOW** 1.0 x 2.0 = 2.0	**LOW** 1.0 x 3.0 = 3.0	**MEDIUM** 1.0 x 4.0 = 4.0	**MEDIUM** 1.0 x 5.0 = 5.0

	UNLIKELY (2.0)	**LOW** 2.0 x 1.0 = 2.0	**MEDIUM** 2.0 x 2.0 = 4.0	**MEDIUM** 2.0 x 3.0 = 6.0	**MEDIUM** 2.0 x 4.0 = 8.0	**HIGH** 2.0 x 5.0 = 10.0
	POSSIBLE (3.0)	**LOW** 3.0 x 1.0 = 3.0	**MEDIUM** 3.0 x 2.0 = 6.0	**MEDIUM** 3.0 x 3.0 = 9.0	**HIGH** 3.0 x 4.0 = 12.0	**HIGH** 3.0 x 5.0 = 15.0
	LIKELY (4.0)	**MEDIUM** 4.0 x 1.0 = 4.0	**MEDIUM** 4.0 x 2.0 = 8.0	**HIGH** 4.0 x 3.0 = 12.0	**HIGH** 4.0 x 4.0 = 16.0	**CRITICAL** 4.0 x 5.0 = 20.0
	CERTAIN (5.0)	**MEDIUM** 5.0 x 1.0 = 5.0	**HIGH** 5.0 x 2.0 = 10.0	**HIGH** 5.0 x 3.0 = 15.0	**CRITICAL** 5.0 x 4.0 = 20.0	**CRITICAL** 5.0 x 5.0 = 25.0

Risk Remediation

- As part of this risk remediation process, the Company shall determine objectives for mitigating or treating risks. All high and critical risks must be treated. For continuous improvement purposes, company managers may also opt to treat medium and/or low risks for company assets.
- Treatment options for risks include the following options:
    - Selection or development of security control(s).
    - Transferring the risks to a third party; for example, by purchasing an insurance policy or signing a contract with suppliers or partners.
    - Avoiding the risk by discontinuing the business activity that causes such risk.
    - Accepting the risk; this option is permitted only if the selection of other risk treatment options would cost more than the potential impact of the risk being realised.
- After selecting a treatment option, the risk owner should estimate the new impact and likelihood values after the planned controls are implemented.

Regular Reviews of Risk Assessment and Risk Treatment

- The Risk Assessment Report must be updated when newly identified risks are identified. At a minimum, this update and review shall be conducted **once per year**.

Reporting

- The results of risk assessments, and all subsequent reviews, shall be documented in a Risk Assessment Report.

Revision History

Version	Date	Editor	Description of Changes
1.0	15.03.2022	Henry Sinclair	Initial Creation