Risk Assessment Policy

Nexelus

Purpose

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

Scope

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

Background

A key element of Nexelus' information security program is a holistic and systematic approach to risk management. This policy defines the requirements and processes for Nexelus to identify information security risks. The process consists of four parts: identification of Nexelus' 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 which could be an individual or a team.
- 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 or team.
- 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:

Risk Level is calculated as Cross Product of Service Weightage, Risk Value and Risk Impact Value.

Service Weightage: All risks are categories into different Service categories. Each service category is given weightage based on their importance. Networks, Support, HR, etc are given different weightage.

Service Weightage

Service Weightage	Value
Critical	3
Medium	2
Low	1

Risk Value: Risk value defines probability of occurrence of a risk.

Risk Values

Probability	Risk	Value
If occurs once or more in a week	Certain	5
if occurs in 2 to 4 months	Likely	4
If occurs in 4 to 6 months	Possible	3
If occurs once or more in six months	Unlikely	4
If occurs once or more in a year	Rare	1

Risk Impact Value: Risk Impact Value defines how much a risk will impact business if it occurs.

Risk Impact

Impact Value	Risk	Value
Business Operations are affected for more than client SLA	Critical	4

Business Operations are affected within limits defined with client SLA	High	3
Disruption in operational or business operations within accepted limits of SLA	Medium	2
Disruption in service(s) but have no impact in SLA	Low	1

Risk Level: Risk level is a cross product of Service Weightage, Risk Value and Risk Impact Value. A Risk with Critical and High level will be treated.

Risk Level = SERVICE VALUE x PROBABILITY x IMPACT

Risk Level		
Risk Level	**Risk**	**Value**
Greater than 16.0	Critical	4
Greater than 9.0 but less than or equal to 16.0	High	3
Greater than 4.0 but less than or equal to 9.0	Medium	2
Less than or equal to 4.0	Low	1

Risk Remediation and Treatment

- 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).
    - 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 realized.
- 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.