

Pgogy Webstuff Ltd.

Registered company number:10681846

Assessment and Treatment of Information Security Risks Policy

Version 1.0

Last updated 5 February 2024

Scope
This procedure covers the following:

1. Risk assessment process.
2. Risk treatment process.

Risk assessment
An information security risk assessment for the entire organisation is carried out when significant changes are proposed or occur, taking account of the established criteria.

Pgogy Webstuff's information security risk assessment process seeks to:

- establish and maintain information security risk criteria that includes:
    - the risk acceptance criteria
    - criteria for performing information security risk assessments
- ensure that repeated information security risk assessments produce consistent, valid and comparable results
- identify the information security risks:
    - apply the information security risk assessment process – to identify risks associated with the loss of confidentiality, integrity, and availability of information within the scope of the information security management system
    - identify the risk owners
- analyse the information security risks
- assess the potential consequences that would result if the risks were to materialise:
    - assess the realistic likelihood of the occurrence of the risks
    - determine the levels of risk
- evaluate the information security risks:
    - compare the results of risk analysis with the risk criteria
    - prioritize the analysed risks for risk treatment

Defining the risk criteria
When defining risk criteria, factors that must be considered include:

- the nature and types of causes and consequences that can occur and how they will be measured
- how likelihood will be defined
- the timeframe(s) of the likelihood and/or consequence(s)
- how the level of risk is to be determined
- the views of stakeholders
- the level at which risk becomes acceptable or tolerable
- whether combinations of multiple risks should be taken into account – if so, how and which combinations should be considered

Risk Assessment Methodology

We've developed our criteria for accepting risks and identifying the acceptable levels of risk.

The selected risk assessment methodology is expected to ensure that risk assessments produce comparable and reproducible results.

The methodology being followed is summarised below.

Identification of information security risks

At this stage, we identify the:

- assets within scope and the owners of these assets
- risks associated with the loss of confidentiality, integrity and availability of information within the scope of the information security management system
- risk owners
- vulnerabilities that could be exploited by the risks (threats)
- assets that are impacted by the risk by way of loss of confidentiality, integrity and/or availability

Analysis and evaluation of the risks

At this stage, we:

- assess the business impact on the organisation that might result from security failures – taking into account the consequences of a loss of confidentiality, integrity or availability of the assets
- assess the realistic likelihood of security failures occurring in light of prevailing threats and vulnerabilities – impacts associated with these assets, and the controls currently implemented
- estimate the levels of risks in numerical terms (Risk Number)
- determine whether the risks are acceptable or require treatment using our criteria for accepting risks
- prioritise the analysed risks for risk treatment

Risk Number is computed as below:

Risk Number (RN) = Impact Score x Likelihood Score x Controllability Score x Legal Requirements Score

Scoring Guidelines

Score	Impact	Likelihood	Controllability	Legal Requirements
1	Minor	Very unlikely	Essentially avoidable through mitigation actions	No – there's no legal requirement
2	Moderate	Somewhat likely	Highly controllable through actions	

3	Significant	50/50 Chance	Moderately controllable through actions	
4	Very significant	Highly likely	Largely uncontrollable	
5	Disastrous	Nearly Certain	Uncontrollable	
10				Yes – there's legal requirement

Example evaluation:

Risk is seen as Moderate (2) + Highly likely (4) + Uncontrollable (5) but no legal requirement. Risk Number (RN) = 11

Pgogy Webstuff's criteria for accepting risks

The identified risk requires treatment if the Risk Number (RN) > 8 or Legal Requirement score = 10, otherwise the risk is acceptable.

The Head of Sustainability, Strategy, and Scale records the evaluations and prioritizes the analysed risks on the basis of Risk Number (RN) for risk treatment.

Head of Sustainability, Strategy, and Scale then prepares a detailed 'Risk Assessment Report' and submits to the Director.

Risk Treatment

Risk owners would, in consultation with the owners of information assets impacted by the risk and the Director, try to find out appropriate methods to eliminate or lower the risk.
In Pgogy Webstuff, the Director takes the responsibility for the preparation of risk treatment plan.

Steps of risk treatment

The steps involved in risk treatment are as following:

1. Selection of appropriate information security risk treatment options, taking account of the risk assessment results (one or more of the following):
    - apply appropriate controls
    - knowingly and objectively accepting risks – if they clearly satisfy Pgogy Webstuff's policies and the criteria for accepting risks
    - avoid risks
    - transfer the associated business risks to other parties (insurers, suppliers)

2. Determine all controls that are necessary to implement the information security risk treatment option(s) chosen:
    - select and implement control objectives and controls to meet the requirements identified by the risk assessment and risk treatment process

Formulating an information security risk treatment plan

The Head of Sustainability, Strategy, and Scale prepares a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks.
Even after risk treatment, there could still be residual risk. These residual risks are also identified and mentioned in the risk treatment plan.

Implementation of risk treatment plan

The Director would oversee the implementation of the risk treatment plan, and report the status of risk assessment and risk treatment to the top management. This should be during the subsequent management review, held at an interval of 6 months.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the Director.

Policy exceptions must describe:

- the nature of the exception
- a reasonable explanation for why the policy exception is required
- any risks created by the policy exception
- evidence of approval by all appropriate parties