Risk Management Procedure

Reference: ISMS DOC 6.1
DocumentKits Issue No: 1.1
Organisation Issue No:
DocumentKits Issue Date: 01/06/2020
Organisation Issue Date:

1. Scope

This applies to the risk management framework in Organisation Name and will be conducted in line with the Context of the Organisation Procedure and the Identification of Interested Parties Procedure.

2. Responsibilities

2.1 The Information Security Manager is responsible identifying risks to the information security management system (ISMS), and for ensuring that all information security and privacy issues have been included and appropriately treated.

3. Risk management

3.1 Risk management is conducted within the internal and external context of Organisation Name, as identified in the Context of the Organisation Procedure.

3.2 Risk management takes Organisation Name's legal and regulatory requirements into account, as identified in the Identification of Interested Parties Procedure.

3.3 The Information Security Manager defines risk criteria accordingly:

3.3.1
"Describe how risks will be defined – most commonly, this is as a combination of likelihood and impact, but may take into account characteristics relevant to your business.
ISO 31000 suggests taking into account the following:

- 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; and

SAMPLE

- Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered."

3.3.2 The Information Security Manager determines risk acceptance criteria for the ISMS.

3.4 The risk assessor identifies risks to the management system.

3.5 The risk assessor analyses the risks to determine their relation to the risk criteria, including their likelihood and impact.

3.6 The risk assessor evaluates the risks by comparing the level of risk identified in 3.5 above to the risk criteria established in 3.3.

3.7 The risk assessor determines risk treatments:

3.7.1 Treatments are selected by agreement with the appropriate process, risk or asset owner.

3.7.2 Risk treatment options are as follows:

3.7.2.1 Eliminate the risk by removing the activity affected by the risk.
3.7.2.2 Accept the risk to pursue an opportunity.
3.7.2.3 Remove the source of the risk.
3.7.2.4 Change the likelihood of the risk coming to pass.
3.7.2.5 Change the consequences of the risk coming to pass.
3.7.2.6 Share the risk with another party or parties (such as via suppliers, insurance or other third parties).
3.7.2.7 Accept the risk by informed decision.

3.8 The risk assessor creates a risk treatment plan providing the following information:

3.8.1 The reasons for selected treatments, including expected benefits.
3.8.2 Those responsible for approving the risk treatment plan.
3.8.3 Those responsible for implementing the risk treatment plan.
3.8.4 Proposed actions.
3.8.5 Resource requirements and contingencies.
3.8.6 Treatment performance measures and limitations.
3.8.7 Requirements for reporting and monitoring.
3.8.8 Timing and schedule for the risk treatment.

SAMPLE

3.9 The risk treatment plan is agreed with the appropriate stakeholders.

3.10 The risk treatment plan is implemented in accordance with Organisation Name's processes and the risk treatment plan itself.

Document owner and approval

The Head of Risk is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in Master List of Document Approval.

SAMPLE