[Company]

Risk Management

Procedure

The procedure for the management of risk.

Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

Document Contents Page

Purpose

The purpose of this procedure is to ensure the effective management of the lifecycle of risk from risk identification through to risk treatment.

Scope

All company employees and external party users.

Risk Management Procedure

Principle

Effective risk identification and management underpins and forms the foundation of the information security management system.

Risk Register

A risk register is drawn up and maintained.

For each risk, at least the following, is recorded

- The risk reference number
- Any external reference numbers.
- Date risk opened
- Date risk closed
- Asset risk applies to

- Asset owner
- Threat
- Vulnerability
- Outcome
- CIA affected
- Existing control description
- Impact score
- Likelihood score
- Risk score (impact x likelihood)
- [redacted]

Risk Identification

Risks are identified as a part of the continual improvement process and from the management and outputs of audits and incidents.

Risks can additionally be identified via risk workshops, data privacy impact assessments under GDPR, [redacted]

Risk assessment

Risks are assed for likelihood of an event occurring and the impact should it occur. The likelihood and impact are scored from 1 to 5. These scores are then used to generate the risk score by the following formula:

Likelihood x Impact = Risk Score

Likelihood

Likelihood	Grading	Description
Highly Probable	5	Likely to happen within the next month
Probable	4	Likely to happen within the next 6 months
Possible	3	[redacted]
Unlikely	2	[redacted]
Rare	1	[redacted]

Impact

Impact	Grading	Description
Very High	5	Legal or regulatory compliance issue or breach System downtime in breach of agreed SLA's, leading to contract loss. Impact on health or safety or individuals.
High	4	Exposure of sensitive information to a non-authorised third party, system downtime, data corruption, impacting upon ability to deliver service (breaching agreed SLA's)
Medium	3	[redacted]
Low	2	[redacted]
Very Low	1	[redacted]

Risk Classification and Mitigation Strategy

Risk Classification	Grading	Description
Critical	16 >=	Reduce risk [redacted] authority required to accept risk at this level.
Major	10 - 15	Reduce risk [redacted] authority required to accept risk at this level.
Moderate	5 - 9	Reduce risk [redacted]
Minor	1 - 4	Accept Risk

Risk Treatment

Risk assessment generates a risk score and risk classification at which point a risk treatment approach needs to be agreed at the Management Review Team meeting. The risk treatment options are:

- **Risk Avoidance** – where the failure cost is too great and therefore the risk is not taken
- **Risk Reduction** – [redacted]
- [redacted]
- [redacted]

Risk owners are assigned, plans and dates for completion agreed and the progress of risk treatment tracked via the management review team meeting.

Risk Monitoring and Risk Review

[redacted] risks are recorded in the risk registered and monitored as a minimum at the [redacted]

Procedure Compliance

Compliance Measurement

The information security management team will verify compliance to this procedure through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the procedure owner.

Exceptions

Any exception to the procedure must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The procedure is updated and reviewed as part of the continual improvement process.