Risk Management Procedure

Reference: FPD0018A-2022

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

To outline FISCAL Technologies' Risk Management process.

Prepared for:
All Employees, select Contractors,
Partners and Customers

Prepared by:
James Pobgee

FISCAL Technologies Ltd
448 Basingstoke Road,
Reading, RG2 0LP
Tel: 0845 680 1905

1 CONFIDENTIALITY

This document is the property of FISCAL Technologies. It may not be copied, distributed, or recorded on any electronic or other medium without the express written permission of the company.

All material contained in this document which is not readily available in the public domain is regarded as confidential to FISCAL Technologies and may not be divulged to any other parties without the express written permission of FISCAL Technologies.

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Risk Management Procedure
Associated Controls:	10.1 6 6.1 6.1.1 6.1.2 6.1.3 8.2 8.3 B.5.2 B.5.37 B.5.7
Reference ID:	FPD0018A-2022
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	17/12/2021
Revision Issued Date:	
Reference Documents:	Linked Policies: • Information Security Governing Policy • Risk Management Policy Linked Procedures: Linked Records: • ISMS Scope

2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1		James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

The purpose of this process is to define how FISCAL Technologies identifies potential information security threats to the organisation, minimises their impact and effectively monitors and evaluates the risk management strategy.

3.2 SCOPE

This process is applicable to all information and IT assets (including networks, systems, and infrastructure), information processing facilities, personnel as well as all third-party services and personnel within the scope of FISCAL Technologies' Information Security Management system.

4 RISK MANAGEMENT

Information Security Risk Management (ISRM) is the process of continuously identifying, assessing, evaluating, and treating risks related to the organisation's information.

FISCAL Technologies utilises HiComply to manage our ISMS and associated Risk Register.

- Organisational and Technical risks must be recorded in HiComply.
- Change Management Risks must be recorded in the departmental task / management tools.
    - Exception: Security changes must be raised via the helpdesk for review and approval.
- Requests for new software, services, suppliers must be raised via the helpdesk for risk review.

4.1 SUMMARY – RISK MANAGEMENT

4.1.1 What is Risk Management?

The process of identifying, assessing, and prioritising risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events.

4.1.2 Risk Assessment and Treatment:

The two core components of risk management. Risk assessment involves identifying potential risks, while risk treatment involves selecting and implementing appropriate measures to address those risks.

4.2 EXAMPLES: RISKS, THREATS, VULNERABILITIES AND CONTROLS

4.2.1 Risks

- **Cybersecurity:** such as insider threats, data breaches, phishing attacks, malware infections, and social engineering attacks.
- **Physical security:** such as theft, vandalism, natural disasters, sabotage, and accidents.
- **Financial:** such as credit risks, supplier risk, fraud, embezzlement, and economic downturns.
- **Legal and regulatory:** such as non-compliance with data protection laws, intellectual property disputes, and environmental regulations.
- **Reputational:** such as negative publicity, customer dissatisfaction, ethical controversies, and social media scandals.
- **Change Management:** such as disruption to operations, resistance and adoption, technical issues, resource allocation, impact to legal or regulatory compliance.
- **Workforce:** Skill shortages, high turnover rates, competitive job markets, and employee satisfaction.

4.2.2 Threats

- **Malware:** Malicious software designed to damage, disrupt, or gain unauthorised access to computer systems, networks, and data. Examples include viruses, worms, trojans, and ransomware.
- **Social engineering:** Manipulation of individuals into divulging confidential information or performing actions that compromise security. Examples include phishing, pretexting, baiting, and tailgating.
- **Physical attacks:** Gaining unauthorised access to a physical location or assets. Examples include theft, vandalism, and espionage.
- **Network attacks:** Network attacks are those that target computer networks and related infrastructure. Examples include denial-of-service attacks, man-in-the-middle attacks, and packet sniffing.
- **Human error:** Unintentional mistakes or action by an individual that results in a security breach. Examples include leaving a device unlocked, failing to update software, or falling for a phishing scam.

4.2.3 Vulnerabilities

- **Vulnerabilities:** are weaknesses that can be exploited by a threat. Examples include bugs in software, unpatched software, misconfigured software / network / hardware, weak encryption.

4.2.4 Controls

- **Controls:** Measures put in place to mitigate risks and protect assets. Examples include company policies, defined processes or standard operating procedures, patch cycles, antivirus software, web protection, authentication processes.

5 RISK MANAGEMENT PROCESS

Risk management is a continuous and proactive process that enables FISCAL to identify, assess, prioritise, and mitigate risks to achieve a specific objective. The process requires continuous monitoring and evaluation to ensure that the risk mitigation strategies are effective and that the risks are being managed effectively.

The risk management process minimises the impact of threats, identify opportunities for improvement, and optimises decision-making. Ensuring better resource allocation, enhanced stakeholder confidence, and improved compliance with legal and regulatory requirements.

By adopting the following systematic and structured approach to risk management, FISCAL can proactively identify and address potential risks, enhance our resilience, and protect our assets and reputation.

5.1 PROCESS

The process involves the following steps that are taken to understand and manage risks effectively:

- **Step 1.** Identify the risks that could impact FISCAL’s ability to achieve its objectives. This involves understanding the potential sources of risk, such as natural disasters, cyber-attacks, or operational failures, and identifying the assets that could be affected.
- **Step 2.** Assess the likelihood and potential impact of each risk. This helps to prioritise the risks based on their level of severity and potential impact on the company.
- **Step 3.** Once the risks have been prioritised, FISCAL can then develop and implement strategies to mitigate the risks. These strategies can include risk avoidance, risk reduction, risk sharing, risk retention, and risk transfer. The goal of risk mitigation is to minimize the likelihood and impact of risks to an acceptable level.
- **Step 4.** Monitor, Review.
- **Step 5.** Repeat.

6 RISK ASSESSMENT PROCESS

Risk Assessments are the process of identifying, analysing, and evaluating risks to determine their likelihood and potential impact on an organisation's assets a threat will have.

FISCAL Technologies operates an asset-based risk assessment methodology, enabling us to effectively identify and assess critical elements within our organisation. This includes Hardware, Software, Networks, and Information that are vital to our business operations. By recognising and understanding associated threats to these assets, we gain valuable insights into potential risks.

This approach empowers us to evaluate the effectiveness of our current security controls and assess the potential impact of risks on our organisation. By focusing on these key assets, we can proactively manage and mitigate risks, ensuring the continued security and resilience of our operations.

6.1 PROCESS

The risk assessment process follows a set of detailed steps to cover the broad areas of:

- Asset identification
- Threat identification
- Vulnerability assessment
- Likelihood determination
- Impact assessment
- Risk evaluation

The detailed steps are as follows:

1. **Identify assets:** Identify the assets that need to be protected and their associated owners. This can include physical assets such as buildings and equipment, as well as digital assets such as data, software, and networks.
2. **Identify threats:** Identify the potential threats that could impact the assets. This can include natural disasters, cyber-attacks, human error, and operational failures.
3. **Identify vulnerabilities:** Identify the vulnerabilities that could be exploited by the threats. This can include weaknesses in physical security, network security, or software security.
4. **Assess likelihood:** Assess the likelihood that the identified threats will occur. This can be done using historical data, expert opinions, or statistical analysis.
5. **Assess impact:** Assess the potential impact of the identified threats. This can include financial losses, reputational damage, or operational disruption.
6. **Determine risk score:** Based on the likelihood and impact assessments, the risk score of each threat can be determined. This can be done using a **risk matrix**, which maps the likelihood and impact assessments onto a grid to identify the level of risk.
7. **Prioritise risks:** Once the risk level of each threat has been determined, they can be prioritised based on their level of severity and potential impact on FISCAL.
8. **Develop risk mitigation strategies:** Based on the prioritised list of risks, FISCAL can then develop and implement strategies to mitigate the risks. This can include risk avoidance, risk reduction, risk sharing, risk retention, and risk transfer.
9. **Monitor and review:** Risk assessment is an ongoing process that requires continuous monitoring and review to ensure that the risks are being managed effectively. This involves regularly updating the risk assessments and mitigation strategies to account for changes in the threat landscape and FISCAL’s objectives.

6.2 RISK REVIEWS

Assessments will be reviewed as follows:

- At least annually or following significant material change.
    - E.g., changes in technology or organisational changes.
- Upon request for new requirements, services, or suppliers.
- Following significant incidents or breaches.
- Following significant changes in Legal and regulatory, or customer requirements.

7 RISK TREATMENT PROCESS

Risk Treatment is the process of selecting and implementing measures to modify risks to an acceptable level. It's important to select the most appropriate risk treatment option for each risk, considering the potential costs and benefits of each option.

It's also important to monitor and review the effectiveness of the chosen risk treatment option over time. This involves regularly reviewing the risk treatment plan and assessing whether the chosen risk treatment option is still appropriate and effective. If necessary, adjustments should be made to the risk treatment plan to ensure that risks continue to be effectively managed.

7.1 TREATMENT OPTIONS:

- **Avoidance:** This involves taking steps to eliminate the risk altogether. This may involve avoiding certain activities or discontinuing certain products or services.
- **Mitigation:** This involves taking steps to reduce the likelihood or impact of a risk. This may involve implementing controls, such as security measures or training programs, to reduce the likelihood of a risk event occurring.
- **Transfer:** This involves transferring the risk to a third party, such as an insurance company or contractor. This can help to reduce the financial impact of a risk event.
- **Acceptance:** This involves accepting the risk and developing a plan to manage it. This may involve monitoring the risk and developing contingency plans to minimize the impact of a risk event.
- **Retention:** This involves accepting the risk and its potential consequences.

7.2 TREATMENT PLAN

After the risk treatment option has been selected, it's important to develop a risk treatment plan that outlines the steps that will be taken to implement the chosen risk treatment option.

The risk treatment plan should include details such as the responsibilities of those involved, the timelines for implementation, and the resources required.

Here are some key considerations when creating a risk treatment plan:

- **Assign responsibility:** The risk treatment plan should clearly identify who is responsible for implementing each step of the plan. This includes identifying who will be responsible for monitoring the effectiveness of the plan and making any necessary adjustments.
- **Set timelines:** The risk treatment plan should include specific timelines for each step of the plan. This can help to ensure that the plan is implemented in a timely and efficient manner.
- **Identify required resources:** The risk treatment plan should identify the resources that will be required to implement the plan. This includes identifying any necessary funding, personnel, and equipment.

- **Define success criteria:** The risk treatment plan should include specific success criteria that will be used to measure the effectiveness of the plan. This may include criteria such as a reduction in the likelihood or impact of the risk, or an improvement in FISCAL's overall risk posture.
- **Develop communication plan:** The risk treatment plan should include a communication plan that outlines how progress on the plan will be communicated to stakeholders. This may include regular reports, meetings, or other forms of communication.
- **Develop monitoring and review procedures:** The risk treatment plan should include procedures for monitoring the effectiveness of the plan over time. This may involve regular reviews of the plan, as well as ongoing monitoring of the effectiveness of risk treatment measures.

It's important to note that creating a risk treatment plan is an iterative process. As new information becomes available or circumstances change, the plan may need to be adjusted to ensure that risks continue to be effectively managed.

8 DEFINITIONS

8.1 IMPACT AND LIKELIHOOD

Impact refers to the magnitude of harm that could be caused if the risk event were to occur. There are several ways to measure impact, including:

- **Financial impact:** The financial impact of a risk can be measured in terms of direct costs, such as the cost of repairing damage, as well as indirect costs, such as lost revenue.
- **Reputational impact:** The reputational impact of a risk can be measured in terms of damage to FISCAL’s brand and reputation.
- **Operational impact:** The operational impact of a risk can be measured in terms of the impact on the FISCAL’s ability to deliver products or services.
- **Legal and regulatory impact:** The legal and regulatory impact of a risk can be measured in terms of potential fines or legal action that could be taken against FISCAL.

Likelihood refers to the probability that the risk event will occur. There are several ways to measure likelihood, including:

- **Historical data:** Historical data can be used to analyse the frequency of past occurrences and estimate the likelihood of future events.
- **Expert opinion:** Expert opinions can be gathered from industry professionals who have experience in the specific area of risk.
- **Statistical analysis:** Statistical analysis can be used to analyse patterns and trends to estimate the likelihood of future events.
- **Scenario analysis:** Scenario analysis involves developing hypothetical scenarios and assessing the likelihood of those scenarios based on factors such as historical data, expert opinion, and statistical analysis.

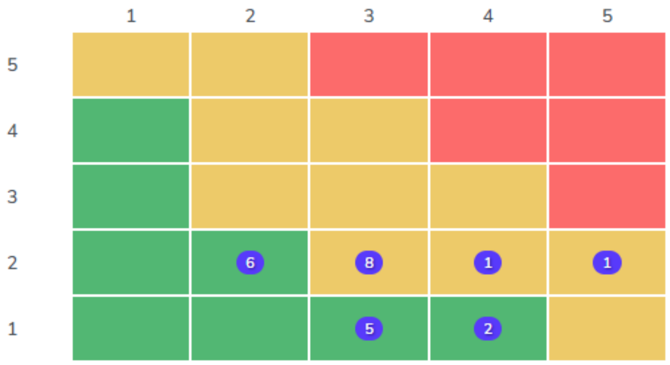
When assessing impact and likelihood, it is important to consider both the potential severity of the risk and the FISCAL's ability to manage the risk. This involves considering factors such as FISCAL's risk appetite, risk tolerance, and risk management capabilities.

8.2 RISK MATRIX

Risk Matrixes are used to visually represent the likelihood and impact of identified risks, and to prioritise risks for treatment. FISCAL uses this tool to help define bands of risk (Acceptable, Tolerable or Intolerable) based on the resulting score of Impact vs Likelihood based on a rating of 1-5 in both areas.

The aim of risk management is to ensure treated risks have a risk score of acceptable wherever possible.

Example Risk Matrix.



	1	2	3	4	5
5	🟨	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟨	🟨	🟨	🟥
2	🟩	🟩 6	🟨 8	🟨 1	🟨 1
1	🟩	🟩	🟩 5	🟩 2	🟨

Green: Acceptable Risks

Yellow: Tolerable Risks

Red: Intolerable Risks

8.3 MEASURES

8.3.1 Impact

1. **Low:** A risk event that may cause some inconvenience or minor disruption but does not significantly affect FISCAL's ability to achieve its objectives. The impact can be addressed using existing resources and procedures.
2. **Minor:** A risk event that may cause some disruption to normal operations or result in minor financial losses. The impact can be addressed using existing resources and procedures but may require additional resources or time to fully address.
3. **Moderate:** A risk event that may significantly disrupt normal operations or result in moderate financial losses. The impact may require additional resources or time to fully address and may require changes to existing procedures or processes.
4. **Major:** A risk event that significantly disrupts normal operations or results in major financial losses. The impact may require significant additional resources or time to fully address and may require changes to existing procedures or processes.
5. **Catastrophic:** A risk event that has a severe and widespread impact on FISCAL's ability to achieve its objectives, potentially resulting in the loss of life, significant financial losses, or damage to FISCAL's reputation. The impact may require a major investment of resources and time to fully address and may require significant changes to existing procedures or processes.

8.3.2 Likelihood

1. **Low:** A risk event that is unlikely to occur but cannot be completely ruled out. The risk event may be rare or highly improbable and may require only minimal or no additional mitigation efforts.
2. **Unlikely:** A risk event that is not expected to occur but is possible given the current conditions and environment. The risk event may require some additional mitigation efforts, but these efforts may be minimal or consistent with current procedures.
3. **Possible:** A risk event that has a realistic chance of occurring given the current conditions and environment. The risk event may require additional mitigation efforts that may require some changes to current procedures or processes.

4. **Likely:** A risk event that is expected to occur given the current conditions and environment. The risk event may require significant additional mitigation efforts, including changes to current procedures or processes.
5. **Certain:** A risk event that is certain to occur given the current conditions and environment. The risk event may require significant additional mitigation efforts, including major changes to current procedures or processes.

9 ENFORCEMENT AND VIOLATIONS

9.1 ENFORCEMENT

All divisions & employees of the organisation must comply with the requirements of this policy. Management is responsible for ensuring that the policy is implemented within its area of responsibility.

FISCAL Technologies expects all users to comply with the terms of this policy and all other policies, procedures, guidelines, and standards published in its support.

9.2 VIOLATIONS

Violations of this policy shall result in disciplinary action / legal ramifications by the organisation. Disciplinary action will be consistent with the severity of the incident as determined by an investigation and as deemed appropriate by Management and HR.

Compliance with this policy will be reviewed by the organisation’s Internal Audit Team.