MOSAIC™
Financial Services Infrastructure

Mosaic Business Solutions Limited, Risk Assessment Methodology

Document Control

Document ref	ISMS202113
Version	1
Dated	12/01/2021
Document author	Russell Fielding
Document owner	Mike Stobbs, Mosaic FSI
Approved by	Mike Stobbs
Confidentiality level	Internal

Revision History

Date	Version	Description	Author
25/01/21	1.1	Q/A	Mike Stobbs

Distribution

Name	Title

Table of Contents

Scope and Introduction

This document aims to define the methodology for the assessment and treatment of information risks in Mosaic FSI.

The acceptable level of risk is based on the ISO/IEC 27001 standard.

Risk assessment and risk treatment are applied to the entire scope of the Information Security Management System (ISMS), i.e., to all assets used within Mosaic FSI or impact information security within the ISMS.

Users of this document are all employees and contractors of Mosaic FSI who take part in risk assessment and risk treatment.

Reference Documents

- ISO/IEC 27001 standard, clauses 6.1.2, 6.1.3, 8.2, and 8.3
- ISO 22301 standard clauses 8.2.1, 8.2.3 and 8.3.2
- Information Security Policy ISMS202102
- GDPR and Privacy Act 2020
- Supplier Assessment ISMS202112
- Statement of Applicability ISMS202109

Risk Assessment and Risk Treatment Methodology

Risk assessment

The process

Risk assessment is implemented through the Risk Assessment Table.

The Information Security Officer coordinates the risk assessment process, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by risk owners.

Assets, vulnerabilities, and threats

The first step in risk assessment is identifying all assets in the ISMS scope – i.e., of all assets that may disrupt operations. Assets may include documents in paper or electronic form, applications and databases, people, IT equipment, infrastructure, tools, machinery, production facilities and external services/outsourced processes.

When identifying assets, it is also necessary to determine their owners – the person or organisational unit responsible for each asset.

The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities are determined using the catalogues included in the Risk Assessment Table. Every asset may be associated with several threats, and every threat may be related to several vulnerabilities.

Mosaic FSI assets and risk are listed in the Information Security Management System (ISMS).

Determining the risk owners

For each risk, a risk owner must be identified – the person or organisational unit responsible for each risk. This person may or may not be the same as the asset owner.

Mosaic FSI roles and responsibilities are highlighted in the information security policy and ISMS.

Consequences and likelihood

Once risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materialises:

Low consequence	0	Loss of confidentiality, availability or integrity does not affect the organisation's cash flow, legal or contractual obligations, or its reputation.
Moderate consequence	1	Loss of confidentiality, availability or integrity incurs costs and has a low or moderate impact on legal or contractual obligations, or the organisation's reputation.
High consequence	2	Loss of confidentiality, availability or integrity has considerable and/or immediate impact on the organisation's cash flow, operations, legal or contractual obligations, or its reputation.

After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk, i.e., the probability that a threat will exploit the vulnerability of the respective asset:

Low likelihood	0	Existing security controls are strong and have so far provided an adequate level of protection. No new incidents are expected in the future.
Moderate likelihood	1	Existing security controls are moderate and have mostly provided an adequate level of protection. New incidents are possible, but not highly likely.
High likelihood	2	Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future.

By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk is calculated automatically by adding up the two values. Existing security controls are to be entered in the last column of the Risk Assessment Table.

Risk acceptance criteria

Values 0, 1 and 2 are acceptable risks, while values 3 and 4 are unacceptable risks. Unacceptable risks must be treated.

Risk treatment

Risk treatment is implemented through the Risk Treatment Table, by copying all risks identified as unacceptable from the Risk Assessment Table. Risk treatment is conducted by Information Security Officer.

One or more treatment solutions must be selected for risks valued 3 and 4:

1. Selection of security control or controls from ISO 27001 Annex listed in Mosaic FSI Statement of Applicability.
2. Transferring the risks to a third party – e.g., by purchasing an insurance policy or signing a contract with suppliers or partners
3. Avoiding the risk by discontinuing a business activity that causes such risk.
4. Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialise.

The selection of options is implemented through the risk treatment table. Usually, option 1 is selected: selection of one or more security controls. When several security controls are selected for a risk, then additional rows are inserted into the table immediately below the row specifying the risk.

The treatment of risks related to outsourced processes must be addressed through the contracts with responsible third parties, as specified in Supplier Assessment document ISMS202112.

In the case of option 1 (selection of security controls), it is necessary to assess the new value of consequence and likelihood in the Risk Treatment Table, to evaluate the effectiveness of planned controls.

Regular reviews of risk assessment and risk treatment

Risk owners must review existing risks and update the risk assessment table and risk treatment table in line with newly identified risks. The review is conducted at least twice a year, or more frequently in the case of significant organisational changes, significant change in technology, change of business objectives, changes in the business environment, etc.

Statement of Applicability and Risk treatment plan

Information Security Officer must document the following in the statement of applicability: which security controls from Annex A of the ISO/IEC 27001 standard are applicable and which are not, the justification for such decisions, and whether they are implemented or not.

On behalf of the risk owners, Mosaic FSI top management will accept all residual risks through the Statement of Applicability.

Information Security Officer will prepare the Risk treatment plan in which the implementation of controls will be planned. On behalf of the risk owners, Mosaic FSI will approve the Risk treatment plan.

Reporting

The Information Security Officer will document the results of risk assessment and risk treatment, and all the subsequent reviews, in the Risk Assessment and Treatment Report.

The Information Security Officer will monitor the progress of implementation of the Risk treatment plan and report the results to the partners each month.

Managing records kept based on this document.

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Risk Assessment Table	Information Security Officer computer, Dropbox, internal website	Information Security Officer	Only Information Security Officer has the right to make entries into and changes to the Risk Assessment Table.	Data is stored permanently.
Risk Treatment Table	Information Security Officer computer, Dropbox, internal website	Information Security Officer	Only Information Security Officer has the right to make entries into and changes to the Risk Treatment Table.	Data is stored permanently.
Risk Assessment and Treatment Report	Information Security Officer computer, Dropbox, internal website	Information Security Officer	The Report is prepared in read-only PDF format	The Report is stored for a period of 3 years
Statement of Applicability	Information Security Officer computer, Dropbox, internal website	Information Security Officer	Only Information Security Officer has the right to make entries into and changes to the Statement of Applicability	Older versions of SoA are stored for a period of 3 years
Risk Treatment Plan	Information Security Officer computer, Dropbox, internal website	Information Security Officer	Only Information Security Officer has the right to make entries into and changes to the Risk treatment plan	Older versions of Risk treatment plan are stored for a period of 3 years

Only senior partners can grant other employees and contractors access to any of the above-mentioned documents.

Validity and document management

This document is valid as of 25/01/2021.

The owner of this document is Information Security Officer Mike Stobbs, who must check and, if necessary, update the document at least twice a year, before the regular review of existing risk assessment.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- the number of incidents which occurred but were not included in risk assessment.
- the number of risks which were not treated adequately.
- the number of errors in the risk assessment and risk treatment process because of unclear definition of roles and responsibilities.

Appendices

- Appendix 1 – Risk Assessment Table spreadsheet
- Appendix 2 – Risk Treatment Table spreadsheet