Cybersecurity
Risk Management

v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information **2**

1 Introduction **4**

2 Purpose **4**

3 Abbreviations and Definitions **5**

4 Criteria of Performing Risk Assessment **6**

5 Roles and Responsibilities **6**

5.1 RACI Matrix 6

6 Risk Management Process **7**

6.1 Establish the Context 8

6.2 Risk Identification 8

6.2.1 Compile/Maintain Asset Inventory 9

6.2.2 Identify Potential Threats 9

6.2.3 Assess Existing Vulnerabilities 9

6.2.4 Identify Risk Scenarios 9

6.3 Risk Analysis 10

6.3.1 Assess the Likelihood 10

6.3.2 Assess the Impact 10

6.3.3 Risk Classification 12

6.4 Risk Evaluation 13

6.4.1 Risk Assessment Report 13

6.5 Risk Treatment 13

6.5.1 Risk Treatment Plan 13

6.6 Management Approval 14

6.7 Risk Monitoring and Reporting 14

6.8 Regular Review 14

1 Introduction

The effective management of Cyber Security has always been a priority for Jadarah For Dept Collections Co. in order to manage risk and safeguard its reputation. For that Jadarah For Dept Collections Co. has an effective risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to counter them.

The purpose of this document is to setup risk management process.

2 Purpose

The objective of Cyber Security risk management is to:

- Safeguard the assets of the business from potential loss
- Ensure that there is compliance with organization policies and procedures or external legislation and regulation
- Ensue that the resources of the business are utilised in an efficient and effective manner
- Ensure that the confidentiality, integrity and availability of information is reliable

3 Abbreviations and Definitions

CS: Cyber Security

CISO: Chief Information Security Officer

CSMS: Cyber Security Management System

SAMA: Saudi Arabian Monetary Authority

Top Management: Leadership team of Jadarah For Dept Collections Co. responsible to drive business strategy and direction

4 Criteria of Performing Risk Assessment

There are a number of criteria that determine when a risk assessment should be carried out within Jadarah For Dept Collections Co..

In general, the criteria are that a risk assessment will be performed in the following circumstances:

- A comprehensive risk assessment will be conducted covering all information assets as part of preparing the baseline for Cyber Security Program.
- Updates to the baseline risk assessment as part of the management review process – this should identify changes to assets, threats and vulnerabilities and possibly risk levels.
- As part of projects that involve significant change to the organization, or its information assets
- As part of the technology change management process when assessing whether proposed changes should be approved and implemented.
- On major change in regulatory, legislation, law, or in case of merger and acquisitions.
- When evaluating and selecting suppliers, particularly those that will play a part in the delivery of technology services (Third Party Risk Assessment).

5 Roles and Responsibilities

Within the process of risk management there are several key roles that play a part in ensuring that all risks are identified, addressed and managed. These roles are shown in the RACI table below, together with their relative responsibilities at each stage of the process.

5.1 RACI Matrix

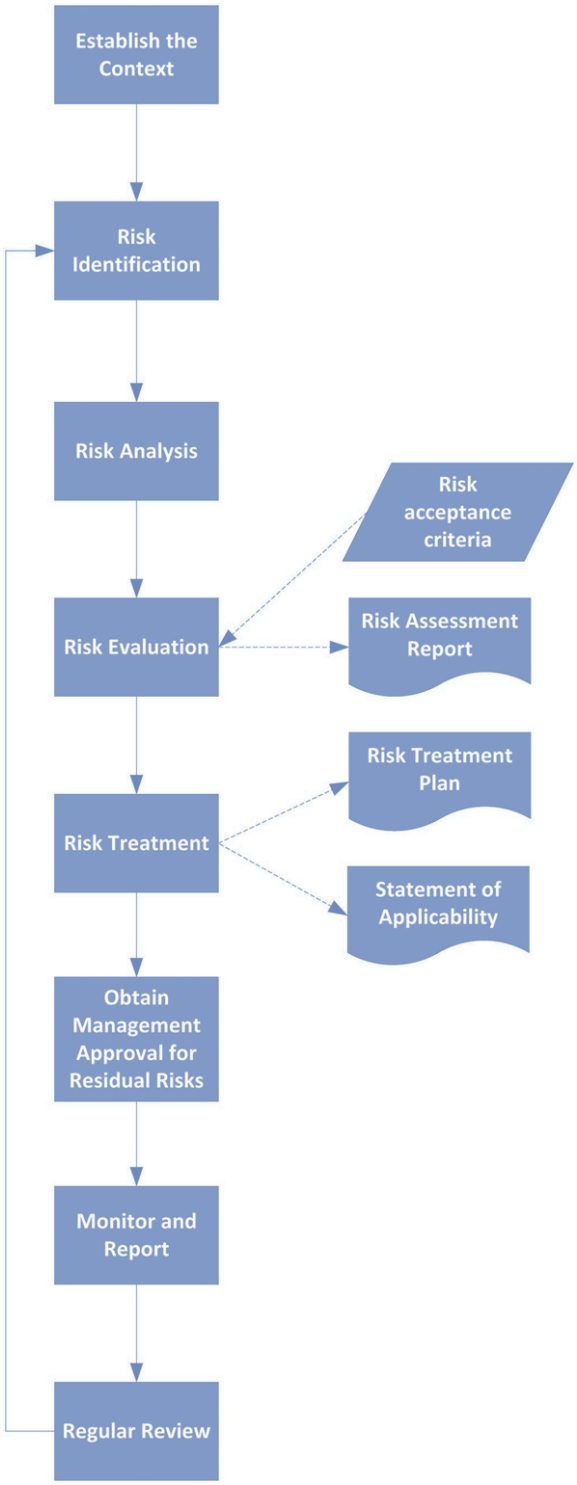
The table below clarifies the responsibilities at each step using the RACI model, i.e.:

- R: Responsible
- A: Accountable
- C: Consulted
- I: Informed

Step	Cyber Security Manager	Risk Owners	Top Management
Establish the context	R	C	A
Risk identification	C	R	A
Risk analysis	C	R	A
Risk evaluation	C	R	A
Risk treatment	R	C	A
Management approval for residual risks	C	C	A/R
Monitor and Report	R	I	A
Regular Review	R	C	A

6 Risk Management Process

The process of risk assessment and treatment is shown below and described in more detail in the following sections. The process used is qualitative in nature in that it uses the terms high, medium and low to describe the relative classification level for each specific risk. In some circumstances it may be appropriate to also use quantitative techniques i.e., using numbers such as financial values within the process to provide a higher degree of detail in assessing risks. In all cases where quantitative techniques are used the criteria should be clearly stated so that the risk assessment is understandable and repeatable.



6.1 Establish the Context

The overall environment in which the risk assessment is carried out must be described and the reasons for it explained. This should include a description of the internal and external context and any recent changes that affect the likelihood and impact of risks in general.

The internal context may include:

- Governance, organizational structure, roles and accountabilities
- Policies, objectives, and the strategies that are in place to achieve them
- The capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems and technologies)
- Information systems, information flows and decision-making processes (both formal and informal)
- Relationships with, and perceptions and values of, internal stakeholders
- Standards, guidelines and models adopted by the organization
- Form and extent of contractual relationships
- The technology stack/infrastructure and services

The external context may include:

The cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local

- Key drivers and trends having impact on the objectives of the organization
- Relationships with, and perceptions and values of, external stakeholders
- The prevailing market or industry view of the security of cloud service providers – this may be affected by any recent breaches involving the loss of personally identifiable information (PII)

The scope of the risk assessment must also be defined. This may be expressed in terms of factors such as:

- Geographical location e.g., countries, offices, data centres
- Organizational units e.g., specific departments
- Business process(es)
- IT services, systems and networks
- Customers, products or services

6.2 Risk Identification

The process of identifying risks to be assessed will consist of the following steps in line with the requirements of SAMA Cyber Security Framework. Risks are identified to the confidentiality, integrity or availability of information within the Jadarah For Dept Collections Co..

There are two types of risk assessment approaches that will be used in Jadarah For Dept Collections Co.:

1. Asset-based Risk Assessment (Detailed)
2. Scenario-based Risk Assessment (High-level)

6.2.1 Compile/Maintain Asset Inventory

A full inventory of assets is compiled and maintained by Jadarah For Dept Collections Co.. The definition of an asset is taken to be “anything that has value to the organization” and is therefore worthy of protection. This will include customer data that Jadarah For Dept Collections Co. stores and processes in its role as a service provider.

Two major types of assets are identified:

- Primary assets – information and business processes and activities
- Supporting assets – hardware, software, network, personnel, site, organization structure

The list of assets is held in the document Information Asset Inventory as part of the Cyber Security Program. Within the inventory every asset is assigned a value which should be considered as part of impact assessment stage of this process. Each asset also has an owner who should be involved in the risk assessment for that asset.

For the purposes of risk assessment, it may be appropriate to group assets with similar requirements together so that the number of risks to be assessed remains manageable.

6.2.2 Identify Potential Threats

For each asset (or asset group), the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or malicious attacks such as viruses, theft or sabotage. Threats will apply to one or more of the confidentiality, integrity and availability of the asset.

6.2.3 Assess Existing Vulnerabilities

Attributes of an asset (or asset group) which may be exploited by any specific threat are referred to as vulnerabilities and will be detailed as part of the risk assessment.

Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of malware) or the existence of paper files in a data centre (which could be exploited by the threat of fire).

6.2.4 Identify Risk Scenarios

The identification of risks to the information security of the organization will be performed by a combination of group discussion and interview with interested parties.

Such interested parties will normally include (where possible):

- Manager(s) responsible for each business-critical activity
- Representatives of the people that normally carry out each aspect of the activity
- Providers of the inputs to the activity
- Recipients of the outputs of the activity
- Appropriate third parties with relevant knowledge
- Representatives of those providing supporting services and resources to the activity
- Any other party that is felt to provide useful input to the risk identification process

Identified risks will be recorded with as full a description as possible that allows the likelihood and impact of the risk to be assessed. Each risk must also be allocated an owner.

6.3 Risk Analysis

Risk analysis within this process involves assigning a numerical value to the likelihood and impact of a risk. These values are then multiplied to arrive at a classification level of high, medium or low for the risk.

6.3.1 Assess the Likelihood

An estimate of the likelihood of a identified risk must be made. This should consider whether it has happened before either to this organization or similar organizations in the same industry or location and whether there exists sufficient motive, opportunity and capability for a threat to be realized.

The likelihood of each risk will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in below table. When assessing the likelihood of a risk, existing controls will be considered. This may require an assessment to be made as to the effectiveness of existing controls.

More detailed guidance may be decided for each grade of likelihood, depending on the subject of the risk assessment.

Grade	Description	Summary
1	Improbable	Has never happened before and there is no reason to think it is any more likely now
2	Unlikely	There is a possibility that it could happen, but it probably won't
3	Likely	On balance, the risk is more likely to happen than not
4	Very Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Almost certain	Either already happens regularly or there is some reason to believe it is virtually imminent

The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

6.3.2 Assess the Impact

An estimate of the impact that the loss of confidentiality, integrity or availability could have on the Jadarah For Dept Collections Co. must be given. This should consider existing controls that lessen the impact, as long as these controls are seen to be effective.

Consideration will be given to the impact in the following areas:

- Customers
- Finance
- Health and Safety
- Reputation
- Knock-on impact within the organization
- Legal, contractual or organizational obligations

The impact of each risk will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table below.

Grade	Description	Customer Impact	Financial Impact	Health & Safety	Impact On Reputation	Legal Impact
1	Negligible	No effect	Very little or none	Very small additional risk	Negligible	No implications
2	Slight	Some local disturbance to normal business operations	Some	Within acceptable limits	Slight	Small risk of not meeting compliance
3	Moderate	Can still deliver product/service with some difficulty	Unwelcome but could be borne	Elevated risk requiring immediate attention	Moderate	In definite danger of operating illegally
4	High	Business is crippled in key areas	Severe effect on income and/or profit	Significant danger to life	High	Operating illegally in some areas
5	Very High	Out of business; no service to customers	Crippling; the organization will go out of business	Real or strong potential loss of life	Very High	Severe fines and possible imprisonment of staff

More detailed guidance may be defined for each grade of impact, depending on the subject of the risk assessment.

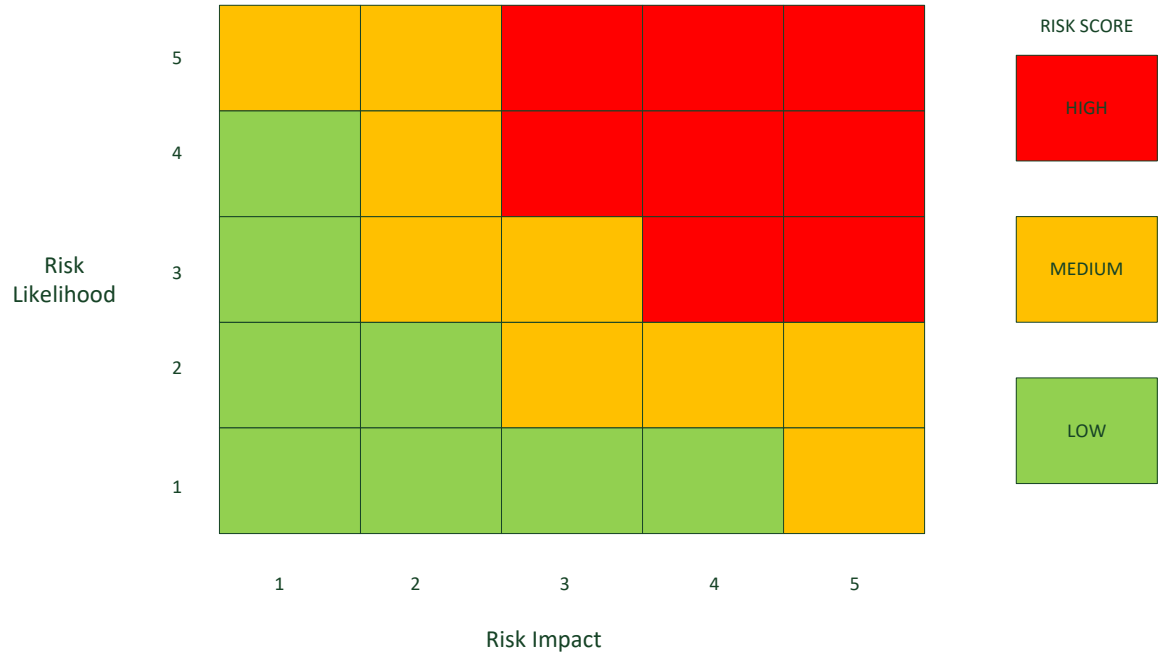
The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

6.3.3 Risk Classification

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers. This resulting score is then used to decide the classification of the risk based on the matrix shown in figure 2.

Each risk will be allocated a classification based on its score as follows:

- High: 12 or more
- Medium: 5 to 10 inclusive
- Low: 1 to 4 inclusive



The classification of each risk will be recorded as input to the risk evaluation stage of the process.

6.4 Risk Evaluation

The purpose of risk evaluation is to decide which risks can be accepted and which ones need to be treated. This will take into account the risk acceptance criteria established for this specific risk assessment (see Risk Acceptance Criteria, above).

The matrix in above figure (Risk Impact) shows the classifications of risk, where green indicates that the risk is below the acceptable threshold. The orange and red areas generally indicate that a risk does not meet the acceptance criteria and so is a candidate for treatment.

Risks will be prioritized for treatment according to their score and classification so that very high scoring risks are recommended to be addressed before those with lower levels of exposure for the organization.

6.4.1 Risk Assessment Report

The output from the risk evaluation stage is the risk assessment report. This shows the following information:

- Assets [asset-based risk assessment only]
- Threats [asset-based risk assessment only]
- Vulnerabilities [asset-based risk assessment only]
- Risk scenario descriptions [scenario-based risk assessment only]
- Controls currently implemented
- Likelihood (including rationale)
- Impact (including rationale)
- Risk Score
- Risk Classification
- Risk Owner
- Whether the risk is recommended for acceptance or treatment
- Priority of risks for treatment

This report is input to the risk treatment stage of the process and must be signed off by management before continuing, particularly in respect of those risks that are recommended for acceptance.

6.5 Risk Treatment

For those risks that are agreed to be above the threshold for acceptance by Jadarah For Dept Collections Co., the options for treatment will then be explored.

The overall intention of risk treatment is to reduce the classification of a risk to an acceptable level. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g., reducing the score from 8 to 6 means it remains a medium level risk. The organization may decide to accept these risks even though they remain at a medium rating. Such decisions must be recorded with a suitable explanation.

6.5.1 Risk Treatment Plan

The output of the risk evaluation is the risk treatment plan that includes:

- Risks requiring treatment
- Risk owner

- Recommended treatment option
- Control(s) to be implemented
- Responsibility for the identified actions
- Cost estimate for implementing the control(s)
- Timeline for actions
- Expected residual risk levels after the controls have been implemented

6.6 Management Approval

At each stage of the risk assessment process management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the following documents:

- Risk Assessment Report
- Risk Treatment Plan

In addition to overall management approval, the acceptance or treatment of each risk must be signed off by the relevant risk owner.

6.7 Risk Monitoring and Reporting

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exception situations can be identified and dealt with as part of the management review process.

6.8 Regular Review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business such as office moves, mergers and acquisitions or introduction or new or changed IT services.