Risk Assessment and Treatment Methodology

Version 9

REZOLVE.ai

Document Information

Name of the document	Risk Assessmentand Treatment Methodology
Release date	19-Dec-2018
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	02-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	01-Mar-2023	Reviewed and no change
7	24-Sep-2023	Updated Document Information
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and updated

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Table of Contents

Purpose and Scope

Purpose

The purpose of this document is to define Risk Assessment & Treatment Methodology.

Scope

The target audience of this document are all stockholders conducting risk assessment.

Responsibility

Role	Responsibility
CISO	• Conduct Risk Assessment with LeadershipTeam
CEO	• Approve Risk Assessment Results
CTO	• Review of Risks Assessment results
Leadership Team	• Assist CISO in Risk Assessment. Identify • acceptable level of Risk. • Ensure implementation of recommendation from Risk Assessment.

Risk Analysis Process

The risk analysis process involves the following activities:

- **Identification of Process / assets**
- **Evaluation of Process / assets**
- **Identification of Threats and Vulnerabilities**
- **Evaluation of Threats and Vulnerabilities**
- **Evaluate the probability of occurrence**
- **Calculate the Risk Impact Rating**
- **Identify existing controls**
- **Evaluate the existing level of Risk**

Guidelines for Identifying Process / Assets

An **asset** is something that has value or utility to the organization, its business operations, and their continuity.
Asset identification based on business needs of an organization is a major factor in risk assessment. The assets should be identified by **individual department members** and the list ratified by the **head of the department**.

A **process-based approach** is used for identifying assets.
This approach involves the following activities:

- **Identify business functions within the scope of the ISMS**
- **Segregate the assets into:**
    - **IT Assets** – Hardware (System / Network / Security / Laptops / Desktops / Backup Devices etc.)
    - **Software / Application Assets**
    - **Service Assets**
    - **People Assets**
    - **Information Assets** (Policies / Procedures / Other departmental documents and records etc. / Digital records)

Guidelines for Evaluating Assets

- In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business, or their potential values given to certain opportunities.
- The input for the valuation of assets should be provided by **owners and users of the early information**, to the organization and its business.
- Based on the **Confidentiality, Integrity and Availability** requirements of an asset, the following criteria are to be applied when evaluating each asset.

Level	Score	Definition
Highest	5	This asset has the highest value to the process. Its loss or destruction could have an immediate and severe impact on the process' viability. It would seriously impact the organization in terms of business activities, financial loss or loss of business.
High	4	This is an asset which is extremely valuable to the business process and its loss or destruction could have a severe impact on the process' viability and cause disruptions to business activities.
Medium	3	This is an asset which can be replaced where the loss or destruction of the information asset would have an immediate impact on business profitability.
Low	2	This is an asset which is replaceable, and whilst the replacement cost is relatively costly, there would only be a moderate impact on overall business profitability.
Negligible	1	This is an asset which forms a part of the process, but does not have real economic value within the business process. It can easily be replaced at minimal cost. Its loss wouldcause minimal or negligible damage to the process or the organization.

The Highest of C-I-A would be taken as the asset value for Risk Impact Rating Calculation.

Guidelines for Identifying Threats and Vulnerabilities

Vulnerability is defined as a weakness that is associated with an asset, which exposes that asset to different threats.
This weakness could be because of an inherent attribute of the asset, the process, the business, or the environment.
This weakness may be exploited by a threat, causing unwanted incidents resulting in loss or damage to the assets.
A **vulnerability** by itself does not cause any harm; it is a condition, or a set of conditions, that may allow a threat to affect an asset.

A **threat** has the potential to cause an unwanted incident which may result in harm to a system, process, or organization and its assets.
This harm can occur from a direct or indirect attack on the organization's information and its resources.
Threats can originate from accidental or deliberate sources or events.

Asset owners and users should list the different threats and vulnerabilities they perceive to the assets.

The **vulnerability identification** should identify the weaknesses in the:

- Physical environment
- Personnel
- Management
- Administration procedures and controls
- Hardware
- Software

- Communications equipment and facilities

Tools

Rezolve employs the usage of **Vanta** for connecting with all assets and reporting any vulnerabilities and threats.
Rezolve also does **VAPT scans** as part of its major release process to identify any software vulnerabilities that get created as part of the software release.
These are as per **OWASP** standards.
Apart from the above, Rezolve also employs external **VAPT assessment** for the live production software periodically.

Evaluation of Vulnerabilities and Threats

The following criteria are to be applied when evaluating vulnerabilities:

Level	Score	Definition
Highestexposure of asset	5	Thisvulnerabilityisaninherentweaknessoftheasset. Thereisnosolutionavailableordifficulttoapply.
Highexposureof asset	4	This vulnerability is weakness caused due to the procedural, customer or business requirements.
Mediumexposure of asset	3	Thereisanunofficialnon-vendorsolutionavailabletofixthevulnerability.
Low or minimal exposureofasset	2	Acompletevendorsolutionisavailable, Eitherthevendorhasissuedanofficialpatchoranupgradeisavailable.
Negligibleexposure of asset	1	This vulnerability is a weakness causing negligible exposure factor for the asset. So even if it gets exploited the impact will be negligible causing no damage to the asset.

The following criteria are to be applied when evaluating the threats.

Level	Score	Definition
Devastating	5	Incidents at this level can be **devastating** and need an immediate and appropriate response. Significant potential financial losses, coupled with a public loss of credibility are all symptoms of this type of incident.
Critical	4	**Critical** incidents are those from which you should be able to recover. With careful management of the incident and the implementation of appropriate safeguards, a 'medium'financiallossandpublicembarrassmentarelikelytobeexperienced.
Controllable	3	The impact of a **controllable** incident is likely to be short term and is controllable. With the right safeguards and response, the impact could perhaps be reduced to minor embarrassment and minimal cost.
Irritating	2	Incidents classified as **irritating** are likely to be ephemeral and generally will result in little more than a localized irritation. Whilst you safeguard against them, they should be straightforward to avoid and manage.
Negligible	1	Theimpactofthethreatisnegligible

For example, a threat like failure of communication lines during business hours will lead to loss of productivity, hence the threat is rated as high or highest. A threat like system (desktop) failure will cause some disruption to business, but the damage would not be large, hence the threat is rated as medium or low.

Evaluate the Vulnerabilities-Threats (VT) Pair

A vulnerability and threat together cause a risk factor for an asset, and hence we need a single value that gives us an idea of the impact of the incident caused due to the threat exploiting a particular vulnerability. When talking about risk, it is difficult to address a vulnerability or threat in isolation.

The following table is used to calculate the **VT Pair** for the incident defined by the vulnerability and threat. By creating a single reference to an incident, the subjectivity of the evaluation of the threats and vulnerabilities is reduced considerably.

VTPairValue	**Vulnerabilities**				
Threats	**1**	**2**	**3**	**4**	**5**
1	2	3	4	5	6
2	3	4	5	6	7
3	4	5	6	7	8
4	5	6	7	8	9
5	6	7	8	9	10

The **VT pair** value ranges from 2-10, where **"10"** indicates the highest impact and **"2"** indicates the least impact.

Guidelines for Calculating the Impact Rating

An **Impact Rating** is calculated for each information asset and in respect of each incident (vulnerability-threat pair) listed against that asset.

An **Impact Rating** calculation comprises the following components:

ImpactRatingComponent	Range
Value oftheInformationAssets	1-5(5beinghighest)
Value ofthe Vulnerability-ThreatPair	2-10(10beinghighest)

Impact Rating (IR) = Asset Value * VT Pair Value

To calculate the **Risk Impact Rating**, it is necessary to multiply each of the **Impact Components** with each other. The **HIGHER** the resultant score, the higher the **Impact Rating**. The highest **Impact Rating** on this basis is therefore, 250, with the lowest possible **Risk Impact Rating** being 2.

Evaluating the Probability of Occurrence

The following criteria are to be applied when calculating a rating score for the Probability of Information Security Incidents:

Level	Score	Definition
Very high	5	Theincidenthasaveryhighprobabilityofoccurringunlesscorrectiveactionisapplied.
High	4	There is considered to be a high probability that this incident will occur if corrective action is not applied.
Medium	3	Thereisconsideredtobeareasonableprobabilitythatthisincidentwilloccur.
Low	2	Therisksofthisincidenthappeningareconsideredtobelow.
Verylow	1	Thereisverylowprobabilitythatthisincidentwillhappen.

GuidelinesforCalculatingtheRiskRating

ARisk Rating is calculated for each *information asset* and in respect of each incident (vulnerability-threat pair) listed against that asset.

A'RiskRating'calculationcomprisesthefollowingcomponents:

RiskRatingComponent	Range
Valueof the Impact Rating	2-10(10beinghighest)
ProbabilityofOccurrenceofaparticularIncident	1-5(5beinghighest)

Risk Rating (RR) = Impact Rating * Probability of Occurrence

To calculate the **Risk Rating**, it is necessary to multiply each of the **Risk Impact Components** with each other. The **HIGHER** the resultant score, the higher the **Risk Rating**. The highest **Risk Rating** on this basis is therefore, 250, with the lowest possible **Risk Rating** being 2.

The Risk rating helps us to prioritize the risk into three different levels:

- **Low,** where the RIR ranges from 2-49 (i.e. $2 \leq RIR < 50$)
- **Medium,** where the RIR ranges from 50-99 (i.e. $50 \leq RIR < 100$)
- **High,** where the RIR ranges from 100-250 (i.e. $100 \leq RIR \leq 250$)

Guidelines for Identifying Existing Controls:

The **risk impact rating** gives us a picture of the overall risk that a particular asset is exposed to. The next step is to identify the existing security controls that have already been implemented. These controls help us to identify the current level of risk faced by the organization.

The **asset owners** and **users** should list the existing controls against each risk that has been identified and list the existing level of risk as **Low, Medium,** or **High.**

The criteria for identifying whether the existing risk level is **low, medium,** or **high** are as follows:

- **Low** - Asset exposure is minimal after considering existing controls.
- **Medium** - Asset exposure is medium even after the application of existing controls. The existing controls do not address the incident and asset completely.
- **High** - Asset exposure is high even after the application of existing controls.

Risk Treatment:

Priority of Risk Treatment

We are establishing controls for all the risks identified in the **Risk Assessment**. The priority of treating the identified risks is as below:

- Any **risk impact rating** which is **HIGH** should trigger an immediate investigation for further controls.
- Any **risk impact rating** which is **MEDIUM** should trigger an investigation for further controls after treating **HIGH** rating risks.
- Any **risk impact rating** which is **LOW** should trigger an investigation for further controls after treating **MEDIUM** rating risks.

Risk Mitigation:

Based on the risk appetite of **Rezolve.ai**, the following approaches may be taken for dealing with the risk:

- **Transfer the risk:** for instance, take an insurance cover.

- **Accept the risk:** if the **risk impact rating** is **medium**, **low** or within the risk appetite of **Rezolve.ai**, nothing needs to be done.
- **Reduce the risk:** reduce vulnerabilities by putting more preventive controls in place, or reduce the impact of the threat with more corrective/detective controls.
- **Avoid the risk:** by removing the threat (i.e. relocating away from an earthquake-prone zone, etc.).

The status of the information assets prior to corrective activity is called **'Existing Risk Level/Absolute Risk Level'** and the status after corrective activity is called **'Residual Risk.'**

Actions to Address Risks and Opportunities:

Rezolve.ai, while planning for the **information security management system**, has taken into consideration the following issues to determine the risks and opportunities that need to be addressed to ensure the information security management system can achieve its intended outcome(s):

- Prevent, or reduce, undesired effects.
- Achieve continual improvement as under **Clients:** Unless there are major changes to the overall business or the foreign exchange norms, the business would not be impacted and is likely to grow as per the current trends and as per the historical growth rate achieved.

Employees

The **recruitment** and **training process** is such that the best pool of resources is hired and nurtured. Attrition is under control, and contingencies are in place so that the business-as-usual activities can be managed through the availability of resources.

Vendors

Key vendors for **Rezolve.ai** are the **ISPs** and other providers for **IT procurement**. Since there are multiple providers, the likely impact has been taken care of.

The organization sees opportunities such as the growth in the overall records and **information management business** and aims to become a leading company in this business sector. Additionally, it leverages opportunities by acquiring companies in the same sector.

Risk Types and Identification of Risk

Not all of the following risks will be applicable to every asset. However, complex or significant arrangements may have definable risks in most areas. The following summary of risks is though not considered all-inclusive:

Strategic Risk

Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the **Rezolve.ai** strategic goals.

Reputation Risk

Reputation risk is the risk arising from negative public opinion.

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.

Transaction Risk

Transaction risk is the risk arising from problems with service or product delivery. A vendor's failure to perform as expected by customers or **Rezolve.ai** due to reasons such as inadequate capacity, technological failure, human error, or fraud, exposes **Rezolve.ai** to transaction risk.

Credit Risk

Credit risk is the risk that a vendor, or any other creditor necessary to the vendor relationship, is unable to meet the terms of the contractual arrangements with **Rezolve.ai** or to otherwise financially perform as agreed.

Compliance Risk

Compliance risk is the risk arising from violations of laws, rules, or regulations, or from non-compliance with internal policies or procedures or with **Rezolve.ai** business standards.

Project Risk Management

There are some inevitable risk factors that need to be considered during the project execution. For **Rezolve.ai**, it could be major changes in the application due to technology changes. Identification of risks in such projects and mitigation of the same is crucial for the success and timely completion of any project.

Risks associated with the project, which could have an impact on effort, schedule, quality, or client satisfaction, will be identified at the beginning of the project and monitored continuously. Appropriate action will be taken to reduce risks based on the contingency plans drawn for each of these as and when required.

Review of Risk Profile

The risk that the organization carries with regard to the threat to its information is the result of a combination of factors. Any change to either of these factors will alter the risk profile.

Currently, the **process owners** will be the **risk owners** and will have the responsibility of identifying the risks and presenting them to the management in the reviews.

Reviewing of **Information Security** on a regular basis is vital to ensure that the safeguards employed continue to offer the appropriate level of protection.

Criterion for Risk Assessment:

The **Risk Assessment & Treatment Plan** shall be reviewed:

- At least once every year.
- In the event of any major changes brought about within the organization such as introducing new application/HW appliances/Technology-based solution/Change in Processes.
- Any of its internal/external functional processes.
- Structural changes in the management.

NOTE:
Next review cycle for this policy is **March 2027**. Management can review the policy anytime and can make changes depending on the situation.

*All documents related to policies and procedures and any reference to **Actionable Science** is as good as **Rezolve.ai**.*