Veranda

RISK ASSESSMENT AND TREATMENT PLAN

©2024 This document may be confidential and legally privileged. It is intended solely for use by Veranda Learning staff and others authorized to receive it.

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

1 Introduction

A crucial part of an ISMS is the management of risks the company faces while working to achieve its business objectives.

A Risk in Veranda Learning is defined as an occurrence of an unwanted event or the non-occurrence of a wanted event that adversely affects a business in a way that,

- The business is not able to meet business goals.
- The assets of the business are not protected from unwanted loss.
- There is non-compliance with organization policies and procedures or external legislation and regulation.
- The confidentiality, integrity, and availability of information are adversely affected.

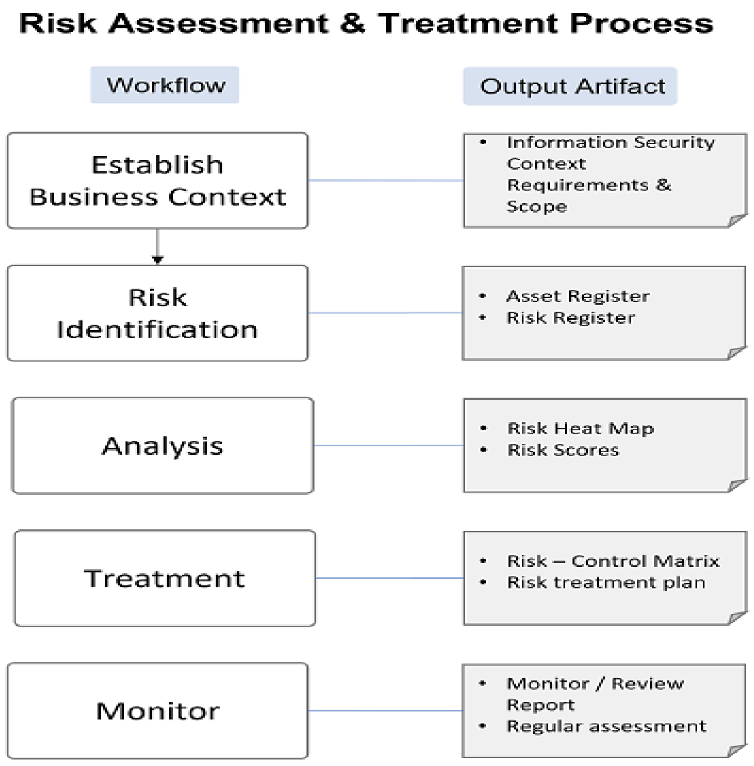
Veranda Learning has put in place an effective, repeatable, and practical risk assessment and treatment process to mitigate the potential impact of risks in case a risk gets realized.

The purpose of this document is to describe this process set by Veranda Learning.

2 Risk assessment and treatment process

2.1 Process Overview

The image below summarizes the risk assessment and treatment process, workflow steps, and the desired output artifact.



2.2 Establish the context

The context of the risk assessment is crucial in Veranda Learning because as the context of the business changes, along with the internal and external issues, the risk assessment is updated and changed. The internal context includes (as per ISO 4.0 Requirement. Refer to template **Information Security Context Requirements And Scope**):

- Governance, organizational structure, roles, and accountabilities
- Products and Services provided by the organization, including
- Both internal and external issues
- Business goals and objectives
- Information systems, information flows, and decision-making processes (both formal and informal)
- Stakeholders and their requirements
- The organizations culture
- Key contractual and other supplier relationships

Other factors that influence the risk assessment are

- 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 (Pll)

2.3 Define the scope

To better prioritize the risk at Veranda Learning, the risk assessment scope is also defined based on the following factors.

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

2.4 Define the criteria for risk assessment

In Veranda Learning risk assessment is performed at regular intervals and under the following circumstances.

- A comprehensive risk assessment covering all information assets as part of the initial implementation of the risk management process.
- Updates are part of the management review process, which should identify changes to assets, threats, vulnerabilities, and possibly risk levels.
- As part of large & significant projects that involve a significant change to the organizations information assets

- As part of the IT change management process when assessing whether proposed changes should be approved and implemented.
- Significant external changes affecting the organization include changes to relevant legislation, mergers, and acquisitions.
- When evaluating and selecting suppliers, particularly those that will play a part in the delivery of cloud services to customers
- Periodic assessment of critical suppliers and vendors.

At the minimum, a risk assessment is performed annually.

2.5 Identify risks

Veranda Learning follows an asset-based / information system-based risk assessment approach. This section outlines the steps involved in an asset-based risk assessment approach.

[Note - if you choose to conduct a risk assessment based on a different approach, please update this section appropriately. Here is a high-level list of assessment techniques. Article]

2.5.1 Compile/maintain an asset inventory

A complete inventory of assets is compiled and maintained by Veranda Learning . The definition of an asset is "anything that has value to the organization" and is therefore worthy of protection. This will include customer data that Veranda Learning stores, supply chain processes, employee data, etc.

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 CONTROLMAP. Within the inventory, every asset has the following attributes

1. Ownership details
2. Type of asset
3. CIA (Confidentially, Integrity, Availability) score
4. Asset value
5. Stores PII or not
6. Retention Period

2.5.2 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 vehicle impact, or malicious attacks such as viruses, theft, or sabotage. Threats will apply to one or more of the assets confidentiality, integrity, and availability.

2.5.3 Assess existing vulnerabilities

Vulnerabilities/weaknesses are listed and are associated with an asset type or an asset that demonstrates that weakness.

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

2.5.4 Identify risk scenarios

In addition to assets, you may also identify specific scenarios which may have inherent risks associated with them. These risks are identified during periodic reviews and regular meetings with senior management, project teams, and department heads. Threats and shortcomings that hinder teams from achieving their objectives are known as probable risks.

2.6 Risk analysis

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

2.6.1 Assess the likelihood

An estimate of the likelihood of a risk occurring is based on various factors, including knowledge from similar organizations in the same industry or location and whether sufficient motive, opportunity, and capability exist for a threat to be realized.

The likelihood of each risk is graded on a numerical scale of 1 (low) to 5 (high). The details are in the table below.

Score	Label	Description
1	Rare	It 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 will not
3	Possible	On balance, the risk is more likely to happen than not
4	Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Certain	Either it 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.

2.6.2 Assess the impact

An estimate of the impact of the loss of confidentiality, integrity, or availability on the organization 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). The general guidance for the meaning of each grade is given in table 2.

GRADE	Description	Health & Safety	Financial	Service	Legal & Compliance	Reputation
1	**Negligible**	No injury or illness	Corporate Financial loss of less than $1 million	Service disruption of <4 hours	No regulatory or civil action	The standard level of complaints.
2	**Marginal**	Minor isolated illness or injury where medical intervention is not required	Corporate Financial loss of $1-$5 million	Service disruption of 4 - 8 hours	Non-conformance identified by an external regulator with a request for further explanation	Regulator issues notices, corrective action order and/or penalties, common law liability confirmed.
3	**Significant**	Localized illness or injury where medical intervention is required	Corporate Financial loss of $5-$10 million	Service disruption of 8 - 24 hours	Non-conformance identified by an external regulator with an infringement notice issued	Adverse reaction among stakeholders. State and national media reporting.

GRADE	Description	Health & Safety	Financial	Service	Legal & Compliance	Reputation
4	**Critical**	Widespread illness or multiple injuries where medical intervention is required	Corporate Financial loss of $10-$50 million	Service disruption of 24 -48 hours	Regulator issues notices, corrective action order and/or penalties, joint law liability confirmed.	State and national media reporting (1 week). Board at risk of sanctions.
S	**Catastrophic**	Fatality or widaespread hospitalization	Corporate Financial loss of > $50 million	Service disruption of > 48 hours	Criminal prosecution imprisonment of the organization officer	State and national media reporting (> 1 week). Board at risk of dismissal.

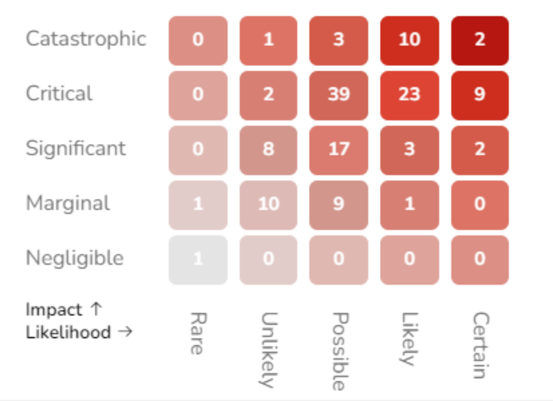
More detailed guidance may be defined for each impact grade, depending on the subject of the risk assessment. The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

2.6.3 Risk classification

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

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



Impact ↑ Likelihood →	Rare	Unlikely	Possible	Likely	Certain
Catastrophic	0	1	3	10	2
Critical	0	2	39	23	9
Significant	0	8	17	3	2
Marginal	1	10	9	1	0
Negligible	1	0	0	0	0

[Note - you may change the definition of high, medium, and low classifications based on your general risk appetite e g. you may decide that only risks with a score of 16 or more will be classified as high.]

Type of risks

The classification score must be applied to the different types of risks.

Inherent: This is the risk that exists before any mitigating controls are applied

Current: This is the risk that exists after the mitigating controls are applied

Target: This is the aspirational risk level the company wants to get to by improving the effectiveness of the controls.

2.7 Risk Evaluation

Risk evaluation aims to decide which risks can be accepted and which need to be treated. This will consider the risk acceptance criteria established for this specific risk assessment (see Risk Acceptance Criteria, above).

The matrix in Figure 2 shows the classifications of risk, where light red indicates that the risk is below the acceptable threshold. The orange and red areas generally indicate that the risk does not meet the acceptance criteria and 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 exposure to the organization.

2.8 When is a risk accepted

Criteria for accepting risks will vary according to several factors, which may change over time. These include the organizations general or cultural attitude to risk, the prevailing financial climate, legal and regulatory requirements, the current view of top management, and the sensitivity of the specific assets or business areas within scope.

Before carrying out a risk assessment, the criteria for accepting risks must be discussed by appropriate people with knowledge of the subject area and, if necessary, top management. This discussion should establish guidelines for the circumstances in which risks will be accepted, i.e., not subjected to further treatment.

These criteria may be expressed in several different ways, depending on the scope of the risk assessment, and may include situations where:

- The cost of an appropriate control is judged to be more than the potential loss
- Known changes will soon mean that the risk is reduced or disappears completely
- The risk is at or lower than a defined threshold, expressed as a level e g. low or as a quantified amount e g., a financial sum
- An area is known to be high risk but also high potential reward, i.e., a calculated risk.

These acceptance criteria must be documented and used as input to the risk evaluation stage of the assessment process.

3. Risk assessment report

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

- Assets
- Threats
- 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. It must be signed off by management before continuing, particularly concerning the risks recommended for acceptance.

4. Risk treatment

For those risks that are agreed to be above the threshold for acceptance by [Veranda Learning], the options for treatment will then be explored.

The overall intention of risk treatment is to reduce risk classification 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

4.1 Risk treatment options

The following options may be applied to the treatment of the risks that have been agreed to be unacceptable:

1. Avoid the risk by taking action that means it no longer applies
2. Reduce the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk
3. Transfer the risk to another party e g. insurer or supplier
4. Share the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk
5. Accept the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk

Judgment will be used in deciding which course of action to follow based on a sound knowledge of the circumstances surrounding the risk e g.

- Business strategy
- Regulatory and legislative considerations
- Technical issues
- Commercial and contractual issues

The Risk Manager will ensure that all parties with an interest or bearing on the risk treatment are consulted, including the risk owner.

4.2 Applying controls

Veranda Learning identifies and applies appropriate controls to address the risk treatment requirements identified as part of the risk assessment exercise.

4.3 Risk treatment plan

The evaluation of the treatment options will result in the production of the risk treatment plan, which will detail:

- 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)
- Timescales for actions
- Expected residual risk levels after the controls have been implemented.

5. MAPPING WITH INDUSTRY STANDARDS

This policy addresses the following risks related to Risk Management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Non-Compliance with the standards and regulations	5.36 Compliance with policies, rules and standards for information security
Information Leakage	7.10 Storage media
Failure to identify security risks	C 6.1 Actions to identify risk and opportunities C 6.2 Information security objectives and planning to achieve them
Lack of systematic approach to risk management	C 8.2 Information security risk assessment C 8.3 Information security risk treatment