Risk Management Policy

Version number	1.1
Last Approved	Apr 25, 2025
Classification	PUBLIC

Overview

We recognize that the Company is exposed to various risks due to the nature of our operations. This policy provides a framework for managing those risks, ensuring the organization's continued success and viability.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview.

Purpose

This policy establishes principles and requirements to ensure that risk to the Company’s business are reliably considered and managed in alignment with the Company’s risk posture as well as its legal, regulatory, and contractual commitments.

Scope

The Risk Management Policy establishes the process for which risks are identified, reviewed, and treated. This policy covers risks such as (but not limited to):

- Business Process or Control Failures
- Cyberattack;
- Disruptions to Systems;
- Financial;
- Fraud;
- Pandemics and Natural Disasters (Floods, Hurricanes, Tornadoes, Earthquakes);

- Privacy Compliance; and
- Workforce disruption.

SOC 2: CC3.3

COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Risk Assessment

The company will maintain a Corporate Risk Register, and ensure that risk treatment plans are identified and implemented as necessary to align with the Company's objectives.

SOC 2: CC3.1

COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. The Corporate Risk Register will be considered when planning for the ISMS and will be used to record risks and opportunities specific to it while taking into consideration any group-wide factors. These factors will be assessed and contribute to a separate document; the information security risk assessment.

SOC 2: CC5.1

COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Ongoing Risk Assessment will capture and scrutinize relevant risks and implement the following:

- Risk scoring is used to benchmark and track the change in risks and allow for them to be prioritized as required.
- Corrective and preventive action will be determined as required. Each action will be given ownership to an appropriate person to be completed within a suitable timescale.

SOC 2: CC4.2

COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Responsibilities

- **Management** is responsible for contributing to the identifications of risks and carrying out treatment plans to address actionable risks as appropriate.
- **The GRC team** is responsible for driving the risk assessment process and engaging appropriate stakeholders as necessary.

- **The VP Information Security** is accountable for the overall performance of the risk assessment process and ensuring that it reliably supports the Company's objectives.

Implementation

Risks are categorized, documented, and assessed to determine the extent to which they are actionable given the organizations risk posture. Actionable risks are assigned ownership and treatment plans.

Risks and treatment plans are periodically reviewed to monitor changes and treatment status.

The **VP Information Security** and **Management** responsible for reviewing the Corporate Risk Register on at least a quarterly basis, or more frequently as changes dictate.

ISO 27001:2022 Control 6.1.1

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:
a) ensure the information security management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) achieve continual improvement.
The organization shall plan:
d) actions to address these risks and opportunities; and
e) how to:

1. *integrate and implement the actions into its information security management system*
2. *evaluate the effectiveness of these actions.*

Methodology

The Company use the following methodology for identifying and evaluating risks.

Identifying & Tracking Risks

The GRC Team regularly engages stakeholders from across the organization to identify emerging risks and to assess changes to existing risks. The results of these assessments are captured within the Corporate Risk Register. On a quarterly basis, the GRC Team formally reviews notable changes to the Corporate Risk Register with the Executive Steering Committee.

Risk Assessment, Classification, and Threshold

Risks are scored by Likelihood and Severity, based on a numeric scale from 1 (lowest) to 5 (highest).

The Risk Rating for each risk is calculated as the product of Likelihood and Severity, resulting is a rating that ranges between 1 and 25.

The Company classifies Risk Ratings as follows:

Rating	Risk Classification
1-6	**Low**
7-15	**Medium**
16-25	**High**

The classification process informs decision-making on whether the Company will **Decrease**, **Avoid, Share**, or **Retain the risk.**

Risks that classify as **Medium** or **High** require either:

- A Treatment Plan and timeline for reducing the risk to a **Low** classification;
- A justification for any alternative that is reviewed and approved at the subsequent Executive Security Steering Committee meeting.

ISO 27001:2022 Control 6.1.2

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1. *the risk acceptance criteria; and*
2. *criteria for performing information security risk assessments;*

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1. *apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and*
2. *identify the risk owners;*

d) analyses the information security risks:

1. *assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;*
2. *assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and*
3. *determine the levels of risk;*

e) evaluates the information security risks:

1. *compare the results of risk analysis with the risk criteria established in 6.1.2 a); and*
2. *prioritize the analyzed risks for risk treatment.*

The organization shall retain documented information about the information security risk assessment process.

ISO 27701:2019 Control 5.4.1.2c-d

c) The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.
NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

d) The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

ISO 42001:2023 Control 6.1.2

The organization shall define and establish an AI risk assessment process that:

a) is informed by and aligned with the AI policy (see 5.2) and AI objectives (see 6.2);

NOTE When assessing the consequences as part of 6.1.2 d) 1), the organization can utilize an AI system impact assessment as indicated in 6.1.4.

b) is designed such that repeated AI risk assessments can produce consistent, valid and comparable results;

c) identifies risks that aid or prevent achieving its AI objectives;

d) analyses the AI risks to:

1. *assess the potential consequences to the organization, individuals and societies that would result if the identified risks were to materialize;*
2. *assess, where applicable, the realistic likelihood of the identified risks;*
3. *determine the levels of risk;*

e) evaluates the AI risks to:

1. *compare the results of the risk analysis with the risk criteria (see 6.1.1);*
2. *prioritize the assessed risks for risk treatment.*

The organization shall retain documented information about the AI risk assessment process.

SOC 2: CC3.2

COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Risk Treatment

Risk Ownership is assigned to the Management Executive with ultimate accountability for managing a given risk; treatment ownership is assigned to the Management individual responsible for implementing the treatment plan for that risk.

The GRC Team negotiates treatment plans with risk action owners to achieve agreed upon treatment objectives.

The GRC Team regularly monitors treatment plans and records formalized updates at least quarterly.

Once a treatment plan is successfully completed, the related risk is reassessed and reclassified as appropriate.

ISO 27001:2022 Control 6.1.3

The organization shall define and apply an information security risk treatment process to:
a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment
option(s) chosen;
NOTE Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.
d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and

c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

e) formulate an information security risk treatment plan;

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.
The organization shall retain documented information about the information security risk treatment process.

ISO 27001:2022 Control 8.3

The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.

ISO 27701:2019 Control 5.4.1.3c-d

c) The controls determined in ISO/IEC 27001:2013 6.1.3 b) shall be compared with the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A to verify that no necessary controls have been omitted.

When assessing the applicability of control objectives and controls from ISO/IEC 27001:2013 Annex A for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.

d) Produce a Statement of Applicability that contains:
— the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)];
— justification for their inclusion;
— whether the necessary controls are implemented or not; and
— the justification for excluding any of the controls in Annex A and/or Annex B and ISO/IEC 27001:2013, Annex A according to the organization's determination of its role (see 5.2.1).

Not all the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation and/or regulation including those applicable to the PII principal.

ISO 42001:2023 Control 6.1.3

Taking the risk assessment results into account, the organization shall define an AI risk treatment process to:

a) select appropriate AI risk treatment options;

b) determine all controls that are necessary to implement the AI risk treatment options chosen and compare the controls with those in Annex A to verify that no necessary controls have been omitted;

NOTE 1 Annex A provides reference controls for meeting organizational objectives and addressing risks related to the design and use of AI systems.

c) consider the controls from Annex A that are relevant for the implementation of the AI risk treatment options;

d) identify if additional controls are necessary beyond those in Annex A in order to implement all risk treatment options;

e) consider the guidance in Annex B for the implementation of controls determined in b) and c);

NOTE 2 Control objectives are implicitly included in the controls chosen. The organization can select an appropriate set of control objectives and controls from Annex A. The Annex A controls are not exhaustive and additional control objectives and controls can be needed. If different or additional controls are necessary beyond those in Annex A, the organization can design such controls or take them from existing sources. AI risk management can be integrated in other management systems, if applicable.

f) produce a statement of applicability that contains the necessary controls [see b), c) and d)] and provide justification for inclusion and exclusion of controls. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment and where they are not required by (or are subject to exceptions under) applicable external requirements.

NOTE 3 The organization can provide documented justifications for excluding any control objectives in general or for specific AI systems, whether those listed in Annex A or established by the organization itself.

g) formulate an AI risk treatment plan.

The organization shall obtain approval from the designated management for the AI risk treatment plan and for acceptance of the residual AI risks. The necessary controls shall be:

— aligned to the objectives in 6.2;

— available as documented information;

— communicated within the organization;

— available to interested parties, as appropriate.

The organization shall retain documented information about the AI risk treatment process.

ISO 42001:2023 Control 6.1.4

The organization shall define a process for assessing the potential consequences for individuals or groups of individuals, or both, and societies that can result from the development, provision or use of AI systems.

The AI system impact assessment shall determine the potential consequences an AI system's deployment, intended use and foreseeable misuse has on individuals or groups of individuals, or both, and societies.

The AI system impact assessment shall take into account the specific technical and societal context where the AI system is deployed and applicable jurisdictions.

The result of the AI system impact assessment shall be documented. Where appropriate, the result of the system impact assessment can be made available to relevant interested parties as defined by the organization.

The organization shall consider the results of the AI system impact assessment in the risk assessment (see 6.1.2). A.5 in Table A.1 provides controls for assessing impacts of AI systems.

NOTE In some contexts (such as safety or privacy critical AI systems), the organization can require that discipline-specific AI system impact assessments (e.g. safety, privacy or security impact) be performed as part of the overall risk management activities of an organization.

SOC 2: CC9.1

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon

Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Apr 25, 2025
Review cycle	ANNUAL	
Next review date	Apr 22, 2026	

Version History

Date	**Author(s)**	**Version**	**Changes**
Apr 25, 2025	@Paul Gordon	1.1	References to controls/standards restructured.
Apr 22, 2025	@Art Machado @Paul Gordon @angelina.kilmer	1.0	Created standalone Risk Management Policy from BCP/DR Policy