Business Continuity and Risk Management Policy

Version number	2.12
Last Approved	Mar 12, 2024
Classification	PUBLIC

Overview

The Business Continuity and Risk Management defines the process in which The Company performs Business Impact Analysis to develop a risk-based resiliency plan.

Disaster Recovery (DR) addresses customer-facing continuity in its hosted systems and is inclusive of customer data.

The policy ensures that The Company will perform regularly scheduled risk assessments and BCP / DR testing to align The Company's capabilities with its risk posture.

Applicability

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

Purpose

It is The Company's policy to ensure that risk of interruption to its business operations are reduced to commercially reasonable levels.

Scope

Business Continuity and Risk Management Policy encompasses the comprehensive set of processes responsible for ensuring protection and continued availability of Company assets and applications at all times. This policy covers subsequent remediation plans for risks such as (but not limited to):

- cyber threats;
- natural disasters;
- fraud;
- attacks to the privacy, confidentiality, availability, integrity, and authenticity of client data.

SOC 2: CC3.3

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

Business Continuity Planning

The Company shall complete the following components of the Business Continuity Planning effort on an annual basis:

Business Impact Analysis

The Business Impact Analysis may include any of the following, as deemed appropriate, through the Risk Assessment Process:

Elements	Guidance
Business Process Inventory	• Captures general information about the process as well as the dependencies on which the process relies, including not only IT systems but also physical, environmental, human or other dependencies • Indicates whether or not each process is mission critical
Dependency Inventory	• Captures dependencies on which business processes rely • Captures estimated or actual recovery time objectives for each dependency
Impact Assessment	Captures management's assessment of the impact to The Company in the event of a critical process outage.
Risks	Describes known risks to business processes continuity
Recovery Plans	Describes existing recovery plans that have been developed for the department's operations
Subcontractors & Suppliers	Lists (and describes the functions performed by) any subcontractors or suppliers that are critical to the continuity of business processes
Other comments	Documents other concerns management wants included in the Business Impact Analysis

Business Continuity Risk Assessment

The Business Continuity Risk Assessment shall quantify the risk of a process outage based on a department's or a process' tolerance for downtime, as compared to recovery time objectives, for all of its mission critical process dependencies.

The Business Continuity Risk assessment is a subsection of The Company's general Risk Assessment process, as defined within this policy.

Business Continuity Plan

At a minimum, the Business Continuity Plan shall address the following scenarios:

- SaaS Customer Facing System outage
- Corporate IT & Internal Business System outage
- Regional natural disaster
- Regional pandemic

Facilities Dependencies

Due to The Company's fully remote-capable workforce, traditional considerations related to facilities dependencies are not applicable; for example, internal call trees and stakeholder communication plans for in-scope facility locations. Residual facility dependencies are Third

Party and therefore, stakeholder contacts and communication plans are maintained via vendor management process.

Plan Improvements, Testing & Risk Acceptance

Improvements to the Business Continuity Plan and acceptance of residual risk to Business Continuity shall be performed by the Executive Security Steering Committee for Business Continuity Planning efforts.

On an annual basis, the Company will perform a thorough test of the Business Continuity Plan to evaluate its comprehensiveness and effectiveness relative to the Company's Business Continuity objectives and commitments.

Any critical deficiencies identified during Business Continuity or Disaster Recovery testing will either be addressed in alignment with the Company's Vulnerability Remediation SLAs (30 days for Critical/High; 90 days for Medium) or contemplated in the subsequent Executive Security Steering Committee to determine appropriate risk management measures. Ownership of follow-up and remediation responsibilities for all critical findings are assigned promptly upon completion of annual testing (not to exceed 30 days).

Risk Assessment

The Company will contribute to the LTG corporate risk register, and play an active part in implementing any improvements and carrying out any activities required by LTG.

The Company will also maintain a separate register of information security and privacy risks, together with objectives for the running and improvement of the ISMS, in line with the requirements of ISO/IEC 27001:2013 and 27701:2019

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 LTG 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.

The 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. Risk scoring is a method of determining acceptable and unacceptable risks and this methodology was created by LTG's CFO and Finance team.
- 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** are responsible for ensuring that activities assigned to The Company by LTG to address items on the corporate risk register are carried out, and that information security risks assessment findings are addressed appropriately.
- **The GRC team** are responsible for data gathering during the annual review of the LTG corporate risk register and updating the current state of activities

- **The VP Information Security** is responsible for driving The Company's risk assessment process and liaising with the GRC team to update the corporate risk register

Implementation

Risks are identified by area, assessed for impact, assigned an owner, and given monitoring and mitigation actions.

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

ISO 27001:2013 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 Risks

The Company use an assets-threats-vulnerabilities method for identifying risks by following the process below. This methodology will be followed by the VP Information Security, VP Hosting Systems and Operations, and suitably experienced staff working on activities within the scope of ISO/IEC 27001:2013 and 27701:2019.

1. At each step of the process outlined the Information Security Statement, we identify the assets that are required.
2. Against each asset, we identify the threats that are present.
3. And against each threat, we identify the particular vulnerabilities that give rise to the threat.

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

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

Risk Owner

When identifying the Risk Owner, three principal criteria are considered.

- Whether there is a 'natural' owner based on roles and responsibilities. For example, physical security might fall under the VP Information Security, hosting issues under the VP Hosting Systems and Operations, and IT infrastructure issues under the LTG IT Team.
- Whether the individual has sufficient authority within the organization to bear the responsibility.
- Whether the individual has sufficient skills, knowledge and experience to deal with the threat and address the vulnerabilities.

Recording the Risk Assessment

The risk assessment and risk treatment are combined into one tab, as are the risk treatment plan and assessment report. It is stored in the GRC drive, where only authorized individuals are able to access it. Access must be requested from a drive owner.

ISO 27001:2013 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.

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.

Information Security Risk Treatment

Once identified, The Company will select appropriate risk treatments for the risks identified, using the Annex A controls to help identify what is required and mapping those against the Statement of Applicability where applicable. Details of the risk treatment, risk owners and residual risk levels are contained within the overall Risk Register.

- The **VP Information Security** is responsible for initially completing the risk management report and keeping it updated

SOC 2: CC5.2

COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

The Risk Register sheet contains high-level details of the chosen treatment. The process for completing the treatment section is as follows.

- Having calculated the risk and identified the owner, the next step is to identify the treatment option. This is a statement identifying what we will do with the risk and the choices are:

1. **Decrease the risk** - put in place some form of protection or mitigation
2. **Avoid the risk** - for example, by completely removing or replacing the source of the risk
3. **Share the risk** - mitigation by sharing the risk, for example by purchasing insurance
4. **Retain the risk** - when the risk is deemed so low, and/or the cost of addressing is disproportionately high

- Once the option has been decided, identify treatment category. These categories are:
  - Change structure, roles and/or responsibilities
  - Implement new or upgraded technology
  - Define new rules, policies or processes
  - Do nothing

When a risk is identified and added to the Risk Register, column X contains the tracking mechanism where further details around the remediation of the risk can be found.

ISO 27001:2013 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 27001:2013 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.

SOC 2: CC9.1

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

Disaster Recovery

Disaster Recover ensures that The Company has well-defined and tested capabilities for restoring in-scope system availability and data that meets defined **Recover Time** and **Point Objectives** (RTO and RPO). The Company will maintain updated documentation of DR procedures for each system. On an annual basis, The Company will thoroughly tests its DR capabilities by conducting disaster recovery tests for each system. The results of DR testing will be measured against the recovery objectives and remediation plans identified and implemented for any gaps.

SOC 2: A1.3

The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Data Center Distance Criteria: Each data center (primary and secondary) shall be no closer than 100 miles or 160 km from its proposed regional counterpart.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview

---

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 @Sarah Zwicker (Unlicensed) @John Cole	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 12, 2024
Review cycle	ANNUAL	
Next review date	Mar 12, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 01, 2024	@angelina.kilmer	2.12	Changed Policy classification from Confidential to Public
Jun 26, 2024	@Art Machado & @angelina.kilmer	2.11	Updated Plan Improvements, Testing, and Risk Acceptance section with regards to critical deficiencies ownership and remediation. Updated Medium and Low risk ratings.
Mar 12, 2024	@Art Machado , @Sarah Zwicker (Unlicensed) , @Paul Gordon	2.10	Annual review, approver change.
May 16, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	2.9	Remediation timeline alignment to Vulnerability Management policy. Considerations for facilities.
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	2.8	Annual Review, logo change, update to Risk Assessment section
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	2.7	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	2.6	Title change for VP InfoSec, Annual Review
Jun 22, 2021	@Sarah Zwicker (Unlicensed) & @Art Machado	2.5	Updated policy to reflect changes in the Risk Assessment section.
Mar 10, 2021	@Sarah Zwicker (Unlicensed)	2.4	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.3	Reformatting, policies linked
Jan 26, 2021	@John Cole	2.2	Annual review, role title change

Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.1	Changed owner. Added sections to refer to LTG policies and organizational change.