Internal Audit and Compliance Policy

Version number	3.4
Last Approved	Aug 29, 2024
Classification	PUBLIC

Overview

The Internal Audit and Compliance Policy establishes the use of audits and/or other evaluation techniques to ensure effective oversight of controls performance and hosting activity.

The Company shall establish a process to ensure that our operations and products are in compliance with applicable laws, regulations, policies, procedures, and the code of conduct.

Applicability

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

Purpose

It is The Company's policy to ensure compliance with the policies and standards set forth by the Information Security Governance Framework, Security Documentation Overview.

The purpose of this policy is to ensure regular auditing and monitoring of the security and privacy controls mandated by the collective policies set forth in the Information Security Statement.

Scope

The scope of the Internal Audit and Compliance policy encompasses the comprehensive set of processes responsible for ensuring the effectiveness and adequacy of The Company's organizational and technical security and privacy measures relating to the security of customer-facing production systems and environments.

Internal Audit Policy

On an ongoing basis, the **Information Security team** will monitor compliance to Information Security policies and processes. Monitoring techniques and review processes may include, but are not limited to:

- Site visits to Company offices and data centers
- Real-time alerting of the attempted or successful transmission of restricted or sensitive materials
- Logging and automated monitoring of activities that occur on The Company's networks and systems

ISO 27001:2013 Control A.12.4.2

Logging facilities and log information shall be protected against tampering and unauthorized access.

Appropriate documented information will be retained as evidence of the monitoring and measurement results.

The **VP Information Security** is responsible for compiling and delivering the results, which will be reported on a quarterly basis to the Executive Security Steering Committee.

ISO 27001:2013 Control 9.1

The organization shall evaluate the information security performance and the effectiveness of the information security management system.
The organization shall determine:
a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; NOTE The methods selected should produce comparable and reproducible results to be considered valid.

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analyzed and evaluated;

f) who shall analyze and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results

On an annual basis, the **VP Information Security** will develop an audit plan to test the effectiveness of security controls across The Company's computing environment. The audit plan may include internally performed audits, external audits (e.g., SSAE-18 and SOC), vendor security audits, or some combination thereof. Control environments included shall be, but are not limited to:

- Corporate Information Security controls
- Production Security controls
- Physical Security controls

Management system internal audits are conducted by the **GRC Team** in order to provide an independent and impartial audit process and and adhere to a program established by the **GRC Team** at the beginning of each year. Management system audits also monitor the activities of outsourced components supplied by CITO where they interface with The Company's activities.

Nonconformities (NCN) and opportunities for improvement (OFI) arising from the audits are brought to the attention of the **VP Information Security** immediately for any corrective actions to be determined and acted upon.

Internal Audit Access to Evidence

Company auditors shall have a level of access to systems or data solely to the extent reasonably necessary to meet Company external and internal audit requirements. This may include access to sensitive data such as employee PII, background checks, performance reviews, employment contracts, etc. Access rights shall be limited to prevent broader access than requested by the Company auditor. Company auditors shall be under a requirement to deploy all necessary security and safeguard as pertains to such data, including sensitive data. Any transfer of data shall strictly comply with all LTG security requirements (e.g. encrypted file transfer vs. email attachments).

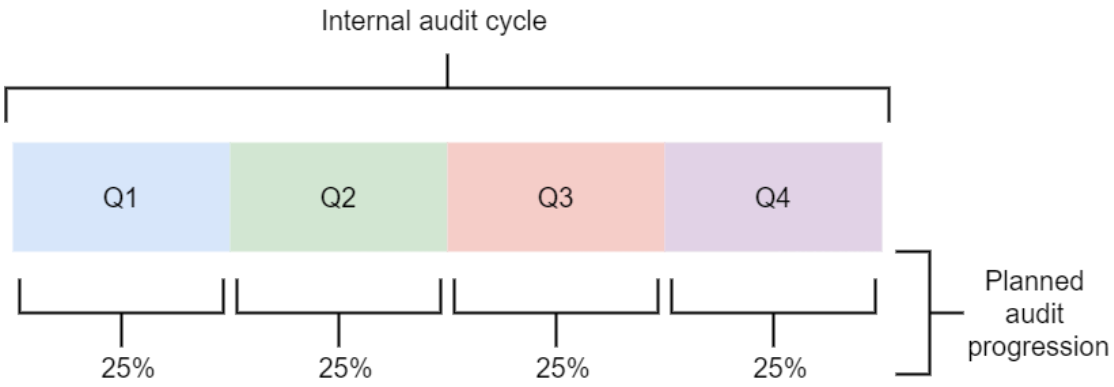
Internal Audit Schedule

A full internal audit will be carried out each year, ensuring all items in scope are audited at least once annually.

Due to reconciling Group certificates and the standardisation of our information security policies, a single audit will be conducted annually to meet the SOC and ISO requirements of all business units. As such, the audit is broken down into approximately 700 singular audit items

which are to be completed throughout the annual audit cycle; 12 months unless justified otherwise.

We will aim to complete audit items throughout the audit cycle on a regular cadence, with the intention to complete 25% each quarter; see diagram below. Completion rates per quarter may vary, however a full and complete audit must be conducted within the timeframe of the audit cycle. The **VP Information Security** will monitor the progression of the internal audits via regular update meeting with the **GRC Team**.



Internal audit procedure rationale

A singular audit document will be used to capture all internal audit requirements for the annual audit cycle. The internal audit has been broken down into approximately 700 items that are needed to meet our SOC and ISO requirements. This heavy fragmentation allows for greater audit resilience, allowing for scheduling of audit items to better fit around existing responsibilities and duties and increases the extent to which the audit items can be distributed.

Internal audits shall aim to capture evidence that is suitable for external audit submission for each internal audit item to the extent possible. Internal audits shall aspire the the same standards of evidence gathering as required by external audits.

Implementation

The full methodology for carrying out Internal Audits can be found in the Internal Audit Procedure.

ISO 27001:2013 Control 9.2

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:
a) conforms to

1. *the organization's own requirements for its information security management system;*
2. *the requirements of this International Standard;*

b) is effectively implemented and maintained.

The organization shall:

c) plan, establish, implement and maintain an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit program(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

d) define the audit criteria and scope for each audit;

e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) ensure that the results of the audits are reported to relevant management;

g) retain documented information as evidence of the audit program(s) and the audit results.

Management Review

The purpose of the management review and this policy are to:

- To ensure that regular, formal management reviews of The Company's ISMS, to ensure they are operating as planned and remain relevant to business activities.
- To ensure that The Company has defined participants, responsibilities and structure of all formal management reviews, including the format and distribution of documented records.

Executive Security Steering Committee will review audit status, findings and remediation plans on a quarterly basis. They will provide feedback on the acceptability of this information and provide guidance on any required changes to the plan or direction.

Quarterly meetings will be used communicate to the MD, Directors, and the GRC team the ongoing activities of the ISMS within The Company over the previous year, and plan for the next period. This meeting shall be the forum for establishing and reviewing information security objectives, key ISMS policies, and certain KPIs and thresholds required for the operation of the ISMS.

- The MD, the VP Information Security and other parties identified by the agenda will be required to attend the quarterly meetings.
- The MD, the VP Information Security, a member of the GRC team, and significant Asset Owners will be required to attend the quarterly meetings.
- The MD, the VP Information Security, and all Directors, significant Asset Owners and other parties identified by the agenda will be required to attend the quarterly and annual meetings.
- The VP Information Security shall be responsible for scheduling Management Review meetings, ensuring that the agenda is covered, outputs agreed and minutes recorded.

In preparation for the quarterly meeting, a report is prepared by the GRC Team, pulling together various reports from across The Company and CITO.

#	Requirement	How this is fulfilled
1	The status of actions from previous management reviews	Action items from previous meeting are summarized at the top of the meeting.
2	Changes in external and internal issues that are relevant to the management system (quality and information security)	GRC Team presents *new* issues.
3	Feedback on information security performance	GRC Team presents InfoSec metrics and elicits feedback.
4	The extent to which management objectives have been met	GRC Team reviews program objectives and provides status.
5	Process performance and conformity of products and services	GRC Team provides internal and external audit statuses.
6	Nonconformities and corrective actions (including trends)	GRC Team highlights audit exceptions and trends, and relevant remediation statuses.
9	The performance of external providers	GRC Team provides Vendor Risk update
10	The adequacy of resources	GRC Team highlights upcoming resourcing needs and constraints related to program objectives.
11	The effectiveness of actions taken to address risks and opportunities	GRC Team provides Risk Assessment summary.
12	Opportunities for continuous improvement	GRC Team brokers ongoing dialog for continuous improvement activities for key processes.

Management review outputs

The outputs are documented in the following way.

Type	Documented how
• Any need for changes to the Management System • Opportunities for improvement • Resource needs	Management Reviews capture immediate outputs and relevant elements are incorporated into Security Program Plan and related documents, e.g. Risk Assessment or ISMS policies.

ISO 27001:2013 Control 9.3

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management system;

c) feedback on the information security performance, including trends in:

1. *nonconformities and corrective actions;*
2. *monitoring and measurement results;*
3. *audit results; and*
4. *fulfillment of information security objectives;*

d) feedback from interested parties;

e) results of risk assessment and status of risk treatment plan;

f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

Nonconformities

The Company will take corrective actions appropriate to the effect of nonconformity events. Nonconformities may be the result of customer-raised tickets, or observations on the performance of tools, processes, personnel, documentation or other components of the ISMS which are contrary to the optimal performance of the ISMS. Nonconformity events should be documented, along with the corresponding corrective action and the results of the corrective action.

- **Every individual** is responsible for reporting nonconformities to their team leader
- **Team leaders** are responsible for documenting/assigning documentation of nonconformities, corrective actions, and results

Implementation of Corrective Action

Nonconformities, corrective actions and results will be recorded in the Risk Assessment and corresponding tickets, unless the nonconformity involves policy infraction by an employee that result in corrective actions to improve or terminate the employee's performance.

Nonconformities involving policy infractions by an employee will be recorded in written communications via email addressed to the employee, team manager, and the MD.

Nonconformities are reviewed during Executive Security Steering Committee meetings, to analyze for trends, anomalies, etc.

ISO 27001:2013 Control 10.1

When a nonconformity occurs, the organization shall:
a) react to the nonconformity, and as applicable:

1. *take action to control and correct it; and*
2. *deal with the consequences;*

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1. *reviewing the nonconformity;*
2. *determining the causes of the nonconformity; and*
3. *determining if similar nonconformities exist, or could potentially occur;*

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken

g) the results of any corrective action.

Continual Improvement

It is the policy of The Company to identify and investigate opportunities for improvement of the ISMS and PIMS, and and where possible, practical and feasible whilst working within the framework and budget agreed with LTG, implement them.

- The **VP Information Security** and **MD** are primarily responsible for driving internal continuous improvement of the ISMS by providing sufficient resources and identifying priorities.
- **All employees** are responsible for identifying potential improvements and reporting them to their respective team leader.

Opportunities for improvement may be identified in any way, but common ones are:

- Actions required to meet strategic and business objectives
- Feedback/actions requested by LTG
- Feedback/actions requested by the management team
- The requirement to use new tools, create new products, develop new features, etc. as a result of new work coming in
- The requirement to use new tools, create new products, develop new features, etc. to develop existing customer relationships
- The requirement to use new tools, create new products, develop new features, etc. to maintain or build market share
- Actions required as a result of corrective actions
- Actions suggested/required to be able to work in partnership with another LTG company
- Feedback suggested by customer surveys, lessons learned or other project close activities
- Actions required to address items identified in the Risk Treatment Plan
- Actions required as a result of a security incident
- Actions required to conform to new legal requirements

ISO 27001:2013 Control 10.2

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Additional Information

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

Supporting Procedures

Internal Audit Procedure

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 @Paul Gordon @angelina.kilmer	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Aug 29, 2024
Review cycle	ANNUAL	
Next review date	Mar 13, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 1, 2024	@angelina.kilmer	3.4	Changed Policy classification from Confidential to Public
Aug 29, 2024	@Art Machado @Paul Gordon	3.3	Addition of a section related to internal auditors level of access to data; update to the audit schedule to reflect an improved audit process
Mar 13, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	3.2	Annual Review
Mar 17, 2023	@Sarah Zwicker (Unlicensed)	3.1	Added Privacy audit controls and considerations. Changed QHSE to GRC.
Feb 23, 2023	@Art Machado @Sarah Zwicker (Unlicensed)	3.0	Annual Review + logo change
Nov 15, 2022	@Sarah Zwicker (Unlicensed)	2.9	Removal of CTO
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	2.8	Added Privacy considerations and components

Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	2.7	Title change for VP InfoSec, Annual Review
Jun 21, 2021	@Sarah Zwicker (Unlicensed)	2.6	Transferred procedural information to PF-PROC-001 3 Internal Audit Procedure ARCHIVED
Mar 12, 2021	@Sarah Zwicker (Unlicensed)	2.5	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.4	Reformatted, policies linked
Jan 26, 2021	@John Cole	2.3	Annual review, role title change
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.2	Changed Owner