Internal Audit and Compliance Policy

Version number	5.0
Last Approved	Mar 2, 2026
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.

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.

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 and Compliance 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 27001:2022 Control 8.15
>
> *Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.*

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

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

> ISO 27001:2022 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

ISO 42001:2023 Control 9.1

The organization shall determine:
— what needs to be monitored and measured;
— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
— when the monitoring and measuring shall be performed;
— when the results from monitoring and measurement shall be analysed and evaluated.
Documented information shall be available as evidence of the results.
The organization shall evaluate the performance and the effectiveness of the AI management system.

On an annual basis, the GRC Team will develop an audit plan to test the effectiveness of controls across The Company's management systems inclusive of security, privacy, AI, etc. The audit plan may include internally performed audits, external audits (e.g., SOC and ISO), vendor security audits, etc. Control environments included shall be, but are not limited to the following controls:

- Corporate information security
- Hosting and engineering security
- Physical security
- Privacy

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

Internal Audit Access to Evidence

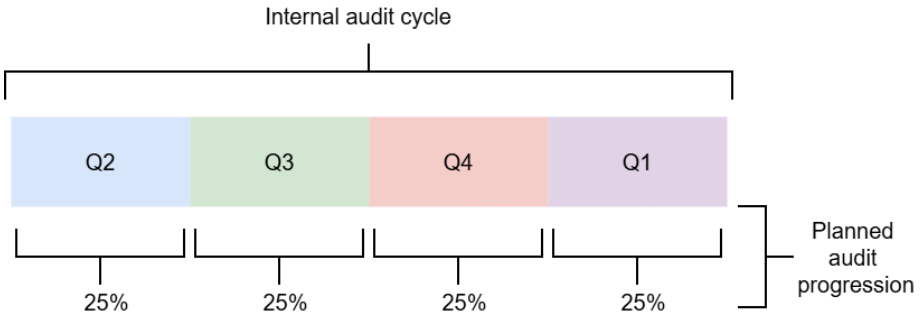
Company auditors shall have a level of access to systems or data solely to the extent reasonably necessary to meet Company external and internal audit requirements. This may include access to sensitive data such as employee PII,

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 reviewed at least once annually.

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 meetings with the GRC Team.



Implementation

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

ISO 27001:2022 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 plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

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

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

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

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

ISO 42001:2023 Control 9.2

The organization shall conduct internal audits at planned intervals to provide information on whether the AI management system:

a) conforms to:

1. *the organization's own requirements for its AI management system;*
2. *the requirements of this document;*

b) is effectively implemented and maintained.

The organization shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:
a) define the audit objectives, criteria and scope for each audit;
b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
c) ensure that the results of audits are reported to relevant managers.
Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

Management Review

The 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.

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 27001:2022 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) changes in needs and expectations of interested parties that are relevant to the information security management system;

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

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

e) feedback from interested parties;

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

g) opportunities for continual improvement.

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

ISO 42001:2023 Control 9.3

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

The management review shall include:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the AI management system;

c) changes in needs and expectations of interested parties that are relevant to the AI management system;

d) information on the AI management system performance, including trends in:

1. *nonconformities and corrective actions;*
2. *monitoring and measurement results;*

3. *audit results;*

e) opportunities for continual improvement.

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the AI management system.

Documented information shall be available as evidence of the results of management reviews.

Nonconformities

The Company will take corrective actions appropriate to the effect of nonconformity events. Nonconformity events should be documented, along with the corresponding corrective action and the results of the corrective action.

Implementation of Corrective Action

The GRC Team is responsible for coordinating and documenting corrective actions relating to nonconformities as well as their ongoing status and results. The status of notable corrective actions is also reported to the Executive Steering Committee during the quarterly meetings.

ISO 27001:2022 Control 10.2

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.

ISO 42001:2023 Control 10.2

When a nonconformity occurs, the organization shall:

a) react to the nonconformity and as applicable:

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

b) evaluate the need for action to eliminate the cause(s) of the nonconformity, so that it does not recur or occur elsewhere, by:

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

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

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

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— 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.

- The **VP Information Security** and **MD** are primarily responsible for driving internal continuous improvement of the ISMS and PIMS 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 interested parties
- The requirement to use new tools, create new products, develop new features, etc.
- Actions required as a result of the risk treatment plan
- Actions required as a result of a security incident
- Actions required to conform to new legal requirements

ISO 27001:2022 Control 10.1

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

ISO 42001:2023 Control 10.1

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

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	Mar 2, 2026
Review cycle	ANNUAL	
Next review date	Mar 2, 2027	

Version History

Date	Author(s)	Version	Changes
Mar 2, 2026	Angelina Kilmer Paul Gordon	5.0	Annual Review
Jul 8, 2025	Art Machado Angelina Kilmer Paul Gordon	4.2	Update to language, no material change.
Apr 9, 2025	Paul Gordon	4.1	References to ISO 42001
Feb 25, 2025	Angelina Kilmer Paul Gordon	4.0	Annual review
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 Paul Gordon	3.2	Annual Review

Mar 17, 2023	Sarah Zwicker	3.1	Added Privacy audit controls and considerations. Changed QHSE to GRC.
Feb 23, 2023	Art Machado Sarah Zwicker	3.0	Annual Review + logo change
Nov 15, 2022	Sarah Zwicker	2.9	Removal of CTO
Mar 24, 2022	Sarah Zwicker	2.8	Added Privacy considerations and components
Mar 16, 2022	Sarah Zwicker Art Machado	2.7	Title change for VP InfoSec, Annual Review
Jun 21, 2021	Sarah Zwicker	2.6	Transferred procedural information to PF-PROC-0013 Internal Audit Procedure ARCHIVED
Mar 12, 2021	Sarah Zwicker,	2.5	Changed owner, updated Overview
Feb 9, 2021	Sarah Zwicker	2.4	Reformatted, policies linked
Jan 26, 2021	John Cole	2.3	Annual review, role title change
Nov 23, 2020	Sarah Zwicker	2.2	Changed Owner