tinQwise

Version 2025.08

TinQwise Policy

002.1

Information Security & Risk Management System (ISRMS) Governance

tinQwise

Validity and document management

Version	Date	Author	Description
01	2019/11/14	Simon Kennedy	Document creation
02	2020/02/05	Simon Kennedy	Policy update.
03	2020/11/18	Simon Kennedy & Emil de Valk	Annual review and policy update.
04	2021/10/28	Simon Kennedy & Emil de Valk	Annual review and policy update.
05	2022/11/01	Simon Kennedy, Emil de Valk, Okke Formsma, Elena Neagu	Annual review and policy update.
06	2023/03/09	Emil de Valk and Reinoud van Dommelen	Update to align with standard Client contract set. Definitions, renumbering and consistency.
07	2023/11/02	Okke Formsma, Emil de Valk	Annual review. Improved definitions and consistency.
08	2024/12/11	Emil de Valk	Annual review, improved consistency, added risk assessment framework clause.

This document is valid as of January 1st, 2025.

The owner of this document is the C.O.O. and head of engineering who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents arising from failed security controls built into the systems
- Feedback from third party security advisors during the annual security reviews
- Client IT organisation feedback & requirements

TinQwise reserves the right to update this Policy to reflect changes in our practices and regulatory requirements. Data subjects will be informed of material changes. Previous versions of this procedure will be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

tinQwise

Table of Contents

tinQwise

1. Relevant to

Management	Finance / Legal	HR	Office Management	Marketing, Sales and Account Management	Professional services	IT Support	Product & Engineering	DevOps	Support & Maintenance
X	X	X	X	X	X	X	X	X	X

2. Purpose

This document defines the governance structure of the Information Security and Risk Management System (ISRMS) implemented by TinQwise Holding BV and its daughter companies (hereafter: TinQwise). It describes the model of governing ISRMS establishment, implementation, operation and improvement. It defines accountabilities and responsibilities of the ISRMS governance body.

3. Objectives

The first step in establishing adequate information security management is to formulate an overall information security governance. Our ISRMS governance plan is established to ensure alignment of information security plans and objectives to TinQwise and our Clients business needs and strategic goals. Our ISRMS governance body directs, monitors, and evaluates IT and information security issues of both strategic and operational nature. This governance body consists of ISRMS Steering Committee who owns the ISRMS and the Security Committee who manages the operation of the ISRMS.

At TinQwise we are fully committed to keeping our own and our Clients data safe and secure. Our Information Security Management System is the process of becoming ISO27001 certified.

tinQwise

4. Organisation of information security

4.1 ISRMS governance body

The Chief Operating Officer (C.O.O.) is ultimately accountable and sponsor for the governance of the Information Security Management System (ISRMS). The members of the Management Team form the ISRMS Steering Committee, who owns the ISRMS. The ISRMS Steering Committee is chaired by the Chief Operating Officer (C.O.O.).

The ISRMS Steering Committee gives overall strategic direction and maintains oversight, but delegates operational responsibilities for physical and information security to the Security Committee.

The ISRMS Steering Committee depends on the Security Committee to coordinate activities throughout TinQwise ensuring that suitable policies and security measures are in place to support the company's security principles, policies and procedures.

The ISRMS Steering Committee also relies on feedback from the Security Committee, external security assessors / auditors, software engineering and other functions to ensure that the principles, and policies are being complied-with in practice.

4.2 ISRMS roles and responsibilities

The ISRMS Steering Committee demonstrates their commitment to information security by:

- A statement of support from the Management Team: **The success of our business is dependent on the satisfaction of our Clients and the secure and compliant handling of Client data. This implies that we set the highest reasonably practicable standards possible to protect our Clients' data and our own software assets.**
- ensuring the Information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
- ensuring the integration of the information security management system requirements into the organization's processes;
- ensuring that the resources and appropriate competencies needed for the information security management system are available;
- communicating and training the importance of effective information security management;
- ensuring that the information security management system achieves its intended outcome(s);
- directing and supporting persons to contribute to the effectiveness of the information security management system;
- promoting continual improvement; and
- supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibilities.

At a high level, the Security Committee chaired by the C.O.O. ensures that our ISRMS operates effectively and works towards compliance with the ISO27001:2013 requirements by:

- Facilitating risk assessments
- Coordinating controls implementation
- Maintaining the ISRMS
- Communicating necessary deliverables and/or security requirements throughout the organization
- Ensuring training and continuous improvement processes are in place to meet those requirements.

If required, further delegation of responsibility for specific security issues will be carried out by Security Committee within the organization as appropriate.

Information and physical security are also a key responsibility of all TinQwise Staff, and this is regularly communicated and reinforced.

Each Physical and Data asset has an owner – who is responsible for ensuring that the Information security policy is followed in relation to that Asset. The asset owner may delegate security tasks in relation to assets for which they are responsible but remain accountable for the security of those assets.

For TinQwise physical and data assets and asset ownership are defined in the in the Asset inventory.

4.3 Information security coordination

Information security activities are coordinated throughout TinQwise to ensure consistent application of the security principles and policy statements. The Steering Committee has charged the Security Committee with the task of securing TinQwise's assets. The Security Committee under supervision of the C.O.O. is responsible for:

- Management oversight and direction for both physical and logical aspects of security, including information security;
- Coordinating and monitoring TinQwise's Security Framework, including the information security controls throughout the organization;
- Commissioning or preparing Information security policy statements, ensuring their compliance with the principles approved by the Steering Committee, and formally have them approved for use throughout TinQwise;
- Periodically reviewing the information security policies to ensure their applicability, alignment with the security strategy and objectives as well as the efficiency and effectiveness of the information security control infrastructure as a whole, recommending improvements wherever necessary;
- Identifying significant trends and changes to TinQwise's information security risks and, where appropriate, proposing changes to policies for example by suggesting to the ISRMS Steering Committee major strategic initiatives to enhance information security;
- Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes;

- Periodically reporting on the status of the security controls infrastructure to the ISRMS Steering Committee using metrics and other information supplied by the control implementers, internal and external security audits, and the risks owners;
- Ensuring appropriate and up-to-date training is in place for all relevant TinQwise and contractor staff;
- Team leads are accountable and responsible for Information security controls implementation. The Security Committee will supervise and consult for implementation of the required controls in alignment with the identified risks. The Security Committee remains responsible for the overall effectiveness and performance evaluation of information security throughout TinQwise.

4.4 Allocation of information security responsibilities

Chief Operating Officer

The C.O.O. is responsible for:

- chairing the Security Committee;
- taking the lead on information security governance. For example, by being responsible for the development information security processes, standards, and by providing the information security objectives in alignment with the business and information security strategy, as well as supporting and reviewing as necessary to ensure that information assets are identified and suitably protected throughout TinQwise;
- The definition, implementation of Information security policy documents and ensuring that development, implementation, monitoring and management of the ISRMS is done properly;
- Ensuring that other policies, procedures and working practices are aligned to the Information security policy documents;
- Ensuring that staff receive appropriate information security training and are aware of their associated responsibilities;
- Monitoring and reporting on the status of information security within the organization;
- Ensuring compliance with relevant legislation and regulation in EU;
- Ensuring that risk assessments are carried out and include appropriate risks;
- Ensuring that appropriate Risk Treatment Plans are defined and the treatment measurements are implemented.

Security Committee

The Security Committee is responsible for:

- Reviewing logs and following up on any exceptions identified.
- Monitoring and logging security alerts and events.
- Coordinating vulnerability management and assessments.
- Coordinating annual penetration testing.
- Following up with system administrators for the identification, risk ranking, testing, distribution, deployment and implementation of technical security configurations, and requirements.

- Investigating any suspicious incident, event or behaviour.
- Categorizing, reporting, analysing, responding and escalating security incidents.

Team leads

Team leads throughout the organization are responsible for:

- Day-to-day compliance and operation of the information security policies.
- ensuring that suitable technical, physical and procedural controls are in place in accordance with risk treatment results and TinQwise policies.
- ensuring that technical, physical and procedural controls are properly applied and used by all employees, contractors, consultants, temporary, and other workers at TinQwise (hereafter workers).
- They should take measures to ensure that workers:
    - are informed of their obligations to fulfil relevant information security policies by means of appropriate awareness and training and education activities;
    - comply with the policies and actively support the associated controls;
    - are monitored to assess their compliance with the policies and the correct operation of the associated controls and reminded of their obligations as appropriate.
- providing the direction, resources, support, and review necessary to ensure that information assets are appropriately protected within their area of responsibility.
- informing the Security Committee of actual or suspected policy violations (information security incidents) affecting their assets.

Staff

All employees, contractors, consultants, temporary, and other workers at TinQwise (workers) are responsible for complying with the principles and the information security policies where relevant to their jobs. They are responsible for maintaining the security of all information entrusted to them. Upon hire, as a condition of employment, each worker undertakes to comply with TinQwise's information security and data privacy policies. Any worker failing to comply with the security and data privacy policies could be subject to disciplinary action, potentially including termination of employment or contract and/or prosecution.

4.5 Risk Assessment Framework

TinQwise employs an enhanced risk assessment framework to proactively identify, evaluate, and address risks impacting systems, data, and operations. This framework integrates key policies to ensure comprehensive coverage:

1. **Dynamic Identification**: Risks are continuously monitored and assessed, including threats from new technologies, cybersecurity incidents, and third-party dependencies.

2. **Integrated Policies**: Risk assessments align with:

    - **Incident Management Policy** for identifying and responding to emerging risks.

- **Secure Development Policy** to mitigate risks during the software lifecycle.
- **Operational Resilience & Disaster Recovery Policy** for continuity planning.
- **System Acquisition, Development & Maintenance Policy** for secure integration of new technologies.

3. **Prioritization and Reporting**: Risks are prioritized based on impact and likelihood, with outcomes documented in the Risk Register and reviewed by the ISRMS Steering Committee.

With this framework TinQwise ensures risks are managed effectively, aligning with ISO 27001 standards and TinQwise's commitment to security and resilience.

5. Managing records kept based on this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Incident reports	SharePoint	H.o.E.	Secure SharePoint. Only security committee members can access these files	5 years
Pentest and other security test reports	SharePoint	C.O.O.	Secure SharePoint. TinQwise Staff can access these files	5 years
Security and Data Policies, i.e. 003.1; 003.2; 003.3; 003.4; 00.4.1; 004.2; 004.3 and 005.1	SharePoint	C.O.O.	SharePoint	5 years