Compliance statement ISMS, 2019

2020-01-31

WhistleB, Whistleblowing Centre AB

Rote Consulting is an independent audit and advisory company specialized in enterprise risk, security, privacy and continuity management. Rote is also a proud standard developer and active member of the technical committee at SIS for the ISO/IEC 27000 standards since 2003.

Executive summary

- Information security framework within WhistleB is aligned to Swedish and international information security standards.
- Records of performance evaluation and improvements available and maintained
- Security level for handling and protection of digital information is corresponding to industry practices and stakeholder expectations and requirements
- Security level for digital information is corresponding to industry practices and stakeholder expectations and requirements
- Information classification scheme is implemented for internal documentation
- Information classification scheme for external documentation is provided as "commercial in confidence" agreement with customers
- Technical solutions including the WhistleB application are designed and maintained on industry and good IT-security practices, corresponding to *security/privacy by design and default* principles
- Underlying platforms and infrastructure for hosting the WhistleB application are well audited and tested by supplier (MS Azure) and third-party assessors

Stockholm, January 31, 2020

Fredrik Rehnström
Senior security advisor and Executive Vice President

Board certified:

- Protection Professional (CPP)
- Information System Security Professional (CISSP)
- Information System Auditor (CISA)
- Information Security Manager (CISM), and
- In the Governance of Enterprise IT (CGEIT)

Table of contents

1 Scope of statement

Scope of assignment is to objectively assess and compare current information security level, including governance, policy, guidelines and implemented safeguards, with industry practices, Swedish and international standards and relevant stakeholder expectations and requirements.

2 Criteria's for assessment and statement

This statement is based on assessment of WhistleB' s information security level towards:

- Swedish and international standard "Information Security Management System – Specification", SS-EN ISO/IEC 27001:2017
- Industry practices from mid-size SaaS providers
- Trusted community security by design practices related to cloud computing service development environment
- Benchmark of security levels, including governance, policy, rules and implemented safeguards, at present SaaS delivery

3 Summary

The security framework within WhistleB is aligned to Swedish and international information security standard.

Artifacts from performance evaluation and related improvements of the ISMS have been enhanced since previous reviews.

WhistleB security level is overall corresponding to industrial practices at mid-size SaaS providers.

A benchmark of security levels, including governance, policy, guidelines and implemented safeguards, at present WhistleB SaaS services/delivery was made. The benchmark confirmed that actual information security level is overall corresponding to good practice security level at SaaS services/delivery.

The security level for handling and protection of digital information is corresponding to industry practices and stakeholder expectations/requirements.

Information classification scheme is implemented for both internal and external documentation, the latter by a "commercial in confidence" agreement with customers.

The concepts security/privacy by design and security/privacy by default are enforced from policy level and follows trusted community principles for cloud computing.

Technical solutions including the WhistleB application are designed and maintained on industry and good IT-security practices. Enhanced IT-security competence for application management is in place and kept maintained.

Underlying platforms and infrastructure for hosting the WhistleB application are well audited and tested by supplier (MS Azure) and third-party assessors. Whistleblowing Centre AB software development team makes use of the security processes and capabilities of the MS Azure environment.

4 Detailed statement

ISMS requirement	Statement	Comments/Improvements
Context of the organization	Adequate	Whistle B ISMS is understanding the needs and expectations of interested parties. The ISMS is clearly determining the scope of the information security management system. The ISMS is adequately established, implemented, maintained and continually improved.
Leadership	Adequate	Whistle B shows relevant leadership and commitment to information security. An adequate information security policy is implemented and kept continually improved. Organizational roles, responsibilities and authorities are adequately deployed within the organization.
Planning	Adequate	Actions to address risks and opportunities are in place and recorded. Fundamental information security objectives and planning to reach them are in place.
Support	Adequate	Whistle B has despite a small organization allocated adequate resources and competence to maintain its ISMS. Fundamental awareness and communication are in place as well as documented information regarding the ISMS.
Operation	Adequate	Operational planning and control are in place, mostly derived from client agreements and expectations. Basic routines for information security risk assessment and treatment are in place and recorded.
Performance evaluation	Adequate	Monitoring, measurement, analysis and evaluation have been improved to adequate level after previous remarks. Records of internal audits are now according to plan. The methods produce comparable and reproducible results. Evidence of the monitoring and measurement results are documented and retained.
Improvement	Adequate	The following two steering documents have been updated to reflect the recent process improvements: - WhistleB Information Security Policy - WhistleB Information Risk Assessment and Treatment guideline The Business Continuity Plan (BCP) is updated for consistency with references to the MS Azure SLA statement.
Security area	Statement	Comments/Improvements
Information security policy	Adequate	Scope, communication and implementation is adequate.
Organization of information security	Adequate	Key roles and responsibilities are defined and allocated. Mobile device management should still be implemented, however is not WhistleB Confidential (e.g. client/PII) accessed by e-mail or stored in mobile devices.
Human Resources Security	Adequate	Basic routines for on- and off-boarding in place.
Information security policy	Adequate	Scope, communication and implementation is adequate.

Security area	Statement	Comments/Improvements
Organization of information security	Adequate	Key roles and responsibilities are defined and allocated. Mobile device management should still be implemented, however is not WhistleB Confidential (e.g. client/PII) accessed by e-mail or stored in mobile devices.
Human Resources Security	Adequate	Basic routines for on- and off-boarding in place.
Asset Management	Adequate	Information assets are identified, and an inventory maintained. The security level for handling and protection of digital information is corresponding to industry practices and stakeholder expectations/requirements. Information classification scheme is implemented for internal documentation, but labelling requirements replaced by a "commercial in confidence" agreement with customers.
Access control	Adequate	Access control routines in WhistleB application is maintained by clients. Guidelines and routines for regular review of administrative access rights including retention of logs are defined and approved. Review of administrative access rights are part of the "management review" by internal ISMS auditor. Evidence of performed reviews and monitoring activities have been improved since previous review.
Cryptography	Adequate	Good practice cryptographic controls in place. Key management for client/PII data is performed by client. Improvements planned for 2018 were implemented by the new application management supplier. Improvements included key revocation routines and allocation of resources to follow trends and vulnerabilities in cryptographic controls and to enforce routines remediate promptly if needed.
Physical and Environmental Security	Adequate	Requirements are defined by a risk assessment and cloud governance model for PaaS and IaaS supplier (MS Azure).
Operations Management	Adequate	Requirements are defined by a risk assessment and cloud governance model for PaaS and IaaS supplier (MS Azure). Development environment is maintained by good practices including recovery solutions and routines. As recommendation, references to MS Azure SLA statement can be added to internal documentation for better transparency
Communications Security	Adequate	Network security management is performed by Nessus scans and towards OWASP top 10. Latest SSL and TLS versions are utilized. Information transfer is following good industry practices and to approved operational procedures.

Security area	Statement	Comments/Improvements
System Acquisition, Development and Maintenance	Adequate	Good practice security requirements are defined and implemented in WhistleB application. Sensitive source code handled securely in a repository. An information security baseline was approved and implemented in 2017, enforced in 2018 and improved in 2019. Due care in place for test data protection, mainly by good maturity and solid routines at WhistleB new application development and management partner.
Supplier relationships	Adequate	Supplier requirements are defined by a risk assessment and cloud governance model for PaaS and IaaS supplier (MS Azure). WhistleB have very few suppliers to enforce and follow up security and privacy requirements with. Supplier compliance framework is simple to maintain.
Information Security Incident Management	Adequate	During 2018 was management reporting, escalation routines, continual improvements and collection of evidence implemented. Due to a low number of incidents, those have not been evaluated during 2019. Hence, for further study in coming assessments.
Business continuity management	Adequate	Business Impact Assessment (BIA) is made and pointing out the WhistleB application as key resource to have recovery plans and controls in place for. Additional requirement from clients were addressed in 2018 and a management decision to establish IT and business continuity plans Q1 2018 was made. Business continuity plans have been evaluated and found adequate. The cloud governance model for PaaS and IaaS supplier (MS Azure) is addressing this requirement and disaster recovery is part of agreement with MS Azure. As earlier stated, references to the MS Azure SLA statement can added to internal documentation for better consistency.
Compliance	Adequate	A solid compliance and internal control organization is described in the "WhistleB Governance of information security" guideline, including the annual *internal ISMS audit* and *ISMS management review*.

5 Information sources consulted for evaluation

- Cloud Security and PII Requirements list, Jan 18, 2017
- Compliance statement ISMS 2018 WhistleB 2019-01-31
- Risk assessment matrix (WhistleB 2019)
- SoA checklist light Uen (WhistleB 2019)
- WhistleB Business Continuity Plan (2019)
- WhistleB Governance of Information Security, January 1 - 2019
- WhistleB Information Risk Assessment and Treatment guideline (2019)
- WhistleB Information Security Policy, January 1 - 2018