



LL-C
Certification

F 43 S
20260115

SURVEILLANCE AUDIT REPORT NO. 270007
ISO/IEC 27001:2022

written on Tuesday, 13 January 2026

in the company

SYNRGISELEARN (PTY) LTD



CUSTOMER GENERAL DATA

SYNRGISELEARN (PTY) LTD

JETLINE HEAD OFFICE 12 THORA CRESCENT
2090 WYNBERG

Reg. No. 2010 / 016796 / 07 4180257794

Contact person

Xenothan Hojem (GM), phone: (+27) 11 719 0700, e-mail:
info@synergise.com, www.synergy-learning.com

The main scope of the company for which certification management system is considered

**The Information Security Management System is applicable to IT Operations Department related to:
Developing, marketing, selling, promoting, supporting, and designing a Learning Management System (LMS) for
managing training, compliance programs, performance tracking, and hosting educational content.**

Corresponding Standard	99.98
Effective number of employees (FTE)	20
Number of filials outside of the registered seat	0
Special processes	
The certified processes are ensured	by own employees without exception
Number of Shifts	1,00

CERTIFICATION DATA PROCESS

Certification standard applied	ISO/IEC 27001:2022
Audit date	2026/01/12 09:00:00 - 2026/01/13 11:30:00
Certificated since	2025/02/04
Place(s) of Audit	headquarters
Audit Coordinator and Lead Auditor	Civelekoğlu Çağlar (ISO/IEC 27001:2022)
Other participants of the audit (and their position)	CEO, CTO, Finance, HR, Development Team, IT Infrastructure Team, ISMS Representative
Audit Plan Date	Wednesday, 07 January 2026
Total Audit Days (on the spot)	1,62 (1,30)
Deviation from the audit plan	NO
Significant issues impacting on audit programme or client's MS	NO
Consultant involved in management system support	N/A
Audit (Report) language	English
Identification of certification body for standard ISO 27001	LL-C (Certification) Czech Republic a.s.

1. AUDIT SCOPE

Audit Criteria

The audit criteria are the requirements of the standard and the established processes as well as the documentation of the organization's management system. The purpose of the audit is to confirm the compliance of the client's management system with the audit criteria, to determine the ability of the management system to ensure that the organization meets the relevant legal and other requirements (but the audit is not an audit of compliance with the legislation). Furthermore, the objective is to determine whether the effectiveness of the management system makes it possible to achieve the objectives set and identify areas for potential improvement.

Description of the audited company and its activities

Corporation details, infrastructure, working places and branch offices, organizational chart description

Operating from a single office with no branches. Infrastructure includes on-premise workstations, cloud environments, firewalls, VPN, endpoint protection, and centralized monitoring. Remote working supported via secure VPN. The organization follows a role-based hierarchy: Executive Management for strategic direction, ISMS Manager for security oversight, IT/Development team with developers and administrators, Cybersecurity Team for monitoring and incident response, and Administrative Staff for HR

Manufacturing equipment or services support activities

Synergise does not engage in physical manufacturing. Operations focus on software development, deployment, and maintenance using cloud platforms and virtualized environments. Service support includes IT helpdesk, system administration, security monitoring, and infrastructure maintenance. IT team ensures system availability, patching, backups, and ISMS compliance. Development support covers version control, code reviews, and CI/CD pipeline management.

Description of the main product or services

The company provides custom software solutions, SaaS products, and cloud-based applications with emphasis on secure software development practices. Services include IT consulting, system integration, security advisory, and performance optimization. Development follows secure SDLC principles with threat modeling, code analysis, and security testing integrated throughout the lifecycle.

Human resources

Synergise employs software developers, IT engineers, cybersecurity specialists, and administrative staff following a structured role-based hierarchy. All employees comply with security policies, access controls, and ISMS procedures. Staff undergo background screening, security awareness training, and sign NDAs. Competence development is ongoing with regular training sessions and phishing simulations.

Scope of certification

The Information Security Management System (ISMS) covering the provision of custom software development, SaaS products, cloud-based applications, IT consulting, and system integration services from the Wynberg, Cape Town office in accordance with the Statement of Applicability.

Areas excluded from certification

No exclusions - all Annex A controls are applicable

Audit Objectives

Audit objectives, where methodologically can 1) confirm the compliance of the client's management system with audit criteria, 2) determine the ability of the management system to ensure that the organization meets the applicable statutory, regulatory and contractual requirements, and 3) achieve the specified objectives, as the management system can identify areas for potential improvement, including management review and internal audits - Were fulfilled.

Certification procedure

Disclaimer

Auditing is based on a sampling process of the available information and consequently there will always be an element of uncertainty present in auditing evidence, which may be reflected in the audit findings. Those relying or acting upon the audit results and conclusions should take into account this uncertainty.

Opening and closing meeting participants

CEO, CTO, CIO (ISMS Representative), HR

Audit methods

On-site audit conducted at Wynberg office. Methods included document review, interviews with key personnel including ISMS Manager and IT staff, observation of operational processes, sampling of records and evidence, and verification of control implementation. Audit covered ISMS documentation, internal audit results, management review records, corrective actions, and continual improvement activities.

Volume of sales, products, orders, services, as applicable

Service-based organization providing SaaS learning management solutions. Currently serving 200+ customer organizations with over 15,000 total end users across various industries. Primary service delivery through cloud-based LMS platform with customization capabilities for client-specific business requirements.

Description of sampling and sampling statistics

Due to low number of employees for screening %20, for customer applications % 3, for general administrative applications %10, for technical applications % 3-4

Significant changes impacting the MS of the organization occurred since the previous audit and unresolved issues

N/A

LOGO of the Certification Body and certification reference

is used by common way and is not misleading and is not inconsistent with business conditions

2. SYSTEM DESCRIPTION AND COMPLIANCE MATRIX - ISO/IEC 27001:2022

System description

Organisation Context - business environment and interested parties

Synergise has documented its organizational context identifying internal and external issues relevant to information security. External factors include the evolving cybersecurity threat landscape, regulatory requirements (particularly POPIA for South African data protection and GDPR for international clients), client contractual obligations, technology trends in cloud computing and SaaS delivery, and competitive market dynamics. Internal factors encompass organizational structure, technical capabilities, staff competencies, corporate culture, and resource availability.

Interested parties have been identified and documented including: customers requiring secure software solutions and data protection; employees expecting safe working environment and clear security responsibilities; cloud service providers and technology partners with mutual security obligations; regulatory authorities including data protection agencies; certification bodies; and shareholders expecting business continuity and reputation protection.

Requirements from interested parties are captured and regularly reviewed, covering contractual security requirements from clients, legal compliance obligations, employee security awareness expectations, and supplier security standards. The context documentation is reviewed during management reviews to ensure continued relevance and to identify any changes that may impact the ISMS scope or objectives.

During the surveillance audit, it was verified that the organization continues to monitor and review its context, with no significant changes identified since the initial certification that would affect the ISMS scope or applicability.

Extent/Scope of the ISMS

The ISMS scope covers the provision of custom software development, SaaS products, cloud-based applications, IT consulting, and system integration services from the Wynberg, Cape Town office location.

The scope encompasses all information assets, processes, personnel, and technology infrastructure supporting these services. This includes software development environments, production systems, customer data handling, internal administrative functions, and supporting IT infrastructure. Cloud-based environments used for development, testing, and production deployment are included within the scope boundaries.

The Statement of Applicability defines all applicable Annex A controls with no exclusions. All 93 controls from ISO 27001:2022 Annex A are applicable to the organization's operations.

During the surveillance audit, it was confirmed that the scope remains unchanged since initial certification, and the organization has maintained appropriate boundaries and interfaces for the ISMS.

ISMS setting

The ISMS is established based on ISO 27001:2022 requirements with a comprehensive documentation framework. Top management demonstrates commitment through an executive support letter, defined security policy, and active participation in management reviews. The Information Security Policy is approved by top management, communicated to all employees, and reviewed bi-annually.

CIO(also Co-Founder) has been appointed with overall responsibility for maintaining and improving the management system. Information security roles and responsibilities are clearly defined and documented, with assignments covering executive management, IT administrators, development teams, and all employees. The organizational structure ensures appropriate segregation of duties for critical security functions.

The ISMS framework includes documented processes for risk management, access control, incident management, business continuity, and supplier security. Process interactions are defined showing how ISMS processes integrate with business operations. Regular activities are scheduled through an ISMS activity calendar ensuring timely execution of audits, reviews, training, and assessments.

Resources are allocated to support ISMS implementation including personnel, technology tools, and training programs. Competence requirements are defined for security-related roles with ongoing development through awareness sessions and specialized training.

The surveillance audit confirmed that the ISMS setting remains effective with continued management support and adequate resource allocation.

Leadership, roles, commitment and policies

The Information Security Policy establishes the organization's commitment to protecting information assets, ensuring confidentiality, integrity, and availability. The policy is approved by top management, communicated to all employees and relevant external parties, and subject to regular review. Supporting policies address specific areas including acceptable use, access control, remote working, mobile devices, and supplier security.

Information security roles and responsibilities are documented and communicated throughout the organization. Key roles include:

Executive Management: Strategic oversight and resource allocation

ISMS Manager: Day-to-day management of the security program, compliance monitoring, and reporting

IT Administrators: Technical implementation of security controls

Department Managers: Ensuring team compliance with security policies

All Employees: Adherence to policies and reporting of security events

Authority levels are defined for access approvals, change management, incident response, and risk acceptance decisions. Segregation of duties is maintained for critical functions to prevent unauthorized actions.

2. SYSTEM DESCRIPTION AND COMPLIANCE MATRIX - ISO/IEC 27001:2022

continuation ...

Measures targeting risks and opportunities

Synergise has implemented a formal risk assessment and treatment process aligned with ISO 27001 requirements. The methodology covers identification, analysis, evaluation, and treatment of information security risks.

Risk assessment follows an asset-based approach where information assets are identified, owners assigned, and threats and vulnerabilities evaluated. Risks are analyzed based on impact to Confidentiality, Integrity, and Availability (CIA) and likelihood of occurrence.

Risk Scoring Methodology:

Impact is assessed separately for C, I, and A on a scale of 1-5 (Negligible to Critical)

Likelihood is rated 1-5 (Rare to Almost Certain)

Risk Score = Highest CIA Impact × Likelihood

Risk levels: Low (1-6), Medium (7-12), High (13-19), Critical (20-25)

Risk treatment options include: mitigate through controls, transfer via insurance or contracts, avoid by eliminating the activity, or accept with management approval. A Risk Treatment Plan documents selected treatments, responsible owners, timelines, and residual risk levels.

Opportunities are also assessed to identify potential improvements such as adopting new security technologies, enhancing automation, or pursuing additional certifications. An Opportunity Assessment Tool captures potential benefits and implementation considerations.

IS Goals and targets, achievement plans

Synergise has established measurable information security objectives aligned with the Information Security Policy and business strategy. Objectives are documented in the Information Security Objectives and Plan, reviewed annually, and communicated to relevant personnel.

Current information security objectives include:

Respond to critical security incidents within 4 hours

Maintain 99.5% uptime for production systems

Achieve 100% staff completion of annual security awareness training

Remediate critical vulnerabilities within 72 hours

Complete quarterly user access reviews

Conduct successful monthly backup recovery tests

Each objective has an assigned owner responsible for implementation and monitoring. Resources are allocated including security tools, training programs, and personnel time. Progress is tracked through regular monitoring activities and reported during management reviews.

Key initiatives supporting objective achievement include continuous security monitoring, regular phishing simulations and awareness campaigns, automated vulnerability scanning and patch management, and documented incident response procedures with defined escalation paths.

Performance against objectives is measured and analyzed to identify trends and improvement opportunities. Where targets are not met, corrective actions are initiated.

The surveillance audit verified that objectives are measurable, actively monitored, and progress is reported to management. Current performance indicates objectives are being achieved.

Resources, competences and awareness

Synergise allocates adequate resources to establish, implement, maintain, and continually improve the ISMS. Resources include dedicated personnel with the ISMS Manager overseeing security operations, budget allocation for security tools and technologies, training programs, and external expertise when required for specialized assessments or audits.

Competence requirements are defined for roles with information security responsibilities. The Information Security Competence Development Procedure outlines the process for:

Identifying competence needs based on role requirements

Evaluating current competence levels through assessments

Providing training and development opportunities to address gaps

Maintaining records of education, training, skills, and experience

Staff competence is assessed during hiring through screening procedures and periodically through competence questionnaires. Development activities include technical training for IT and security personnel, security certifications support, and role-specific skill development. A Competence Development Report tracks progress and identifies ongoing development needs.

Security awareness is maintained through a structured program ensuring all personnel understand their security responsibilities. The program includes:

Mandatory induction training for new starters covering ISMS policies and procedures

Annual security awareness training for all employees

Regular phishing simulations to test and reinforce awareness

Targeted communications on emerging threats and security updates

Awareness Training Presentations covering topics such as data handling, incident reporting, and social engineering

Training completion is tracked and reported to management. Employees acknowledge their understanding of security policies and their responsibilities.

The surveillance audit confirmed that resources remain adequate, competence records are maintained, and awareness activities are conducted as planned with evidence of training complet

2. SYSTEM DESCRIPTION AND COMPLIANCE MATRIX - ISO/IEC 27001:2022

continuation ...

Internal communication and documented information

Internal communication methods include:

- Management meetings with documented minutes capturing decisions and actions
- Email communications for policy updates and security alerts
- Intranet or shared platforms for policy and procedure access
- Team briefings for department-specific security matters
- Incident notifications and lessons learned distribution
- Security awareness bulletins on emerging threats

External communication is managed for interactions with customers, suppliers, regulators, and certification bodies. Communication responsibilities are assigned to appropriate roles ensuring consistent and authorized messaging on security matters. Documented information is controlled through the Procedure for the Control of Documented Information. The procedure addresses:

- Creation and updating with appropriate identification, format, and approval
- Version control ensuring current versions are available and obsolete versions are prevented from unintended use
- Distribution and access controls based on classification and need-to-know
- Storage and preservation ensuring legibility and retrievability
- Retention periods aligned with legal, regulatory, and business requirements
- Secure disposal when no longer required

An ISMS Documentation Log maintains the register of all controlled documents with version history, review dates, and ownership. Documents are classified, labelled, and stored securely with appropriate access restrictions. Records demonstrating ISMS performance and conformity are maintained including audit reports, risk assessments, training records, incident logs, and management review minutes. The surveillance audit confirmed that documented information is properly controlled, current versions are accessible, and communication processes are functioning effectively.

Operations planning and management

Synergise has established operational planning and control processes to ensure ISMS requirements are met. The ISMS Process Interaction Overview documents how security processes integrate with business operations, defining inputs, outputs, and interfaces between processes.

Operational planning includes:

- Defining criteria for security processes and controls
- Implementing controls in accordance with risk treatment decisions
- Maintaining documented information to demonstrate processes are carried out as planned
- Managing planned changes and reviewing unintended changes

Risk assessments are conducted at planned intervals and when significant changes occur to the organization, systems, or threat landscape. Assessment results inform control implementation priorities and resource allocation. Risk treatment plans are executed with progress tracked and reported to management.

Change management is controlled through a formal Change Management Process ensuring that all modifications to systems, applications, and infrastructure are assessed for security impact before implementation. Changes are documented, approved, tested, and reviewed with rollback procedures in place. The ISMS Change Log maintains records of changes to the management system itself.

Outsourced processes relevant to information security are identified and controlled through supplier agreements, security clauses, and periodic assessments. Cloud services and external development activities are subject to security requirements and ongoing monitoring.

An ISMS Regular Activity Schedule ensures timely execution of planned activities including risk reviews, access reviews, vulnerability assessments, backup tests, and policy reviews. Responsibilities and frequencies are defined for each activity.

Documented operating procedures are maintained for critical security processes ensuring consistent execution regardless of personnel changes.

The surveillance audit verified that operational controls are implemented as planned

2. SYSTEM DESCRIPTION AND COMPLIANCE MATRIX - ISO/IEC 27001:2022

continuation ...

Risk assessment and managing/addressing the information risks

Example risk assessment entry:

Asset: Customer Database

Threat: Unauthorized access leading to data breach

Vulnerability: Insufficient access controls

Impact scores: Confidentiality=5, Integrity=3, Availability=2

Highest Impact: 5 (Confidentiality)

Likelihood: 3 (Possible)

Risk Score: $5 \times 3 = 15$ (High)

Treatment: Implement MFA, enhance access logging, conduct quarterly access reviews

Residual Risk: Medium (accepted by management)

Risk treatment options applied include mitigating through implementation of controls, transferring through insurance or contractual arrangements, avoiding by eliminating risky activities, or accepting with documented management approval.

The Risk Treatment Plan documents selected treatments with responsible owners, implementation timelines, required resources, and target residual risk levels. The Statement of Applicability links identified risks to applicable Annex A controls with justification for inclusion.

Risk assessments are reviewed annually, upon significant changes, and following security incidents. Results are reported during management reviews for oversight and resource allocation decisions.

The surveillance audit confirmed that risk assessments are current and comprehensive, treatment plans are being executed, residual risks are formally accepted by management, and the risk register reflects the current threat landscape.

Monitoring, measuring, analysis, internal audits and reviews.

Key monitoring and measurement activities include:

Security incident metrics and response times

System availability and uptime statistics

Vulnerability scan results and remediation timelines

Access review completion rates

Training completion and awareness metrics

Backup success rates and recovery test results

Supplier security compliance status

Results are analyzed to identify trends, evaluate control effectiveness, and determine if security objectives are being met. Analysis outputs feed into management reviews and continual improvement activities.

Internal audits are conducted according to the Procedure for Internal Audits and planned through an Internal Audit Programme. Audits are scheduled to cover all ISMS processes and Annex A controls over defined intervals, with consideration for process importance and previous audit results. The most recent internal audit was conducted prior to this surveillance audit covering the full ISMS scope.

Internal audits are performed using an Internal Audit Checklist ensuring consistent coverage. Auditors are selected to ensure objectivity and impartiality. Audit findings are documented in the Internal Audit Report, communicated to relevant management, and tracked through the Internal Audit Action Plan. Nonconformities identified trigger corrective actions through the nonconformity management process.

Management reviews are conducted according to the Procedure for Management Reviews using a defined agenda covering:

Status of actions from previous reviews

Changes affecting the ISMS

Security performance and metrics

Audit results and findings

Risk assessment status

Opportunities for improvement

Review outputs include decisions on improvement opportunities, resource needs, and any changes required to the ISMS. Meeting minutes document discussions, decisions, and assigned actions.

The surveillance audit confirmed that monitoring activities are ongoing.

Improvement





















Synergise has established processes for managing nonconformities and driving continual improvement of the ISMS. The Procedure for the Management of Nonconformity defines the approach for identifying, documenting, and addressing nonconformities with root cause analysis and corrective actions. The Nonconformity and Corrective Action Log tracks all findings with responsible owners, target dates, and closure verification.

During the current surveillance period, no external nonconformities were raised. Two minor nonconformities were identified during internal audits, both have been appropriately addressed with corrective actions implemented and verified as effective prior to this surveillance audit.

Continual improvement is embedded in the organizational culture. Improvement inputs include internal audit findings, management review outputs, incident lessons learned, risk assessment updates, and employee feedback. The organization proactively enhances security controls and processes based on emerging threats, industry best practices, and operational experience.

The surveillance audit confirmed that the nonconformity process is functioning effectively and the organization demonstrates genuine commitment to continual improvement of its ISMS.

Compliance matrix - ISO/IEC 27001:2022

Standard element	Fulfillment degree	Next audit verification
Understanding the organisation and its context (4.1)		YES
Understanding the needs and expectations of interested parties (4.2)		YES
Determining the scope of the information security management system (4.3)		YES
Information security management system (4.4)		YES
Leadership (5)		YES
Actions to address risks and opportunities (6.1)		YES
Information security objectives and planning to achieve them (6.2)		YES
Resources (7.1)		YES
Competence (7.2)		YES
Awareness (7.3)		YES
Communication (7.4)		YES
Documented information (7.5)		YES
Operational planning and control (8.1)		YES
Information security risk assessment (8.2)		YES
Information security risk treatment (8.3)		YES
Monitoring, measurement, analysis and evaluation (9.1)		YES
Internal audit (9.2)		YES
Management review (9.3)		YES
Continual improvement (10.1)		YES
Nonconformity and corrective action (10.2)		YES



Standard requirements and own management dossier are properly met. Outstanding deficiencies are recognised and removed during the process



Standard requirements and own management dossier are properly met. Outstanding deficiencies are not always recognised/removed during the process; or fall under disclosure requirements of standard with no benefit for a company. Auditor can make exceptions



Standard requirements and own management dossier are not properly met. Auditor opts for exception or non-conformity according to the extent and its impact on system functionality

List of reviwed documents - ISO/IEC 27001:2022

Document Name	Document No. (or Date)	Reviewed
Statement of Applicability (SoA)	01.03.2024	YES
NONAME		NO



3. AUDIT OUTCOME SUMMARY

3.1. Strengths of the company

ISO/IEC 27001:2022

- Strong management commitment with active leadership involvement in ISMS governance
- Comprehensive and well-structured ISMS documentation framework
- Mature risk assessment methodology with CIA-based scoring approach
- Proactive security awareness culture with regular training and phishing simulations
- Effective internal audit program with demonstrated corrective action closure

3.2. Nonconformities and Areas of improvement

Summary of nonconformities and areas of improvements

No nonconformity or area of improvement

3.4. Previous audit (2025)

Audit type	Certification audit
Aannounced / Unannounced	Announced
Audit date	2025/01/13 08:00:00 - 2025/01/16 15:15:00
Name of auditing organization	LL-C (Certification) Czech Republic a.s.
Coordinating auditor	Çağlar Civelekoğlu
Action taken on NCs raised at previous audit	Please, refer to section 3.3 "Findings from the previous audit and verification of effective implementation of corrective actions."

3.5. Obstacles encountered that could compromise reliability of the audit findings and conclusions

N/A

4. CONSECUTIVE ACTION, FINAL PROVISIONS AND RECOMMENDATION

Thanks to all who participated in the organization and also to those who took part in the audit. We are glad that the management system audit in your company runs smoothly and in a friendly atmosphere.

Expected Outcomes

Applicant for certification (certified company) has been informed about the suitability of the accredited certification in the sense, that: "for the defined certification scope, an organization with a certified management system, which meets and appropriately applies the applicable management system requirements, can ensure the permanent provision of its service or/and its products satisfying customer requirements, relevant laws and regulations in order to increase customer satisfaction".

Use of the LL-C logo

Upon obtaining a valid certificate, the client is entitled, for the duration of the certificate validity, to use an approved logo of the certification company or a private scheme. In case of system certification, process certification or technical documentation completeness assessment, this mark shall not be used on a product or product packaging seen by the consumer or in any other way that may be interpreted as denoting conformity of a specific product. The use and placement of the logo must not create confusion between the client and the certifying company, or convey a false impression that the certification applies to a specific product instead of the management system, unless it is clear from the certification scheme that it is not about assessment of a specific product, where its compliance with essential requirements is verified, which are given by a normative or other legal document.

Settlement of nonconformities, areas for improvement

The findings of the audit are given in a previous chapter, in the form of nonconformities and Areas for improvements. We kindly ask you to settle them as follows:

Major nonconformity

If it has been found, it shall be formulated in the Nonconformity Protocol, which is annexed to this report. Major Nonconformity is such insufficient fulfilment of the standard requirements that the certificate cannot be issued (or must be commenced its removal) unless is finished its settlement by the applicant for certification. When a major nonconformity is issued during an audit, the client must provide the CB with objective evidence of an investigation into causal factors and the risks they expose and their proposed corrective action plan (CAP). This shall be provided within 30 days after the audit. Settlement procedure must be formulated by the applicant on the same form (Nonconformity Protocol). The major nonconformity shall be closed within a further 30 days by implementing a corrective action (CA) and submitting evidence to the CB. When a satisfactory settlement of nonconformity is finished, audit can be completed with positive results. The CB provides the method of verifying of the nonconformity settlement.

Minor nonconformity

The Minor nonconformity is such insufficient fulfilment of the standard requirements that the certificate can be issued without finishing Minor Nonconformity settlement by the applicant. A root analysis and a proposed corrective action plan is required within 30 days after the audit. Certification body must be informed about the settlement or about the objection on its relevance within 12 months from the last day of the audit or during the next audit. The method for verifying the settlement of this minor nonconformity is subject to surveillance or recertification audit. In the case of insufficient settlement of the minor nonconformity, it should be reclassified as major nonconformity and threaten the validity of the certificate.

Area for improvement

The area for improvement is a comment for improving of the management system or the better and efficient fulfilment of standard certain requirements (notably the removal of formal fulfillment of the standard requirements of or optimization solutions) . According to the accreditation criteria the certified company need not respond actively to these findings, but when there are lots of areas for improvement and will be ignored, it can be considered during the subsequent audit as a reduced level of system performance.

Certification period and certificate validity

The period, for which certified company is committed to maintain a functional management system and certification body is committed to provide the surveillance audits, corresponds to the certificate validity. During its validity, the certification body is obliged to perform surveillance audits every year in the place of the certified company activities, unless a normative or legal requirement exceptionally states otherwise. The first surveillance audit after initial certification shall be commenced within 12 months from the date of the completion of the certification audit; the second surveillance audit must be initiated in the annual period from the date of completion of the first surveillance audit with a maximum tolerance of 45 calendar days.

Before the termination of the certificate validity a contract with possible price advantage will be offered for the next certification period, if the client is interested in it (while the scope of certification will remain). To keep the price advantage, the recertification audit/ assessment shall be carried before the expiration of the original certificate. In severe cases, it is possible to request a postponement of surveillance audit, the approval of this exemption is solely on the certification body. In case of failure to cooperate in a surveillance audit we must begin the process of withdrawing of the certificate and we must publish that fact, according to the accreditation criteria.

Obligations of the certified company

The basic duties of certified company arise from the contract and business conditions that are part of it.

The certificate holder shall maintain its management system functional throughout the certificate validity period and apply all changes in the management systems that result from the changes in the relevant standards requirements or accreditation criteria based on the recommendations sent by the certification body

Further the certified company is obliged to register and document all complaints by third parties relating to its management system and properly inform the certification body.

Obligation of the CB / NB 2435

The basic duties of certification body arise from the contract and business conditions that are part of it. Certification body shall maintain its accreditation status, conduct regular audits and surveillances according to the specified dates and time frames and provide objectivity in determining the operability of the management system. Further the certification body is obliged monitor changes in the requirements of the relevant standards and notifies the certified company accordingly in advance and process complaints and reservations raised by the client or a third party in a timely manner.

Appeal

Applicant for certification (certified company) is entitled to lodge any complaint against procedure of the certification body or individual auditors. Complaint of the applicant for certification (certified company) is to be sent in writing. Likewise applicant for certification (certified company) can comment this report. Severe appeal, as the claim against auditor impartiality or the decision of the certification company to refuse issuing or withdrawal of the certificate, are solved by the independent Appeal Committee within the period 30 days. Other comments and objections are dealt with operationally in an appropriate period of time.

Report provision to third parties

This report summarizes the results of the audit. The report is provided to the customer, one copy in electronic format is deposited with the LL-C (Certification). The customer is entitled to present to any third party the full report only. The contents of this report and all audit records are considered confidential. The contents of this report and all audit records are considered confidential. The reports may be presented to any third party only with the consent of the customer, without that authorization if the accreditation body and the owners of private schemes will request it.

Recommendation

The overall audit target (as specified in the plan) was achieved. The documented system management conformity was measured through highly qualified process. Further, client's activity was compared with standard requirements. It was confirmed that the organization's MS is capable to meet the applicable requirements of the relevant standard(s) and achieve the expected outcomes for accredited Certification as stated in ISO-IAF Communiqué for Accredited Certification. The organization meets and appropriately implements the applicable MS requirements, and can ensure the continued provision of this service or products in conformity to customer requirements and relevant laws and regulations in order to increase customer satisfaction. This statement was made on the assessment of the individual standard's requirements fulfilment level, as evidenced in the compliance matrix of this report. The audit objectives as specified in Section 1 - Audit Scope were successfully met. Furthermore, the scope of certification has been assessed to be fully representative of the current activities of the audited organization.

I recommend, taking into account the audit results:

to maintain management system certificate with the requirements of the standard **ISO/IEC 27001:2022**

for the scope

The Information Security Management System is applicable to IT Operations Department related to:

Developing, marketing, selling, promoting, supporting, and designing a Learning Management System (LMS) for managing training, compliance programs, performance tracking, and hosting educational content.

LL-C (Certification) Czech Republic a.s. Çağlar Civelekoğlu



LL-C (Certification) Czech Republic a.s.
Pobřežní 620/3, 186 00 Praha 8 - Karlín
Reg. No. 27118339

5. ADDITIONAL SPECIFICATIONS

Annex A - 5 - Organizational controls

Annex A - 5

5	Organisational controls	Confirmation	Notes
5.1	Polices for information security	OK	Information security policies are documented, approved by management, communicated to employees, and reviewed bi-annually. Policies cover key areas including access control, acceptable use, incident management, and data protection.
5.2	Information security roles and responsibilities	OK	Roles and responsibilities are clearly defined and assigned including ISMS Manager, IT administrators, and department managers. Documented in ISMS policies and job descriptions.
5.3	Segregation of duties	OK	Segregation implemented for critical functions including access management, system administration, and security monitoring. Role-based access controls and multi-level approvals enforced.
5.4	Management responsibilities	OK	Management demonstrates commitment through oversight of ISMS implementation, resource allocation, and regular review of security performance and audit results.
5.5	Contact with authorities	OK	Designated personnel maintain contact with regulatory bodies, data protection agencies, and cybersecurity response teams. Procedures in place for incident reporting and legal inquiries.
5.6	Contact with special interest groups	OK	Organization engages with cybersecurity forums, industry associations, and regulatory working groups to stay informed on emerging threats and best practices.
5.7	Threat intelligence	OK	Structured threat intelligence process implemented gathering information from cybersecurity agencies, threat platforms, and vendor security alerts. Threat Intelligence Reports produced regularly.
5.8	Information security in project management	OK	Security requirements integrated into all project phases. Risk assessments, access management, and secure coding practices embedded in project lifecycle.
5.9	Inventory of information and other associated assets	OK	Comprehensive asset inventory maintained with defined ownership and CIA classification. Regularly updated and reviewed.
5.10	Acceptable use of information and other associated assets	OK	Acceptable Use Policy defines proper handling of IT systems, networks, and data. Employees acknowledge compliance requirements.
5.11	Return of assets	OK	Formal process for asset return upon termination or role change. Includes verification, access revocation, and secure data erasure.
5.12	Classification of information	OK	Information classification policy categorizes data as confidential, internal, or public with corresponding handling and protection measures.
5.13	Labelling of information	OK	Structured labelling system applied to electronic documents, emails, and physical records according to classification level.
5.14	Information transfer	OK	Secure transfer procedures implemented using encryption, VPNs, and TLS. Information Transfer Agreements in place for external transfers.
5.15	Access control	OK	Access control framework based on RBAC, least privilege principles, and MFA. Access granted based on business need.
5.16	Identity management	OK	Structured identity management with MFA, RBAC, and automated provisioning/de-provisioning. User accounts regularly reviewed.
5.17	Authentication information	OK	Strong password policies, MFA, and secure storage mechanisms enforced. Periodic credential updates required.
5.18	Access rights	OK	Access rights granted based on business needs and least privilege. Regular reviews conducted with rights modified or revoked as necessary.
5.19	Information security in supplier relationships	OK	Formal security requirements established for suppliers. Agreements include security clauses, periodic assessments, and compliance monitoring.
5.20	Addressing information security within supplier agreements	OK	Supplier agreements include specific security clauses covering access controls, data handling, incident reporting, and audit rights.
5.21	Managing information security in the information and communication technology (ICT) supply chain	OK	ICT supply chain risks managed through vendor audits, security assessments, and contractual obligations. Ongoing monitoring conducted.
5.22	Monitoring, review and change management of supplier services	OK	Regular supplier monitoring and periodic reviews conducted. Formal change management process for modifications in supplier relationships.
5.23	Information security for use of cloud services	OK	Cloud services controlled through provider security assessments, encryption requirements, MFA enforcement, and SLA monitoring.
5.24	Information security incident management planning and preparation	OK	Incident management plan established with defined response procedures, escalation paths, and regular drills. Dedicated personnel assigned.
5.25	Assessment and decision on information security events	OK	Structured process for assessing security events based on severity, affected assets, and business impact. Escalation decisions documented.
5.26	Response to information security incidents	OK	Incident response procedures include containment, root cause analysis, forensic investigation, and corrective action implementation.
5.27	Learning from information security incidents	OK	Incidents analyzed to identify root causes and trends. Lessons learned integrated into policies, training, and risk management.

5.28	Collection of evidence	OK	Procedures established for secure collection and preservation of digital evidence following chain-of-custody principles.
5.29	Information security during disruption	OK	Business continuity measures maintain security during disruptions including data backups, failover systems, and predefined response plans.
5.30	ICT readiness for business continuity	OK	ICT continuity plans implemented with backup systems, failover mechanisms, and redundant infrastructure. Regular disaster recovery testing conducted.
5.31	Legal, statutory, regulatory and contractual requirements	OK	Applicable requirements identified and documented including POPIA and GDPR. Compliance ensured through audits and policy reviews.
5.32	Intellectual property rights	OK	IP protection policies in place covering copyright compliance, software licensing, and employee confidentiality agreements.
5.33	Protection of records	OK	Security controls ensure confidentiality, integrity, and availability of business records. Retention policies enforced per legal requirements.
5.34	Privacy and protection of personal identifiable information (PII)	OK	PII protection measures implemented including encryption, access controls, and data minimization. Compliant with POPIA and GDPR requirements.
5.35	Independent review of information security	OK	Regular independent ISMS reviews conducted through internal audits and third-party assessments. Findings reported to management.
5.36	Compliance with policies, rules and standards for information security	OK	Compliance ensured through regular audits, employee training, and enforcement of security controls. Non-compliance addressed through corrective actions.
5.37	Documented operating procedures	OK	Operating procedures documented for critical security processes including access control, incident management, backup management, and system maintenance.

Annex A - 6 - People controls

Annex A - 6

6	People controls	Confirmation	Notes
6.1	Screening	OK	Formal screening process implemented for employees, contractors, and third-party personnel. Background checks include identity verification, employment history, and criminal record screening before granting access.
6.2	Terms and conditions of employment	OK	Information security roles and responsibilities defined within employment contracts. Employees acknowledge obligations regarding confidentiality, data protection, and ISMS policy compliance.
6.3	Information security awareness, education and training	OK	Structured awareness program implemented with mandatory induction training, annual refresher sessions, and phishing simulations. Training covers secure data handling, threat awareness, and incident reporting.
6.4	Disciplinary process	OK	Formal disciplinary process established for security policy violations. Actions range from verbal warnings and retraining to formal sanctions depending on severity.
6.5	Responsibilities after termination or change of employment	OK	Strict offboarding procedures enforced including access revocation, asset retrieval, and reinforcement of confidentiality obligations through NDA compliance.
6.6	Confidentiality or non-disclosure agreements	OK	NDAs enforced for employees, contractors, and third parties handling sensitive information. Agreements define data protection and post-employment confidentiality obligations.
6.7	Remote working	OK	Remote working policy and security controls implemented including VPN usage, MFA enforcement, encrypted communications, and remote device management.
6.8	Information security event reporting	OK	Formal process for reporting security events through designated channels. Employees required to report incidents promptly enabling timely investigation and mitigation.

Annex A - 7 - Physical controls

Annex A - 7

7	Physical controls	Confirmation	Notes
7.1	Physical security perimeters	OK	Defined physical security perimeters established to protect critical infrastructure. Security measures include restricted access zones, surveillance systems, visitor controls, and secure entry points.
7.2	Physical entry	OK	Strict physical entry controls implemented using electronic key cards and visitor registration logs. Unauthorized access to premises and sensitive areas prevented.
7.3	Securing offices, rooms and facilities	OK	Security measures protect offices and facilities containing critical assets. Controls include restricted server room access, surveillance cameras, alarm systems, and secure document storage.
7.4	Physical security monitoring	OK	Continuous monitoring through surveillance cameras and access control logs. Monitoring data regularly reviewed and retained for security investigations.
7.5	Protecting against physical and environmental threats	OK	Protection measures implemented against fire, floods, and power failures. Controls include fire suppression systems, UPS, and climate control for server rooms.
7.6	Working in secure areas	OK	Secure areas established for handling sensitive information with access restricted to authorized personnel. Controlled entry points, surveillance monitoring, and strict visitor policies enforced.
7.7	Clear desk and clear screen	OK	Clear Desk and Clear Screen policy enforced. Employees required to lock screens when away, store confidential documents securely, and prevent unauthorized viewing.
7.8	Equipment siting and protection	OK	Controls ensure secure placement and protection of IT equipment preventing unauthorized access, environmental damage, and theft.
7.9	Security of assets off-premises	OK	Security controls protect company assets used outside office premises. Measures include encrypted storage, remote device management, and secure VPN access.
7.10	Storage media	OK	Security measures protect storage media from unauthorized access, loss, or damage. Controls include encryption, access restrictions, secure storage, and disposal procedures.
7.11	Supporting utilities	OK	Reliability and security of supporting utilities ensured including power, cooling, and network infrastructure. Redundancy measures include UPS and backup generators.
7.12	Cabling security	OK	Security controls protect power and data cabling from tampering, interception, or physical damage.
7.13	Equipment maintenance	OK	Scheduled maintenance program established for critical IT and security equipment. Maintenance performed by authorized personnel with secure handling of data storage components.
7.14	Secure disposal or re-use of equipment	OK	Secure disposal and re-use procedures implemented. Measures include data wiping, degaussing, physical destruction, and controlled disposal processes.

Annex A - 8 - Technological controls

Annex A - 8

8	Technological controls	Confirmation	Notes
8.1	User end point devices	OK	Security controls protect endpoint devices including laptops, desktops, and mobile devices. Measures include endpoint encryption, anti-malware protection, remote device management, and enforced security policies.
8.2	Privileged access rights	OK	Strict controls over privileged access rights enforced. Measures include RBAC, MFA, logging and monitoring of privileged activities, and periodic access reviews.
8.3	Information access restriction	OK	Strict access restrictions ensure information only accessible to authorized users based on business needs. Controls include role-based permissions, least privilege, and access monitoring.
8.4	Access to source code	OK	Strict controls protect source code access. Measures include RBAC, version control systems, MFA, logging of access activities, and periodic security code reviews.
8.5	Secure authentication	OK	Robust authentication mechanisms implemented including MFA and strong password policies to prevent unauthorized access to systems and data.
8.6	Capacity management	OK	Structured capacity management process monitors IT resources including storage, processing power, and network bandwidth. Current capacity at 41% with 80% threshold triggering upgrades.
8.7	Protection against malware	OK	Robust anti-malware controls implemented using Norton security solutions. Measures include endpoint protection, real-time monitoring, regular scans, automatic updates, and user awareness training.
8.8	Management of technical vulnerabilities	OK	Structured process for identifying, assessing, and mitigating technical vulnerabilities. Regular vulnerability scanning and timely remediation implemented.
8.9	Configuration management	OK	Structured configuration management ensures systems are securely configured and maintained. Controls include baseline configurations, change management, regular reviews, and automated monitoring.
8.10	Information deletion	OK	Secure data deletion procedures prevent unauthorized access to residual information. Methods include cryptographic wiping, secure overwriting, degaussing, and physical destruction.
8.11	Data masking	OK	Data masking techniques protect sensitive information while maintaining usability. Measures include tokenization, pseudonymization, and encryption-based masking.
8.12	Data leakage prevention	OK	DLP controls monitor, detect, and prevent unauthorized data transmission. Measures include DLP software, endpoint monitoring, email filtering, USB restrictions, and network traffic analysis.
8.13	Information backup	OK	Structured backup strategy ensures data availability, integrity, and recoverability. Measures include automated backups, encryption, offsite replication, and periodic recovery testing.
8.14	Redundancy of information processing facilities	OK	Redundancy measures implemented for critical facilities ensuring continuous availability. Controls include backup servers, failover mechanisms, redundant network infrastructure, and cloud-based recovery.
8.15	Logging	OK	Centralized logging captures security events, system activities, and access records. Logs protected against tampering, regularly reviewed, and retained for forensic analysis.
8.16	Monitoring activities	OK	Continuous monitoring of network traffic, system activities, and security events. Security monitoring includes SIEM tools, IDS, and real-time alerting.
8.17	Clock synchronization	OK	Centralized clock synchronization across critical systems using NTP servers ensures accurate timestamps for logging, monitoring, and forensic analysis.
8.18	Use of privileged utility programs	OK	Strict controls over privileged utility programs prevent unauthorized modifications. Measures include restricted access, usage logging, MFA, and periodic reviews.
8.19	Installation of software on operational systems	OK	Strict controls over software installation. Measures include whitelisting approved software, administrative authorization, security assessments, and installation audit logs.
8.20	Networks security	OK	Network security controls implemented including firewall protections, IDS/IPS, VPN encryption, network segmentation, and continuous monitoring.
8.21	Security of network services	OK	Network services protected from unauthorized access and disruptions. Measures include firewall protections, IDS/IPS, VPN encryption, and continuous monitoring.
8.22	Segregation of networks	OK	Network segregation isolates critical systems and reduces attack surfaces. Measures include VLAN configurations, firewalls, ACLs, and separate networks for production, development, and guest access.
8.23	Web filtering	OK	Web filtering controls restrict access to malicious and unauthorized websites. Measures include DNS filtering, category-based restrictions, blacklisting, and real-time traffic monitoring.
8.24	Use of cryptography	OK	Cryptographic controls protect sensitive data during storage, processing, and transmission. Measures include AES encryption for data at rest, TLS for communications, and key management policies.
8.25	Secure development life cycle	OK	Security integrated into SDLC to mitigate vulnerabilities. Measures include threat modeling, static and dynamic code analysis, secure coding guidelines, and security testing at each phase.
8.26	Application security requirements	OK	Defined security requirements for applications ensure protection against vulnerabilities. Measures include secure coding guidelines, authentication controls, encryption, and regular security testing.
8.27	Secure system architecture and engineering principles	OK	Secure architecture principles embedded in IT infrastructure and application development. Measures include least privilege, defense-in-depth, secure design reviews, and industry best practices.
			Secure coding practices enforced to prevent vulnerabilities including injection attacks and XSS.

8.28	Secure coding	OK	Developers follow code review processes, static and dynamic analysis, and secure development frameworks.
8.29	Security testing in development and acceptance	OK	Security testing integrated into development and acceptance phases. Measures include SAST/DAST, penetration testing, vulnerability assessments, and compliance checks.
8.30	Outsourced development	OK	Security controls manage outsourced development risks. Measures include contractual security clauses, supplier assessments, secure coding standards, and regular security audits.
8.31	Separation of development, test and production environments	OK	Strict separation enforced between environments preventing unauthorized access and data leaks. Measures include RBAC, network segmentation, data masking, and restricted deployment permissions.
8.32	Change management	OK	Formal change management process ensures modifications are assessed, approved, and documented. Measures include risk assessments, version control, rollback procedures, and approval workflows.
8.33	Test information	OK	Controls protect test data ensuring sensitive information not exposed. Measures include data masking, anonymization, synthetic test data, and strict access controls.
8.34	Protection of information systems during audit testing	OK	Security controls ensure audit testing does not compromise systems. Measures include isolated testing environments, restricted live system access, activity logging, and prior risk assessments.