STAGE 1 EVIDENCE REVIEW REPORT

ISO/IEC 27001:2022 Information Security Management System with ISO/IEC 27032 Cybersecurity Extension

High-level senior audit evidence report - A4 format

Organization	SYLINK TECHNOLOGIE
Client reference	ST120260604001
Audit type	Stage 1 audit evidence review - initial certification / transfer support
Applicable sector	IAF 33 - Information Technology; activity aligned with NAF / APE 6201Z, computer programming and cybersecurity services
Declared personnel	155 employees / users declared for audit planning purposes
Registered / operational site	35 Rue Blatin, 63000 Clermont-Ferrand, France; operational scope includes remote work and relevant controlled service environments
Audit evidence source	Stage1_69_en.pdf, Audit Report - Stage 1, Form AR_01.2 Rev. 004, dated 29 August 2025; client information and website evidence provided by the client
Report date	04 June 2026

Document status: *This report is a senior technical synthesis of the evidence provided for Stage 1. It is intended to support audit file review, readiness assessment and Stage 2 planning. It does not replace the certification body decision, the formal audit report, or the requirement to verify objective evidence during Stage 2.*

Contents

1. Executive conclusion

Based on the Stage 1 evidence provided, SYLINK TECHNOLOGIE has defined an ISMS scope that is coherent with its business model as a French cybersecurity technology and service provider operating in IAF 33. The declared scope - design, development, implementation, management and support of cybersecurity solutions - is appropriate for ISO/IEC 27001 and for a cybersecurity extension based on ISO/IEC 27032.

The reviewed evidence shows that the main management system architecture is in place: organizational context, interested parties, ISMS scope, process interaction, information security policy, risk assessment results, risk treatment plan, Statement of Applicability, security objectives, operational planning, monitoring, internal audit programme and Annex A documentation were reported as present in the Stage 1 file.

However, the Stage 1 evidence also identifies several partial or incomplete areas that are relevant to mandatory ISO/IEC 27001 requirements. These include risk evaluation and acceptance criteria, residual risk acceptance, competence and training evidence, awareness evidence, internal and external communications, documented information control, management review records and nonconformity / corrective action management. These items do not necessarily demonstrate a failed ISMS, but they require objective closure before Stage 2 can be considered robust and defensible.

The senior audit judgement is that the organization may be technically eligible for Stage 2 only after documented closure of the identified observations and submission of objective evidence. If the missing evidence cannot be provided or remains materially incomplete, a focused Stage 1 follow-up or repeat Stage 1 review is required before proceeding.

Area	Stage 1 evidence status	Senior judgement
Scope and applicability	Defined and aligned with cybersecurity activities	Adequate for Stage 1; verify operational boundaries in Stage 2
Core ISMS documentation	Largely present with several partial items	Acceptable only if partial items are closed before Stage 2
Risk management	Risk assessment and treatment present; criteria and residual acceptance partial	High priority closure required
Annex A / SoA	SoA and selected Annex A evidence reported as present	No blanket exclusions supported; control applicability to be verified by sampling
Stage 2 readiness	0 major, 0 minor, 23 observations reported	Proceed only after evidence closure; otherwise repeat or focused Stage 1 follow-up

2. Audit context, criteria and normative alignment

The purpose of Stage 1 is to evaluate the client documented management system, confirm the scope and boundaries, understand the organization context and processes, collect information on applicable requirements, review readiness for Stage 2, and identify areas that may prevent a successful Stage 2 audit if not resolved.

For ISO/IEC 27001:2022, the evidence review has been structured against clauses 4 to 10, with particular attention to the documented scope, risk assessment and treatment process, Statement of Applicability, internal audit, management review and continual improvement. The Annex A evidence has been reviewed as supporting control evidence, not as proof of full operational effectiveness.

For the ISO/IEC 27032 cybersecurity extension, the evidence has been assessed in relation to cybersecurity governance, protection of cyberspace interactions, stakeholder coordination, cyber threat and vulnerability management, incident coordination, monitoring and resilience of digital services. These aspects are especially material because the organization is itself a cybersecurity provider.

Reference	Expected audit focus	Evidence implication
ISO/IEC 27001 clauses 4-10	Management system context, leadership, planning, support, operation, performance evaluation and improvement	Documented information must be complete, approved, controlled and implemented.
ISO/IEC 27001 Annex A	Organizational, people, physical and technological controls selected through the SoA	Applicability must be justified and linked to risk treatment and operational evidence.
ISO/IEC 27032 extension	Cybersecurity practices for digital environments and stakeholder coordination	Evidence must show cyber-specific governance, monitoring, response and coordination processes.
IAF 33 audit context	IT and cybersecurity service delivery with development, operations and customer interfaces	Audit sampling must include technical environments, privileged access, secure development and customer-facing services.

3. Organization, scope and boundaries

SYLINK TECHNOLOGIE is presented as a cybersecurity technology organization providing software, platforms and related professional or managed cybersecurity services. The scope defined in the Stage 1 file is: Design, develop, implement, manage and support cybersecurity solutions.

The scope is considered appropriate because it captures the essential lifecycle of the services: design, secure development, implementation, operational management, maintenance, customer support and service improvement. It also reflects the security-sensitive nature of the organization activities, including firewalls, DPI probes, EDR, SOC services, cyber audit, vulnerability assessment, penetration testing and incident-related support.

The organizational boundary includes management, information security governance, software development, technical operations, SOC and monitoring activities, customer support, commercial processes, purchasing, supplier management, human resources, finance and administration. The technical boundary includes assets, networks, endpoints, applications, development and production environments, logs, source code, security configurations, cloud or hosted services, and third-party services used for delivery or support.

Boundary type	Senior assessment
Organizational boundary	Adequately described; must be supported by an approved organizational chart, role allocation and ISMS responsibilities before Stage 2.
Geographical boundary	Registered / operational site in Clermont-Ferrand and controlled remote working arrangements are included; secondary or service delivery sites must be confirmed.
Technical boundary	High complexity: development, production, SOC, monitoring, privileged administration, customer support and hosted/cloud interfaces must be mapped.
Customer environments	Included only where under contractual responsibility or operational control; interfaces, remote access and responsibilities must be evidenced.
Third-party providers	External infrastructures remain outside direct scope but must be covered through supplier controls, contracts, security requirements and monitoring.

4. Evidence reviewed and audit trail

The following evidence was reviewed as part of this senior synthesis. The assessment is limited to the material provided and does not replace direct verification of records, personnel interviews or technical sampling during Stage 2.

Evidence source	Content reviewed	Audit relevance
Stage 1 audit report form	Client reference, organization data, scope, sector, address, audit mode, audit team, opening and closing meeting records	Confirms audit basis, context and audit trail.
Scope and boundaries section	ISMS scope, cybersecurity extension boundaries, organizational and technical perimeter	Supports ISO/IEC 27001 clause 4.3 and Stage 2 planning.
Processes and services section	Cybersecurity software, firewall, DPI, EDR, SOC, vulnerability assessment, audit, penetration testing and support processes	Supports process understanding and risk-based sampling.
Documentation review matrix	Clauses 4 to 10, present and partial documented information	Identifies readiness gaps and mandatory evidence to be closed.
Annex A documentation matrix	Asset inventory, incidents, ICT continuity, suppliers, backups, access control, secure development	Supports SoA and control evidence planning.
Findings table	0 major, 0 minor and 23 observations recorded	Defines areas needing closure before Stage 2.
Company and public context evidence	Business registration, IAF 33 / APE 6201Z context and cybersecurity website information provided by the client	Supports audit sector, activity consistency and scope plausibility.

5. ISO/IEC 27001 Stage 1 evidence assessment

The Stage 1 file demonstrates that the ISMS is structured and that the principal documents required for a Stage 1 readiness assessment have been considered. Nevertheless, several mandatory records are reported as partial and must be completed, approved and controlled before Stage 2.

ISO/IEC 27001 area	Evidence reported	Stage 1 result	Stage 2 expectation
Clause 4 - Context and scope	Context analysis, interested parties, scope and process interaction reported as present	Adequate	Confirm scope boundaries, interfaces and interested-party requirements through interviews and records.
Clause 5 - Leadership	Information security policy present; roles and	Partially adequate	Approve and communicate ISMS roles, responsibilities,

	responsibilities partial		authorities and escalation lines.
Clause 6.1.2 - Risk assessment	Risk assessment results present; risk criteria and acceptance criteria partial	Partial	Define risk methodology, likelihood/impact criteria, acceptance thresholds and review frequency.
Clause 6.1.3 - Risk treatment	Risk treatment plan and SoA present; residual risk acceptance partial	Partial	Link SoA to risks, treatment decisions, control owners and signed residual risk acceptance.
Clause 6.2 - Objectives	Security objectives and implementation plans reported as present	Adequate	Verify measurable KPIs, owners, deadlines and monitoring evidence.
Clause 7.2 / 7.3 - Competence and awareness	Training plan and awareness evidence partial	Partial	Provide competence matrix, role-based training records and awareness completion evidence.
Clause 7.4 - Communication	Internal and external communication plan partial	Partial	Define communication channels for incidents, customers, authorities, suppliers and cyber stakeholders.
Clause 7.5 - Documented information	Required documented information and document control partial	Partial	Provide master list, version control, approvals, retention rules and access controls.
Clause 8 - Operation	Operational planning, updated risk assessment and treatment implementation present	Adequate for Stage 1	Sample operational controls, secure development, SOC and customer service delivery.
Clause 9 and 10 - Performance and improvement	Monitoring and internal audit present; management review and corrective action process partial	Partial	Provide management review minutes, NC/CA log, root cause analysis and effectiveness checks.

6. Annex A and Statement of Applicability evidence

No evidence has been provided to support the exclusion of entire Annex A control domains. For a cybersecurity provider, Annex A controls are broadly relevant and must be evaluated individually in the SoA based on risk, legal, contractual and operational requirements.

The Stage 1 file reports the SoA as present and identifies several Annex A evidence categories as present. At Stage 2, the audit shall verify not only the existence of documentation but also the effectiveness of selected controls in real operating conditions.

Annex A control area	Evidence reported at Stage 1	Stage 2 sampling focus
A.5.9 Information assets	Asset inventory and responsibilities reported as present	Verify completeness for source code, logs, customer data, credentials, platforms and cloud assets.
A.5.24-A.5.27 Incident management	Incident response procedures and incident register reported as present	Sample incident workflow, classification, escalation, lessons learned and customer notification rules.
A.5.30 ICT readiness / continuity	ICT continuity plan reported as present	Verify backup, recovery, continuity objectives and crisis coordination for SOC and customer-facing services.
A.5.19-A.5.22 Supplier security	Supplier security assessment and agreements reported as present	Sample hosting, cloud, software, support and security tooling providers.
A.8.13 Backup	Backup plan and test records reported as present	Verify backup coverage, restoration tests, segregation, encryption and retention.
A.5.15-A.5.18 / A.8.5 / A.8.2 Access, authentication and cryptography	Policies reported as present	Sample privileged access, MFA, administrative accounts, secrets, encryption and remote access.
A.8.25-A.8.29 Secure development	Secure development lifecycle and security test records reported as present	Verify SDLC, code review, vulnerability management, test evidence, change control and release governance.

7. ISO/IEC 27032 cybersecurity extension assessment

The ISO/IEC 27032 extension is particularly material because SYLINK TECHNOLOGIE operates as a cybersecurity technology and service provider. The extension should not be treated as a generic appendix to ISO/IEC 27001; it requires evidence of cybersecurity practices addressing interactions in cyberspace, coordination between stakeholders, cyber threat management and incident response support.

The Stage 1 scope includes prevention, detection, monitoring, response support, vulnerability management, cyber threat management, coordination with customers and relevant stakeholders, and protection of information exchanged through digital environments. These elements are appropriate for the extension, but they require targeted evidence during Stage 2.

Cybersecurity extension area	Expected evidence	Audit priority
Cybersecurity governance	Defined responsibilities for cyber operations, SOC, vulnerability management, incident escalation and customer communication	High
Stakeholder coordination	Customer, supplier, hosting provider, authority and emergency contact matrices; contractual security responsibilities	High
Threat and vulnerability management	Threat intelligence sources, vulnerability scanning, prioritization, remediation tracking and disclosure rules	High
Monitoring and detection	SOC procedures, alert triage, logging, use cases, escalation, evidence retention and performance metrics	High
Incident response support	Cyber incident playbooks, notification criteria, customer support workflow, forensic preservation and lessons learned	High
Secure digital service delivery	Secure deployment, change control, hardening, access control, backup and continuity for customer-facing platforms	High
Awareness and human factors	Cyber role-based awareness for developers, SOC analysts, administrators, support teams and management	Medium

8. IT system complexity and Stage 2 sampling implications

The IT system should be considered high complexity for audit planning purposes. The organization does not only consume IT services internally; it designs, develops, operates and supports cybersecurity products and services for external customers. This dual role increases the importance of segregation, privileged access management, secure development, change control, monitoring, incident management and customer data protection.

Stage 2 sampling should therefore include both management system evidence and technical-operational evidence. The audit should not be limited to policies and procedures; it should verify live or recent records from development, operations, SOC, customer support, supplier management and incident / vulnerability processes.

Complexity driver	Reason for significance	Stage 2 implication
Cybersecurity service provider model	Services involve sensitive customer security data, alerts, vulnerabilities and incidents	Sample confidentiality, integrity and availability controls over customer data.
Software development and maintenance	Source code and release pipelines are critical information assets	Sample secure SDLC, access to repositories, testing and release approval.
SOC and monitoring activities	Logs, alerts and detection rules may be business-critical	Sample detection workflow, alert handling, retention and escalation.
Privileged and remote access	Customer support and administration may require elevated privileges	Sample MFA, least privilege, session control and customer authorization.
Third-party hosting and cloud services	External dependencies affect availability and security assurance	Sample supplier due diligence, contracts, SLAs and monitoring.
ISO/IEC 27032 extension	Cybersecurity coordination goes beyond internal ISMS boundaries	Sample stakeholder communications, incident coordination and threat management.

9. Findings, observations and readiness risk

The Stage 1 file reports no major nonconformities and no minor nonconformities, but 23 observations. The absence of major or minor nonconformities does not automatically mean that the organization is ready for Stage 2. In Stage 1, the most important question is whether the documented system is sufficiently complete and implemented to permit effective Stage 2 sampling.

The observations related to mandatory documentary elements should be treated as pre-Stage 2 closure requirements. In particular, partial evidence for risk criteria, residual risk acceptance, training, documented information control, management review and corrective action management may compromise the defensibility of a Stage 2 audit if not resolved.

Some audit planning items recorded as areas of concern, such as no scope changes, no temporary sites, no significant travel time, no seasonality, no employee changes and no night shift, should be interpreted as planning confirmations rather than nonconformities, provided the answers remain accurate and documented.

Area	Finding type	Risk if unresolved	Required action
Risk criteria and residual risk acceptance	Observation / partial mandatory evidence	Risk treatment may not be auditable or management-approved	Complete methodology and signed residual risk acceptance.
Roles, responsibilities and authorities	Observation / partial evidence	Unclear accountability for ISMS and cybersecurity operations	Approve RACI, organization chart and security

			responsibilities.
Competence, training and awareness	Observation / partial evidence	Personnel may not be demonstrably competent for security-sensitive roles	Provide competence matrix and training / awareness records.
Documented information control	Observation / partial evidence	Policies, procedures and records may lack control, approval or traceability	Implement master list, revision control, approval and retention rules.
Management review and corrective action	Observation / partial mandatory evidence	Performance evaluation and improvement loop may be incomplete	Provide management review minutes, NC/CA log and effectiveness evidence.

10. Required evidence before Stage 2

The following evidence should be submitted, reviewed and formally accepted before the Stage 2 audit is confirmed. Evidence must be approved, version-controlled, aligned with the certified scope and supported by implementation records where applicable.

No.	Evidence required	Minimum content expected	Priority
1	Organizational structure and ISMS responsibilities	Approved organization chart, ISMS roles, process owners, cyber operations roles, deputies and escalation lines	High
2	Risk assessment and acceptance criteria	Methodology, risk scales, likelihood and impact criteria, acceptance thresholds, review rules and approval	High
3	Residual risk acceptance	List of residual risks, treatment status, risk owners and top management acceptance	High
4	Updated SoA	Applicability of all Annex A controls, justification for non-applicability, control owners and link to risk treatment	High
5	Training and competence evidence	Competence matrix, role-based training plan, training records for developers, SOC, support, administrators and management	High
6	Awareness evidence	Awareness programme, attendance/completion records and evaluation of effectiveness	Medium
7	Communication plan	Internal/external communication rules, incident communications, customer notifications, authority/supplier contacts	High
8	Documented information control	Document master list, approvals, versions, retention, access restrictions and change history	High
9	Internal audit evidence	Audit programme, audit plan, audit report, findings, corrective actions and auditor independence evidence	High
10	Management review records	Minutes covering mandatory inputs and outputs, decisions, improvement actions and resource needs	High
11	Nonconformity and corrective action process	NC/CA procedure, register, root cause analysis, corrective action status and effectiveness checks	High
12	ISO/IEC 27032 cyber evidence	Cyber stakeholder matrix, incident coordination procedures, threat/vulnerability management records and SOC evidence	High
13	Technical operational records	Access review, backup test, vulnerability management, incident log, secure development and supplier review samples	High

11. Senior recommendation

The Stage 1 evidence is sufficient to understand the organization, confirm the general scope, identify the applicable sector and plan the technical focus of Stage 2. The defined scope is coherent with the organization activities and the ISO/IEC 27001 / ISO/IEC 27032 audit perimeter.

The organization should not proceed to Stage 2 without prior closure of the identified mandatory evidence gaps. The recommended certification file decision is: Not recommended for Stage 2 until objective evidence is submitted, reviewed and the Stage 1 concerns are closed. If the evidence remains incomplete or materially inconsistent, a further Stage 1 audit or focused Stage 1 follow-up review should be performed.

Once the required evidence is closed, Stage 2 should concentrate on operational effectiveness, with sampling across governance, risk management, secure development, SOC operations, incident response, access control, supplier security, backup / continuity, vulnerability management, customer support and cybersecurity stakeholder coordination.

Decision item	Senior conclusion
Major nonconformities	None reported in the Stage 1 file.
Minor nonconformities	None reported in the Stage 1 file.
Observations	23 observations reported; several relate to mandatory ISO/IEC 27001 evidence and must be closed before Stage 2.

Prepared by: *Senior audit support synthesis generated from the evidence provided. Final certification decisions remain under the responsibility of the accredited certification body and its competent decision-making function.*