STAGE 2 CLOSURE EVIDENCE REPORT

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

Organization	SYLINK TECHNOLOGIE
Registered / verified permanent site	35 Rue Blatin, 63000 Clermont-Ferrand, France
Certification scope	Design, development, implementation, management and support of cybersecurity solutions.
IAF sector	IAF 33 - Information Technology
Audit stage	Stage 2 - Certification audit closure evidence
Document date	04 June 2026

Prepared as objective evidence summary for audit closure and certification recommendation.

Confidentiality note: This report is intended to support the audit file and shall be used together with the applicable audit report, documented evidence and sampled records reviewed during the Stage 2 audit.

1. Executive closure statement

The Stage 2 audit verified the effective implementation, maintenance and operational effectiveness of the ISO/IEC 27001 Information Security Management System, including the ISO/IEC 27032 cybersecurity extension, for SYLINK TECHNOLOGIE.

The audit confirmed that the management system is aligned with the organizational context, certification scope, cybersecurity service delivery model, applicable requirements, identified risks and selected Annex A controls. The evidence reviewed supports the conclusion that the ISMS is suitable, adequate and effective for the defined scope.

Final audit conclusion: Conforming
No major nonconformity was identified. No minor nonconformity was identified that would prevent certification. The organization is recommended for certification for the declared scope, subject to the normal certification decision process.

2. Organization and certification scope

Organization	SYLINK TECHNOLOGIE
Address / permanent site verified	35 Rue Blatin, 63000 Clermont-Ferrand, France
Declared employees	155
IAF sector	IAF 33 - Information Technology
Standard	ISO/IEC 27001 with ISO/IEC 27032 cybersecurity extension
Scope	Design, development, implementation, management and support of cybersecurity solutions.
Core activities verified	ISMS governance, information security risk management, secure software development, cybersecurity solution implementation, operational support, customer support, supplier / hosting partner management, vulnerability management, monitoring, incident support and continual improvement.

3. Permanent site verified during the audit

Site details and address	Activity carried out
SYLINK TECHNOLOGIE - 35 Rue Blatin, 63000 Clermont-Ferrand, France	Permanent site verified during the Stage 2 audit. Activities include management and governance of the ISMS, information security risk management, cybersecurity risk treatment, secure design and development of cybersecurity solutions, implementation, management and support of cybersecurity products and services, technical operations, customer support, supplier and hosting partner management, monitoring and incident support activities, vulnerability management, internal coordination, administrative processes and continual improvement of the ISMS.

4. Audit method and objective evidence basis

The conclusions are based on interviews, sampled review of documented information, evidence of implementation, operational records and management-system outputs. The audit approach was based on sampling and therefore does not imply verification of every record or transaction.

- Review of Stage 1 areas of concern and verification of closure before certification decision.
- Review of the ISMS scope, context, interested parties, policies, processes and documented information.
- Review of risk assessment criteria, risk assessment results, risk treatment plan, residual risk approval and Statement of Applicability.
- Sampling of Annex A implementation evidence, including access control, supplier security, incident management, backup, ICT readiness, secure development, vulnerability management, monitoring, logging, cryptographic controls and protection of customer information.
- Review of internal audit, management review, monitoring and measurement, corrective action and continual improvement records.

- Verification of cybersecurity-specific evidence supporting the ISO/IEC 27032 extension, including vulnerability management, penetration testing, incident support, cyber threat monitoring and secure interaction with customers and stakeholders.

5. Closure of Stage 1 areas of concern

The Stage 1 audit identified areas requiring completion or stronger formalization before Stage 2. During Stage 2, the organization provided updated and sufficient objective evidence demonstrating closure of the relevant areas.

Stage 1 area	Stage 2 evidence verified	Closure status
Roles and responsibilities	Updated organizational structure, ISMS roles, risk owners and process responsibilities reviewed.	Closed
Risk analysis and acceptance criteria	Risk methodology, likelihood / impact criteria, acceptance thresholds and risk ownership verified.	Closed
Residual risk approval	Residual risk review and acceptance by competent owners / management verified.	Closed
Training and competence	Training plan, competence evidence and role-based records reviewed.	Closed
Awareness	Awareness evidence, internal communications and sampled interviews confirmed understanding of information security duties.	Closed
Communication	Internal / external communication arrangements and event / incident reporting channels verified.	Closed
Documented information	Document control, versioning, approval, accessibility, retention and protection mechanisms verified.	Closed
Management review	Management review records and outputs reviewed, including risks, objectives, audit results and improvements.	Closed
Nonconformities and corrective actions	Corrective action process, action tracking and effectiveness verification records reviewed.	Closed

6. Clause-by-clause Stage 2 evidence summary

Clause	Objective evidence and audit conclusion	Result
5.3 Roles, responsibilities and authorities	Specific ISMS roles have been assigned and are understood. Responsibilities are reflected in operational management, risk ownership, secure development, incident management, supplier controls and cybersecurity service delivery.	Conforming
6.1.2 Information security risk assessment	Risk analysis and acceptance criteria are established, documented and consistently applied. Risk assessments are updated when significant changes occur and feed into treatment planning.	Conforming
6.1.3 Information security risk treatment	Risk treatment plan and SoA are approved and maintained. Residual risks are formally reviewed and accepted. Actions are assigned, traceable and monitored.	Conforming
6.2 Information security objectives	Objectives are defined, measurable, monitored and aligned with the policy and business processes. Results are used for improvement.	Conforming
6.3 Planning of changes	ISMS changes are planned, authorized and assessed for risks and control impacts before implementation where applicable.	Conforming
7.1 Resources	Human, technological and infrastructural resources are available and proportionate to the scope and complexity of the ISMS.	Conforming
7.2 Competence	Personnel influencing ISMS performance are competent based on education, training and experience. Records and gap management are maintained.	Conforming
7.3 Awareness	Personnel are aware of the policy, objectives, responsibilities and impact of their activities or omissions on information security.	Conforming
7.4 Communication	The organization has determined what to communicate, to whom, how often and by which means. Security event reporting channels are known and accessible.	Conforming
7.5 Documented information	Required documented information is created, reviewed, accessible, maintained and protected from unauthorized access, alteration or loss.	Conforming
8.1 Operational planning and control	Operational processes are planned and controlled in line with ISMS requirements, risk treatment actions and selected controls.	Conforming
8.2 Information security risk reassessment	Risk assessments are repeated following significant changes, with results documented and used to update controls and treatments.	Conforming
8.3 Risk treatment implementation	Planned risk treatment measures are implemented, assigned, monitored and supported by implementation evidence.	Conforming
9.1 Monitoring, measurement, analysis and evaluation	KPIs and monitoring activities are defined and used to evaluate ISMS effectiveness and feed into management review.	Conforming
10.1 Continual improvement	Improvement opportunities are identified, evaluated, formalized and integrated into the ISMS through a structured process.	Conforming
10.2 Nonconformities and corrective actions	Nonconformities are identified, documented, analysed for cause, corrected and verified for effectiveness with records preserved.	Conforming

7. Annex A and Statement of Applicability evidence

The Statement of Applicability was verified as defined, approved, maintained and aligned with the information security risk assessment, risk treatment plan, legal and contractual requirements, cybersecurity service obligations and operational controls. No unjustified exclusion of Annex A controls was identified.

Control area	Stage 2 evidence verified
Asset management	Information assets, ownership and responsibilities are identified and controlled.
Access control and authentication	User access, privileged access and authentication controls are implemented and periodically reviewed.
Supplier security	Supplier and hosting partner requirements, responsibilities and monitoring arrangements are defined.
Incident management	Event / incident reporting, escalation, response, analysis and improvement records are maintained.
Backup and ICT readiness	Backup and continuity arrangements support availability and resilience of relevant services and information assets.
Secure development	Secure design, development, testing, change control and vulnerability handling practices are implemented.
Technical vulnerability management	Vulnerabilities are identified, assessed, prioritized, assigned and followed up through remediation or approved treatment.
Monitoring and logging	Monitoring and logs support detection, investigation, operational control and performance evaluation.
Cryptographic controls	Cryptographic mechanisms and key management arrangements protect confidentiality, integrity and secure transmission.
Customer information protection	Customer data, security logs, alerts, credentials, source code and technical documentation are protected by appropriate controls.

8. Vulnerability management and penetration testing

Vulnerability management and penetration testing activities were verified as part of Annex A and cybersecurity extension evidence. The organization applies a risk-based approach for identifying, assessing, prioritizing, treating and following up technical vulnerabilities affecting systems, applications, cybersecurity platforms, development environments, customer-facing services and supporting infrastructure.

- Testing activities are planned, authorized and scoped with defined objectives, rules of engagement, limitations, timing and responsibilities.
- Findings are documented, classified by severity and business impact, assigned to owners and tracked until remediation, approved acceptance or other treatment decision.
- Outputs are used to update controls, secure development practices, configuration hardening, risk assessment, risk treatment plan and SoA where applicable.
- For significant findings, follow-up verification or re-testing is performed to confirm effective remediation and acceptable residual risk.

Vulnerability / penetration testing conclusion: Conforming
The process is planned, authorized, documented, risk-based, traceable and used to improve ISMS and cybersecurity control effectiveness.

9. Cryptographic controls and key management

Cryptographic controls and related key management arrangements were verified as part of Annex A and SoA implementation evidence. Cryptographic controls are applied based on the classification of information, risk assessment outcomes, service criticality, legal and contractual requirements and customer expectations.

- Encryption is applied where appropriate to data in transit and data at rest, including secure remote access, administrative access, communications, backups and sensitive repositories.
- Responsibilities are defined for creation, distribution, storage, use, renewal, revocation and protection of cryptographic keys and certificates.
- Access to cryptographic keys, certificates and key management functions is restricted according to role, responsibility and need-to-know principles.
- Cryptographic weaknesses, expired certificates, insecure protocols or vulnerabilities are managed through vulnerability management, change management or corrective action processes.

Cryptographic controls conclusion: Conforming

Cryptographic controls and key management arrangements are risk-based, maintained and aligned with the SoA, Annex A controls and cybersecurity extension.

10. Audit results and objective evidence used

Audit result area	Conclusion	Objective evidence used
Context of the organization	Context, interested parties, ISMS scope and cybersecurity context are defined and consistent with the organization as an IAF 33 cybersecurity technology provider.	Context analysis, interested parties matrix, ISMS scope, process map, management interviews, review of services.
Strengths	Strong technical alignment between business activity and ISO/IEC 27001 / ISO/IEC 27032 requirements; cybersecurity is core to service delivery.	SoA, risk treatment plan, secure development evidence, vulnerability / penetration testing records, incident management and monitoring evidence.
Weaknesses	No major weakness affecting certification was identified. Continued consolidation of traceability is recommended as an improvement opportunity.	Review of Stage 1 findings, updated documented information, management review and corrective action evidence.
Legislative compliance	Applicable legal, regulatory and contractual requirements relevant to information security and cybersecurity are identified and considered.	Legal / contractual requirements register, customer requirements, supplier agreements, data protection considerations, SoA and risk assessment.
Leadership and participation	Top management supports the ISMS through policy, roles, resources, objectives, risk review and continual improvement.	Policy, organizational chart, roles, management review, objectives, interviews and awareness evidence.
Planning and risk management	Risk assessment, risk treatment, SoA and residual risk acceptance are implemented and aligned.	Risk methodology, risk register, treatment plan, SoA, residual risk approvals, change and reassessment evidence.
Support	Resources, competence, awareness, communication and documented information support effective ISMS operation.	Training records, competence evidence, communication plan, document control, controlled repositories and interviews.
Operational activities	Operational processes are planned and controlled in line with risk treatments and selected controls.	Operational procedures, access reviews, vulnerability records, incident logs, backup evidence, supplier controls and monitoring evidence.
Performance evaluation	Monitoring and KPIs support evaluation of ISMS effectiveness and informed decisions.	Security objectives, KPIs, monitoring records, incident data, internal audit outputs and management review inputs.
Audit and management review	Internal audits and management reviews are performed and documented, with outputs used for improvement.	Internal audit programme and reports, management review minutes, action tracking and follow-up evidence.
Improvement	Nonconformities, observations and improvement opportunities are managed through corrective action and continual improvement processes.	NC / corrective action log, root cause analysis, action plans, effectiveness verification records and improvement register.
Schema-specific information	ISO/IEC 27032 cybersecurity extension practices are implemented for cyber threat monitoring, vulnerability management, incident support, secure development, customer coordination and secure digital information exchange.	SoA, Annex A evidence, vulnerability / penetration records, cryptographic controls, SOC / monitoring evidence, secure development and supplier controls.

11. Nonconformities, observations and certification recommendation

Major nonconformities	0
Minor nonconformities preventing certification	0
Stage 1 concerns	Closed for Stage 2 purposes based on sampled evidence.
Improvement opportunities	Any improvement opportunities communicated during the audit are to be managed through the ISMS continual improvement process.
Final recommendation	Recommended for certification.

The organization demonstrated conformity with applicable ISO/IEC 27001 requirements and with the ISO/IEC 27032 cybersecurity extension. The ISMS is considered suitable, adequate and effective for the declared scope.

The certification recommendation is based on the sampled evidence reviewed during the Stage 2 audit and remains subject to the independent certification decision process of the certification body.

12. Final auditor statement

Based on the evidence reviewed, interviews performed and samples assessed, the ISMS is implemented and operational. The organization has demonstrated effective application of risk management, Annex A controls, cybersecurity-specific controls, operational processes, performance evaluation and continual improvement mechanisms.

Certification recommendation: Recommended for certification
The Stage 2 audit confirms that SYLINK TECHNOLOGIE is ready for certification for the scope: design, development, implementation, management and support of cybersecurity solutions.

Representative / Referent of the organization	**Lead Auditor**
Name / Signature: _____	Name / Signature: _____
Date: ____ / ____ / _____	Date: ____ / ____ / _____