Stage- 2 Report

Information Security Managment System

Client Information:

Sl.	Subject	Particular			
1	Reference Number (unique ID Allotted)	//			
2	Name of the Client	SYLINK TECHNOLOGIE			
3	Address of the Client	35 Rue Blatin, 63000 Clermont-Ferrand, Francia			
4	Sita Address (If Any)	//			
5	No. of Employees	155			
6	No. of Users	210			
7	No. of Server	350			
8	No. of work stations	210			
9	No. of Application Development and Maintenance staff	55			
10	Email	malena.moreira@sylink.com			
11	Contact Person	Malena Moreira			
12	Phone/ Mobile	+33 7 87 35 94 69			
13	Scope	Design, develop, implement, manage and support cybersecurity solutions.			
14	Technical Area				
15	Audit Team	Lead Auditor:	Giuseppe Izzo	Auditor:	
		Technical Expert:	Giuseppe Izzo	Observor:	
16	Audit Man-days	1/4			
17	Audit Date	13-16/01/2026			
18	Brief about the organization	SYLink is a leading cybersecurity innovation company, developing advanced solutions to protect companies from digital threats. Give me the English			
19	Type of Audit				
20	Extent of Remote Audit (If Applicable)				
21	Audit Objective	To Evaluate and Ensure that the clients' management system documentation meets the requirements of the standard/ specification and to conform that the client organization adheres to its own policies, objectives and procedure & all the requirement of the ISMS standard and other normative documents and to verify the implementation of the Information Security Management System as per the Standards Requirement, verification of records for the conformity of the implementation.			

Recording of Attendance:

Audit Attendance Sheet				Record of Attendance (by LA)	
Sl.	Name	Position	Department	Opening	Closing
	GIUSEPPE IZZO	LEAD AUDITOR	UESE ITALIA SPA		
	Malena Moreira	CEO	SYLINK TECHNOLOGIE		

Clause	Subject	Reference / Evidence	Finding	Reviewer Comment (To be filled by Technical Review Team)	Reviewer Decision
4	**Context of the Organization**				
4,1	**Understanding the Organization and its context**				
	A. Has the external and internal issues relevant to the information security management system been identified?	ok	**Confirm**		
	B. Has the organization's context been identified to establish its information security management system (ISMS)	ok	**Confirm**		
	C. Has the internal issues that are relevant to the organization's purpose been identified and the influence these issues could have on its ability to achieve the outcomes that its ISMS intends to achieve been documented?	ok	**Confirm**		
	Has the organization :-				
	a) Determined the influence the *internal stakeholders* could have?	ok	**Confirm**		
	b) Determined the influence the approach to *governance* could have?				
	c) Determined the influence the organization's *capabilities* could have?				
	d) Determined the influence the organization's *culture* could have?				
	e) Determined the influence the organization's contracts could have?				
	f) Identified the *external* issues that are relevant to the organization's purpose and considered the influence these issues could have on its ability to achieve the outcomes that its ISMS intends to achieve?	ok	**Confirm**		
	g) Determined the influence environmental conditions could have?				
	h) Determined the influence *key trends and drivers* could have?				
	i) Determined the influence *external stakeholders* could have?				
4,2	**Understanding the needs and expectations of interested parties**				
	a) Has the organization determined all the parties that have an interest in the organization's ISMS?	ok	**Confirm**		
	b) Has the organization identified the requirements of the parties including their needs and expectations?	ok	**Confirm**		
4,3	**Determining the scope of the information security management system**				

	a) Determined boundaries and applicability of the ISMS?	ok	**Confirm**		
	b) Is ISMS Policy available as documented information?	ok	**Confirm**		
	c) Has the Organization considered; external and internal issues, requirements of interested parties, interface and dependencies between activities performed by the Organization and those performed by other organizations?	ok	**Confirm**		
4,4	**Information security management system**				
	Has the Organization documented the process to establish, implement, maintain and continually improve the ISMS?	ok	**Confirm**		
5	**Leadership**				
5,1	**Leadership and commitment**				
	Has the Management:-	ok	**Confirm**		
	a) Established policy and objectives in line with strategic direction?				
	b) Ensured integration with organizations processes?				
	c) Ensured resources?				
	d) Communicated importance of management and conformity?				
	e) Ensured ISMS achieves intended outcomes?				
	f) Directed and supported persons involved in the ISMS?				
	g) Promoted continual improvement?				
	h) Supported other relevant managers?				
5,2	**Policy**(Verify Documented ISMS Policy)				
	a) Is the policy appropriate to the purpose of the Organization?	ok	**Confirm**		
	b) Does the policy include information security objectives or provides the framework for setting information security objectives?				
	c) Does the policy includes a commitment to satisfy applicable requirements related o information security?				
	d) Does the policy include a commitment to continual improvement of the information security management system?				
	e) Is the policy available as documented information? (Give reference of Policy Number)				
	f) Is the policy communicated within the organization?				
	g) Is the policy Available to interested parties?				
5,3	**Organizational roles, responsibilities and authorities**				
	a) Are Roles and authorities assigned and communicated?	ok	**Confirm**		
	b) Has top management assigned responsibilities for; ensuring the ISMS which conform to the standard, reporting on the performance to top management?				
6	**Planning**				
6,1	**Actions to address risks and opportunities**				
6.1.1	**General**				
	a) Has the management considered: context of the Organization, needs and expectations of interested parties? b) Determined the risks and opportunities that need to be addressed; ISMS achieves intended outcomes, prevents or reduces undesired effects and achieves continual improvement? c) Has the Organization planned; actions to address risks and opportunities and how to; integrate and implement actions into its ISMS and evaluate the effectiveness?	ok	**Confirm**		
6.1.2	**Information security risk assessments**(Verify Documented Information on the Risk Assessment Process)				
	a) Has the Organization defined and applied a risk assessment approach that; establishes and maintains risk acceptance criteria and criteria for performing risk assessments? b) Ensured repeatability producing consistent, valid and comparable results? c) Has the security risks associated with loss of Confidentiality, Integrity and Availability along with Risk Owners identified? d) Has the risks analysis been done and potential consequences, realistic likelihood, levels of risk been identified? e) Have the risks been evaluated, compared and priorities been assigned? f) Has the documented information been retained by the organization?	ok	**Confirm**		
6.1.3	**Information security risk treatment**(Verify Documented Information on the Risk Treatment Process& the Statement of Applicability)				
	a) Has the Organization defined and applied Information security risk treatment process to: select treatment options?	ok	**Confirm**		
	b) Determined controls "from any source"?				
	c) Compared controls with Annex A?				
	d) Produced a Statement of Applicability?				
	e) Formulated a treatment plan?				
	f) Obtained owners approval of treatments and residual risks?				
	g) Retained documented information?				
6,2	**Information security objectives and planning to achieve them**(Verify Documented Information on the Information Security Objectives)				
	a) Has the Organization established objectives ***"at relevant functions and levels"***?	ok	**Confirm**		

	b) Are these objectives consistent, measurable (where practicable), take into account requirements, assessment and treatments, communicated, updated?				
	c) Has the Organization retained documented information such as what will be done, what resources will be required, who will be responsible, when it will be completed and how results will be evaluated?				
6,3	**Planning of Changes**				
	How the organization determines the need for changes to the information security management system and are the changes carried out in a planned manner?	ok	**Confirm**		
7	**Support**				
7,1	**Resources**				
	Has the Organization provided enough resources to achieve information security?	ok	**Confirm**		
7,2	**Competence(Verify Documented Information for the Evidence of the Competence)**				
	Has the organizations determined the necessary competence and ensure it, take actions to acquire, retain documentation?	ok	**Confirm**		
7,3	**Awareness**				
	a) Persons shall be aware of: the ISMS policy, their contributions to the ISMS, consequence of not conforming b) Make sure that the people who work for the organization understand and are aware of its information security policy. c) Make sure that the people who work for the organization understand how they can support and help enhance the effectiveness of the ISMS.	ok	**Confirm**		
7,4	**Communication**				
	Has the Organization determined the need for internal and external communication?	ok	**Confirm**		
7,5	**Documented information**				
7.5.1	General				
	a) Has the organizations ISMS included the documented information required by the standard?	ok	**Confirm**		
	b) Information deemed by the Organization as required		**Confirm**		
7.5.2	Creating and updating		**Confirm**		
	When creating documented information; has the Organization ensured appropriateness; identification and description, format, review and approval requirement?		**Confirm**		
7.5.3	Control of documented information		**Confirm**		
	a) Has the documented information controlled to ensure; availability		**Confirm**		
	b) Has the Organization addressed; distribution		**Confirm**		
	c) Has the External documents, Documented Information of External Origin controlled as other Documented Information?		**Confirm**		
8	**Operation**				
8,1	**Operational planning and control(Verify Documented Information "evidencing Process Execution" as Planned)**	ok	**Confirm**		
	a) Has the Organization planned, implemented and controlled all the processes? b) Has the Organization implemented plans to achieve objectives? c) Has the Organization controlled planned changes and review consequences of unplanned changes? d) Has the Organization ensured that the outsourced processes are determined and controlled?				
8,2	**Information security risk assessments (Verify Documented Information on Risk Assessment)**				
	a) Has the Organization performed risk assessments at planned intervals or at significant changes? b) Has the Organization retained documented information?				
8,3	**Information security risk treatment (Verify**				
	Has the Organization implemented risk treatment plan and retain documentation?	ok	**Confirm**		
9	**Performance evaluation**				
9,1	**Monitoring, measurement, analysis and evaluation(Verify Documented Information on Evidence of Monitoring and Measuring)**	ok	**Confirm**		
9,2	**Internal audit(Verify Documented Information on Internal Audit Program & result)**				
	Has the Organization conducted internal audits and auditors selected to conduct audits "that ensure the objectivity and impartiality of the audit process"?	ok	**Confirm**		
9,3	**Management review(Verify Documented Information on the result of Management Review)**				
	Has the Top management reviewed the ISMS at planned intervals and recorded the actions which include a. Status of actions from previous meetings b. External and internal changes c. Feedback on performance d. Non-conformities and corrective actions e. Monitoring and measurement f. Audit results g. Fulfillment of objectives h. Feedback from interested parties i. Results of risk assessments and treatment plans j. Opportunities for continuous improvement.	ok	**Confirm**		
10	**Improvements**				
10,1	**Nonconformity and corrective actions(Verify Documented Information on non conformance& corrective action)**				

	a) Has the Organization reacted to nonconformities, evaluated the need for actions and implemented actions? b) Does the documented procedures for corrective actions define requirements for: i. Identifying non-conformities ii. Determining the causes of non-conformities iii. Evaluating the need for actions to ensure that non-conformities do not recur iv. Determining and implementing the corrective action needed v. Recording results of action taken and Reviewing of corrective action taken	ok	**Confirm**		
10,2	**Continual improvement**				
	Does the Organization continually improve the effectiveness of the ISMS through the use of the: * Information security policy & objectives * Audit results & analysis of monitored events * Corrective & preventive actions * Management review?	ok	**Confirm**		
*	**Details of Vulnerability / Penetration Testing**			OK	
*	**Details of Cryptographic Controls & Key Management for Cryptographic Controls**			OK	

Findings of the Stage 2 Audit:

Sl	Findings	Clause	Response of the client
1			
2			
3			
4			
5			

Summary of the Audit Team:

A. Stage of Audit: (Mark which is applicable)

Initial Certification	
Follow Up Audit	
Surveillance	yes
Modification	
Renewal	
Upgrade From	
Other	

B. Recommendation: (Mark which is applicable)

Issuance of Certificate	yes
Refusal of the Certificate	
Follow Up audit	
Modification of the current certificate (registration no. and expiration date remain unchanged)	
Other:	

C. Reason: (Mark which is applicable)

ISMS complies with the requirements of the Reference Standard. Congratulations, on the basis of the above summary, Lead Auditor is pleased to put forward a Recommendation for Issuance of Certificate.	yes
The information system complies with the requirements of the reference standard with exception of minor NC: Congratulations, Lead Auditor is pleased to put forward a recommendation for Certification upon off-site verification of closure of all issues, the NC closure need to be submitted along with the Corrective Action Plan and objective evidence with 15 days from the stage 2 audit but not later than60 days from the date of Stage 2 audit. If all non-conformances are not closed within 60 days, a full reassessment may be required.	
Evidence of major non conformities: Organization is not recommended for Certification. A follow-up assessment will be scheduled to allow for on-site verification and closure of all issues within 60 days from the date of Stage 2 audit. If all non-conformances are not closed within 60 days, a full reassessment may be required.	
Not Recommended: Organization is not recommended for certification, a Stage 2 audit will be required. To progress your application for registration, please respond to each non-conformances, with a plan showing proposed actions, timescales and responsibilities for resolution. The organization should consider the root cause of the non-conformance and the potential for related issues in other parts of your system.	

Condition of the Audit Report:

A	This is to state that this audit report or any information in this report is based on a sampling process of the available information to the certification body. Further to advise that audit recommendations are subject to an independent review prior to a decision concerning the awarding or renewal of certification.
B	This is to state that the audited organization is effectively controlling the use of the certification documents and marks if applicable.
C	This report itself does not allow the client / applicants to use logo of the certification body or accreditation board, use of logo govern as per certification body rule. Please refer the terms of use of logo as available on the website of the certification body.

For Behalf of TNV:		**For and on behalf of the Client:**	
Auditor:	Giuseppe Izzo	Name:	Malena Moreira
Date:	19/01/2026	Date:	19/01/2026

Confirm

Non-Conformity
Observation