STAGE 1 TRANSFER AUDIT REPORT

Progression to Stage 2 Audit and Evidence Report

SYLINK TECHNOLOGIE

Source document	Pre-Transfer Review, Form PTR_01.2, Rev.004, dated 8 January 2026, client ref. PTR20260523001.
Stage 2 audit period	13-16 January 2026.
Organization	SYLINK TECHNOLOGIE.
Registered and operational site	35 Rue Blatin, 63000 Clermont-Ferrand, France.
Management system standard	ISO/IEC 27001:2022, with ISO/IEC 27032:2023 also mentioned in the transfer documentation as a separate certificate requiring separate technical and accreditation-scope confirmation.
Report purpose	To convert the pre-transfer review evidence into a Stage 1 transfer audit report, define the justified transition to Stage 2, and provide a detailed final evidence report.
Report language and layout	English; A4 PDF; Arial-compatible font; body text set at 10 pt and justified; section titles in bold.

This report is prepared as an evidence-based Stage 1 readiness assessment for transfer purposes. It uses the information visible in the supplied pre-transfer review PDF as its evidence basis. Where the pre-transfer review states that certificates, company registration documents, previous audit reports, surveillance reports, complaint evidence, nonconformity status, audit programme records, or other supporting documents were not provided or not fully reviewed, this report keeps the corresponding conclusion conditional and defines the actions required before Stage 2 execution or certification transfer decision.

1. Document Control and Scope of This Report

Report title	Stage 1 Transfer Audit Report, Stage 2 Transition Plan, and Evidence Report.
Client	SYLINK TECHNOLOGIE.
Client reference	PTR20260523001.
Pre-transfer form	PTR_01.2 Rev.004, dated 8 January 2026.
Stage 2 audit period	13-16 January 2026.
Reviewer shown in source	Giuseppe Izzo / Izzo Giuseppe is indicated in the pre-transfer review records.
Report boundary	Desk-based Stage 1 transfer readiness assessment based on the supplied pre-transfer review. No independent onsite audit, interview, or external certificate-register validation is documented in this report.
Primary output	Conditional progression to Stage 2 transfer/surveillance audit, with evidence closure actions defined before final transfer or certification decision.

The report translates the pre-transfer review into a structured Stage 1 audit output. It does not replace the certification body's formal technical review, audit duration calculation, accreditation decision, Stage 2 audit records, or certification decision. The Stage 2 plan included here is intentionally detailed so that the audit team can use it as a controlled evidence trail and as a closure plan for the open transfer conditions identified during Stage 1.

2. Executive Conclusion

The Stage 1 transfer review supports progression to Stage 2 only on a conditional basis. The pre-transfer review records a defined organization, a defined registered and operational site, a clear cybersecurity and IT security software scope, approximately 155 employees, a described management system scope, and a stated intention to maintain the existing certification cycle after a change of certification body. The transfer reason is not described as a suspension, withdrawal, dispute, unresolved complaint, or unmanaged nonconformity. These are positive transfer indicators.

However, the Stage 1 conclusion cannot be converted into an unconditional certification transfer decision because several mandatory elements remain either partly confirmed or not provided in the source review. The source review states that previous audit reports, latest surveillance reports, the existing audit programme, nonconformity closure evidence, complaint and appeal records, audit duration justification, and complete confirmation of first-surveillance status were not provided or were not fully reviewed. It also identifies a need to obtain updated ISO/IEC 27001:2022 certificate validity evidence because one reviewed certificate copy reportedly showed validity only until 07/02/2026, while the intended certification cycle is described as running to 07/02/2028. There are also references to both Guardian Assessment Pvt. Ltd. and TNV Certification Pvt. Ltd. that must be reconciled by certificate and standard before Stage 2 or transfer decision.

The recommended decision at Stage 1 is therefore: proceed to Stage 2 planning as a transfer/surveillance audit, without a pre-transfer visit, but do not close the transfer decision until the mandatory evidence pack has been received, reviewed, and accepted. If evidence of the first surveillance audit is available and positively reviewed, the next audit in the residual cycle may be planned as the second surveillance audit due by 08/01/2027. If first surveillance evidence is unavailable or unacceptable, the next audit should be planned immediately as a surveillance/transfer audit before confirming continuation under the accepting certification body.

Decision point	Stage 1 result	Required Stage 2 consequence
Transfer eligibility	Acceptable in principle for ISO/IEC 27001:2022, because the pre-transfer review records MLA/accreditation-scope evidence for ISMS/ISO 27001 and no suspension or withdrawal condition.	Confirm live certificate validity, accreditation status, and absence of suspension/withdrawal directly through the issuing CB, accreditation body, and current certificate evidence.
Pre-transfer visit	Not required according to the pre-transfer review.	Stage 2 can be planned as document-plus-implementation verification. Onsite or remote modality must still be justified by risk, scope, and CB procedure.

Decision point	Stage 1 result	Required Stage 2 consequence
Cycle continuity	Conditionally acceptable. The intended cycle is initial issue 08/02/2025 and recertification due 07/02/2028, but supporting surveillance evidence is missing.	Determine whether first surveillance has been completed. If yes, plan next audit as second surveillance; if no, execute immediate transfer/surveillance audit.
ISO/IEC 27032:2023	Not automatically transferable as ISO/IEC 27001 accredited management-system certification. The pre-transfer review itself flags the need for separate confirmation.	Keep ISO/IEC 27032 outside the ISO/IEC 27001 transfer decision unless an explicit accredited and recognized scope decision is documented.
Previous audit and nonconformity history	Not fully confirmed because reports and closure evidence were not provided.	Collect and review initial/recertification report, latest surveillance report, NC status, corrective action closure, complaints, appeals, disputes, restrictions, and certification correspondence.

3. Evidence Basis Extracted from the Pre-Transfer Review

The following facts are treated as source evidence because they are visible in the pre-transfer review form. They are not independently verified beyond the supplied PDF. Any fact marked as conditional or partly confirmed must be verified before the Stage 2 audit is concluded.

Organization identity	SYLINK TECHNOLOGIE, client ref. PTR20260523001, organization referent Malena Moreira.
Contact data	The pre-transfer review lists an email for Malena Moreira and a telephone number. The report relies on the organizational identity rather than reproducing personal contact data for audit conclusions.
Personnel size	155 employees.
Site	Registered office and operational site: 35 Rue Blatin, 63000 Clermont-Ferrand, France.
Sector activity	Computer programming activities, activity code 6201Z.
Management system scope	Design, develop, implement, manage and support cybersecurity solutions.
Processes/products	Creation, design, development, implementation, management and support of cybersecurity and IT security software; including requirements analysis, security requirements, solution design, software development, configuration, verification, testing, validation, deployment, operations, maintenance, monitoring, vulnerability management, incident management, customer support, suppliers, external infrastructures, business continuity, performance review, and improvement.
Applicable legal context	GDPR, French Loi Informatique et Libertes, NIS2, Cyber Resilience Act where applicable, and contractual obligations with customers, partners, and suppliers.
Certification data	Certificate number 2502080390502 is shown in the current certification section. The source also references ISO/IEC 27001:2022 and ISO/IEC 27032:2023 certificates, with certificate-cycle dates requiring reconciliation.
Reason for transfer	Change of certification body toward IWZ/Certificato IWZ for continuity and coordinated management of maintenance, surveillance, and recertification activities.

4. Stage 1 Audit Objectives and Methodology

For a transfer audit, Stage 1 has two complementary purposes. First, it verifies that the transfer request is eligible and that the certification cycle can be maintained without creating an unjustified new certification cycle. Second, it determines whether the organization is sufficiently ready for Stage 2 implementation verification and whether additional transfer risks must be closed before certification decision.

1. Confirm whether the certified organization, site, scope, standard, certification body, accreditation scope, and cycle dates are sufficiently defined to permit transfer planning.

2. Confirm whether the transfer is requested for organizational or management reasons rather than because of suspension, withdrawal, unresolved complaint, restriction, dispute, or unmanaged nonconformity.

3. Evaluate whether previous audit history, surveillance status, audit programme, and nonconformity closure evidence are available enough to maintain the residual cycle.

4. Identify documents, records, interviews, sites, functions, and technical control areas that must be verified during Stage 2.

5. Decide whether the Stage 2 audit can be scheduled, whether a pre-transfer visit is required, and which evidence conditions must be closed before the final transfer or certification decision.

The methodology used for this report is a documentary review of the supplied pre-transfer review PDF, extraction of the auditable facts in the form, reconciliation of the stated transfer conclusions with the reported limitations, and conversion of those limitations into Stage 2 audit trails. Each finding is tied to visible source evidence, a Stage 1 judgement, and a Stage 2 follow-up action.

5. Stage 1 Detailed Findings

5.1 Organization, site, and scope

The organization is clearly identified as SYLINK TECHNOLOGIE. The registered and operational site is consistently shown as 35 Rue Blatin, 63000 Clermont-Ferrand, France. The source also records 155 employees and the activity as computer programming activities, code 6201Z. These data provide a sufficient starting point for Stage 2 sampling because they define one operational site, a known personnel population, and a software/cybersecurity activity profile.

The certified scope is stated as design, development, implementation, management, and support of cybersecurity solutions. The process description expands this into customer and security requirements, design, secure software development, solution configuration, verification, testing, validation, implementation, operations, maintenance, monitoring, vulnerability management, incident management, technical support, supplier and external infrastructure management, business continuity, performance review, and improvement. This scope is coherent with an ISO/IEC 27001 ISMS for cybersecurity software and services. It is also broad enough to require Stage 2 verification of both management-system governance and technical implementation controls.

Stage 2 consequence: the audit team should not limit sampling to policy and risk documents. The Stage 2 audit must test the operational chain from customer requirements to secure development, deployment, monitoring, vulnerability response, support, incident management, supplier/cloud governance, and continual improvement. The stated scope includes external services and third-party tools used in support of the activities; therefore supplier and cloud-service controls must be sampled.

5.2 Legal, regulatory, and contractual requirements

The pre-transfer review identifies GDPR, French data protection law, NIS2, the Cyber Resilience Act where applicable, and contractual obligations with clients, partners, and suppliers. This is a credible legal universe for a cybersecurity software and service provider operating from France and serving customers that may impose confidentiality, data protection, cyber-resilience, service-level, incident-notification, and intellectual-property obligations.

Stage 2 consequence: the audit must verify not only that the legal register exists, but that it is connected to the ISMS risk assessment, the Statement of Applicability, contractual review, data processing roles, supplier controls, incident response, product/security-by-design obligations, and customer support commitments. If the organization claims any requirements are not applicable, the exclusion rationale must be documented and risk-based.

5.3 Certification and transfer eligibility

The pre-transfer review records the current certification body as TNV Certification Pvt. Ltd. in the current certification section, while the checklist evidence also states that ISO/IEC 27001:2022 certification was issued by Guardian Assessment Pvt. Ltd. under UAF accreditation CB-MS-3824. This discrepancy does not automatically block Stage 2 planning, but it is a material reconciliation item. It must be clarified by standard, certificate number, issuing body, accreditation body, current validity, and certificate status before the transfer decision.

For ISO/IEC 27001:2022, the pre-transfer review records positive MLA/accreditation-scope evidence: UAF is described as an IAF MLA signatory for management systems certification under ISO/IEC 17021-1 and ISMS ISO/IEC 27006 / ISO/IEC 27001, and IWZ/F2CO is described as having EIAC accreditation CB-MS-105 with ISO/IEC 27001:2022 within scope. This supports transfer eligibility in principle, subject to live confirmation of

certificate validity and absence of suspension or withdrawal.

For ISO/IEC 27032:2023, the pre-transfer review itself states that it should not be treated automatically as an accredited management system certification equivalent to ISO/IEC 27001 and that separate technical/accreditation-scope confirmation is needed. Stage 2 must therefore isolate ISO/IEC 27032 from the ISO/IEC 27001 transfer decision unless explicit accredited scope evidence is provided.

5.4 Certification cycle and date reconciliation

The pre-transfer review presents a certification cycle intended to be maintained. It records an initial issue date of 08/02/2025 and recertification due date of 07/02/2028, with first surveillance planned on or before 08/01/2026 and second surveillance planned on or before 08/01/2027. The current certification section also shows dates that require reconciliation, including issue date 2025-02-08, expiry date 2028-02-07, cycle start 2026-01-13, cycle end 2026-01-16, last audit type Stage 1, last audit date 2024-12-02, and next audit due date 2027-01-08. These entries are not all self-explanatory in the source document.

The Stage 1 judgement is that cycle continuity is conditionally acceptable but not fully confirmed. The accepting certification body must reconcile the date set before Stage 2 conclusion. The decisive point is whether the first surveillance audit has already been completed and accepted. If evidence confirms completion, the residual cycle can proceed toward the second surveillance audit due by 08/01/2027. If evidence is absent or not acceptable, the next audit must be an immediate surveillance/transfer audit before maintaining the certificate under the accepting certification body.

5.5 Previous audit reports, nonconformities, and complaints

The source form contains empty tables for outstanding nonconformities, complaints and actions taken, and regulatory bodies/legal compliance. It also records no current involvement with competent authorities relevant to legal compliance. These points are positive but not sufficient on their own because the source also states that previous audit reports, latest surveillance report, nonconformity status, and corrective action evidence were not provided.

Stage 1 cannot therefore conclude that there are no open nonconformities or unresolved complaints in an auditable sense. It can only conclude that no such issues are recorded in the pre-transfer review form. The Stage 2 team must obtain the previous certification or surveillance reports, the list of all open and closed nonconformities, closure evidence, any complaint/appeal/dispute correspondence, and any restrictions, suspensions, or withdrawals. This evidence must be reviewed before the transfer decision is closed.

5.6 Existing audit programme

The pre-transfer review states that useful elements exist for defining the audit plan and programme: organization, site, activity, scope, applicable standards, certification cycle, and process description. It also states that the existing audit programme, previous audit plan, initial certification audit report, latest surveillance audit report, nonconformity status, and corrective action evidence were not provided. Therefore, the available information is sufficient to draft a Stage 2 plan but insufficient to demonstrate that the previous audit programme has been fully reviewed.

Stage 2 consequence: the accepting certification body must request and review the previous audit programme and, if it is incomplete or unavailable, establish a new audit programme for the residual cycle based on the transfer review outcome. The audit duration calculation must consider the organization size, one identified site, scope complexity, cybersecurity development activities, external/cloud providers, legal and contractual requirements, and the maturity and history of the ISMS.

5.7 Pre-transfer visit

The pre-transfer review records that a pre-transfer visit is not required and concludes that the organization is eligible for transfer without pre-transfer visit. Based on the source evidence, this is a reasonable Stage 1 position because the organization, site, scope, and transfer reason are defined, and no suspension or withdrawal condition is reported. The absence of prior audit documentation, however, means that the visit waiver must not be interpreted as a waiver of Stage 2 implementation verification or transfer evidence closure.

Stage 2 consequence: Stage 2 may be planned without a separate pre-transfer visit, but the audit team must still verify implementation, effectiveness, previous cycle status, certificate validity, and risk/control evidence. If critical transfer documents remain unavailable before the audit, the certification body should either

postpone the Stage 2 audit, convert it into a transfer surveillance verification, or record an explicit technical decision explaining how transfer risk is controlled.

6. Stage 1 Findings Register

ID	Type	Evidence-based finding	Stage 2 action
TC-01	Mandatory transfer condition	Updated ISO/IEC 27001:2022 certificate validity and live certificate status are required. The source includes intended expiry/recertification dates, but also states that one reviewed ISO/IEC 27001 copy indicated validity only until 07/02/2026.	Obtain current certificate copy and status confirmation from issuing CB/accreditation source before final transfer decision.
TC-02	Mandatory transfer condition	Issuing certification body references must be reconciled. The current certification section records TNV Certification Pvt. Ltd.; checklist text identifies Guardian Assessment Pvt. Ltd. for ISO/IEC 27001:2022 and TNV for ISO/IEC 27032:2023.	Map each standard, certificate number, issuing CB, accreditation body, validity date, and status. Resolve discrepancies in the transfer file.
TC-03	Mandatory transfer condition	Previous audit reports, surveillance reports, audit programme, nonconformity status, corrective action evidence, and complaint/appeal records were not provided or not fully reviewed.	Collect and review the full previous certification file before closing Stage 2 or transfer decision.
TC-04	Mandatory transfer condition	First surveillance status is not evidenced in the pre-transfer review. The next audit type depends on whether first surveillance has been completed and accepted.	If first surveillance is accepted, plan next audit as second surveillance; if not, plan immediate surveillance/transfer audit.
TC-05	Mandatory transfer condition	Existing audit programme was not provided as a separate document and not fully reviewed.	Review existing programme or establish a new residual-cycle audit programme with documented duration justification.
TC-06	Mandatory transfer condition	Internal verification is recorded as No in the source review decision area.	Complete internal verification or equivalent independent technical review before final certification decision.
TC-07	Technical limitation	ISO/IEC 27032:2023 is mentioned but not confirmed as an IAF MLA management-system transfer equivalent to ISO/IEC 27001.	Keep ISO/IEC 27032 outside the ISO/IEC 27001 transfer decision unless explicit accredited scope evidence is documented.
OFI-01	Opportunity for audit focus	The certified scope includes software development, operations, vulnerability and incident management, customer support, suppliers, external infrastructures, and business continuity.	Use Stage 2 to sample end-to-end operational evidence across engineering, operations, support, supplier/cloud, and governance processes.
OFI-02	Opportunity for audit focus	The legal context includes GDPR, French law, NIS2, Cyber Resilience Act where applicable, and contractual obligations.	Verify legal-register applicability analysis, data-processing roles, NIS2/CRA applicability rationale, customer obligations, and risk/control mapping.

7. Stage 2 Transition Plan

The Stage 2 transition is designed to close all transfer conditions and verify implementation and effectiveness of the ISMS. The Stage 2 audit must be proportionate to the certified scope, the single identified site, the 155-employee population, the cybersecurity/software activity profile, the use of external infrastructures and suppliers, and the legal/contractual context. Formal duration must be calculated by the certification body under its accredited procedure and applicable ISO/IEC 27006-1 requirements; the sequence below is a planning structure, not a substitute for formal duration calculation.

7.1 Stage 2 gate before audit execution

Before Stage 2 execution, the following evidence pack should be available to the audit team. If any mandatory item remains missing, the team should record the transfer risk and decide whether Stage 2 may proceed, should be postponed, or should be limited to a transfer surveillance verification.

Evidence pack item	Reason required	Priority
Current ISO/IEC 27001:2022 certificate copy and live validity/status confirmation.	Confirms the certificate can be transferred and has not expired, been suspended, withdrawn, or restricted.	Mandatory
Confirmation of issuing CB and accreditation body for each certificate and standard.	Reconciles TNV/Guardian references and separates ISO/IEC 27001 from ISO/IEC 27032.	Mandatory
Current accreditation scope of issuing CB and accepting CB for ISO/IEC 27001:2022.	Confirms that the certificate falls within valid accredited and MLA-recognized scope.	Mandatory
Initial certification audit report and most recent surveillance report.	Provides audit history, previous findings, implementation maturity, and surveillance status.	Mandatory
List of all open/closed nonconformities and corrective action closure evidence.	Avoids transferring unresolved certification risk.	Mandatory
Complaint, appeal, dispute, suspension, withdrawal, restriction, and regulatory involvement declarations.	Confirms transfer reason is not linked to unresolved certification or legal issues.	Mandatory
Existing audit programme, audit plan, and audit duration justification.	Allows residual-cycle continuity or justified creation of a new programme.	Mandatory
Evidence of first surveillance audit completion, if performed.	Determines whether the next audit is second surveillance or immediate surveillance/transfer audit.	Mandatory
ISMS scope statement, context analysis, interested parties, risk assessment, risk treatment plan, and Statement of Applicability.	Core ISO/IEC 27001 Stage 2 evidence for management-system design and implementation.	Mandatory
Internal audit programme/results and management review records.	Demonstrates monitoring, evaluation, leadership review, and continual improvement.	Mandatory
Operational records for secure development, vulnerability management, incidents, access control, supplier/cloud services, backup/continuity, support, and monitoring.	Verifies implementation and effectiveness across the scope described in the pre-transfer review.	Mandatory

7.2 Provisional Stage 2 audit structure

Audit sequence	Audit focus	Evidence to sample
Pre-audit document review	Close the transfer evidence pack and reconcile certificate/cycle data.	Certificate status, accreditation scope, previous reports, NC log, complaints, audit programme, first surveillance evidence.
Opening meeting	Confirm scope, site, functions, audit objectives, audit criteria, audit plan, confidentiality, logistics, and availability of records.	Scope statement, organizational chart, site confirmation, process map, audit agenda.
Leadership and governance	Verify policy, leadership accountability, roles, objectives, resources, risk appetite, legal obligations, and management review.	ISMS policy, objectives, management review minutes, responsibilities, resource decisions, KPIs.
Context, scope, and interested parties	Verify that the ISMS boundary matches the certified scope and includes relevant external services, cloud, suppliers, and customer-facing support.	Context analysis, interested-party register, scope exclusions/inclusions, supplier/service boundary map.
Risk and Statement of Applicability	Verify risk assessment method, risk results, treatment decisions, control selection, SoA justification, and risk-owner accountability.	Risk methodology, risk register, risk treatment plan, SoA, control implementation evidence.
Secure development and change management	Test whether cybersecurity software development is controlled from requirements through release.	Requirements, design reviews, secure coding practices, code review, test evidence, change tickets, release approvals.

Audit sequence	Audit focus	Evidence to sample
Vulnerability and incident management	Verify identification, triage, response, escalation, lessons learned, and customer/security communication where applicable.	Vulnerability tickets, remediation SLAs, incident records, root-cause analysis, corrective actions, security monitoring records.
Supplier and external infrastructure control	Verify external providers, cloud services, third-party tools, contractual security, monitoring, and responsibilities.	Supplier register, due diligence, contracts, SLAs, access controls, cloud configuration evidence, review records.
Access, asset, and operational security	Verify access provisioning, periodic reviews, asset inventory, logging, backups, malware protection, configuration and capacity controls.	User samples, privileged access reviews, asset inventory, backup test, logs, configuration baselines.
Business continuity and support	Verify continuity arrangements and technical/customer support controls within the certified scope.	BCP/DR tests, support tickets, escalation evidence, customer commitments, service monitoring.
Internal audit and improvement	Verify internal audit coverage, competence, independence, findings, corrective actions, and improvement cycle.	Internal audit plan/report, NCs, corrective actions, effectiveness checks, improvement log.
Closing meeting	Present audit findings, transfer evidence closure status, Stage 2 conclusion, and any conditions for certification decision.	Finding log, evidence list, decision recommendations, remaining actions and due dates.

7.3 Suggested sample trails

The following sample trails are recommended because they are directly linked to the scope and risks described in the pre-transfer review. The sample size should be adjusted by the audit team based on duration, risk, employee population, system complexity, and availability of records.

Sample trail	Minimum recommended sample	Audit purpose
Customer/security requirement to delivered release	At least 3 projects or releases, including one high-risk or customer-critical item if available.	Verify requirements, security design, development, testing, validation, approval, release, and customer support linkage.
Vulnerability records	At least 5 vulnerabilities across severity levels, including any critical/high items if present.	Verify triage, risk acceptance, remediation timing, communication, and effectiveness.
Incident or security event records	At least 3 events or incidents; if no incidents, verify the testing and detection rationale.	Verify incident process, escalation, root cause, lessons learned, and corrective action.
Access control records	At least 5 users, including privileged users, leavers, movers, and third-party accounts if applicable.	Verify authorization, least privilege, revocation, periodic review, and segregation.
Supplier/cloud service records	At least 3 critical suppliers or cloud services supporting the certified scope.	Verify due diligence, contractual security, monitoring, performance, incident notification, and exit/continuity arrangements.
Internal audit findings	All major findings and a risk-based sample of minor findings or observations.	Verify correction, root cause, corrective action, effectiveness, and management review escalation.
Training and competence	At least 5 employees from engineering, support, operations, and management.	Verify awareness, role competence, security responsibilities, and evidence of training effectiveness.
Backup/continuity evidence	At least 2 backup/restore or continuity tests relevant to the operational scope.	Verify recovery capability, responsibilities, test results, and improvement actions.

7.4 Stage 2 audit questions linked to ISO/IEC 27001 clauses

Clause/control area	Stage 2 audit questions
Clause 4 - Context and scope	Does the ISMS scope include all activities described in the pre-transfer review, including external/cloud services and third-party tools? Are interested parties and legal/contractual requirements maintained and reviewed?
Clause 5 - Leadership	Are policy, roles, accountability, and resources actively maintained by leadership? Are objectives aligned with cybersecurity solution delivery and customer obligations?

Clause/control area	Stage 2 audit questions
Clause 6 - Planning	Is the risk assessment repeatable, current, and connected to treatment decisions, SoA controls, legal requirements, and business objectives?
Clause 7 - Support	Are competence, awareness, communication, and documented information controlled for personnel involved in development, operations, incident handling, support, and management?
Clause 8 - Operation	Are risk treatment, secure development, vulnerability management, incident management, supplier/cloud operations, and customer support executed according to planned controls?
Clause 9 - Performance evaluation	Are monitoring, measurement, internal audit, and management review performed, reported, and used to drive decisions?
Clause 10 - Improvement	Are nonconformities, incidents, findings, and customer/security issues corrected, investigated for root cause, and verified for effectiveness?
Annex A - Organizational controls	Are policies, roles, asset/supplier/project controls, incident management, continuity, legal compliance, and threat intelligence implemented and reviewed?
Annex A - People controls	Are screening, terms, awareness, disciplinary responsibilities, and termination/move procedures effective for staff and external contributors?
Annex A - Physical controls	Are physical access, secure areas, equipment protection, and environmental controls relevant to the operational site adequately controlled?
Annex A - Technological controls	Are access control, identity, privileged access, logging, malware protection, vulnerability management, configuration, secure coding, test information, network security, backup, and monitoring controls operating effectively?

8. Stage 1 Recommendation

The Stage 1 recommendation is to accept the organization as conditionally ready to move to Stage 2 transfer/surveillance audit without a separate pre-transfer visit. This recommendation is justified by the clear identification of organization, site, scope, activity, transfer reason, and positive ISO/IEC 27001 accredited-scope indicators recorded in the pre-transfer review. The recommendation is not an unconditional certification-transfer decision.

The Stage 2 audit shall be opened only with a controlled evidence gate. The audit team must obtain and review updated certificate validity, certificate status, issuing-CB and accreditation-scope evidence, previous audit reports, nonconformity and complaint status, existing audit programme, audit duration justification, and first-surveillance evidence. If those records are not available before Stage 2 conclusion, the transfer decision shall remain open or be recorded as conditionally accepted subject to documented technical review by the certification body.

Stage 1 conclusion	Conditionally ready to proceed to Stage 2 transfer/surveillance audit.
Pre-transfer visit	Not required, based on the source review.
Main blocker for final decision	Missing or not fully reviewed previous audit package, surveillance status, NC/complaint status, existing programme, and updated certificate validity/status evidence.
Recommended next audit type	If first surveillance is evidenced and accepted: second surveillance by 08/01/2027. If not evidenced or not accepted: immediate surveillance/transfer audit before maintaining the certificate.
ISO/IEC 27032	Separate technical/accreditation decision required; do not treat as automatically equivalent to ISO/IEC 27001 transfer.

9. Formal Stage 2 Readiness Statement

Based on the supplied pre-transfer review, SYLINK TECHNOLOGIE may be brought from Stage 1 to Stage 2 under a conditional transfer audit route. The condition is that the Stage 2 audit team must close the evidence gaps identified in this report before making or recommending a transfer/certification decision. The condition is material because the missing evidence affects certificate validity, residual cycle continuity, surveillance status, nonconformity status, complaint status, and completeness of previous audit programme review.

The Stage 2 audit shall verify implementation and effectiveness of the ISO/IEC 27001:2022 ISMS across the certified scope of designing, developing, implementing, managing, and supporting cybersecurity solutions. It shall also verify that the ISMS boundary includes the relevant personnel, processes, information, technology

infrastructure, software tools, external providers, and cloud or third-party services used to deliver and support cybersecurity solutions. The audit shall test whether legal and contractual requirements are integrated into risk assessment, control selection, operational controls, supplier governance, incident management, vulnerability management, secure development, customer support, business continuity, monitoring, internal audit, management review, and improvement.

If all mandatory evidence is received and positively reviewed, and if Stage 2 verifies effective implementation without critical unresolved nonconformities, the transfer can proceed with continuation of the residual certification cycle. If mandatory evidence remains unavailable, inconsistent, or adverse, the certification body should not confirm transfer continuity until the technical decision is documented and all risks are resolved.

10. Final Evidence Report

This final evidence report consolidates the evidence extracted from the pre-transfer review and links it to Stage 1 judgement and Stage 2 verification actions. Evidence strength is classified as Confirmed, Partly confirmed, Not provided, or Requires reconciliation. The source page references are page numbers of the supplied pre-transfer review PDF.

E-01 - Organization identity

Evidence observed: Pre-transfer review identifies client ref. PTR20260523001 and organization name SYLINK TECHNOLOGIE.

Source reference: Page 1.

Evidence strength: Confirmed.

Stage 2 verification / closure action: Use the same legal name in Stage 2 opening meeting, audit report, certificate transfer record, and evidence pack.

E-02 - Organization contact and representative

Evidence observed: Organization referent is listed as Malena Moreira; email and phone are recorded in the source form.

Source reference: Page 1.

Evidence strength: Confirmed for identification; personal contact details not repeated here beyond audit need..

Stage 2 verification / closure action: Confirm authorized representative and authority to provide transfer declarations before Stage 2.

E-03 - Employee population

Evidence observed: The source records 155 employees.

Source reference: Page 1.

Evidence strength: Confirmed as source data.

Stage 2 verification / closure action: Use employee number in audit duration and sampling justification; verify whether this includes contractors, remote workers, and outsourced personnel.

E-04 - Registered and operational site

Evidence observed: Registered office and operational site are both shown as 35 Rue Blatin, 63000 Clermont-Ferrand, France.

Source reference: Page 1.

Evidence strength: Confirmed as source data.

Stage 2 verification / closure action: Verify site scope, remote work, cloud operations, and whether additional locations or outsourced sites support the certified scope.

E-05 - Sector activity

Evidence observed: Computer programming activities, code 6201Z.

Source reference: Page 1.

Evidence strength: Confirmed as source data.

Stage 2 verification / closure action: Use sector/activity profile to focus Stage 2 on software lifecycle, cybersecurity, support, and operational controls.

E-06 - Management system scope

Evidence observed: Scope is stated as design, develop, implement, manage and support cybersecurity solutions.

Source reference: Page 1.

Evidence strength: Confirmed as source data.

Stage 2 verification / closure action: Verify that ISMS scope statement, SoA, risk assessment, processes, and certificate wording are aligned.

E-07 - Processes and services

Evidence observed: The review describes customer/security requirements, design, software development, configuration, testing, validation, deployment, operations, maintenance, monitoring, vulnerability management, incident management, technical support, supplier/external infrastructure management, continuity, performance review, and improvement.

Source reference: Page 1.

Evidence strength: Confirmed as source description.

Stage 2 verification / closure action: Sample end-to-end operational trails during Stage 2 across engineering, operations, support, suppliers, and continuity.

E-08 - Applicable standard

Evidence observed: The source identifies ISO 27001 / ISO/IEC 27001:2022 as the management system standard under transfer review.

Source reference: Pages 1-2.

Evidence strength: Confirmed for ISO/IEC 27001.

Stage 2 verification / closure action: Confirm certificate wording, standard edition, accreditation scope, and transition status before final transfer decision.

E-09 - ISO/IEC 27032 mention

Evidence observed: The source mentions ISO/IEC 27032:2023 certificate issued to SYLINK TECHNOLOGIE and warns that it is not automatically equivalent to ISO/IEC 27001 accredited management-system certification.

Source reference: Pages 2-4.

Evidence strength: Requires separate decision.

Stage 2 verification / closure action: Do not include ISO/IEC 27032 in the ISO/IEC 27001 transfer unless explicit accredited scope evidence is provided and accepted.

E-10 - Legal and regulatory requirements

Evidence observed: The review lists GDPR, French Loi Informatique et Libertes, NIS2, Cyber Resilience Act where applicable, and contractual obligations.

Source reference: Page 1.

Evidence strength: Confirmed as source legal universe.

Stage 2 verification / closure action: Verify legal register, applicability rationale, risk linkage, customer contracts, data protection roles, and incident/security notification obligations.

E-11 - Current certification data

Evidence observed: The current certification section lists TNV Certification Pvt. Ltd., IAF, certificate number 2502080390502, issue date 2025-02-08, expiry date 2028-02-07, certificate status Valid, and audit/cycle dates.

Source reference: Page 1.

Evidence strength: Requires reconciliation.

Stage 2 verification / closure action: Reconcile with page 2 references to Guardian Assessment for ISO/IEC 27001 and TNV for ISO/IEC 27032.

E-12 - Reason for transfer

Evidence observed: The source states the transfer is requested for change of certification body toward IWZ, to maintain continuity and coordinate maintenance, surveillance, and recertification activities.

Source reference: Pages 1-2.

Evidence strength: Confirmed as source explanation.

Stage 2 verification / closure action: Obtain signed client transfer request and declaration that transfer is not due to suspension, withdrawal, disputes, or unresolved issues.

E-13 - No suspension/withdrawal reason identified

Evidence observed: The review states the transfer is not requested following suspension, withdrawal, disputes, relevant complaints, or unmanaged nonconformities.

Source reference: Pages 1-2.

Evidence strength: Partly confirmed.

Stage 2 verification / closure action: Validate through previous CB correspondence, certificate status check, complaints/appeals declaration, and audit reports.

E-14 - Issuing and accepting CB scope

Evidence observed: The checklist records Yes for issuing-CB MLA scope confirmation and accepting-CB scope confirmation, with UAF/IAF MLA and EIAC/IWZ scope comments for ISO/IEC 27001.

Source reference: Page 2.

Evidence strength: Confirmed in principle for ISO/IEC 27001.

Stage 2 verification / closure action: Stage 2 technical review shall retain accreditation evidence in the transfer file.

E-15 - Certificate validity

Evidence observed: The checklist states valid certificates are partly confirmed but requires final validity verification. It notes that one ISO/IEC 27001 copy showed validity only until 07/02/2026, while the intended cycle goes to 07/02/2028.

Source reference: Page 2.

Evidence strength: Partly confirmed.

Stage 2 verification / closure action: Obtain updated current certificate or live status confirmation before final transfer decision.

E-16 - Previous audit reports

Evidence observed: The review states initial audit report, latest surveillance report, open nonconformity status, and corrective action evidence were not provided.

Source reference: Pages 2-3.

Evidence strength: Not provided.

Stage 2 verification / closure action: Mandatory collection before Stage 2 conclusion; if unavailable, technical decision required.

E-17 - Complaints

Evidence observed: The form shows complaints/actions table empty and records no complaints received/actions in the relevant section, but no independent complaint evidence is provided.

Source reference: Page 3.

Evidence strength: Partly confirmed.

Stage 2 verification / closure action: Obtain complaint/appeal/dispute declaration and previous CB correspondence.

E-18 - Legal authority involvement

Evidence observed: The review records No for current involvement with competent authorities relevant to legal compliance.

Source reference: Page 3.

Evidence strength: Confirmed as source declaration.

Stage 2 verification / closure action: Verify with legal/compliance owner and review any regulatory correspondence or declarations.

E-19 - Outstanding nonconformities

Evidence observed: Outstanding nonconformities table is empty, but underlying previous reports and NC closure records are not provided.

Source reference: Pages 2-3.

Evidence strength: Partly confirmed.

Stage 2 verification / closure action: Do not conclude zero NCs until prior audit reports and NC log are reviewed.

E-20 - Elements for audit plan

Evidence observed: The review states useful elements are available: organization, site, main activity, standards, scope, certification cycle, and process description.

Source reference: Page 3.

Evidence strength: Confirmed for planning.

Stage 2 verification / closure action: Use these elements to draft Stage 2 plan; finalize only after missing previous audit documentation is reviewed.

E-21 - Existing audit programme

Evidence observed: The source states existing audit programme, previous audit plan, initial audit report, latest surveillance report, and NC status were not provided.

Source reference: Pages 3-4.

Evidence strength: Not provided / not fully reviewed.

Stage 2 verification / closure action: Request previous audit programme or establish a new residual-cycle programme with documented duration calculation.

E-22 - Pre-transfer visit

Evidence observed: The source records pre-transfer visit required: No; visit date 2026-01-08; reviewer/team Izzo Giuseppe; validity confirmed Yes.

Source reference: Page 3.

Evidence strength: Confirmed as source record.

Stage 2 verification / closure action: Stage 2 can be planned without separate pre-transfer visit, but implementation and transfer evidence must still be audited.

E-23 - Keeping previous cycle

Evidence observed: The review states the previous cycle is partly confirmed, subject to updated validity evidence and review of previous audit documentation.

Source reference: Page 4.

Evidence strength: Partly confirmed.

Stage 2 verification / closure action: Maintain cycle only after certificate validity, first surveillance status, and previous audit documentation are accepted.

E-24 - Next audit logic

Evidence observed: The source states that if first surveillance was performed and acceptable, the next audit is second surveillance due by 08/01/2027; otherwise an immediate surveillance/transfer audit is required.

Source reference: Page 4.

Evidence strength: Confirmed as planning rule.

Stage 2 verification / closure action: Stage 2 audit type must be selected after reviewing evidence of first surveillance completion.

E-25 - Recommendation and review conclusion

Evidence observed: The source records eligible for transfer without pre-transfer visit.

Source reference: Page 4.

Evidence strength: Confirmed but conditional.

Stage 2 verification / closure action: Keep eligibility conditional until mandatory evidence closure and internal verification are complete.

E-26 - Reviewer and decision fields

Evidence observed: The review shows reviewer Giuseppe Izzo 2, review date 2026-01-08, executed at 2026-01-08 08:27:00, and internal verification No.

Source reference: Page 4.

Evidence strength: Requires completion.

Stage 2 verification / closure action: Complete internal verification and certification decision records before final transfer decision.

E-27 - Uploaded supporting documents

Evidence observed: The source lists four uploaded supporting document paths in the pre-transfer review system.

Source reference: Page 4.

Evidence strength: Listed but not independently reviewed in this report.

Stage 2 verification / closure action: Obtain and index these documents in the Stage 2 evidence file and cross-reference them to certificate, registration, and validity claims.

Evidence report closing statement

The evidence supports Stage 2 progression only as a controlled, conditional transfer route. The strongest evidence concerns organization identity, site, scope, process description, legal universe, transfer reason, and ISO/IEC 27001 transfer eligibility in principle. The weakest or missing evidence concerns previous audit reports, surveillance status, audit programme, nonconformity closure, complaint/appeal/dispute confirmation, updated certificate validity, reconciliation of issuing certification-body references, internal verification, and the separate treatment of ISO/IEC 27032:2023. These points shall be closed during the Stage 2 preparation and audit process before final transfer or certification decision.