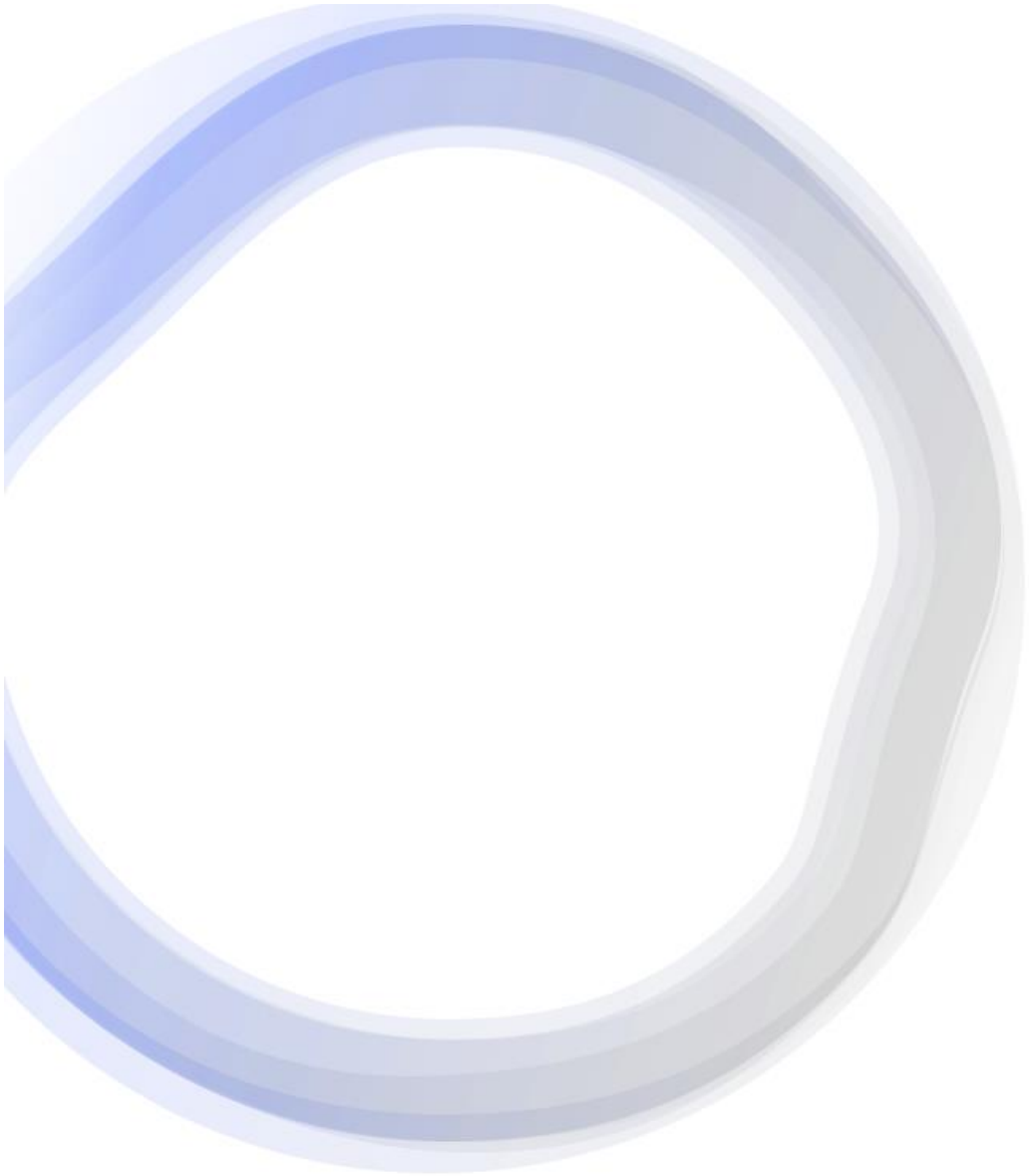
NORFINNA

Scope of Services Audit and Certification for ITAD Companies



NORFINNA
Finnish ISO certification organisation

Management systems for the secure and responsible collection, processing, and recycling of IT equipment

This scope of services describes the independent auditing and certification of management systems at companies in the IT Asset Disposition (ITAD) sector. The focus is on information security, traceable equipment flows, quality, environmental protection, and occupational health and safety.

NORFINNA assesses the effectiveness of management systems along the agreed-upon ITAD process chain. The scope and significance of a certification are determined by the applicable standard and the scope of application stated on the certificate.

Document Status

Version dated October 21, 2026
Approved by NORFINNA
Public

1 NORFINNA and Scope of Services

NORFINNA is a Finnish certification body specializing in the auditing of ITAD companies. Its services are aimed at organizations that collect, transport, inventory, erase, refurbish, resell, or send used IT equipment for material recycling.

1.1 Management system certifications

- ISO/IEC 27001 for information security management, particularly the protection of collected devices, data storage media, customer information, and documentation.
- ISO 9001 for quality management, specifically clear customer requirements, controlled processes, inventory reconciliation, and reliable reporting.
- ISO 14001 for environmental management, specifically reuse, waste streams, hazardous substances, and the oversight of recycling partners.
- ISO 45001 for occupational health and safety, specifically regarding storage, transportation, disassembly, machinery, and the handling of batteries.

The applicable version of the standard and any transitional provisions are specified in the offer and in the audit program. Integrated audits can assess multiple management systems simultaneously; the requirements and decisions remain traceable for each standard.

1.2 Accreditation and Scope of Services

According to the company information provided for this draft, “NORFINNA is currently in the process of becoming accredited by FINAS (Finnish Accreditation Service). Accredited certifications are offered and issued exclusively within the scope of the currently valid and published accreditation. The scope of services specifies which services are covered.

A management system certification confirms that the assessed management system complies with the specified standard. It is not a blanket certification of every device, every data erasure, or every individual ITAD service. Additional technical tests or industry-specific assessments require their own agreed-upon criteria and results.

1.3 Scope

Prior to accepting an engagement, legal entities, locations, activities, outsourced processes, and interfaces are identified. The scope distinguishes, for example, between in-house data erasure, external data carrier destruction, refurbishment, remarketing, and recycling. Activities that have not been audited must not be implied as covered by the wording of the certificate.

2 Impartiality and Confidentiality

2.1 Independent Assessment

Audit results and certification decisions are based on verifiable evidence. Economic interests, sales targets, or personal relationships must not influence the assessment. Risks to impartiality are assessed and documented prior to accepting the assignment and throughout the collaboration.

Audit teams are assigned based on their technical expertise and independence. Decisions regarding the granting, maintenance, extension, restriction, suspension, or revocation of a certification are made by authorized persons who were not involved in the audit in question.

2.2 Conflicts of Interest and Consulting

NORFINNA separates certification services from activities that could compromise its impartiality. Individuals with relevant consulting relationships or other conflicts of interest are not assigned to the certification tasks in question. The requirements of the respective certification system are decisive.

General training and explanations of standard requirements must not replace customer-specific development or implementation of the management system to be certified. A pre-audit serves to assess readiness for the audit and does not constitute a commitment to certification or an automatic shortening of the certification audit.

2.3 Confidential Information

Information from the application, audit, and certification is treated confidentially. This obligation applies to internal and external employees as well as other persons involved. Access is granted only to authorized persons to the extent necessary. Audits shall generally be conducted without access to live customer data on provided data storage media. Suitable materials include anonymized order documents, technical logs, metadata, and controlled demonstrations. If access to sensitive information is necessary, the purpose, authorization, and protective measures shall be defined in advance.

Any disclosure required by law or contract shall be made to the extent permitted. The affected organization will be informed of this to the extent permitted by law. The retention, access control, and deletion of audit documents are managed in accordance with documented rules and the relevant requirements.

3 Auditing the ITAD Process Chain

The audit tracks selected devices, data storage media, or orders through the process chain. The following audit areas are considered on a risk-based basis and in accordance with the agreed scope of standards. They do not constitute an independent ITAD certification standard.

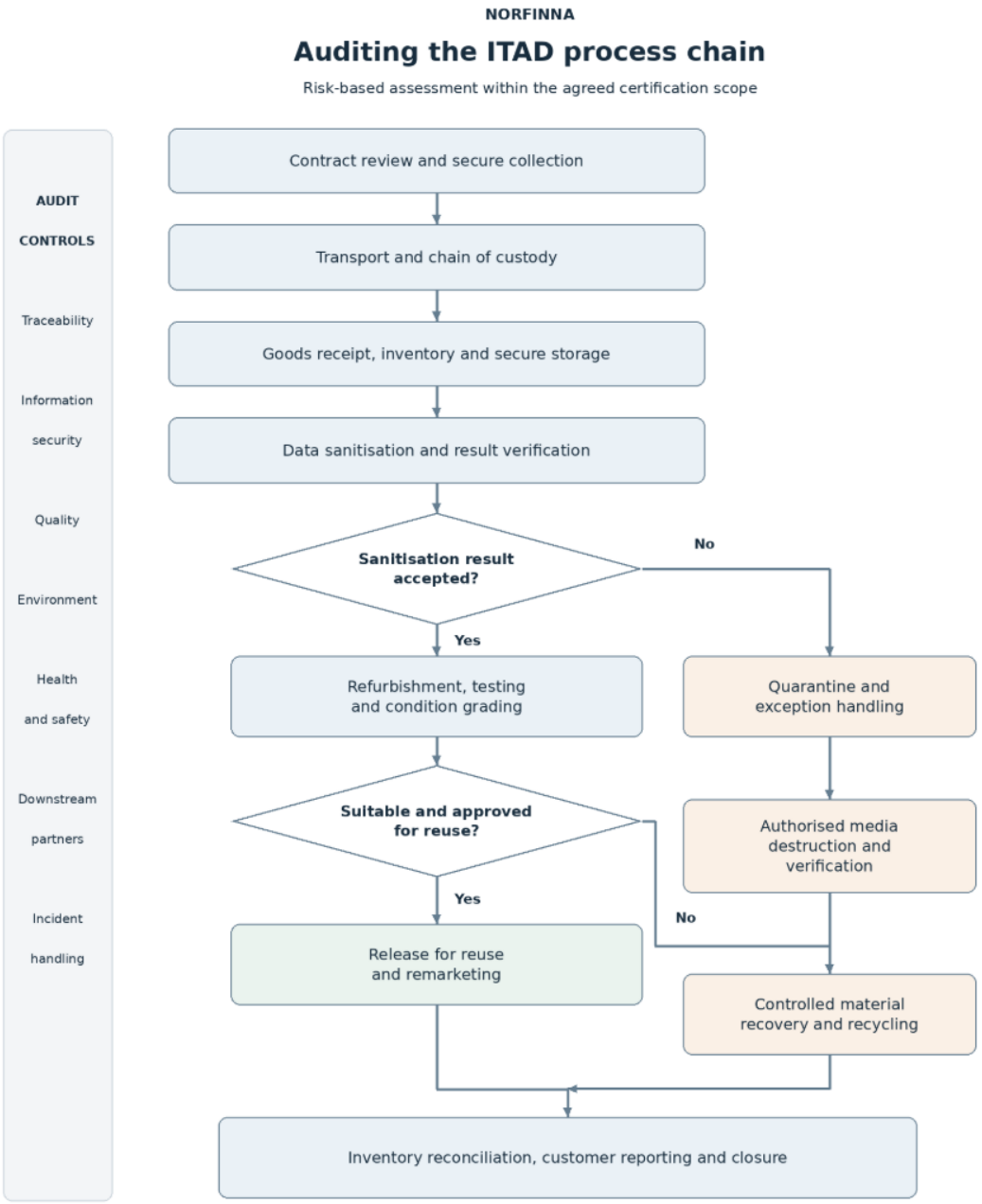


Figure 1 ITAD process chain and key audit checkpoints

3.1 Order Clarification and Secure Acceptance

The audit examines customer requirements, authorization to dispose of data, protection needs, agreed-upon erasure procedures, transfers of ownership, and responsibilities. The acceptance must be traceable through appropriate lists or documentation. Discrepancies between announced and actually accepted quantities are investigated.

3.2 Transportation and Seamless Traceability

The chain of custody (documented handover and accountability) encompasses pickup, transport, receipt, internal relocation, and transfer. Depending on the risk, identification, handover documents, containers, access controls, and transport partners used are assessed. Missing devices or damaged seals must trigger a defined clarification process.

3.3 Goods Receipt and Secure Storage

The following are evaluated: unique device identifiers, serial numbers, data carrier assignment, inventory reconciliations, and processing status. Devices and data carriers that have not yet been released must be protected against unauthorized access and accidental disclosure. Access rights, visitor policies, and secure areas are reviewed for effectiveness.

3.4 Data Deletion and Data Storage Medium Destruction

The following are reviewed: the selection of appropriate procedures based on the type of data storage medium and the level of protection required; the competence of the personnel performing the task; the control of the tools; and the verification of the results. Technical references are valid only to the extent that they have been agreed upon and are suitable for the medium; a mere reference to a deletion method is not sufficient proof of effectiveness.

Failed or incomplete deletions require a documented exception process. This includes locking, reprocessing, or approved physical destruction. Evidence must be clearly traceable to the specific device or data carrier in question. Approval for reuse requires an accepted result.

3.5 Preparation and Approval for Reuse

Random inspections include functional tests, condition assessments, repairs, remaining device locks, and the removal of customer identifiers and configurations. Approval rules must prevent devices from entering the sales process without sufficient proof of erasure and quality.

3.6 Remarketing and Downstream Partners

The evaluation covers accurate device descriptions, sales traceability, and the selection and monitoring of downstream partners. Outsourced data erasure, destruction, or recycling must be managed through traceable guidelines, defined responsibilities, and appropriate documentation.

3.7 Environment and Responsible Recycling

The audit considers the distinction between reusable devices and waste, secure collection and storage, quantity reconciliations, and documented recycling pathways. Permits and requirements for cross-border shipments are assessed in accordance with the regulations applicable to the organization. Special attention is given to batteries and other hazardous components.

Statements regarding reuse rates, material recovery, or avoided emissions must be based on verifiable data and disclosed calculation methods. Separate verification of such key performance indicators is only part of the scope of the engagement if it has been expressly agreed upon.

3.8 Occupational Safety and Health

Relevant risks include, among others, manual handling of loads, industrial trucks, electrical testing, sharp components, dust, noise, and damaged lithium batteries. The audit covers risk assessments, training, appropriate work equipment, protective measures, as well as emergency preparedness and incident analysis.

3.9 Reports and Safety Incidents

Customer reports must clearly document agreed-upon services, quantities, device identifiers, processing results, and outstanding exceptions. Records of deletion and destruction are cross-checked on a random basis against order data and system logs. Retention periods and access permissions must be regulated.

Reporting channels, escalation procedures, investigations, and corrective actions are reviewed for loss, unauthorized access, incorrect allocation, or unexplained inventory discrepancies. Contractual and legal information obligations must be taken into account in operational processes.

3.10 Selection of Evidence

The sample takes into account different locations, device types, data storage technologies, shifts, customer requirements, and exceptions. Possible forms of evidence include interviews, observations, system queries, transfer documents, inventory lists, technical logs, and partner documentation. A sample audit does not provide a complete review of all transactions.

4 Certification Process

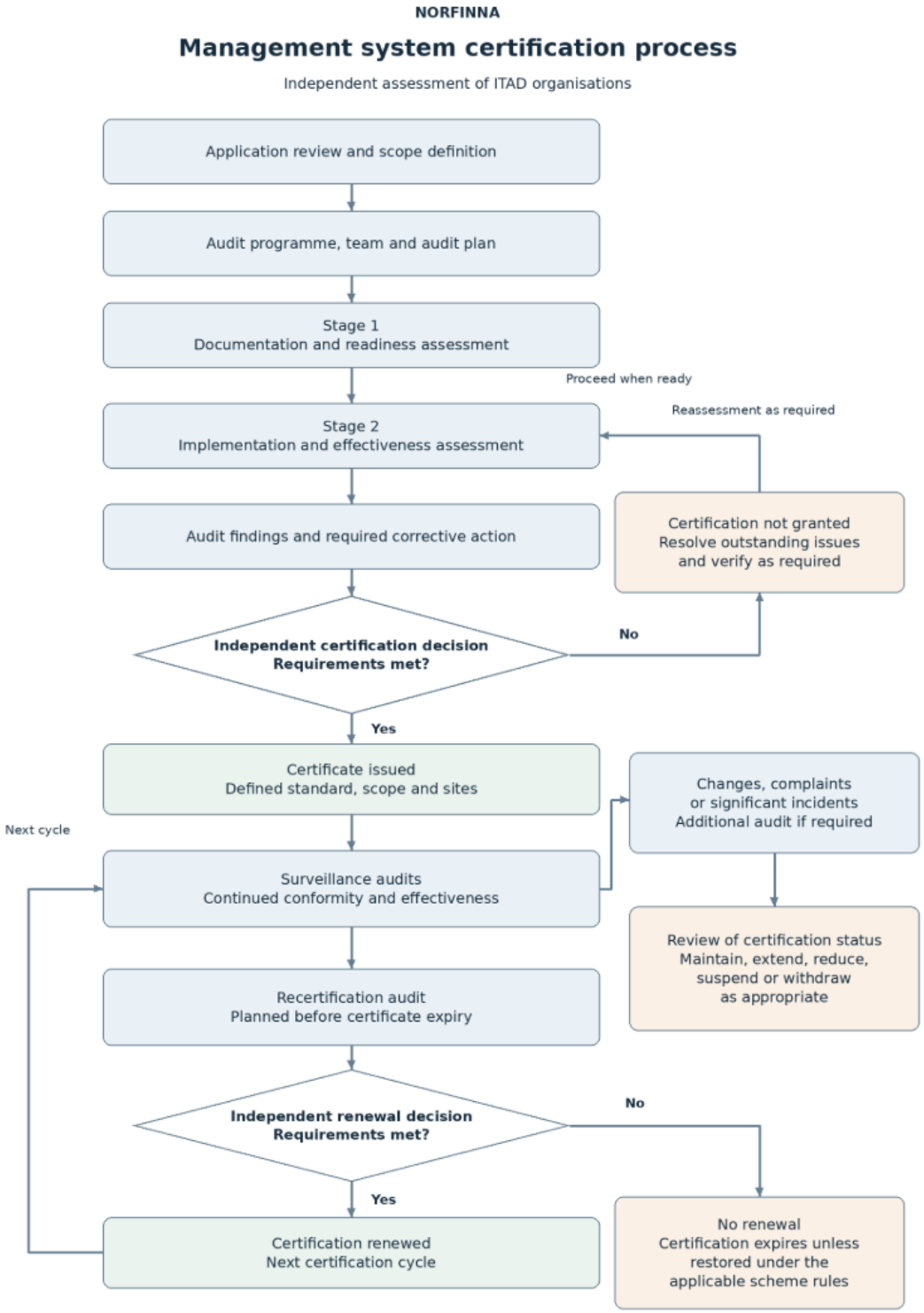


Figure 2 Certification, surveillance and recertification process

4.1 Application and Audit Program

NORFINNA clarifies the desired scope of the standard, locations, number of employees, processes, shifts, outsourced services, and significant risks. Based on this, the audit duration, required expertise, and an audit program for the certification cycle are determined. Multi-site arrangements or remote assessments are applied only to the extent permitted by the relevant requirements.

4.2 Audit Team and Planning

A designated audit team leader coordinates the assignment. Collectively, the team possesses the necessary expertise in standards, the industry, and processes. Specialists may be brought in to address technical issues. The audit plan, responsibilities, deadlines, and necessary access requirements are coordinated with the organization.

4.3 Stage 1

Stage 1 serves to evaluate the documented foundations and readiness for Stage 2. The scope, significant risks and environmental aspects, applicable obligations, process control, internal audits, and management review are examined. For ITAD companies, the focus is particularly on the security chain and the control of data erasure, release, and downstream partners.

Results and concerns are documented. Any necessary clarifications and the gap to Stage 2 depend on audit readiness and applicable certification requirements.

4.4 Stage 2

Level 2 assesses the implementation and effectiveness of the management system. The team reviews operational activities, records, objectives, responsibilities, and improvement measures. Security-critical processes and physical conditions are evaluated through appropriate on-site inspections; supplementary remote methods require suitability and sufficient evidence.

4.5 Findings and Corrective Actions

Nonconformities are documented with the applicable requirement, objective evidence, and a clear description. The organization provides a root cause analysis, corrective actions, and measures to prevent recurrence. Deadlines and follow-up reviews are determined based on the classification, risk, and the requirements of the certification system.

Before a positive decision can be made, the requirements for addressing significant and other nonconformities must be met. Acceptance of an action plan does not replace a required effectiveness review.

4.6 Certification Decision

A competent decision-making body, independent of the audit, reviews the audit report, scope, recommendations, and resolution of nonconformities. Certification is granted only if the required evidence is sufficient and the certification requirements are met. Rejections are justified in a transparent manner.

4.7 Surveillance and Recertification

For management system certification, a three-year certification cycle with regular surveillance audits is typically applied. The specific timeframes are determined by the applicable certification rules. The first surveillance audit must generally be conducted no later than twelve months after the initial certification decision; subsequent surveillance audits take place at least once per calendar year, except in the year of recertification.

The surveillance audit takes into account changes, complaints, internal audits, management reviews, corrective actions, and selected operational processes. Specifically for ITAD, traceability, exceptions to data deletion, and the management of downstream partners are re-evaluated.

Recertification is planned well in advance of the expiration date. It assesses ongoing effectiveness and compliance with requirements throughout the entire cycle. Renewal is contingent upon the completion of the required assessments and a positive decision.

4.8 Changes and Additional Audits

The certified organization shall promptly inform NORFINNA of any significant changes, such as new locations, changes in data erasure technologies, relevant third-party services, changes in ownership, or serious security and environmental incidents. NORFINNA shall assess the impact on the audit program and the scope of certification.

Expansions of the scope of certification require a corresponding assessment and decision. Additional or short-notice audits may be necessary to investigate complaints, significant changes, or for follow-up verification. The conditions are governed by contract.

4.9 Suspension, Restriction, and Withdrawal

Certification may be suspended, restricted, or revoked in the event of serious or ongoing noncompliance, refusal to undergo audits, misleading statements, or other relevant breaches of contract. During a suspension, the certification must not be presented as valid. Reinstatement requires timely rectification and a positive evaluation.

5 Complaints and Appeals

Complaints may concern, for example, NORFINNA's performance or the conduct of a certified organization. Appeals are directed against a certification decision. Both are recorded, reviewed for jurisdiction, and handled without prejudice to the submitting party.

NORFINNA acknowledges receipt and gathers the necessary information. The investigation and decision are conducted or reviewed by individuals who were not involved in the underlying matter. In the case of complaints about certified organizations, the impact on the affected management system is taken into account.

To the extent permitted, the submitting party receives updates on the progress and a formal conclusion. Confidentiality, data protection, and the legitimate interests of other parties involved are safeguarded. General feedback is used to improve the process.

6 Acceptance of Assignments and Use of Certificates

6.1 Acceptance or Rejection of an Assignment

Prior to accepting an engagement, NORFINNA assesses competence, capacity, impartiality, and the clear definition of the scope of the assessment. An engagement may be rejected or terminated if these requirements are not met, if significant safety risks exist, or if the organization fails to provide necessary evidence and access. The reasons are documented and communicated appropriately.

6.2 Permissible Statements and Marks

Certificates and certification marks may be used exclusively for the designated organization, standard, activities, and locations. Statements must accurately reflect the current status and scope. Design and use are governed by the rules provided by NORFINNA; accreditation marks are additionally subject to the requirements of the accreditation body.

Advertising must not suggest either a complete guarantee of information security or the certification of individual devices, data erasure tools, erasure reports, or products. A data erasure confirmation from the ITAD company must be distinguished from the management system certificate. In the event of restriction, suspension, expiration, or revocation, affected statements and marks must be adjusted or removed accordingly.

NORFINNA will pursue instances of misuse of references and demand their correction. Further measures are governed by the certification rules and the contract.

7 Public Information and Disclosure

7.1 Information on Certification Status

NORFINNA provides information on certification procedures, standards, geographic areas of operation, and the status of issued certifications in accordance with applicable guidelines. For individual certifications, the name of the organization, scope, affected locations, standard, and certificate status may be confirmed. Confidential audit reports and customer-specific security information are excluded from this.

7.2 Contact

Norfinna Oy Ltd.
Ariel Figueras
Länsikatu 15, 80110 Joensuu, Finland
Tel: +358 50 387 89 70
E-mail: ariel.figueras@norfinna.com
Support page: https://norfinna.freshdesk.com/support/home
Website: www.norfinna.com
Follow: https://www.linkedin.com/company/norfinna-oy-ltd/home/?viewAsMember=true

7.3 Basis for Processing

Template: Service_Description_261020_Norfinna.pdf, 18 pages. The content is titled “Norfinna Certification Service Description,” October 2026.

NORFINNA Company Profile and ITAD Services Page, accessed on October 21, 2026:
https://www.norfinna.com/
https://www.norfinna.com/performance/itad

FINAS Directory of Accredited Bodies and Valid Scopes of Accreditation, accessed on October 21, 2026:
https://www.finas.fi/sites/en/operators/Pages/default.aspx

The ITAD test fields are an editorial elaboration for the described intended use. They do not replace the relevant standard texts or the confirmation of the actual scope of accreditation.