blancco

How Blancco Helps Organizations Comply with ISO 27001 Data Destruction Controls

Used by tens of thousands of organizations worldwide, the ISO/IEC 27001: 2022 framework is the world's best known information security standard. This Solution Brief shows how Blancco's data erasure solutions support compliance with the ISO 27001 security controls applying to data destruction.

The ISO/IEC 27001: 2022 update

In 2022, the **ISO 27001** framework for information security management systems (ISMS) was updated from the previous 2013 version.

In addition to some changes in scope and context, one of the major changes was the reorganization of the security controls in Annex A. The 2022 version reduced the total number of controls from 114 to 93, and restructured them into four themes: Organizational, People, Physical, and Technological.

What does ISO 27001:2022 say about data destruction?

From a data sanitization perspective, one of the biggest changes between 2013 and 2022 was the introduction of a new control: 8.10 – Information deletion. This control says:

"Information stored in information systems, devices or in any other storage media should be deleted when no longer required."

While the 2013 version had talked specifically about the destruction of data on physical media, control 8.10 explicitly elevates "deletion" as a standalone technical control, and expands the scope to potentially include cloud storage, virtual environments, and all other places where data is stored.

The update reflects the need for security-conscious organizations to focus on the **data lifecycle** rather than the asset lifecycle alone.

Control 8.10 requires that sensitive information should be destroyed in a secure, verifiable way when it is no longer needed. The standard gives several possible methods of data sanitization—such as secure overwriting or cryptographic erasure—based on business needs and legal requirements. It also calls for businesses to keep records as evidence. If third parties are involved in storing or deleting data, contracts should explicitly require secure deletion, and organizations should obtain proof that it has been carried out.

Deletion, destruction & sanitization: What do they all mean?

In this context, "deletion" and "destruction" are not given a technical definition. Rather, both words are used generally to discuss the process of destroying data so that it can no longer be recovered.

In control 7.14, the ISO 27001 standard suggests that:

"Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable ***rather than using the standard delete function.****"*

This broadly aligns with the **definition of data sanitization** used by Gartner and others, where data erasure (i.e., secure overwriting), cryptographic erasure, and some forms of physical destruction are acceptable when they can be verified and certified.

Methods like basic file deletion, formatting, unverified wiping, and factory resets are often seen as incomplete forms of data destruction because they either do not provide readily accessible forms of verification or may leave remnants of data recoverable.

As industry leaders in the data sanitization space for over 20 years, Blancco has built solutions that completely erase data through software-based sanitization techniques that conform with all major international standards, including **NIST SP 800-88** (now including Rev. 2) and **IEEE 2883**. We also maintain our own **ISO 27001 certification** using these data erasure processes.

Copyright © 2026 Blancco Technology Group. All Rights Reserved.

ISO 27001 data destruction & your Statement of Applicability

At the heart of any ISO 27001 audit is the SoA (Statement of Applicability). Having conducted a thorough risk assessment to identify threats and select security controls that align with vulnerabilities, business objectives, regulatory requirements, and feasibility, your SoA will:

- List all the controls necessary for your organization.
- Compare against the Annex A list of controls to ensure nothing significant has been excluded (in practice this may mean listing all Annex A controls).
- Mark each control as included or excluded.
- Justify their inclusion or exclusion.
- Confirm whether they have been implemented or not.

Based on your specific risk factors—e.g., around the confidentiality of information you handle, the number of IT assets you use and decommission, or legal and industry regulations about data disposal—your organization's approach to the ISO 27001 data destruction controls will vary.

Here are two possible examples of where data destruction may be a necessary control. These are generic examples and a non-exhaustive list, so this should not be taken as advice about your environment.

ISO 27001 control 7.14 – Secure disposal or re-use of equipment

This control states that items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.

Where it might be included

You may need to include this control if your company uses laptops, servers, mobile devices, and other IT assets that store data locally. Ultimately, these assets will need to be redeployed or disposed of, leading to a clear risk of residual data remaining on devices unless they are comprehensively and verifiably sanitized.

ISO 27001 control 5.34 – Privacy and protection of PII

With a specific focus on legal, regulatory, and contractual compliance, control 5.34 requires organizations to identify and meet the requirements regarding the preservation of privacy and protection of Personally Identifiable Information (PII).

Where it might be included

This is a broad control that will apply to most organizations. If you are involved in the processing of personal data (e.g., employees, customers, users, and business partners), **EU GDPR** and other data protection laws are likely to apply to you. Given that many data protection regulations have requirements regarding the disposal of end-of-life data, it's essential to identify and mitigate possible risks from data breaches, leaks, and non-compliance.

Copyright © 2026 Blancco Technology Group. All Rights Reserved.

blancco

How Blancco supports ISO 27001 data destruction

We support organizations to achieve ISO 27001 compliance with data sanitization solutions for all asset types.

ANNEX A CONTROL	REQUIREMENT	BLANCCO
5.34 PRIVACY AND PROTECTION OF PII	"The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements."	Blancco enables organizations to securely and verifiably erase personal data in line with control 5.34 by ensuring that PII is permanently removed from IT assets, endpoints, and storage environments. Tamper-proof audit reports provide evidence of erasure, supporting accountability and demonstrating compliance with privacy obligations during audits or data subject requests.
5.9 INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS	"An inventory of information and other associated assets, including owners, should be developed and maintained."	Inventory management requires asset/information owners to consider the entire lifecycle, including at end-of-use. Blancco supports organizations to maintain up-to-date, secure inventories by ensuring that information and associated assets can be certifiably erased when required.
7.10 STORAGE MEDIA	"Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements."	Blancco enables organizations to meet control 7.10 by ensuring that data stored on all types of storage media is securely erased before transfer, reuse, or disposal. This reduces the risk of unauthorized access or data leakage. Our standardized, certified erasure processes and audit-ready reports provide assurance that different types of storage media (including HDDs, SSDs, NVMEs, and USB drives) have been handled and sanitized in accordance with security policies and regulatory requirements.
7.14 SECURE DISPOSAL OR RE-USE OF EQUIPMENT	"Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."	Control 7.14 recognizes that techniques for securely overwriting storage media differ according to the technology and the classification level of the information it holds. To support this, overwriting tools must be applicable to the technology of the storage media. Blancco offers secure data erasure for a wide range of storage technologies in line with the NIST 800-88 and IEEE 2883 Purge and Clear sanitization methods. Blancco Drive Eraser has been independently tested and certified by ADISA for NIST and IEEE Clear and Purge.

Copyright © 2026 Blancco Technology Group. All Rights Reserved.

blancco

8.10 INFORMATION DELETION

"Information stored in information systems, devices or in any other storage media should be deleted when no longer required."

Blancco supports compliance with control 8.10 by enabling organizations to securely overwrite sensitive information across endpoints, storage media, and live storage environments in line with defined retention policies and legal requirements. Our automated erasure processes and verifiable audit trails ensure that data is permanently removed and that deletion activities can be evidenced for compliance and audit purposes.

Erase internally or work with data destruction providers?

Organizations pursuing or maintaining ISO 27001 certification need to decide whether data erasure should be handled internally or outsourced to specialist data destruction companies such as ITAD vendors. This decision typically hinges on control, risk, scalability, and assurance.

In-house erasure offers direct control over processes, tooling, and data handling. It can simplify integration with internal policies, asset inventories, and security operations, and may reduce dependency on third parties. It requires investment in certified tools and staff training to ensure consistency across all asset types and locations.

An alternative or supplementary approach involves outsourcing some of this work to ITAD providers, Managed Service Providers, or other local data destruction companies. This can provide access to certified erasure technologies, established processes, and expertise in handling diverse asset types, often with built-in reporting aligned to audit requirements. One of the main benefits here is the reduction of operational burden. However, it introduces third-party risk, requiring due diligence, contractual controls, and verification of service delivery—particularly around chain of custody and evidence of erasure.

From an ISO 27001 perspective, either approach may be valid provided your organization can demonstrate that risks are appropriately managed, controls are effective, and evidence is available. The key consideration is whether the process is secure, consistent, and auditable.

We advise that even if you work with an ITAD or other vendor to dispose of end-of-use IT assets, your team should erase data onsite before the assets are removed. Even if devices are destined for physical destruction, erasing data while they are still in your control reduces the impact of potential theft or loss during the disposition process.

Consolidate Your Security Controls

Learn how to make secure data erasure a seamless part of your ISO 27001 strategy.

Get Started

Copyright © 2026 Blancco Technology Group. All Rights Reserved.