blancco

WHITE PAPER

6 Data Sanitization Controls to Strengthen Your Enterprise GRC Strategy

blancco.com

blancco

This paper explains how enterprise governance, risk, and compliance (GRC) teams can optimize end-of-life data processing to reduce risk and increase compliance. We identify six controls that can help embed data sanitization into your GRC strategy.

Gain clarity on where data sanitization fits alongside GRC disciplines and learn how to operationalize secure data erasure across your enterprise.

Where enterprise GRC strategy & data sanitization meet

As enterprises grow more complex and globally distributed, dedicated governance, risk, and compliance (GRC) professionals are being tasked with reducing risk and achieving compliance with laws and internal standards.

Yet some GRC programs remain incomplete in key areas, and McKinsey's **2025 Global GRC Benchmarking Survey** highlighted widespread gaps in maturity. 42% of respondents said their use of GRC technology "needs improvement," and 44% reported that the head of risk sits more than one level below the CEO.

One of the key areas in GRC development is data lifecycle management.

While organizations attempt to secure and scale their GRC strategies, the regulatory environment continues to demand more from them. Data protection regimes (such as the EU GDPR and the 20 U.S. state data privacy laws), cybersecurity requirements (including NIS2 and ISO certifications, for example), and emerging sustainability reporting rules (such as the EU CSRD) create overlapping obligations for the same enterprise data sets. In this data-centric environment, organizations must demonstrate that sensitive data is handled, stored, and disposed of compliantly.

This is where data sanitization can help.

Data sanitization, as defined by the **International Data Sanitization Consortium**, refers to three methods of destroying data (with verification) so that it cannot be recovered by any known means. These methods are:

- software-based data overwriting (data erasure)
- cryptographic erasure
- physical destruction of data-bearing assets

Advanced data sanitization processes, regardless of method, should also go beyond the simple destruction of data. An enterprise-grade data erasure solution, for example, also verifies the data is gone and produces evidence it has been irrecoverably removed.

Given the regulatory interest in controlling the data lifecycle, organizations whose data retention and destruction policies are misaligned with their GRC stances risk creating significant vulnerabilities.

blancco

Why include data sanitization in your GRC strategy?

Poor sanitization controls expose organizations to financial and security risks. If storage devices such as loose drives or employee laptops leave your organization without verified sanitization, for example, they can enter secondary markets intact or insufficiently wiped. This may lead to unintended disclosure of sensitive records, compliance fines, and a loss of trust.

Reporting over recent years has highlighted several cases where retired drives containing regulated data were resold rather than properly sanitized, creating the conditions for privacy breaches and regulatory intervention. In other incidents, weak chain-of-custody processes during IT asset disposition have enabled theft of devices intended for destruction. These scenarios demonstrate that the risk is not limited to technical mistakes and may be better approached with a holistic risk strategy.

To date, regulators have issued fines in the tens of millions of dollars, underscoring that end-of-life data controls should be a core enterprise GRC obligation.

Who manages data sanitization?

In many enterprises, the responsibility for data sanitization is fragmented. This is one reason it may not be embedded in your GRC strategy yet.

IT asset managers, compliance leads, cybersecurity teams, and sustainability professionals may all have partial ownership of data lifecycle activities.

While senior leaders are increasingly involved, and most enterprises have policies in place or nearing completion, shared responsibility can create gaps without strong, unified governance.

Fragmentation of sanitization accountability has practical consequences. Teams may default to simple deletion rather than verified sanitization, or apply sanitization inconsistently across leased devices, vendor-managed hardware, and cloud environments.

Without a clear governance mandate and enterprise-wide responsibility assignment, sanitization becomes an afterthought rather than a documented control.

Takeaway

Formalize decision-making processes by adding a data sanitization RACI (Responsible, Accountable, Consulted, Informed) matrix as part of your broader GRC strategy.

blancco

Data sanitization vs. incomplete data destruction: Why it matters

Many common data destruction practices fall short of achieving complete sanitization.

Basic reformatting of endpoints can leave residual data behind. Factory resets vary widely by device and crypto erase may not remove all sensitive information unless encryption and key removal are confirmed. File shredding or basic wiping tools may overwrite selected areas without proving full coverage or producing compliance evidence.

Similarly, physical destruction can be effective, but only when the method matches the media type and is properly verified. Degaussing, for example, is effective on magnetic storage media (HDDs) but not on flash-based storage.

Three factors distinguish strong sanitization practices from basic data destruction:

- **Method of removal:** Overwriting data, cryptographic erasure of encryption keys, and some forms of physical destruction all offer varying levels of assurance. It should be noted that each method will also have specific interactions with your IT environment. If all employee endpoints were not initially encrypted, for example, crypto erase may not be a feasible solution.
- **Verification:** Assurance mechanisms confirm that sanitization has been completed successfully according to defined standards. In the case of data erasure software, this may look like sector-level verification checks confirming overwrite completion.
- **Certification:** Generation of objective evidence that sanitization met documented requirements, supporting audit and compliance evidence.

For GRC data protection and cybersecurity controls, these differences matter because regulators and auditors look for evidence that sensitive data has been rendered unrecoverable when no longer needed. For example, **control 8.10 of ISO 27001:2022** speaks to the need for organizations using data erasure software to obtain sufficient evidence. This is particularly relevant where data subject rights (such as GDPR deletion requests) intersect with device lifecycle management.

Adding data sanitization to your GRC framework

With so much at stake if your data security should fail, it's essential to build up a robust process for handling end-of-life data. These six controls will help you create a provable, procedural strategy that reduces vulnerabilities.

Control 1: Be aware of both the data lifecycle & the asset lifecycle

A strong enterprise GRC strategy recognizes that data risk persists across its lifecycle, from creation and active use to retirement and final disposal. Your data sanitization controls should apply to:

- **Asset disposition:** End-of-life devices, storage media, and decommissioned environments require controls that remove organizational data before transfer, lease return, resale, or recycling. This may be achieved through in-house sanitization or working with third parties such as trusted IT asset disposition (ITAD) vendors or managed service providers (MSPs).
- **Live environments:** In contexts where data retention must be limited to business needs or legal requirements, sanitization methods should support automated removal of obsolete data from active systems. This may include the erasure of files and folders from active systems, including employee endpoints.

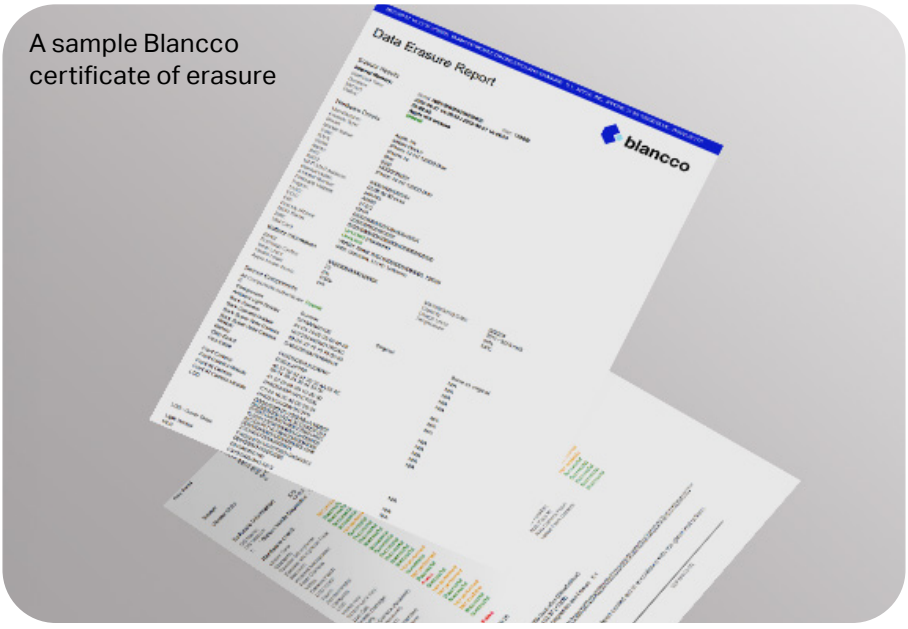
Treating sanitization as a lifecycle control gives you a more granular ability to control data destruction.

Control 2: Automate data sanitization & reporting

Instead of manually wiping data or destroying assets and then spending time compiling spreadsheets or point-in-time screenshots, integrated, automated data erasure ensures that sanitization activities produce centralized records.

These records, such as the tamper-proof certificates Blancco solutions generate for each erasure, reduce audit effort and enhance reliability.

Evidential automation should be able to capture key attributes: what was sanitized, the method used, time and operator metadata, and confirmation of success.



A sample Blancco certificate of erasure

Control 3: Use sanitization metrics to support ESG & sustainability goals

Environmental, social, and governance (ESG) reporting may include indicators related to responsible resource use. Data sanitization intersects with sustainability objectives in multiple ways, from how organizations dispose of hardware (i.e., whether they physically destroy end-of-use assets or securely erase them and allow them to be redeployed elsewhere) to the amount of energy they use in the storage of redundant, obsolete, and trivial (ROT) data.

Incorporating data erasure into your GRC strategy not only boosts sustainability performance, but it can also improve reporting.

Within the Blancco Management Portal (our centralized tool for managing and recording all erasures), a dedicated sustainability dashboard offers a record of the CO_2 emissions saved with Blancco products. The sustainability calculator delivers insights into the number of devices erased by volume, weight, and the CO_2 emissions avoided.

Control 4: Strengthen third-party risk management with ITAD/MSP partners

Third-party risk is a persistent challenge in enterprise GRC. Organizations routinely work with MSPs, independent software vendors, and ITAD partners. GRC risk management frameworks call for assessment and mitigation of these external dependencies.

For devices and storage media leaving your enterprise's direct control, sanitization controls must extend to partners. Contractual requirements could mandate adherence to recognized protocols (e.g., R2v3 or ADISA standards), regular attestation of compliance, and independent verification. Embedding these expectations into third-party risk assessments and procurement processes reduces risk and aligns external practices with internal GRC data protection requirements.

blancco

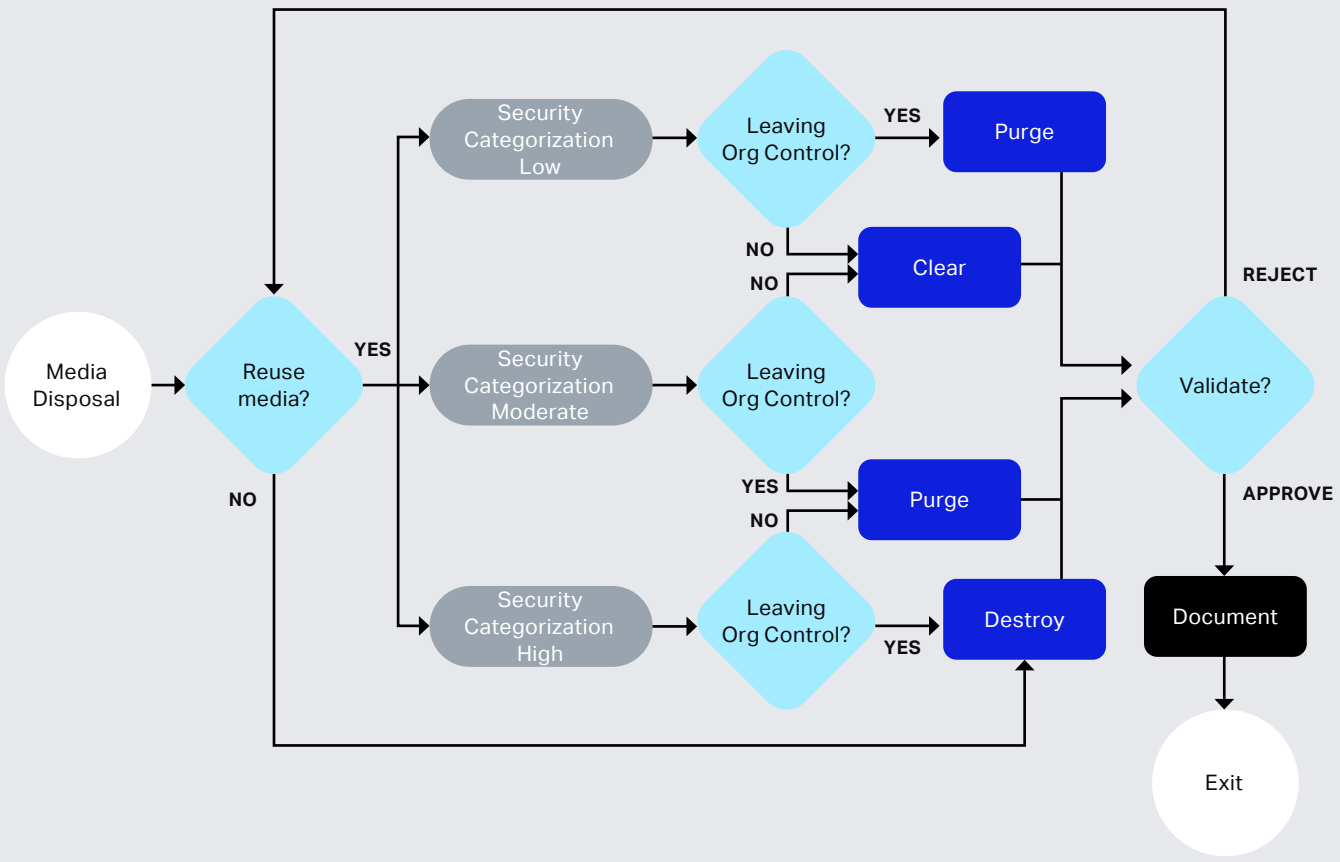
Control 5: Align sanitization programs with recognized standards & certifications

One factor that might be limiting the implementation of data sanitization within your GRC strategy is lack of knowledge around best practices. This lack of awareness is more common than you might think. In fact, our **State of Data Sanitization Report** found that only 37% of IT and ESG leaders know about one of the most high-profile media sanitization protocols: NIST 800-88.

While the DoD 5220.22-M disk wiping standard may still be one of the best known approaches, it is considered outdated by many and has been surpassed by more recent standards, including IEEE 2883 and NIST 800-88.

Using standardized frameworks reduces subjective interpretation of sanitization requirements. It provides a consistent benchmark for internal teams and external partners to follow and enables comparability across business units and geographies.

The recent **NIST SP 800-88 Rev2** update contains information on establishing a data sanitization program, including via the decision-making flowchart below.



Republished from NIST SP 800-88 Rev2, p. 20, "Fig. 1. Sanitization and disposition decision flow"

Control 6: Benchmark GRC maturity

One effective way to strengthen sanitization as an enterprise GRC control is to map its implementation against an established maturity framework. The **OCEG GRC Maturity Model** provides a practical benchmark for assessing governance, risk, and compliance activities across your organization.

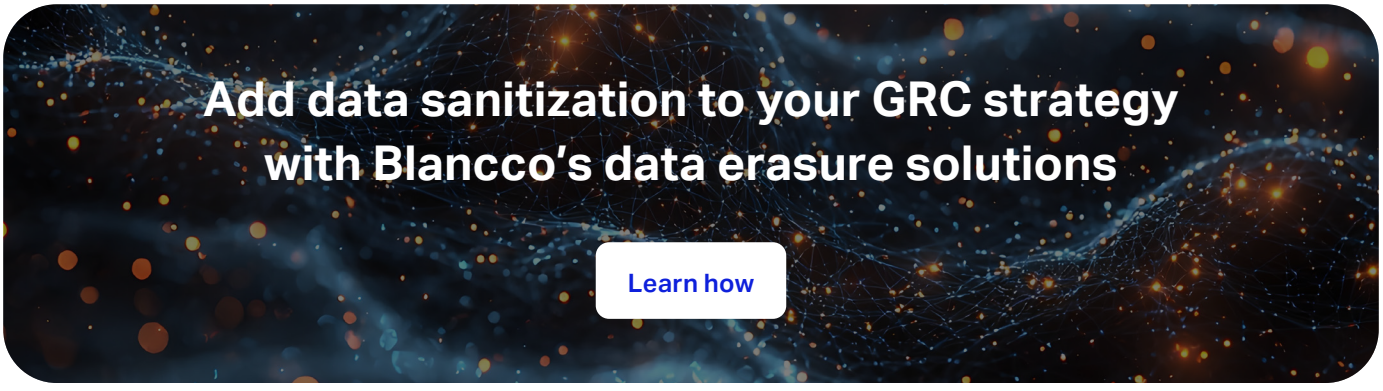
Applied to data sanitization, maturity typically progresses from inconsistent, team-specific practices to standardized, enterprise-wide controls supported by automation and audit-ready evidence. Early-stage organizations may rely on ad hoc disposal processes or vendor assurances. More mature programs define sanitization as a formal control, link it to risk assessments, and require verification and certification.

If your maturity score is advanced for other GRC disciplines but less so on data sanitization, a maturity model could help you spot gaps in your current process and make the same journey from siloed to connected that you have already taken elsewhere.

Take control of end-of-life data

Data sanitization should be part of any mature enterprise GRC strategy that seeks to manage data risk, prove compliance, and deliver actionable insights to leadership. By embedding sanitization controls into technology-enabled compliance workflows, enterprises reduce residual risk and improve assurance.

Centralized reporting, alignment to standards, integration with third-party risk management, and metrics tied to ESG and cybersecurity outcomes all contribute to a stronger GRC data protection posture.



Certified, Defensible
Data Erasure Software