CI Information Management

2026

NAID AAA + ISO 27001: *Why Both Matter*

AAA NAID CERTIFIED

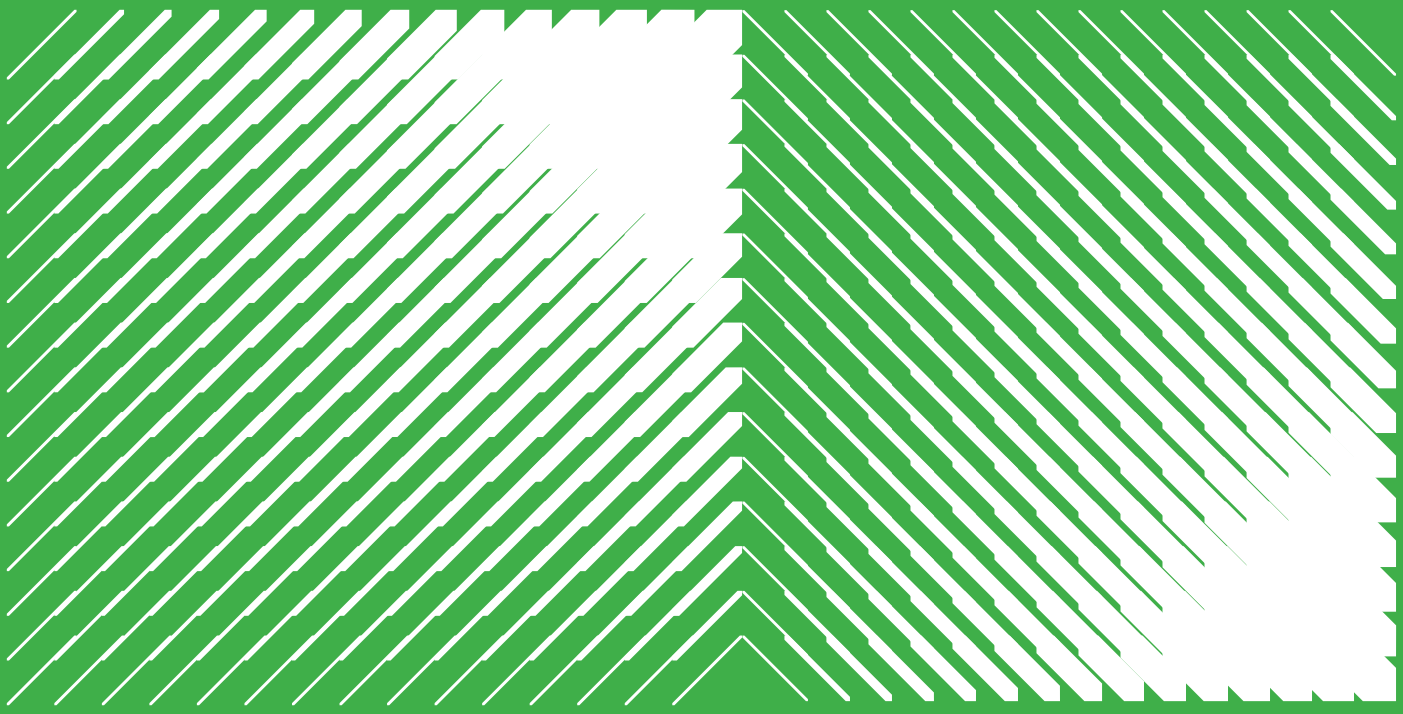
AMTIVO

ISO 27001:2022 Certified

Information Security Management

Presented By

CI Information Management



Two certifications. Two different jobs. One stronger security framework.

Why Certification Matters in Secure Destruction

When you're looking for shredding companies for your business, anyone can claim they are “secure,” “trusted,” or “confidential.” These terms are easy to use but don’t independently prove how the company actually operates. When a business hands over sensitive, data-bearing, or confidential documents, whoever they choose as a provider becomes a part of that business’s information security environment, including the risks. Therefore, businesses shouldn’t choose one lightly. Every vendor should be evaluated just as carefully as a company’s own internal security practices.

Third-party certification can provide external validation against established standards. Depending on the certification type, it can show that the shred vendor meets industry standards for policies, procedures, operational controls, security practices, and ongoing requirements. However, not all certifications validate the same things. A certification may be strong within its own scope while not addressing other areas.

CI Information Management holds both NAID AAA Certification and ISO 27001:2022 Certification. As of 2026, we are one of two secure destruction companies in Washington State that hold both certifications. That often leads our customers to ask, “What does each certification actually verify?” and “Why does it matter that CI holds both?”

In this white paper, we answer these questions by explaining what each certification verifies, why it matters, what dual certification means for your business, and how to evaluate a secure destruction provider. At the end of the day, certification matters because it replaces unsupported security claims with independent verification, but only if customers understand what each certification actually covers.

NAID AAA: Verifying the Secure Destruction Process

A NAID AAA Certification is considered the gold-standard third-party verification for secure information destruction. As one of the most recognized certifications in the industry worldwide, more than 950 i-SIGMA's NAID AAA Certified locations now operate on 5 continents. Dozens of government agencies require this certification for media destruction, and IRS Publication 1075 (2016) acknowledges the value of NAID AAA Certification. Additionally, this certification qualifies as compliance support for major regulations like FACTA, HIPAA, and PCI.

An NAID AAA Certification verifies that the following meets rigorous industry requirements for protecting information throughout the destruction process:

- **Employee screening:** Employees handling sensitive records are properly screened, and personnel controls are in place to reduce the risk of unauthorized access.
- **Physical security:** Secure facilities and controlled access are defined to help protect documents and media before destruction.
- **Handling procedures:** Materials remain protected while being collected, transported, stored, and prepared for destruction.
- **Destruction processes:** Confidential records and media are destroyed in a way that prevents reconstruction or recovery.
- **Chain-of-custody controls:** Businesses are able to demonstrate where information went and who was responsible for it.

Essentially, an NAID AAA Certification matters to businesses because secure destruction is more than just the moment it enters the shredders. Critical risk points exist throughout the custody process, and this certification provides independent verification focused specifically on those destruction-related risks.

ISO 27001: Verifying the Information Security Management System

An ISO 27001 Certification (officially known as the ISO/IEC 27001 Information Security Management standard) operates at a broader organizational level and complements NAID AAA's destruction-specific focus. It is considered the world standard for information security management systems (ISMS). Over 70,000 ISO 27001 certificates have been issued to organizations in over 150 countries. While it is not a legal requirement, it is frequently a prerequisite in contracts, requests for proposal, and international partnerships. (CERT, 2026)

This standard provides companies of various sizes and sectors with guidance for establishing, implementing, maintaining, and continually improving an information security management system in three core principles: (CI Information Management, 2026)

- **Confidentiality:** Ensuring that data is accessible only by authorized personnel.
- **Integrity:** Ensuring the data is accurate, complete, and trustworthy throughout its lifecycle.
- **Availability:** Ensuring authorized users have access to data when needed.

An ISO 27001 certification matters to businesses because organizations today face increasing security risks related to data breaches, cyber threats, privacy regulations, and secure information handling (CI Information Management, 2025). Certification shows that a service provider follows strong security controls across employees, vendors, technology, internal systems, policies, and security processes.

Why Both Matter: Two Certifications, Two Different Jobs

It is vital to recognize that different certifications check different things. Knowing what each one actually verifies matters when you're trusting a vendor with sensitive information. These are not competing certifications; rather, they examine different aspects of security. Looking at the questions each certification helps answer makes the distinction clearer.

Security Question	NAID AAA Certification	ISO 27001 Certification
Does this certification specifically evaluate how confidential information is securely destroyed?	**Yes.** Secure information destruction is its primary focus.	**No.** ISO 27001 evaluates the broader information security management system rather than certifying a specific destruction process.
Does it verify controls for securely handling and transporting materials before destruction?	**Yes.** The certification program includes secure handling, transportation, and chain-of-custody controls.	**Not specifically as a destruction requirement.** These risks may be managed within the organization's broader ISMS.

Security Question	NAID AAA Certification	ISO 27001 Certification
Does it specifically evaluate employee screening for people involved in secure destruction?	**Yes.** Employee background screening is among the controls independently evaluated.	**Not specifically for destruction personnel.** ISO 27001 takes a broader, risk-based approach to organizational information security.
Does it specifically verify chain-of-custody procedures for confidential materials?	**Yes.** Chain of custody is a core component of secure destruction operations.	**Not as a destruction-specific requirement.** The organization can address relevant custody risks through its broader security controls.
Does it evaluate how the organization identifies and manages information-security risks across the business?	**Not its primary purpose. Its scope centers on secure information destruction.**	**Yes. Risk identification, assessment, treatment, and ongoing management are fundamental to an ISMS.**
Does it evaluate organization-wide information-security policies and access controls?	**Only where they relate to the secure destruction process and certification requirements.**	**Yes.** The ISMS encompasses broader policies, responsibilities, and information-security controls.
Does it evaluate how the organization prepares for and responds to information-security incidents?	**Not as its primary focus.**	**Yes.** Incident management is part of the broader information-security management framework.
Does it address security risks involving suppliers and other third parties?	**Not as its primary focus.**	**Yes.** Supplier security is addressed within the broader ISMS framework.
Does it require security practices to be regularly reviewed rather than treated as a one-time exercise?	**Yes.** Certified providers undergo ongoing scheduled and unannounced audits and annual renewal.	**Yes**. Continual monitoring, review, maintenance, and improvement are core parts of the ISMS model.

As you can see, holding only one of these certifications can leave a gap in your business. While the NAID AAA verifies the destruction process, the ISO 27001 verifies the security system behind it. However, it doesn't mean there is a failure. Holding only NAID AAA doesn't mean a provider is insecure elsewhere, and holding only ISO 27001 doesn't mean its destruction practices are weak.

Rather, together, they demonstrate that security isn't simply a claim or a checkbox. It is a documented, independently audited, and continuously managed commitment to protecting your information from the moment it enters custody through its final destruction. The value of dual certification is not duplication; it is complementary coverage.

What Dual Certification Means for Your Business

When you choose a secure destruction provider, you are not simply hiring someone to shred paper or destroy a hard drive. You are entrusting that company with information that could expose your customers, employees, or organization if it is mishandled. Many destruction providers hold only one certification or none at all.

A perfect example of trusting a mismanaged company is the Morgan Stanley Smith Barney LLC data destruction case. (Rivera, 2025) After "trusting" an inexperienced vendor to decommission servers with sensitive client information, the result was disastrous. The company failed to handle the destruction properly, and some unencrypted devices were sold on a third-party auction site. It is estimated that approximately 15 million customers may have been affected. (U.S. Securities and Exchange Commission, 2022)

The consequences Morgan Stanley Smith Barney LL faced included a $35 million penalty from the U.S. Securities and Exchange Commission and a $6.5 million multi-state attorney general settlement. (Mason, 2023) Yet the financial implications don't begin to cover the reputational backlash the company faced. That is why taking the time to perform due diligence when selecting vendors and choosing those with reputable certifications to demonstrate their operations is critical.

As of 2026, CI Information Management is one of two Secure Destruction Companies in Washington State that hold both certifications. How does this translate into practical customer value?

#1: More Complete Vendor Due Diligence

Without certification, businesses may have to rely heavily on vendor claims, forcing them to trust that the vendor has the appropriate controls in place.

Dual certifications give procurement, compliance, IT, and security teams documented, third-party-verified information on how the shredding vendor operates in both secure destruction and organization-wide information security management. There are no loose ends or loopholes, only readily available, accurate, and maintained information. Rather than relying solely on a provider's description of its security practices, your organization can review established certifications that have been independently audited.

#2: Greater Confidence Across Custody Lifecycle

Before your documents or media are finally destroyed, they go through a chain of custody. Typically, this looks like: ***Your Office → Secure Collection → Transportation → Handling → Destruction → Documentation.***

Security matters at every point and transition in this chain, but non-certified vendors often focus only on security during and after destruction. NAID AAA focuses specifically on the controls surrounding the handling, transport, custody, and destruction of confidential information. ISO 27001 adds another layer by evaluating the broader system used to identify and manage information-security risks throughout the organization.

Together, these two certifications show that document and media security isn't limited to what happens at the shredder; it's managed intimately throughout the entire service.

#3: Strong Accountability

When disposing of sensitive information, businesses want to know who is handling the content, what they are doing, and how they are held responsible. Rather than having a blanket policy that loosely applies to all employees, dual certification supports a more structured approach to accountability.

Secure destruction is clearly defined in its people, policies, access controls, documented procedures, risk management, and ongoing oversight. Each point has a clear procedure. For businesses, this provides additional confidence that responsibilities have been defined, processes are documented, and security risks are regularly evaluated rather than handled informally.

#4: Support for Compliance and Audit Readiness

Organizations in regulated industries, like those under FACTA, HIPAA, and PCI, may need to demonstrate how they select and oversee vendors that handle confidential information. For example, should a business be audited or under a security review, they may be asked:

- How vendors were selected
- What security requirements were evaluated
- How sensitive information was handled
- Whether destruction was documented

Rather than scrambling to get documented information from a non-certified vendor, who may or may not have a pre-set explanation, dual certification provides this information readily. Certification documentation, chain-of-custody records, and Certificates of Destruction can additionally help support that process.

#5: Ongoing Oversight

A common problem among any business is complacency. They think that once they achieve their goal, they are done. However, for security, especially for data destruction, that cannot be allowed. One benefit of dual certifications is that both require ongoing oversight. NAID AAA and ISO 27001 are not permanent designations that a company earns once and keeps indefinitely.

NAID AAA Certified providers are subject to continuing audits and annual renewal requirements. This includes scheduled and unannounced audits designed to verify that secure destruction practices continue to meet certification standards over time. That ongoing review helps ensure controls around employee screening, handling, transportation, chain of custody, and destruction remain in place, rather than being demonstrated only during an initial audit.

ISO 27001 also requires continued maintenance of the organization's Information Security Management System. Certified organizations must continue monitoring risks, reviewing controls, addressing deficiencies, and improving security practices as their operations and threat environment change. Organizations maintain certification by completing process updates, conducting regular internal audits, passing an annual external audit, and completing a recertification process every three years.

For businesses, this matters because security expectations never stand still. Ongoing certification requirements provide additional assurance that the provider's security program is being regularly reviewed and updated instead of relying on practices that may have been adequate years ago but are no longer sufficient.

How to Evaluate a Secure Destruction Provider

The first step in evaluating a secure destruction vendor is to ask about their certifications. Asking whether they are NAID AAA- and ISO 27001-certified is an excellent place to start.

However, don't stop at asking whether a company is "certified." Ask for proof of certification, what it covers, and whether the documentation supports your organization's security requirements.

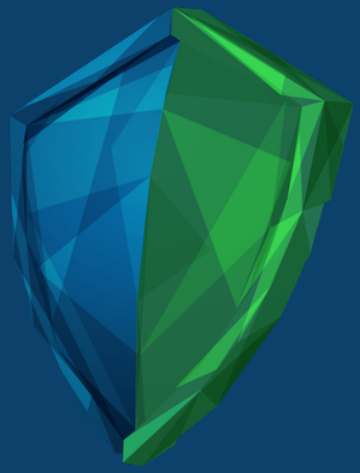
Start by verifying their claims. Don't simply trust a logo on a website; request current certification documentation. Make sure it matches what should be provided. Then, ensure whoever is performing vendor due diligence understands the differences between certifications and what that means for your business's security and compliance.

Lastly, we recommend following this line of questions to the vendor:

- Are you NAID AAA Certified? Are you ISO 27001 certified?
- Can you provide current certification documentation?
- What services and operations fall within the scope of each certification?
- How are employees who handle confidential information screened?
- What security training do employees receive?
- How is material secured during pickup? How is it transported?
- How is custody documented?
- Who has access before destruction?
- How is access to facilities and destruction areas controlled?
- How is confidential material secured while awaiting destruction?
- How are paper records destroyed?
- How are hard drives and electronic media handled?
- Is destruction verified? Do you provide Certificates of Destruction?
- What documentation is available for audits or vendor-security reviews?
- What happens if a security incident occurs?
- How are incidents documented and escalated?
- How are security controls reviewed?
- How frequently are audits conducted?
- How are weaknesses or corrective actions addressed?
- How are we informed should anything change?

The answers your vendor provides to these questions will tell you a lot. If they can answer these questions quickly, accurately, and provide the necessary information, that is a green flag. While it may seem like a hefty line of questioning, it is better than taking your vendor's word for it and hoping for the best.

CI Information Management



Certified Security, Inside and Out

CI Information Management holds both an NAID AAA Certification and an ISO 27001:2022 Certification, demonstrating how we securely destroy information and how we manage information security as a whole. We ensure uncompromising security while adhering to recognized standards for information protection and operational excellence.

For over two decades, CI Information Management has provided secure document shredding and media destruction for businesses throughout the Tri-Cities, Yakima, Wenatchee, and the greater Central Washington and Northeastern Oregon region. With our certified expertise, compliance with state and federal regulations, and commitment to secure information lifecycle management, you can trust us to handle and permanently destroy your confidential business information with the highest level of care and accountability.

Our comprehensive destruction solutions include:

- On-Site Mobile Paper Shredding
- Scheduled Shredding Services
- One-Time Purge Shredding
- Hard Drive and Media Destruction
- Residential Shredding
- Secure Drop-Off Paper Shredding
- Product Destruction

Contact CI Information Management to request our NAID AAA and ISO 27001 documentation, discuss your vendor-security requirements, or request a quote for secure document and media destruction.