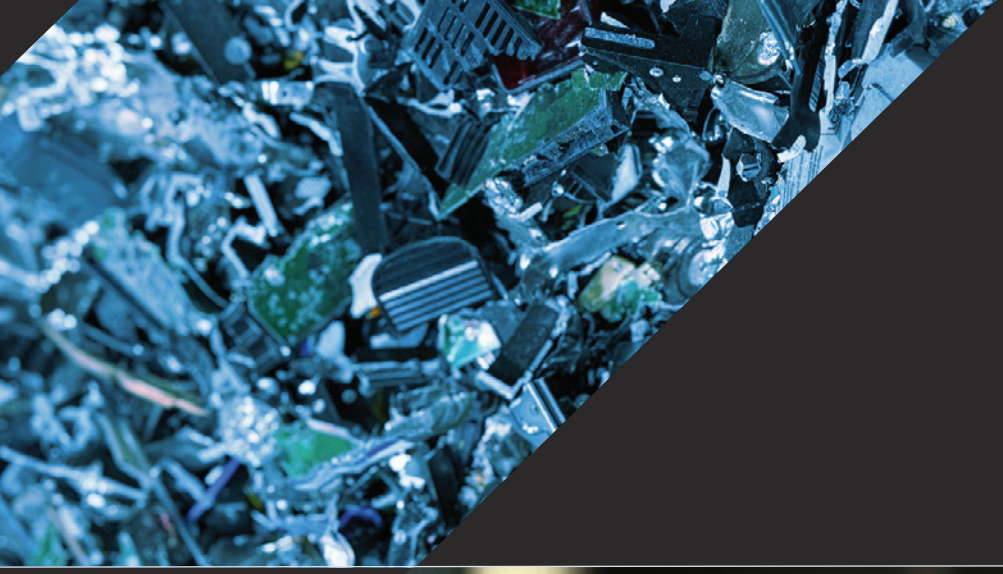


SECURIS
IT Asset Auditing, Recycling & Destruction

From Risk to ROI:

The CIO's Playbook for Secure IT Asset Disposition & Value Recovery

How enterprise IT leaders turn end-of-life hardware into audit-ready security and measurable financial upside

WWW.SECURIS.COM

Chapter One
The CIO's Mandate: Security, Value, and Proof

A Leadership Moment Hidden in the Lifecycle

Every CIO reaches the same crossroads: how to dispose of technology without losing control, value, or credibility.

End-of-life devices don't just carry data; they carry your organization's reputation, compliance standing, and audit trail.

When an asset powers down, its lifecycle isn't over. It enters a phase where risk peaks, oversight blurs, and accountability becomes personal. This is the moment when governance either holds or fractures. The risk is invisible at first. The consequences are not.

CIOs don't just manage systems. They safeguard trust. They are judged not by how they launch technology, but by how they close it out—with precision, proof, and confidence.

CIO Takeaway:
End-of-life is the final stage of leadership accountability. The way you handle end-of-life assets directly affects compliance, reputation, and ROI.

What's at Stake

Focus Area	Security & Compliance	Operational Continuity	Financial Stewardship	Audit Confidence
Why It Matters	One missed data drive can create a multimillion-dollar breach event.	Delays in asset removal stall refresh cycles and impact user productivity.	Every idle day drains resale value.	Without documentation, proof of compliance is opinion, not evidence.

The Cost of Inaction

US $4.88 Million
Average global data breach cost in 2024 (IBM)

1.5% Per Day
Typical depreciation rate for unused enterprise assets (Gartner)

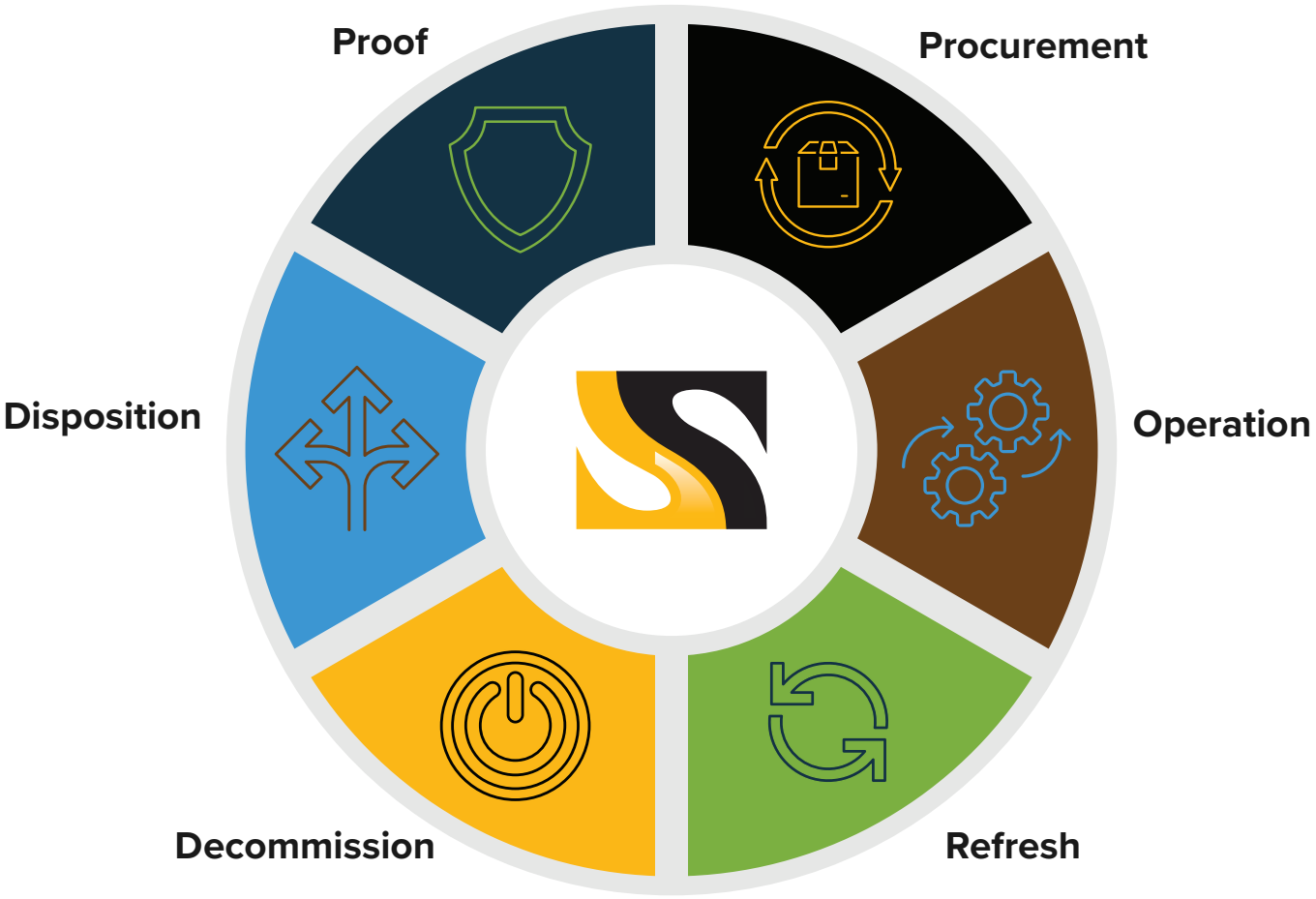
US $17.5 Billion → **US $29.5 Billion**
ITAD market growth 2024–2030 (Strategic Market Research)

82 Million TONNES by 2030
Global e-waste projection (The Business Research Company)

CIO Takeaway:
The faster you reconcile, the more value you protect — and the more confidently you can face an audit.

The Technology Lifecycle, Completed With Proof

Secure ITAD and Value Recovery form the proof point of stewardship. They complete the technology lifecycle with evidence, not assumption.

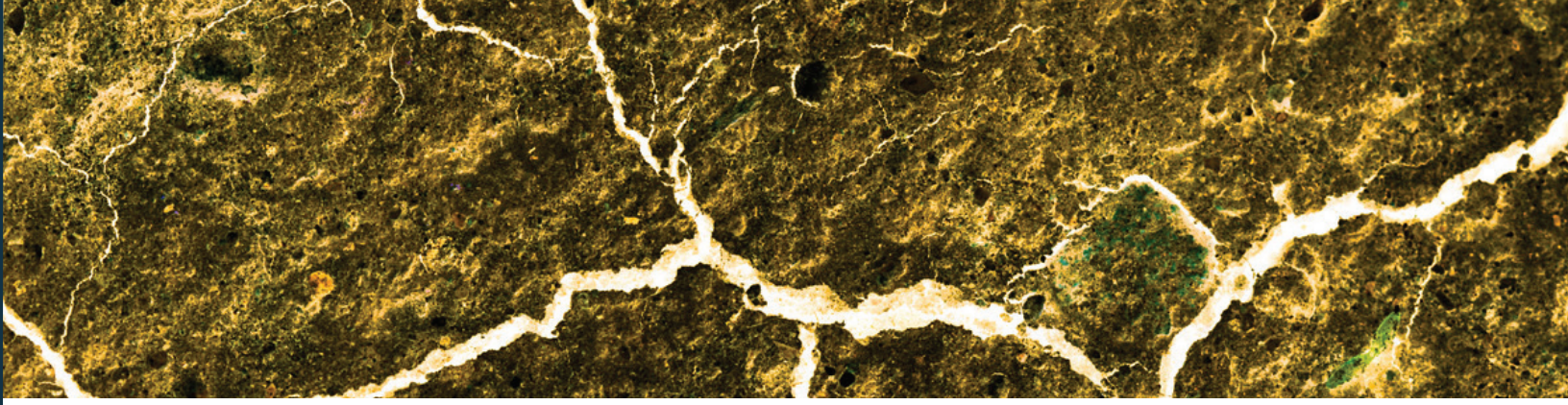


99%+
Accuracy

3-7 Day
Certificates of Destruction

AAA NAID CERTIFIED

R2 V3



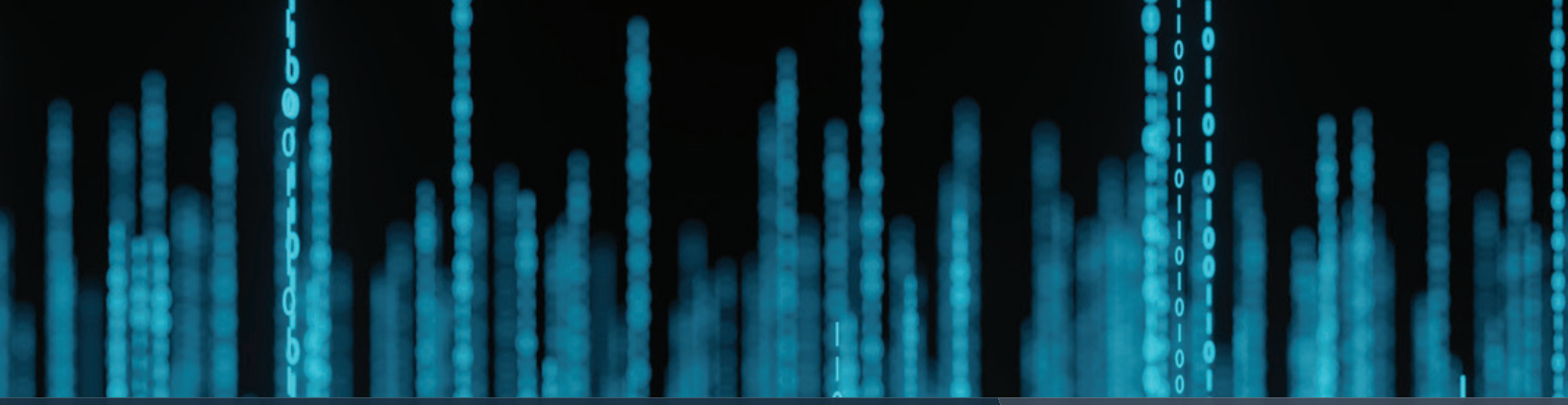
Chapter Two
Where Value Leaks and Risk Spikes

A Leadership Moment Hidden in the Lifecycle

Every enterprise has a blind spot, and for most CIOs, it appears the moment hardware powers down. Decommissioning feels procedural — label, ship, recycle — yet it's the most dangerous stage in the technology lifecycle.

Each drive, server, and mobile device holds fragments of data that can reopen risk long after retirement. A single mislabeled pallet or undocumented handoff can unravel years of careful governance. The danger isn't hypothetical. It accumulates in silence until it surfaces in an audit, an article, or a courtroom.

CIO Takeaway:
Every handoff is a moment of decision. Control it, or risk it.



External Pressure Points

External Factor	Multi-Site Operations	Residual Data on Devices	Third-Party Handoffs	Delayed Resale or Recycling
Impact on the CIO	Greater distance increases custody risk and weakens visibility.	HDDs, SSDs, and MFDs often retain recoverable data despite logical wipes.	Each vendor transition expands the chain of custody and potential failure points.	Idle time erodes value and exposes sensitive information to unnecessary risk.

Internal Tensions That Magnify Risk

Inside the enterprise, responsibility for ITAD is spread across several teams. IT Asset Management tracks serial numbers. Security enforces sanitization and control standards. Finance measures value recovery. Each group operates with good intent, yet often without shared visibility or synchronized workflows.

Fragmentation makes room for quiet failures. Inventory reports drift away from reality. Devices expected to be sanitized are discovered long after they should have been processed. Certificates show up incomplete, late, or in formats that auditors question. These gaps appear small at first. At scale, they grow into operational blind spots that leaders rarely see until something goes wrong.

A single, accountable ITAD partner removes that friction. Unified reporting, unified controls, and unified chain of custody give every team the same source of truth. When one vendor owns the full lifecycle, the gaps between departments close, and the risks that thrive in those gaps never take root.

CIO Takeaway:
Fragmented ownership creates invisible risk.

What Keeps the CIO Up at Night

01

Data Breach

The nightmare scenario. One forgotten drive or server can expose terabytes of confidential information and trigger a multimillion-dollar event.

01

02

Disclosure of Sensitive Information

Customer data, employee records, or trade secrets escaping through unmanaged hardware become front-page news within hours.

02

03

Regulatory Fines and Legal Penalties

Failure to prove compliance with NIST 800-88, HIPAA, GLBA, or state privacy laws can lead to severe financial penalties and mandatory reporting.

03

04

Public Relations Fallout

Loss of control in ITAD can turn into a media crisis overnight, undermining stakeholder trust and investor confidence.

04

05

Corporate Reputation Damage

Even a single incident can undo years of careful brand building and erode long-term credibility with clients and partners.

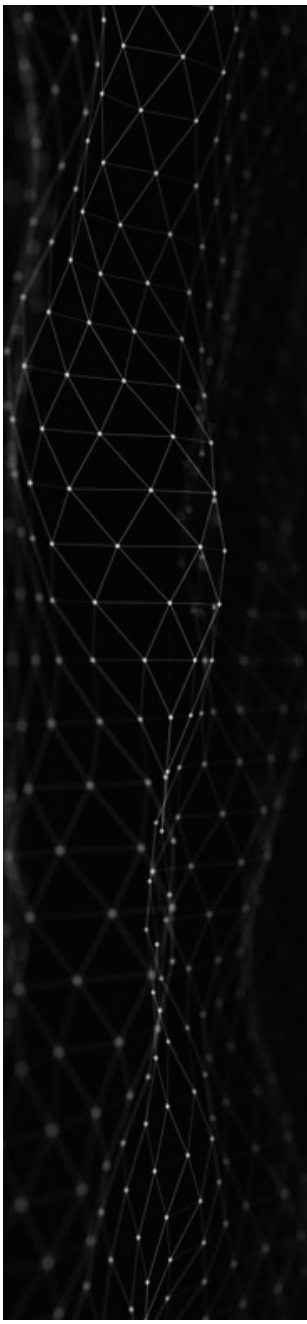
05

06

Personal Accountability

In today's compliance environment, the CIO's name is often on the incident report. Oversight becomes personal when accountability is written into the chain of command.

06



Leadership carries the weight of proof. Every gap in ITAD control is more than a data risk — it's a career-defining event.

Where Value Slips Away

Delays, confusion, and slow reconciliations all erode value recovery. A laptop stored for 30 days can lose nearly 25% its resale potential. Multiply that across thousands of devices and the impact becomes measurable and painful.

Every day of delay also increases the chance that untracked data remnants remain within the network. Speed is not only about efficiency. It's about control, protection, and proof of due diligence.

Philosophy Shift: From Disposal to Discipline

Disposal ends a process. Discipline closes a loop. The difference is visibility.

When CIOs treat ITAD as a control framework rather than a cleanup task, everything changes. Reports reconcile faster. Audits pass cleaner. ESG metrics improve naturally because sustainability and security move in parallel.

Technology leadership is no longer defined by deployment speed. It's defined by how effectively you can document closure.

Governance doesn't fail in the middle of a project. It fails at the end when everyone assumes someone else has proof

Where Value Leaks and Risk Spikes

Risk rises when visibility fades. The CIO's goal is to shorten the distance between power-down and proof.

Chapter Three
The Power of Partnership: Why the Right ITAD Partner Changes Everything

When Expertise Becomes the Difference Between Control and Chaos

CIOs live in a constant balancing act. Budgets contract while expectations expand. Refresh cycles accelerate, yet procurement freezes halt progress. Data regulations multiply faster than teams can update their processes.

Every device retired today represents data that could resurface tomorrow. Every missed pickup, delayed reconciliation, or undocumented transfer is a potential headline, a board meeting, or a breach disclosure waiting to happen.

In this reality, ITAD is not a logistical exercise. It's an act of governance. And the right partner determines whether that act builds confidence or exposes risk.

CIO Takeaway:
Technology leadership isn't just about innovation. It's about knowing who you trust when control is on the line.

The CIO's Reality

You manage distributed teams, global vendors, and an audit calendar that never sleeps. ESG metrics, data privacy standards, and executive optics converge on a single point: your ability to ***prove*** that everything leaving your environment is accounted for and securely destroyed.

You know how fast one oversight can escalate — how a misplaced drive or incomplete certificate can turn into a corporate incident. You also know that 'good enough' is never good enough when accountability has your name on it.

Your world is a sequence of trade-offs: Security versus speed. Compliance versus cost. Proof versus pressure. That tension defines the modern CIO.

You don't need another vendor promising speed. You need a partner who understands the weight of your responsibility — and matches it with the rigor it deserves.

What Trust Looks Like in Practice

Securis delivers the kind of precision that gives CIOs real peace of mind. Our systems, certifications, and AI-driven workflows are designed to remove doubt from every stage of the disposition process. Each credential is a safeguard — proof that security, speed, and accountability can exist together without compromise.

AAA NAID CERTIFIED

Every data destruction process is independently verified for integrity and compliance.

R2 V3

Full traceability and ethical downstream recycling to protect your ESG commitments.

NIST

800-88 Compliant Workflows

Meets or exceeds the highest federal data sanitization standards.

Securis Triple Check Guarantee

Verification at the job site, during physical disassembly, and through system-level validation to catch hidden or missed data-bearing devices.

99%+

Audit-Ready Accuracy

AI-powered asset tracking ensures every drive serial number is validated and documented.

NSA-Approved Shredders and Disintegrators

HDD shredders and NSA/CSS EPL (2021) solid-state disintegrators, validated for high-assurance destruction.

Average

3-7 Day

Closure

Certificates of Destruction and reconciliation reports delivered quickly and reliably.

DriveSnap AI

Pre-destruction photo documentation of each drive or SSD, with AI-driven serial number extraction from device labels to reduce human error and deliver 99.9% accuracy.

120,000+

Positive Feedback Ratings

Long-standing reliability in secure value recovery, demonstrated at scale.

Each one of these standards matters because they eliminate uncertainty. They mean your organization can move fast without losing control. They mean every audit ends with confidence instead of questions. They mean you can prove the integrity of your process any day, at any scale.

CIO Takeaway:

Real expertise replaces assumptions with evidence and turns process into protection.

What Good Looks Like for CIOs

Security

Verified data destruction and compliant handling for all assets.

Speed

Completion of full inventory and CoDs within SLA

Value

Documented recovery percentage of eligible equipment

Proof

Serialized inventory reports, data device, photos, and Certificates of Destruction

Audit-Readiness

Client portal with exportable compliance data on demand

When every box is checked, governance becomes confidence.

Chapter Four
The Plan: A Clear Path to Secure, Accurate, and Valuable ITAD

A strong ITAD plan protects the enterprise on multiple fronts: security, compliance, cost, and operational continuity. This chapter provides a high-level roadmap, something a CIO can hand to their team and know the essentials are covered. The full details, checklists, and technical matrices appear in the Appendix.

A. Physical Security from Decommission to Final Disposition

When an asset powers down, your exposure increases. Physical controls keep risk contained.

1. Stage Assets by Sensitivity

Use three staging tiers based on data classification and device type:

- **Low:** standard user hardware in locked rooms with basic logging.
- **Regulated:** caged storage, sealed bins when required, and camera coverage.
- **High-Sensitivity:** restricted cages, sealed & locked bins, restricted (controlled and monitored) access, and continuous video.

CIO Takeaway:
Staging discipline is the first line of defense.

2. Choose the Correct Destruction Method

Match data classification and device type with the right method:

- Software Purge for resale, aligned with NIST Clear/Purge.
- Shred (1-inch strips) for HDDs and tapes.
- Degauss for magnetic media (can also be combined with shredding for maximum data security).
- Disintegrate (2 mm fragments or smaller) for SSDs and flash media.

CIO Takeaway:
Choose purge to preserve value and destroy to eliminate doubt.

3. Decide on On-Site or Off-Site Destruction

Use on-site destruction for high-sensitivity environments where transport is an added risk. Use off-site destruction for typical corporate assets where sealed custody and portal-visible proof provide sufficient assurance. Hybrid models work best for large or mixed environments.

4. Secure Storage Before Pickup

If assets must wait before pickup, mitigate risk with locked storage, access logs, and tamper-evident measures where appropriate. For low- and moderate-risk devices, a software purge before pickup reduces the impact of potential internal misuse or theft.

CIO Takeaway:
Any device that is not moving should be sanitized or tightly controlled.

Day-0 Checklist

- ☑ **Decommission authorized and logged.**
- ☑ **Assets tagged and matched to CMDB exports.**
- ☑ **Drive counts recorded for hosts and arrays.**
- ☑ **Seals applied where policy requires tamper evidence.**
- ☑ **Chain-of-custody forms completed and signed.**

5. Control Day-0

Day-0 defines audit success. Tag assets, record serials, apply seals where required, and use a formal chain-of-custody process. Validate the identity of transport staff and document the handoff.

6. Reconcile Assets

Export the expected device list from the Configuration Management Database (CMDB). Securis performs an independent inventory audit, reconciles serial numbers and device types, and documents exceptions. DriveSnap AI captures pre-destruction photos of each drive and extracts serials, with all images and metadata archived in the customer portal.

CIO Takeaway:
Reconciliation turns ITAD from a vendor activity into a verifiable control.

B. Physical Security from Decommission to Final Disposition

Governance transforms ITAD from an operational task into an auditable control. Integrate ITAD into policy, CMDB lifecycle management, and reporting structures so that asset disposition is visible within your broader risk and compliance program.

C. Vendor Due Diligence

Vendor selection determines your real-world risk posture. Due diligence should include NAID AAA and R2v3 certification, NIST 800-88 aligned workflows, serialized chain of custody, secure logistics, photographic verification of drives, environmental compliance, and complete reconciliation reporting. It must also account for physical and digital inspection of data-bearing devices, including layered verification processes such as the Securis Triple Check Guarantee, AI-powered data scanning and inventory management

On-Site Visit: Non-Negotiable

- Inspect the facility and its access controls (restricted areas, surveillance, badge systems, visitor protocols).
- Inspect trucks and secure transport procedures (locking mechanisms, GPS tracking, custody handoff).
- Watch shredding and destruction equipment in operation (HDD shredder, SSD disintegrator, degausser, baler, cage complexes).
- Review downstream vendors and environmental handling (R2v3 material flows, recycling paths, no-landfill confirmation).
- See the client portal in action (single sign-on, job status, DriveSnap AI images, reconciliation reports, Certificates of Destruction)

to reduce human error, and rapid job completion to limit exposure and protect value. On-site visits are mandatory before selection. The ITAD Vendor Checklist is located in the appendix.

D. Controls Maturity Model

Four maturity levels define the state of your ITAD program: L1 Ad Hoc, L2 Repeatable, L3 Managed, and L4 Audit-First. Each level increases visibility, reconciliation accuracy, and executive confidence. The maturity ladder visual in the appendix outlines how to move from reactive disposal to audit-first lifecycle closure.

E. Value Recovery Without Compromising Security

Idle assets depreciate rapidly. Faster pickup, reconciliation, and sanitization or destruction reduce exposure and help assets move into resale channels more quickly, thereby improving overall financial return. Finance and IT Asset Management should align on net proceeds KPIs and realistic cycle-time expectations so that speed and security reinforce each other.

Chapter Five
The Decision Point: Turning Insight Into Action

A lifecycle only becomes secure when it becomes intentional. CIOs are not measured by how many devices they deploy. They are measured by how they close them out, how they protect the data, and how they preserve the value locked inside every asset.

You now have a clear view of the risks, the governance gaps, and the opportunities. The next step is the moment where intention becomes action. This chapter brings that decision point into focus.

What the Consultation Call Actually Delivers

A strong ITAD and Secure Value Recovery program begins with clarity. The consultation call is a structured diagnostic designed to provide that clarity in a single conversation.

During the call, your team reviews current decommissioning workflows, staging and storage practices, chain-of-custody controls, destruction requirements, reporting expectations, reconciliation processes, and your objectives for value recovery.

You provide your asset list. Device counts, types, ages, classifications, and locations shape everything that follows. Without this, no vendor can provide an accurate quote or a responsible plan.

Security Requirements You Confirm During the Call

Data destruction is not a single decision. It is a sequence of controlled choices that must align with policy and classification. The consultation call ensures that your requirements are captured and translated into enforceable processes.

You confirm whether software purge is acceptable for resale, whether shred, degauss, or disintegrate is required, whether destruc-

tion must be witnessed, whether on-site destruction is mandatory, whether sealed custody applies, and whether additional audit documentation or dual-control handling is required.

Security Requirements You Confirm During the Call

Idle assets lose value every day. The consultation call helps you understand how timing, security controls, and internal workflows shape your overall financial return.

The discussion focuses on how pickup and reconciliation delays slow value recovery, how sanitization choices affect resale readiness, how industry benchmarks guide expectation setting, and how to streamline your process so assets reach resale channels faster.

CIO Takeaway:
Stronger control and faster cycles lead to better financial outcomes.

Schedule your Audit-Ready ITAD and Secure Value Recovery Consultation Call. In one discussion, you will understand your current risk posture, ITAD maturity level, destruction requirements, potential value recovery improvements, audit readiness, and next steps for lifecycle closure.

CIO Takeaway:
Leadership protects value. Action protects reputation.

Your Next Move: Secure. Documented. Valuable.

One roadmap. One asset list. Complete clarity.

Schedule Your Consultation Call. 866.416.3069

Chapter Six
Snapshots of Success and Failure: Proof That Process Matters

Every CIO carries the same concern: the hidden risk no one sees until it becomes a crisis. In IT Asset Disposition, success is quiet. Failure becomes a headline. This chapter shows both sides — the wins that prevent disasters and the real-world failures that prove why governance matters.

Success Story 1: Financial Services — The 86 Drives Nobody Knew Existed

Securis was hired to perform on-site shredding for a financial services company disposing of eight server cabinets. The client assured us that all storage devices had been removed. They had not.

Securis identified 86 drives still installed through its Triple Check Guarantee, which requires physical inspection of every unit. The drives included 72 SSDs and 14 HDDs, all containing sensitive financial data that had been previously marked as "removed." These 86 drives represented 15 percent of the total drives the company believed were already accounted for.

Securis removed, verified, and shredded every drive on-site, fully documented with DriveSnap AI photos and Certificates of Destruction.

Success Story 2: Telecom Provider — The 30 Drives Still in the Chassis

A telecom company sent 300 servers to Securis for destruction, stating that all drives had been removed. Through the Securis Triple Check Guarantee, which requires physical inspection of every unit, technicians identified 30 drives still installed in the equipment. Each drive contained sensitive operational data.

Securis opened each chassis, removed the drives, documented serials with DriveSnap AI, and performed compliant destruction. Each exception was logged and attached to the final reconciliation report.

CIO Takeaway:
Verification protects you from inherited assumptions and upstream errors.

Failure Example 1: Morgan Stanley — Vendor Mismanagement Becomes a Regulatory Event

In 2020, Morgan Stanley disclosed that a third-party vendor failed to properly sanitize and dispose of retired hardware. Devices were later found with unencrypted customer data still present. The Office of the Comptroller of the Currency issued a $60 million civil penalty for deficient oversight and vendor management.

Control That Prevents It: Physical inspection of every device, serialized chain of custody, verified downstream controls, and documented proof through reconciliation and Certificates of Destruction.

Source: OCC Consent Order & Ncontracts summary

Failure Example 2: HealthReach — Improper Drive Disposal Exposes PHI

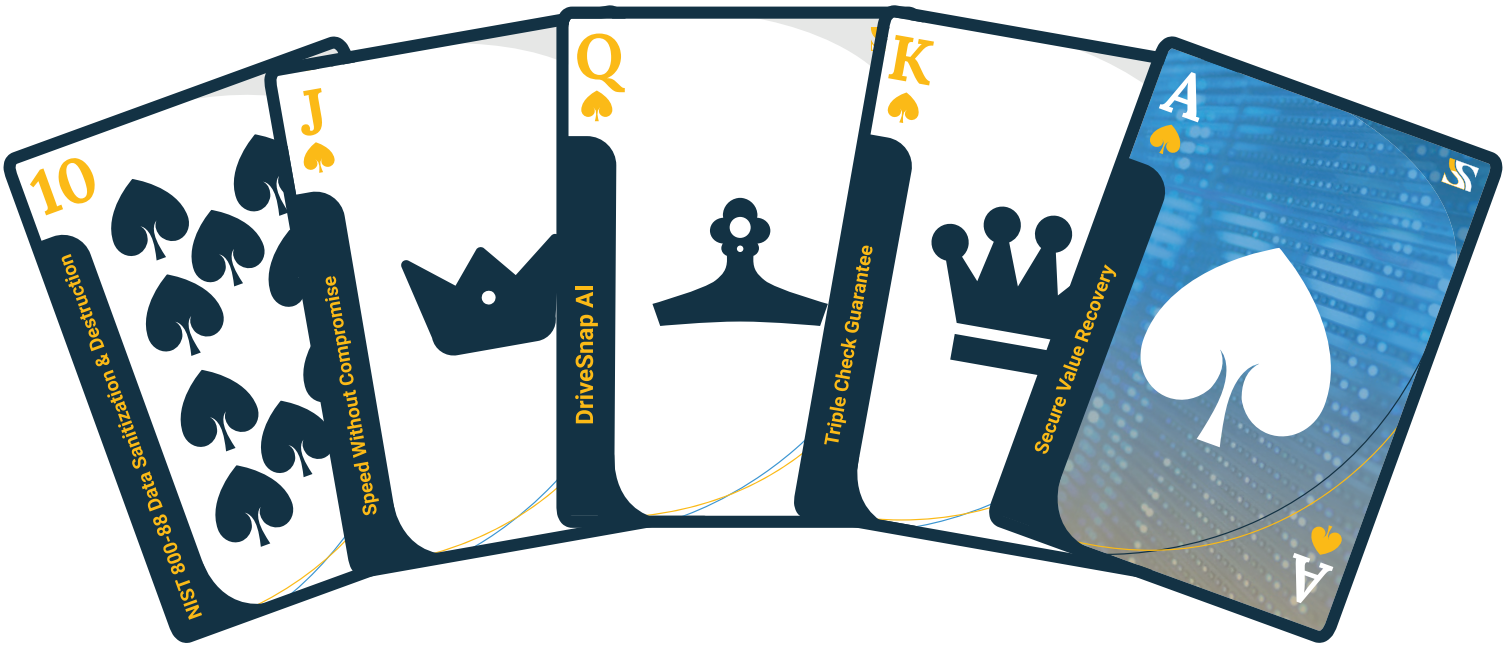
In 2023, HealthReach reported a data breach after improperly disposed hard drives were discovered at a recycling facility. The drives contained protected health information for more than 15,000 patients, triggering regulatory notifications, reputational damage, and legal exposure.

Under Securis' process, this outcome would have been prevented. The Triple Check Guarantee requires physical inspection to locate hidden or missed drives before equipment leaves controlled custody. Drives identified as data-bearing are isolated, documented, and destroyed using approved methods. Certificates of Destruction and reconciliation reporting provide verifiable proof that no device exits the process without resolution.

Control That Prevents It: Mandatory physical inspection, controlled handling of data-bearing devices, compliant destruction, and documented proof through reconciliation and Certificates of Destruction.

Source: BitRaser breach coverage

The Securis Royal Flush



Hold the winning hand in secure, accurate, and compliant ITAD.

SECURIS
IT Asset Auditing, Recycling & Destruction

Make the Winning Move

You have everything you need.

The risks are clear, the path is defined, and the advantage is yours.

Strong IT leaders do not wait for a breach, an audit finding, or a story in the news.

They make the move that protects their organization and closes the lifecycle with certainty.

Securis is ready to help you finish strong.

One call puts your ITAD program on the path to secure, accurate, and fully documented closure.

Make the winning move.
Call Securis. (866) 416-3069 | Securis.com

NORTHERN VIRGINIA HEADQUARTERS
3900 STONECROFT BLVD. SUITE F, CHANTILLY, VA 20151
(866) 416-3069 | info@securis.com