



**THINK
YOUR
IT ASSET
DISPOSITION
PROCESS IS
SECURE?**

PROVE IT.

PROVE IT.



HOW TO USE THIS SCORECARD

Benchmark the program you operate today, not the process you intend to build. For each of the 14 practices, select the description that most closely reflects your current environment and validate the choice with evidence.

3

CONTROLLED

Repeatable, documented, measurable, and audit ready.

2

INCONSISTENT

Partially defined, but variable across teams, sites, or events.

1

EXPOSURE

Uncontrolled, undocumented, or unable to produce evidence.

SCORING RULES

- Choose the lowest defensible score. If a process is strong in one location but weak in another, score the enterprise-wide reality.
- Evidence wins. If your team or vendor cannot produce the document, report, certificate, or system record, do not assume the control exists.
- Do not average away critical risk. A score of 1 in tracking, chain of custody, reconciliation, or data security should be treated as an immediate priority.
- Add the 14 scores. The maximum is 42 and the minimum is 14. Use the maturity bands at the end of the guide to prioritize next steps.



A BENCHMARK BUILT FROM REAL PROGRAM OPERATIONS

The practices in this guide reflect the controls, evidence, and operating discipline required to manage enterprise asset disposition at scale. The following FY25 figures were supplied by Green4Good IT Lifecycle Solutions for this scorecard.

90+ CUSTOMERS SUPPORTED

150K ASSETS PROCESSED

96% OF LAPTOPS REPURPOSED

\$6.75M RETURNED TO CUSTOMERS

24K CARBON CREDITS ISSUED

887K LBS OF E-WASTE DIVERTED

This benchmark is grounded in the same operating discipline Green4Good IT Lifecycle Solutions applies across enterprise ITAD programs. These processes align with recognized controls, including R2v3, ISO, and NIST-aligned data sanitization, with proactive updates and defined response targets throughout every engagement.



PROGRAM GOVERNANCE & OPERATING MODEL

Mature ITAD is a managed business process, not a disposal event. Clear ownership, documented workflows, service expectations, and regular reviews make the program repeatable across locations, teams, and vendors.

EVIDENCE TO LOOK FOR

- Approved ITAD policy
- Signed SOW and documented SOPs
- Response-time and escalation targets
- Exception log and closure process
- QBR records and KPI dashboard

BENCHMARK QUESTION

Could the program run consistently tomorrow if the people who know it best were unavailable?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Enterprise policy defines scope, roles, approvals, and exception handling.
- Signed SOWs, SOPs, and SLAs standardize every handoff.
- Proactive updates, QBRs, KPIs, and escalation paths are built into delivery.

2

INCONSISTENT

PARTIAL & VARIABLE

- Core steps exist, but vary by site, team, or vendor contact.
- Ownership and escalation are understood informally rather than documented.
- Communication becomes reactive when volume or exceptions increase.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Disposition is handled ad hoc with no single process owner.
- Requirements live in inboxes, spreadsheets, or individual knowledge.
- Scope, service levels, and accountability are undefined.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



INTERNAL ASSET TRACKING

Chain of custody starts inside your organization, not with your vendor. A current, centralized record of every asset creates accountability from active use through retirement, collection, processing, and final disposition.

EVIDENCE TO LOOK FOR

- Serial-level inventory export
- Named system of record and owner
- Retirement queue and aging report
- Asset transfer history
- Storage location and custodian records

BENCHMARK QUESTION

Can you produce a current list of every device awaiting disposition, including owner, location, and status, in minutes?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Real-time, centralized inventory is integrated with ITAM systems.
- Serial number, owner, location, status, and retirement date are maintained.
- Transfers and status changes are timestamped.

2

INCONSISTENT

PARTIAL & VARIABLE

- Tracking covers some asset groups, locations, or lifecycle stages only.
- Updates are delayed and manual reconciliation is required.
- Multiple sources of truth create ownership and status conflicts.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Spreadsheets or no formal inventory are used.
- The organization cannot confirm where retired devices are stored.
- Assets can leave active service without a traceable disposition record.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



LIFECYCLE MANAGEMENT

Planned retirement protects performance and security while preserving residual value. Mature programs set refresh standards by asset type, forecast trade-ins, and coordinate disposition before devices age beyond their strongest resale window.

EVIDENCE TO LOOK FOR

- Lifecycle policy by asset class
- 12-24 month refresh forecast
- Warranty and repair-cost data
- Residual-value assumptions
- Trade-in calendar linked to procurement

BENCHMARK QUESTION

Is disposition planned when assets are acquired, or only when a storage room becomes a problem?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Policy-based refresh cycles are defined by asset type, typically 3-4 years for end-user devices.
- Annual forecasts align warranty, repair history, budgets, and residual value.
- The ITAD partner supports trade-in planning before each refresh wave.

2

INCONSISTENT

PARTIAL & VARIABLE

- Refresh timing varies by department, budget, or asset condition.
- Devices commonly remain in service for 4-7 years without a consistent rationale.
- Forecasts are incomplete and disposition planning begins late.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Devices are run to failure or cleared only when storage is full.
- No lifecycle forecast or residual-value strategy exists.
- Aging assets create rising repair costs, support risk, and value loss.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



VENDOR SELECTION

The right ITAD partner must prove security, compliance, operational discipline, environmental responsibility, and value recovery. Vendor selection should test the entire operating model, not simply compare pickup fees.

EVIDENCE TO LOOK FOR

- RFP scoring matrix and references
- Insurance and audit rights
- Downstream vendor transparency
- Pricing, fee, and credit schedule
- Signed SOW and service levels

BENCHMARK QUESTION

Can your provider explain exactly how and where each asset category is processed, sold, reused, or recycled?

3

CONTROLLED

REPEATABLE & AUDIT READY

- A structured RFP evaluates certifications, controls, service capability, reporting, and resale outcomes.
- Commercial terms are transparent, with clear fees, credits, and audit rights.
- A signed SOW defines scope, responsibilities, timelines, and exceptions.

2

INCONSISTENT

PARTIAL & VARIABLE

- Due diligence is limited or focused on only one area, such as security or price.
- The incumbent is retained without regular market benchmarking.
- Downstream processes and value recovery are only partially understood.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Selection is based on free pickup or lowest cost alone.
- There is no proof of processing quality, downstream controls, or financial transparency.
- The relationship operates without defined scope or service expectations.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



CERTIFICATIONS

Certifications provide independent validation that a provider follows defined, audited controls. Names and logos are not enough: the scope, facility address, legal entity, and current status must match the operation handling your assets.

EVIDENCE TO LOOK FOR

- Current certificate and expiration date
- Scope statement and facility address
- Legal entity match
- Most recent audit or attestation
- Downstream qualification process

BENCHMARK QUESTION

Are the certifications held by the exact facility and legal entity that will receive and process your assets?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Current certifications match the service scope and processing location.
- Relevant standards may include R2v3, e-Stewards, NAID AAA, ISO 27001, and ISO 9001.
- Audit findings and corrective actions are actively managed.

2

INCONSISTENT

PARTIAL & VARIABLE

- Only a limited certification set is held or evidence is difficult to validate.
- A downstream partner is certified, but the primary handling facility is not.
- Certificates may be current, but their scope does not cover all services.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- No recognized certifications are held or proof is unavailable.
- The provider relies on self-attestation rather than independent audits.
- Downstream partner qualification is undocumented.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



LOGISTICS & CHAIN OF CUSTODY

Security begins at collection. Mature logistics preserve a documented chain of custody from the customer site through transport and receipt, with stronger controls for data-bearing devices that are not encrypted.

EVIDENCE TO LOOK FOR

- Pre-pickup serial manifest
- Bill of lading and pickup record
- Seal or lock identifier
- Driver, time, and transfer signatures
- Exception and loss escalation log

BENCHMARK QUESTION

Who has custody of each device at every moment from the employee desk to the processing floor?

3

CONTROLLED

REPEATABLE & AUDIT READY

- A customer-validated, serial-level asset list is prepared before pickup.
- Every handoff, time, location, count, and custodian is documented.
- Non-encrypted data-bearing devices use dedicated locked or sealed transport, with the seal ID verified at receipt.

2

INCONSISTENT

PARTIAL & VARIABLE

- Counts are captured, but serials, handoffs, or pickup documents are incomplete.
- Courier collection is used without confirmed encryption, MDM, or clear exception controls.
- Shared transport is used without a validated lock or tamper-evident seal process.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Bulk pickup occurs with no asset-level visibility.
- Non-encrypted devices move in non-dedicated or unsecured loads.
- There is no defensible record of who had custody at each stage.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



ASSET RECONCILIATION

Reconciliation proves that the assets expected to move are the assets that arrived and were processed. A formal receiving audit exposes missing, extra, or mismatched devices before the event is closed.

EVIDENCE TO LOOK FOR

- Expected vs. received report
- Serial-level match status
- Discrepancy owner and SLA
- Investigation and resolution notes
- Final closure approval

BENCHMARK QUESTION

How quickly would you know that a device listed for pickup never arrived at the processing facility?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Expected, collected, received, and processed assets are compared at serial level.
- Discrepancies are investigated, communicated, and resolved within a defined SLA.
- The event remains open until reconciliation and customer signoffs are complete.

2

PARTIAL & VARIABLE

- A receiving list is supplied, but comparison to the customer manifest is limited.
- Exceptions are noted without a clear owner, timeline, or resolution record.
- Reports arrive late and require manual investigation.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- No customer asset list is provided before collection.
- No formal receiving audit or discrepancy process exists.
- The only confirmation is a quantity, weight, or pickup receipt.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



PORTAL & TECHNOLOGY

A mature portal becomes the central system of record for the ITAD program. It gives authorized users direct, audit-ready access to collection activity, asset status, certificates, reports, and historical evidence.

EVIDENCE TO LOOK FOR

- Role-based access controls
- Collection and shipment status
- Asset-level search and date filters
- Certificate retrieval and exports
- User and change audit logs

BENCHMARK QUESTION

Can an auditor retrieve proof for one serial number without emailing your vendor or searching multiple folders?

3

CONTROLLED

REPEATABLE & AUDIT READY

- A secure self-service portal supports collection requests and live status tracking.
- Users can retrieve receiving audits, wipe or destruction certificates, and asset-level details.
- Search, filters, exports, audit logs, and role-based access support internal reviews.

2

INCONSISTENT

PARTIAL & VARIABLE

- Static spreadsheets or PDFs are delivered by email.
- Reports require ad hoc requests and cannot be searched at asset level.
- Historical data is available, but slow to retrieve or difficult to validate.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- No portal or reliable system of record exists.
- Program evidence is scattered across inboxes and shared drives.
- Status, certificates, and final outcomes cannot be accessed on demand.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



Of the millions of enterprises across North America, only a fraction can account for every retired device.





DATA SECURITY

Secure disposition requires a standardized, validated, and auditable process for every data-bearing asset. Mature programs align sanitization decisions with recognized guidance and preserve evidence at the asset level.

EVIDENCE TO LOOK FOR

- Sanitization decision tree
- Tool, method, and result log
- Serial-linked certificate
- Failure and exception procedure
- Physical destruction evidence when required

BENCHMARK QUESTION

What happens, and what proof is produced, when a drive cannot be wiped successfully?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Processes align with NIST 800-88 Clear, Purge, or Destroy methods as appropriate.
- Results are verified and certificates are tied to serial numbers.
- Failures, locked devices, damaged media, and destruction exceptions follow a documented escalation path.

2

INCONSISTENT

PARTIAL & VARIABLE

- Basic wiping is performed, but validation or quality checks are limited.
- Certificates may be batch-level rather than asset-level.
- Exception handling varies by technician, device, or facility.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- No defined sanitization or destruction standard exists.
- There is no reliable evidence that data was removed.
- Data-bearing assets are handled like ordinary scrap.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



SOFTWARE INTEGRATION

Integration connects ITAD to the systems where asset decisions already happen. Linking ServiceNow, ITAM, or CMDB workflows reduces manual effort, improves reconciliation, and keeps status data current across teams.

EVIDENCE TO LOOK FOR

- System and field mapping
- Unique asset identifier strategy
- Sync frequency and ownership
- Error and exception handling
- Access and change controls

BENCHMARK QUESTION

How many manual touches are required to move one device from retired to reconciled and finally disposed?

3

CONTROLLED

REPEATABLE & AUDIT READY

- ITAD data integrates with customer's ITAM software (CMDB), like ServiceNow through automated exchange.
- Asset status, identifiers, and disposition outcomes sync on a defined cadence.
- Data ownership, mapping, and exception handling are documented.

2

INCONSISTENT

PARTIAL & VARIABLE

- Teams exchange flat files, manual uploads, or emailed exports.
- Updates are delayed and duplicate or mismatched records are common.
- Integration depends on individual effort rather than a controlled workflow.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Internal and vendor records are isolated with no repeatable exchange.
- Disposition status is updated manually, if at all.
- There is no end-to-end view from retirement through final outcome.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



REPORTING & COMPLIANCE

Reporting is the evidence layer of the program. Mature reporting confirms what happened to every asset, supports audit and compliance needs, and connects operational, financial, security, and sustainability outcomes.

EVIDENCE TO LOOK FOR

- Serialized asset disposition status with date
- Chain-of-custody record
- Wipe or destruction certificate
- Fees, proceeds, and settlement
- ESG metrics and retention policy

BENCHMARK QUESTION

Could you answer an audit request today without assembling evidence from multiple people, systems, and inboxes?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Asset-level final disposition, chain-of-custody, and sanitization evidence are complete.
- Financial and ESG metrics are included with consistent definitions and retention.
- Reports are customizable, timely, and ready for internal or external audit.

2

INCONSISTENT

PARTIAL & VARIABLE

- Summary reports are available, but asset-level detail or required fields are missing.
- Teams manually combine documents from different systems and vendors.
- Evidence is produced, but timing and format vary by event.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- No defensible documentation exists beyond invoices, weight tickets, or pickup receipts.
- Final disposition and data-destruction outcomes cannot be verified.
- Audit requests trigger a manual search for incomplete evidence.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



RECYCLING & SUSTAINABILITY

A mature ITAD program follows the highest-value circular outcome available: reuse first, then resale or donation, followed by certified recycling. Results should be measurable and usable in ESG and sustainability reporting.

EVIDENCE TO LOOK FOR

- Reuse and repurpose rate
- Resale, donation, and recycling outcomes
- Material weights and diversion rate
- Carbon credit methodology and certificate
- Downstream recycler documentation

BENCHMARK QUESTION

What percentage of your equipment is reused before recycling is considered, and can the result be proven?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Reuse and repurposing are prioritized before recycling.
- Certified downstream recycling and zero-landfill goals are supported by evidence.
- Landfill diversion, weights, reuse rates, and verified carbon credits are reported.

2

INCONSISTENT

PARTIAL & VARIABLE

- Some recycling and diversion metrics are provided, but reuse is not optimized.
- Environmental data is aggregated, delayed, or difficult to verify.
- The program supports sustainability goals inconsistently across locations.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- The model is disposal-focused with little visibility into downstream outcomes.
- Reusable assets are treated as scrap.
- Environmental claims are unsupported or absent.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



REMARKETING & VALUE RECOVERY

Residual value depends on timing, condition, market reach, and how close the provider is to the end buyer. Mature programs treat remarketing as a managed revenue channel rather than an afterthought.

EVIDENCE TO LOOK FOR

- Mixed remarketing channels
- Transparent condition grading criteria
- Quick receipt to sale timelines
- Settlement reporting

BENCHMARK QUESTION

How much value is lost because assets are sold late, graded inconsistently, or passed through too many intermediaries?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Condition grading, market timing, and multiple resale channels maximize return.
- The provider can explain the percentage sold to end users versus brokers.
- Fees, prices, credits, and settlement timing are transparent at asset or category level.

2

INCONSISTENT

PARTIAL & VARIABLE

- Resale channels are limited or heavily broker-dependent.
- Grading and pricing are inconsistent, blended, or difficult to benchmark.
- Settlement is delayed and lifecycle forecasts do not include expected returns.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- Assets are scrapped by default or sold without a defined resale strategy.
- No market evidence or transparent customer credit is provided.
- Devices are held until residual value has materially declined.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



VENDOR VALUES & ESG ALIGNMENT

A long-term ITAD partner should reinforce the organization's values, not create hidden ESG risk. Mature alignment is demonstrated through transparent downstream practices, circular outcomes, community impact, and evidence-backed claims.

EVIDENCE TO LOOK FOR

- Published policies and measurable goals
- Proof behind environmental claims
- Community impact or donation options
- Contracted reporting commitments
- Alignment review during QBRs

BENCHMARK QUESTION

Can the provider prove its ESG claims at asset level and translate outcomes into metrics your organization can use?

3

CONTROLLED

REPEATABLE & AUDIT READY

- Vendor policies and operating practices align with customer ESG priorities.
- Circular economy, community impact, donation, and carbon-credit options are measurable.
- Sustainability commitments and reporting requirements are embedded in the relationship.

2

INCONSISTENT

PARTIAL & VARIABLE

- The provider expresses sustainability values, but reporting and delivery are limited.
- Programs vary by location or rely on broad corporate claims.
- Customer ESG requirements are discussed but not consistently documented.

1

EXPOSURE DETECTED

UNCONTROLLED & HIGH RISK

- There is no sustainability focus or values alignment.
- Downstream outcomes are opaque and claims cannot be substantiated.
- The vendor cannot support the customer's ESG reporting needs.

YOUR SCORE

1

Exposure

2

Inconsistent

3

Controlled



BUILD YOUR ITAD MATURITY PROFILE

Record one score for each practice. Use the notes line to capture the evidence you reviewed or the first improvement you need to make.

01 PROGRAM GOVERNANCE & OPERATING MODEL

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

02 INTERNAL ASSET TRACKING

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

03 LIFECYCLE MANAGEMENT

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

04 VENDOR SELECTION

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

05 CERTIFICATIONS

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

06 LOGISTICS & CHAIN OF CUSTODY

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

07 ASSET RECONCILIATION

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

08 PORTAL & TECHNOLOGY

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

09 DATA SECURITY

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

10 SOFTWARE INTEGRATION

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

11 REPORTING & COMPLIANCE

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

12 RECYCLING & SUSTAINABILITY

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

13 REMARKETING & VALUE RECOVERY

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

14 VENDOR VALUES & ESG ALIGNMENT

Evidence / priority: _____

☐ 1 ☐ 2 ☐ 3

TOTAL SCORE

_____ / 42

14-23
EXPOSURE

24-34
INCONSISTENT

35-42
CONTROLLED



WHAT YOUR SCORE SAYS ABOUT THE PROGRAM

Your total shows the overall operating model. Your lowest individual scores reveal where the next incident, audit issue, financial loss, or reporting gap is most likely to occur.

35-42

CONTROLLED

STRONG, REPEATABLE, AND AUDIT READY.

- Automate remaining manual handoffs and exception workflows.
- Improve reporting speed, resale velocity, and forecasting accuracy.
- Use financial and ESG outcomes in executive reporting and procurement planning.

24-34

INCONSISTENT

CAPABLE, BUT VARIABLE ACROSS TEAMS.

- Standardize the operating model and evidence requirements.
- Fix the lowest-scoring handoffs before adding new technology.
- Formalize vendor SLAs, reporting fields, and reconciliation timelines.

14-23

**EXPOSURE
DETECTED**

MATERIAL CONTROLS/EVIDENCE MISSING.

- Stop untracked asset movement and establish a verified inventory.
- Require secure custody, receiving reconciliation, and sanitization proof.
- Reassess vendor scope, certifications, and downstream transparency before the next event.

CRITICAL RISK OVERRIDE

Any score of 1 in Asset Tracking, Chain of Custody, Asset Reconciliation, or Data Security requires immediate action, regardless of the total score.



TURN THE SCORE INTO A 90-DAY ACTION PLAN

Start with visibility and control, then improve automation, value recovery, and reporting. The sequence matters: technology cannot compensate for an undefined process.

DAYS
0-30

SEE IT

- Map the current process, owners, vendors, locations, and storage points.
- Create a verified baseline of assets awaiting disposition.
- Collect contracts, certifications, reports, and security evidence.
- Pause or escalate any movement that cannot be tracked and reconciled.

DAYS
31-60

CONTROL IT

- Approve a RACI, policy, SOP, SOW, and service-level expectations.
- Require pre-pickup manifests, secure logistics, and receiving audits.
- Standardize NIST-aligned sanitization and exception evidence.
- Define the minimum asset-level report and certificate package.

DAYS
61-90

OPTIMIZE IT

- Connect portal and ITAM or ServiceNow workflows where practical.
- Build lifecycle, residual-value, and refresh forecasts.
- Track resale, reuse, recycling, carbon, and customer-return metrics.
- Launch a recurring QBR with KPI trends and improvement actions.

BY DAY 90, AIM TO HAVE

An approved operating model, a vendor evidence pack, a complete baseline score, a prioritized remediation backlog, and an executive view of security, financial, and ESG outcomes.



CAN YOU ACCOUNT FOR EVERY RETIRED DEVICE?

Green4Good IT Lifecycle Solutions can benchmark your current ITAD process against the 14 practices in this guide, identify exposure, and map a practical path toward a controlled, auditable program.

A MATURITY REVIEW CAN INCLUDE

- Stakeholder and workflow review
- Sample evidence and report assessment
- 14-practice maturity benchmark
- Prioritized 90-day improvement roadmap

REQUEST AN ITAD MATURITY REVIEW

Talk to Green4Good about a personalized benchmark for your enterprise.



This scorecard is a directional benchmark, not a formal compliance audit. Requirements vary by jurisdiction, asset type, risk profile, and contractual scope.

1. What “Mature ITAD” Means

A mature ITAD program includes full lifecycle control, documented processes, certified data destruction, and measurable outcomes in security, compliance, and sustainability

2. Internal Asset Tracking

“Chain-of-custody starts inside your organization, not with your vendor.”

A strong internal asset tracking capability is critical to ITAD because it ensures complete visibility and accountability of every asset from active use through final disposition, enabling secure chain-of-custody, verifiable data destruction, and audit ready compliance.

Good: Real-time centralized asset tracking integrated with ITAM/CMDB systems.

Bad: Partial tracking, inconsistent updates.

Ugly: Spreadsheet-based or no inventory.

3. Lifecycle Management

Strong lifecycle management is critical to ITAD because it ensures end user devices are retired within the optimal three to four year window, which typically aligns with OEM and supplier warranty periods, allowing organizations to avoid declining performance, rising repair costs, and support risks, while still capturing maximum residual value before devices rapidly depreciate and lose remarketing potential.

Strong Lifecycle management enables more accurate forecasting and lifecycle planning. Organizations can recover meaningful residual value during refresh cycles, helping to offset new hardware acquisition costs and reduce total cost of ownership. In a mature model, the ITAD partner works collaboratively with the client to build annual trade in forecasts, creating predictable financial inputs that support budgeting, procurement strategy, and long term planning.

Are you having these proactive conversations with your ITAD supplier ?

Good: Defined lifecycle from procurement to disposal with planned refresh cycles. 3-4 years

Bad: Inconsistent lifecycle processes. 4-7 years

Ugly: Reactive disposal with no lifecycle planning.

4. Vendor Selection

Vendor selection is a critical component of a mature ITAD process because it enables organizations to thoroughly evaluate a partner's capabilities, certifications, and operational processes, ensuring they can deliver not only secure and compliant asset disposition, but also maximize both financial return and environmental outcomes.

Free is not always better in ITAD, because it often means you are missing out on transparency, process quality, and value recovery. Many of our current customers come from providers that either charge for services or offer "free" models that lack true optimization, but a properly structured ITAD program should deliver credits back to the customer. While fees may apply depending on asset mix, location, and service requirements, the expectation should be a net positive outcome, and in many cases organizations can achieve a revenue generating program annually when assets are managed and remarketed effectively.

Vendor selection provides valuable insight into the broader market, enabling organizations to benchmark capabilities and identify leading practices. Even when a preferred vendor is established, this visibility allows organizations to drive continuous improvement by requesting the adoption of new processes or services that enhance program performance.

Documented workflows and SOPs to ensure customer requests are handled consistently rather than on an ad hoc basis

Good: Structured RFP process with certifications, auditability, and transparency.

Bad: Limited due diligence.

Ugly: Selection based only on cost.

5. Certifications

ITAD certifications provide independent validation that a vendor operates in a secure, compliant, and environmentally responsible manner. Without certifications, organizations are relying on trust rather than proven, audited processes, which increases risk.

Certified ITAD providers are required to follow defined processes, undergo regular audits, and demonstrate continuous compliance with industry best practices across data security, environmental handling, and downstream vendor management.

Key certifications include R2v3, e-Stewards, NAID AAA, ISO 27001.

Good: Vendors hold multiple certifications.

Bad: Limited certifications.

Ugly: No certifications.

6. Logistics & Chain of Custody

Security in ITAD does not begin in the warehouse or configuration centre, it begins at collection. Organizations should critically assess how their vendor protects assets during pickup and transport, including whether there is a documented chain of custody, asset level tracking, and controls to prevent loss or tampering. Without these, risk is introduced before processing even begins. Courier solutions are a great way to collect small quantities or remote users assets, but you should confirm that devices have encryption, like BitLocker, Intune, ABM/MDM.

In a mature lifecycle management program, customers maintain a pre-defined list of assets prior to each collection event. This serves as the foundation for accurate reconciliation, ensuring all devices are tracked, received, and processed as expected.

For data bearing / non-encrypted devices, trucks should be dedicated and locked or sealed with a tamper proof logistics seal. The seal number should be noted on the onsite paperwork left behind with the customers site contact and verified at the time of delivery.

Good: End to end serialized tracking with complete chain of custody documentation. Standardized pickup documentation captures asset counts by type at the time of collection. A customer validated asset list at the serial number level is prepared in advance of pickup, forming the basis for accurate reconciliation and auditability.

For data bearing / non-encrypted devices, trucks should be dedicated and locked or sealed with a tamper proof logistics seal. The seal number should be noted on the onsite paperwork left behind with the customers site contact and verified at the time of delivery.

Bad: Inconsistent tracking with gaps in chain of custody documentation. Asset lists are not established prior to collection, and pickup documentation is either incomplete or not provided, limiting visibility and hindering accurate reconciliation. No seal or lock.

Ugly: Bulk pickup with no visibility. Non-dedicated transfer for data bearing (non-encrypted) devices.

7. Asset Reconciliation

Asset reconciliation is a foundational component of a mature ITAD program. Upon delivery, the ITAD provider should conduct a formal receiving audit, validating collected assets against the customer's documented inventory. Any discrepancies are identified, investigated, and communicated, ensuring transparency, accountability, and audit readiness.

Good: Full reporting of collected vs processed assets with a receiving audit.

Bad: Just sending a receiving list.

Ugly: No asset list provided, this is common with free ITAD solution providers.

8. Portal & Technology

ITAD portals are a key component of a mature service offering. A well designed portal provides customers with full visibility and control across the ITAD lifecycle. At a minimum, an effective ITAD portal should enable customers to:

- Request and monitor scheduled collection events
- Access shipment level receiving and audit results
- Retrieve certificates of data wipe and destruction
- Search asset level data and run customizable reports across defined date ranges
- Extract data needed to support internal audits, compliance requirements, and reporting

In a mature model, the portal serves as a central system of record, providing transparent, audit ready access to all asset, processing, and disposition information.

Good: Real-time portal with audit logs and reporting.

Bad: Static reports, ad hoc requested reports.

Ugly: No portal.

9. Data Security

A mature ITAD processing facility does not just perform data destruction, it provides standardized, certified, and fully auditable proof that every asset has been securely sanitized or destroyed in alignment with recognized industry standards.

Good: NIST 800-88 compliant processes (clear, purge, destroy). ISO 27001

Bad: Basic wiping with limited validation.

Ugly: No structured data destruction process.

10. Software Integration

Integration with platforms like ServiceNow enables organizations to maintain a single source of truth for asset data. By connecting ITAD processes directly into existing IT workflows, organizations gain real time visibility, reduce manual effort, and ensure that asset tracking, reconciliation, and reporting are accurate and audit ready.

Good: Integration with ITAM and ServiceNow.

Bad: Manual workflows like sending SNOW flat files.

Ugly: No system integration.

11. Reporting & Compliance

In a mature ITAD program, reporting is not an afterthought, it is a core capability that provides complete, audit ready visibility into every asset processed and every outcome achieved.

This includes ensuring that customers receive complete, asset level information confirming final disposition, supported by audit ready evidence that validates end of life processing and compliance.

Good: Full audit-ready reporting with ESG metrics.

Bad: Basic reporting.

Ugly: No documentation.

12. Recycling & Sustainability (ESG values)

A mature ITAD program transforms asset disposition into a measurable ESG driver, combining reuse, certified recycling, verified carbon credits, and transparent reporting to deliver both environmental and business value.

Carbon Credits

Good: Focus on reuse, resale, and certified recycling. Alignment with ESG and sustainability reporting and customer goals.

Bad: Limited sustainability efforts.

Ugly: Disposal-focused approach.

13. Remarketing & Value Recovery

The maturity of an ITAD remarketing program is defined by how close the vendor is to the end user market, the closer the connection, the greater the value returned to the customer.

Are you getting the best dollar value for your assets, ask your vendor what types of verticals they sell into and what percentage is sold to end user vs brokers.

Good: Structured resale maximizing asset value.

Bad: Limited resale efforts.

Ugly: Scrap everything.

14. Vendor Values & ESG

Good: Alignment with ESG and sustainability reporting.

Bad: Minimal ESG alignment.

Ugly: No sustainability focus.