

# ITAD Primer

## Beyond the Basics: 6 Critical Requirements for Selecting the Right ITAD Provider

Each retired IT asset is a potential pitfall of privacy and environmental liability. Selecting the right IT asset disposition (ITAD) provider is critical for both compliance and value for the service delivered.

The ITAD industry is highly fractured. Most large cities have at least one local company claiming to be an ITAD provider. Large regional and national ITAD providers have formed in recent years to meet the growing demand from companies that want a higher level of service and accountability.

### ITAD Basics

The basics of ITAD are data destruction, remanufacturing, remarketing, and recycling. While each company manages these basics differently, potential providers should be able to demonstrate that they follow Department of Defense 5220.22-M standards for wiping data on any storage device, using a tool that flags when sectors are inaccessible and provides robust reporting of configurations and confirmation the wipe has been completed. They should have a well-defined process for sorting, tracking, and determining the value of any assets. The providers should have well-developed channels for reselling assets that still have value – and a clear explanation of how they share revenue with the client. Anything that cannot be remarketed should be tracked – at the component level – to its final disposition.

These basic services should operate in line with IAITAM’s Best Practices Library for Disposal Management. The six core disposition goals are:

- To dispose of assets legally and securely
- Asset disposal requirements are identified and understood
- Disposed assets are accurately tracked
- The end-of-life process is defined and the disposal procedures are implemented
- Software is harvested and reallocated during the disposal cycle
- Information security for disposed assets is ensured

### Risks Require Greater Scrutiny

The risks associated with retired IT assets require a level of review and comparison that goes beyond cost and delivery of the basic services.

Knowing the right questions will give you insights that go deeper than just services and allow you to decide which providers can best meet your ITAD goals. Here are six critical requirements and how to evaluate the answers.

### 1. What is the ITAD provider’s financial health?

An ITAD provider’s revenues and balance sheet indicate its financial stability and ability to provide enterprise-wide service.

As a rule of thumb, small-to-medium businesses should select an ITAD provider with at least \$15 million in annual revenues and a business record of at least five years. However, these small providers are not a good option for Fortune 1000 and other highly regulated organizations because they do not always have the financial stability to ensure ongoing operation and protect the client assets in the event of closure.

The financial strength of small providers may also limit their ability to carry proper insurance coverage. Poor insurance coverage means significant risk in terms of their ability to indemnify their customers against information security and environmental risks.

Revenues are also a relative measure of a provider’s overall processing capacity and remarketing capabilities that yield cost-saving operational efficiencies and greater remarketing proceeds for clients.

Large national and multi-national companies should narrow their list to ITAD providers with at least \$40 million in annual revenues and a 10-year business record in order to be more confident.

### 2. Can the ITAD provider meet client needs across multiple, geographically diverse locations?

Transportation represents a significant cost for asset disposition. An ITAD provider should have a geographically diverse network of processing locations to minimize these costs regardless of whether your organization directly manages its return logistics or outsources logistics management. A provider with many facilities not only reduces the cost of transportation, but also assures the capacity to meet your asset-processing needs wherever your business is concentrated. All facilities should be fully integrated (both operationally and technically) and follow standardized processes. Facility and process security must be in place and actively managed at all

facilities.

At the opposite end of the spectrum are ITAD providers that form ad-hoc partnerships with their competitors to avoid logistics costs for clients with multiple sites. This practice can create inconsistencies in service and, worst of all, immeasurable data security and environmental recycling risk surrounding a client's assets.

Best-in-class ITAD providers offer a transparent and secure chain of custody between their facilities and client locations. Demonstrating chain of custody is a critical component of auditing for compliance with data security and environmental laws. Some providers maintain their own logistics fleet and secure logistics cross-docks, which allow them to transport assets on their own trucks using trained and qualified employee drivers, who can also provide on-site services. ITAD providers using their own employee drivers and vehicles should be able to confirm each driver has undergone thorough criminal background checks as well as training on packing, loading, and unloading the assets to best protect their residual value and security of any data. If used to consolidate logistics, cross-docks should maintain a high level of security to guard against theft, very similar to the security seen at the processing centers. This secure chain of custody provides assurance that unqualified and unauthorized people do not handle your assets.

### 3. Does the ITAD provider have robust

### information systems and provide total organizational transparency?

Robust information systems ensure proper asset tracking, compliance, and auditing. ITAD providers should allow their clients open access to information and critical processes. The information systems deployed by the provider are a critical element of this transparency. For example, the system should be able to track the following:

- How an asset was processed, including objective evidence that the data was completely destroyed
- When it was processed, including when it was picked up and delivered and the time spent in processing
- Which technician(s) handled it
- Asset-specific information such as make/model/serial number/configuration
- The final disposition of each asset and associated downstream information

This provides the tracking information that is essential in the unlikely event an asset is not handled properly and for documenting compliance.

At a minimum, a provider will have serialized information about each asset and allow clients to conduct planned audits. Top providers will have robust information systems that provide:

- A secure, online reporting interface
- Timely and accurate information about each asset processed
- A documented disaster recovery plan
- Guaranteed back-up procedures

They should also allow unannounced audits to validate compliance to all privacy and environmental regulations and provide quarterly business reviews.

### 4. How does the ITAD provider manage downstream recycling partners?

A poorly managed downstream process results in high potential risks. Your company may be exposed unwittingly to environmental liability unless your ITAD provider audits all downstream processors and scrap purchasers to guarantee all recyclable materials are handled properly.

At a minimum, an ITAD provider will have a subcontractor who is responsible for auditing all immediate recyclable processors, as well as tracing hazardous waste to its final resting place. Best-in-class providers will have long-term relationships and consistent annual environmental audit records for their entire downstream network of material buyers and processors. A provider with a full-time Environmental Compliance Manager has taken the ultimate step through auditing and managing all downstream recycler relationships, complying with the Basel Action Network's pledge of





environmental stewardship, and enforcing the ban on the use of prison labor for any processing activities. These providers will have a zero-landfill target and ISO 14001 and OHSAS 18001 certifications.

**5. How does the ITAD provider maximize the financial return from retired assets?**

Maximizing the financial return from selling retired assets into the secondary market is critical to minimizing the total cost of ownership. The ITAD provider should have remarketing channels that can handle more than just PCs, laptops, monitors, and low-end servers. Top providers should have fully developed secondary markets for bridges, routers, UNIX equipment, switches, printers, phones, and other IT equipment. They should also have a demonstrated capacity to handle selling assets into a variety of markets, including consumer-direct and large-volume purchasers as well as via their own high-traffic websites and brick-and-mortar retail outlets.

Remarketing channels depend on a robust capability to repair a variety of assets, resulting in a higher percentage of remarketable assets. Many providers fail a large percentage of assets due to poor processing capabilities or to reduce labor costs. A best-in-class provider will have a history of repairing assets along with offering at least a 30-day warranty on remarketed equipment.

**6. What insurance coverage does the ITAD provider carry?**

Many ITAD providers claim they will indemnify clients against the risk associated with data security and environmental recycling of retired assets. However, simple umbrella coverage is not enough. The ITAD provider should carry a significant level of insurance coverage commensurate with the number of assets being handled for any indemnification to have any value.

Providers need to have both pollution insurance and errors and omission insurance. Coverage should include pollution insurance to cover liability and costs of clean up arising from contamination due to the accidental release of hazardous

materials into the environment. At a minimum, your provider should have \$5 million in coverage. Top providers will have \$10 million or more from an AAA rated carrier.

Errors and omission insurance covers damages arising out of the insured’s negligence as well as mistakes or failure to take appropriate action in the performance of business or professional duties. The minimum coverage is \$2 million; best-in-class providers will have \$5 million or more in coverage.

**The High Cost of Failure**

The following are some relevant fines for data security breaches.

Law	Maximum Fine
✦ Gramm-Leach-Bliley Act (Financial Institutions)	\$100,000 per violation
✦ Sarbanes-Oxley Act (Accounting)	\$5,000,000
✦ Health Insurance Portability and Accountability Act (HIPAA)	\$250,000
✦ Fair and Accurate Credit Transactions Act	\$2,500 per violation

Fines alone can easily run into the millions, with litigation possibly being even more expensive. However, the cost of failure can be much greater than dollars. A single retired asset disposed of improperly can cause damage to a company’s brand, lead to identity theft that affects customers and/or employees, and create long-term damage to the environment and health in developing countries.

**Chip Slack**  
*Chairman and CEO of  
 Intechra, LLC*