WE DO ITAD RIGHT

Lifespan

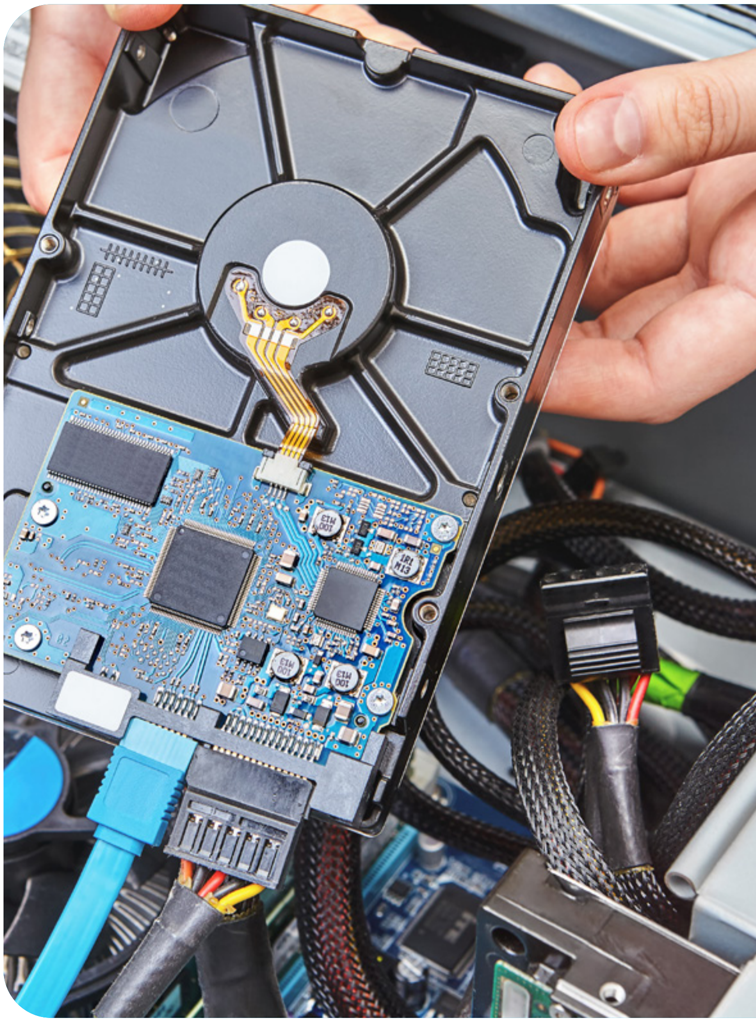
A Guide to Minimizing the Risk of IT Asset Disposition

Overview

Who is concerned about risk? They may not think about it in terms of risk, but almost everyone at your organization is worried about the chinks in its armour. Where is your organization exposed to uncertain factors that can negatively affect its objectives and bottom line? The task of identifying these factors and accounting for them – minimizing the likelihood of their occurrence – is risk management. Modern best practices for businesses and other corporate enterprises call for the development of a risk management strategy that will **identify** the top risks faced by an organization as well as implement a plan for dealing with them.

If you're involved with identifying and planning for risk at your organization, one source you can't overlook is the process through which your organization disposes of its retired IT equipment. IT asset disposition (ITAD) involves removing pieces of surplus or obsolete IT equipment from your company's facilities and sending them to be recycled or, if they still have value, to be resold. It can be triggered by an equipment refresh cycle, a data center decommission, the changing of office settings or the shutdown of an office, for example.

Table of Contents



01 IT Asset Disposition & Risk

Your IT asset disposition process can be a hidden source of risk because it presents opportunities for:

- Data Breach
- Non-compliance with industry regulations
- Environmental violation

Data security, is one area risk management policymakers are zeroing in on. The average cost of a data breach continues to skyrocket. When you factor in fines, legal fees, the cost of bad publicity and loss of customer confidence, and a possible drop in stock price, any given data breach incident can cost an organization in the thousands and often millions of dollars to resolve. Wherever a company risks leaking data into the outside world is a serious exposure. Most troubling of all, it only takes one drive to get through the disposition process with data still on it to trigger a serious breach. The data stored on the drives of your retired IT assets must be properly destroyed before they leave the control of your organization.

Closely linked to data security is the risk of **non-compliance** with industry regulations. Depending on its industry, an organization is required to comply with any number from an alphabet soup of regulatory standards: HIPAA/HITECH, PCI, SOX, FACTA, GLB. Generally, these standards place a high value on data security and come down hard on organizations that let sensitive data leak. If your organization has regulatory obligations, does it have an airtight data sanitization procedure backed up by auditable records? If not, the organization is at risk of a negative audit (and a possible fine) even without a breach.

An organization's **environmental** concerns stem both from the government regulations it must comply with as well as its own culture of environmental stewardship and sustainability. However, there is potential for risks that will lead to paying fines and legal fees, the risk of company resources being diverted to avoidable remediation efforts, and the risk of negative publicity. To minimize these risks, your company must recycle the assets it cannot resell according to all local, state, and federal regulations; and be able to produce evidence in proving the company has diverted every bit of materials from the landfills back into the supply chain. Further, if you sell the used assets, you must be sure that the buyer will properly dispose of any assets that do not function or can't be sold. Remember, you are still liable after the equipment leaves your dock.

02

Governance, Risk Management & Compliance

Many organizations are planning for risk now as part of their corporate governance, risk management and compliance (GRC) strategies. A sound governance policy is a high priority with increased government and public scrutiny. For IT, risk management and planning involve ensuring a company's IT systems are aligned with its overall risk management and compliance strategies and integrated with its sound governance practices. This alignment with strategy and governance should apply to ITAD processes. In many companies, however, the complete end-of-life process is overlooked in the plans and policies.

The solution for ITAD risk

The right approach to avoid IT asset disposition-related risks is to implement a structured program. This program should address data security, regulatory compliance, and environmental concerns on an enterprise-wide scale while ensuring the process is completed correctly each time at every organizational location. This guide will discuss best practices to follow for minimizing the risk involved with IT asset disposition and how the programmatic approach to ITAD is the best way to put those practices in place.

Risk Avoidance Strategy #1: Choose a Certified Data Destruction Vendor

As unsecured data can be such a significant source of risk, you need complete assurance sensitive data has been fully removed from your company's surplus IT equipment. There are two ways to handle data destruction:

- Physical destruction of data-bearing drives or media
- Data sanitization: using certified software to overwrite hard drive data beyond a recoverable state

Both approaches meet data security standards, but there are cost-benefit differences. For some risk-conscious organizations, the only way to ensure absolute data security is to physically destroy the drives from every piece of retired IT equipment. However, on the resale market, intact systems always sell for more than systems lacking components – including hard drives. IT assets without hard drives can lose up to 30 percent of their remarket value. Companies who also have the goal to reduce costs and maximize the value of their IT assets should consider their options for data sanitization. All major standards organizations in the U.S. and Europe accept properly executed data erasure as meeting the standards.

Data sanitization: Do it yourself or outsource?

Data sanitization can be done internally or by partnering with a data sanitization provider (good ITAD vendors provide data erasure services). A vendor partnership may be preferable because it saves your organization the cost of taking your IT staff away from other projects. Perhaps more importantly, when a vendor does data sanitization right, it can ensure it's always done according to the latest and best practices and in compliance with your industry's regulations. A partner-vendor should also have documented quality checks in place – something your staff may not have the resources to do. How to choose a data sanitization partner If you choose to partner with an ITAD vendor for data sanitization, how can you be sure your vendor's team members know their stuff?

How to choose a data sanitization partner

If you choose to partner with an ITAD vendor for data sanitization, how can you be sure your vendor's team members know their stuff?

Risk Avoidance Strategy #1: Choose a Certified Data Destruction Vendor

- ▸ Have you observed your vendor’s data erasure process?
- ▸ Have you visited the vendor’s facilities?
- ▸ Do you know which data erasure tools the vendor uses?
- ▸ Do you have reports that show every serial number and whether the erasure was successful or not?
- ▸ Have the vendor’s employees received proper training and background checks?

Partnering with a vendor that has been certified by a third-party industry organization ensures the work has been done for you. In the realm of data destruction, one of the most reliable certifications to look for is from the National Association for Information Destruction (NAID). NAID provides the only third-party certification that focuses exclusively on information security, and it performs both a scheduled and a surprise audit each year on the organizations it certifies.

The NAID AAA certification is viewed as an industry-leading certification for data sanitization. If you use a NAID certified IT asset disposition vendor, you can be sure that it meets the highest standards for data security and its entire disposition process has been documented.

On-site data wiping

NAID certifies its members for either or both plant-based and onsite data sanitization. For many organizations, on-site data sanitization is the least risky option. This ensures sensitive data will never be exposed to the unpredictability of the outside world.

Some ITAD providers can accommodate the need for on-site data sanitization with a mobile wiping system. A vendor certified by NAID for on-site data sanitization can bring a trained staff to your facility and perform data sanitization to the same level as can be accomplished offsite. Similarly, an ITAD provider should be able to physically destroy drives on-site, in situations where that’s a more appropriate method.

Data security tip: Laptops, desktops, and servers are not the only IT devices that store sensitive data in their hard drives. Don’t forget copiers, network printers, and smartphones and tablets in your data security policy

04

Risk Avoidance Strategy #2: Choose a Certified Electronics Recycler

Data sanitization is a reliable way to ensure absolute data security, but there are cases when hard drives can't be wiped. If a drive is damaged and won't boot, data sanitization software won't be able to complete the erasure. Sanitization may not always be the most cost-effective choice. Erasing data from equipment that won't have resale value can be a waste.

One method—erasure or destruction—does not fit all the possible disposition scenarios, even within the same organization.

When drives are destroyed, the material needs to be disposed of in full compliance with all local, state and federal environmental regulations. **Remember, your organization could be liable if the equipment has been disposed of improperly by the vendor, as it can be traced back to your organization.**

R2

R2 is the Responsible Recycling certification accredited by Sustainable Electronics Recycling International (SERI). It is recognized as the global environmental, worker health and safety standard.

Risk Avoidance Strategy #3: Get Detailed Reports for Every Disposition

The steps to any regulatory compliance are:

1. Understand the implications of each regulation for asset disposition.
2. Develop processes and document them.
3. Make sure everyone who literally touches the disposition process understands the process and requirements.
4. Be prepared to prove you have followed the process if challenged in an audit.

Documentation is necessary. All the effort your team puts into compliance practices will be wasted if you can't show you've done the work. For IT asset disposition, that means being able to document the disposition and data erasure/destruction status of each piece of equipment, generally by serial number, with all the details required by your industry regulations.

A strong ITAD vendor can work with you to ensure your entire disposition process meets industry best practices and regulatory standards. If your ITAD vendor doesn't provide detailed disposition reports for each piece of equipment, it's not giving you the tools you need to ensure complete regulatory compliance and is therefore exposing your organization to risk.

06

Risk Avoidance Strategy #4: Vendor Insurance

Uncertainty plays a role in even the tightest ITAD procedure. If something does go wrong, you need to be sure your company is protected financially. This is a key strategy for minimizing risk. Validate that your vendor has the right amount and types of coverage, including:

- ▶ E&O (Errors and Omissions)
- ▶ Environmental
- ▶ Data Breach

Data breach insurance is a separate policy or rider specific to data breach costs.

In addition to reducing financial risks, evidence of insurance also tells you that the vendor is committed to doing asset disposition right, that it has the financial stability to buy the insurance, and that it is willing to stand by its processes and organization.

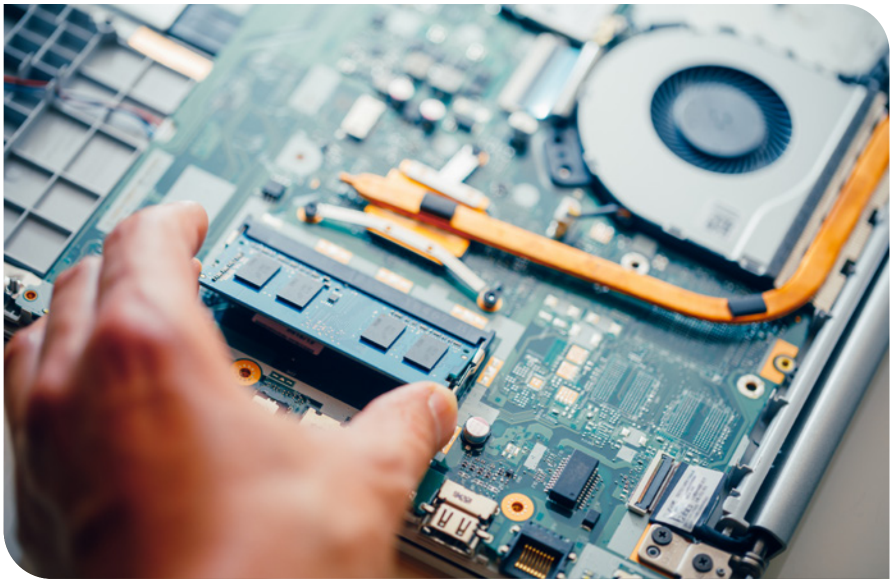
Risk management tip: Don't just take your ITAD vendor's word for it that they're covered with data breach and other important insurance policies. Ask to see their certificates of insurance.

07 The Benefits of Holistic ITAD Approach

Your company needs an ITAD plan that will fit into its governance, risk management, and data security policies. The challenge of IT asset disposition is ensuring that every disposition, at every location, is done according to your corporate standards; and the needs of every department with a stake in IT asset disposition are being met while minimizing the resources and hassle required to get it done. That challenge increases with the size of your enterprise.

A holistic approach to ITAD responds to that challenge by implementing an enterprise-wide program with specific roles and procedures. The program should include every link in the chain, recognizing the differences among the various departments & locations in your organization and tailoring the process to fit their needs & capabilities. This approach makes it as easy as possible for team members to do ITAD right, every time, for every location, with the documentation to back it up. This will give you better peace of mind that your data security, compliance, and environmental risks associated with ITAD are being managed.

By implementing and following a programmatic approach to ITAD, your organization will also be able to better manage costs and maximize returns, with an enterprise-wide pricing and service structure from your ITAD vendor.



ITAD Program and Your Organization’s Departments

Other departments and team members in your organization will find their concerns addressed by a holistic ITAD solution as well. Here are some of those stakeholders and the concerns they might have about IT asset disposition.

Information Security/Risk Management

- Compliance: HIPAA/HITECH, SOX, GLB, PCI, etc.
- Corporate Policies, Governance

Facilities Management

- Space for secure storage.
- Availability of knowledge and materials to pack resale items for safe shipment.
- Time/resources to do packing, audits.

IT Operations/Infrastructure

- Refresh and end-of-life decision-making to ensure maximum value and return on investment (ROI) for capital budget.
- Resource availability for hard drive data destruction.
- Quality assurance process; ability to audit.

Supply Chain Management

- Ensure vendors meet corporate requirements.
- Minimal costs.

Finance

- Inventory accuracy by asset, status on books.
- Software and operating system license compliance.
- Minimal cost.
- Maximum investment recovery.

Environmental/Sustainability/Green Team

- Compliance with all environmental regulations and corporate sustainability goals.
- Report details for corporate environmental/ sustainability reporting.

Talk to one of our Lifespan experts today to discover your ITAD program requirements. We can help you identify the goals, concerns, and priorities of your organization’s stakeholders and provide a roadmap for starting the process of aligning your business objectives into a comprehensive ITAD program.

To speak with one of Lifespan’s disposition professionals call:
888-720-0900

Schedule a Call
› CLICK TO SCHEDULE ‹

01-2022

LIFESPAN INTERNATIONAL INC.

4675 E. Cotton Center Blvd., Ste. 155, Phoenix, AZ 85040 USA
951 Valley View Lane #180, Irving, TX, 75061 USA
75 Clegg Road, Markham, ON, L6G 1A1 Canada

Tel: (888) 720 – 0900
Email: info@lifespantechnology.com

WE DO ITAD RIGHT

Lifespan