

BUILDING A SUCCESSFUL GLOBAL IT ASSET DISPOSITION PROGRAM

WHITE PAPER



SIMS
LIFECYCLE
SERVICES

IT equipment today is the lifeline of any business, and while upkeep and proper maintenance is important, it is not easy. From maintenance and upgrades to final disposition, each phase of managing the lifecycle of IT assets within an organization presents its own set of unique challenges.



Similar to IT asset management (ITAM) processes within an organization, the IT asset disposition (ITAD) process has matured in recent years. Companies have begun to understand data security and environmental compliance risks associated with disposition programs that do not follow rigorous processes. This is why over the last few years Sims Lifecycle Services has seen many global RFPs as companies started recognizing their own inconsistent ITAD programs at their locations around the world.

“

ITAD is the last stage [of the ITAM process] and too often becomes an afterthought; a “necessary evil” that carries with it significant risks without a thorough, detailed, end-to-end process that is consistently executed throughout your enterprise.

Noted Gartner, Inc. in the Gartner Market Guide for IT Asset Disposition, July 26, 2018.

Wondering where to start?

It does not always have to be as drastic as tearing up your current ITAD program, and starting over; although that may be necessary in some cases. Start first by assessing your current situation, then understanding where you can improve to ensure your program will be successful.

Assessing the Situation

Perhaps you are unsure if your ITAD and electronics recycling program could be vulnerable to security threats. The following checklist will help you understand your program's current strengths and weaknesses, allowing you to create an action plan for improvement.

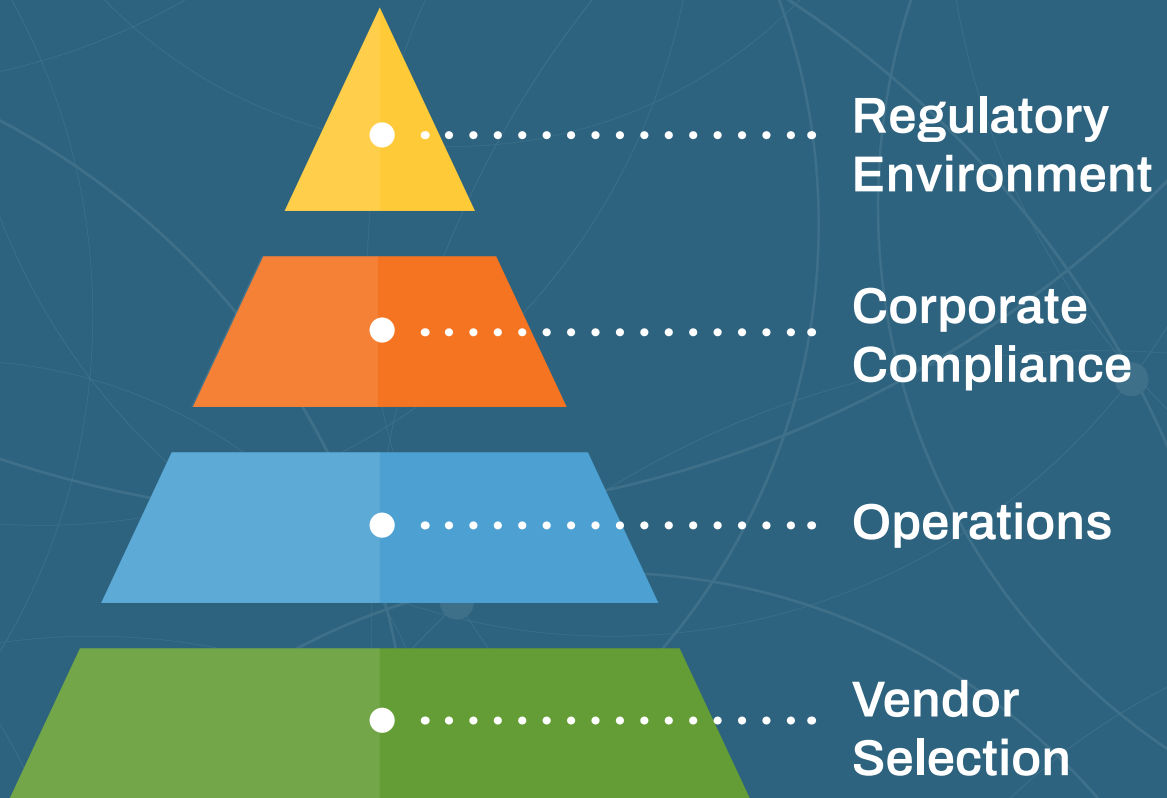
Do any of these sound familiar?

Check the box if the description reflects any part of your current ITAD or e-recycling process.

- I have no clear audit trail for corporate and regulatory compliance (Regulatory Environment)
- I have insufficient/no visibility into data destruction, chain-of-custody (Corporate Policies)
- I do not have consistent asset reports, invoices or certificates of data destruction (Corporate Policies)
- My disposal program is not aligned to our corporate risk management program (Corporate Policies)
- I do not have a defined process for securely handling data bearing equipment (Corporate Policies)
- It is difficult for me to get accurate asset lists from different locations (Operations)
- I have trouble determining asset condition, count and age for each location (Operations)
- I have an ITAD process that is different from other locations (Operations)
- I have inconsistent billing and no overall visibility of total costs (Operations)
- I have no guidance on how to manage retired IT assets within our corporate data privacy program (Operations)
- I do not have a line item in my budget to manage my ITAD program or for asset disposition activities (Operations)
- I manage multiple vendors who were onboarded years ago with regional vs. global focus (Vendor Selection)
- My current vendors cannot fulfill all of my needs I have today (Vendor Selection)

If you checked any box off this list, you should review, update and add to your ITAD program plan. Use the following chart to determine what areas you want to focus on the most.

What is important to consider?



- **1. Regulatory Environment (bullet 1)**
Companies must adhere to data security and environmental legislation in the macro environment. Globally this regulatory framework is typically by country or region.
- **2. Corporate Compliance (bullet 2-5)**
ITAD programs should be consistent with a company's risk management and data security policies.
- **3. Operations (bullet 6-11)**
Many global companies are restructuring ITAD programs to be centrally managed and consistent at locations worldwide.
- **4. Vendor Selection (bullet 12-13)**
The breadth and depth of services offered by ITAD and electronics recycling vendors vary dramatically. It is important to select a vendor who has capabilities that best match your requirements.

*A more detailed discussion for each of these four segments follows.

Regulatory Environment

Global Data Privacy Regulations

European Union (EU)

In May 2018, the EU's General Data Protection Regulation (GDPR) came into effect. GDPR is a huge legislative change in Europe that outlines significant financial penalties for non-compliant handling of EU citizens' data. It does not matter where you are based, where you do business or where your headquarters is located. If your company handles, processes or stores data of EU citizens, you need to be GDPR compliant. The consequences of non-compliance are severe. Companies can face fines of up to €20,000,000 or four percent of global revenue.

United States (U.S.)

In the U.S., there is no federal legislation but instead a patchwork of legislations for including:

- Californian Consumer Privacy Act (CCPA) which extends privacy protections to the internet.
- Nevada's Senate Bill 220, or "An Act relating to Internet privacy," will require operators of internet websites and online services to follow a consumer's direction not to sell his or her personal data.
- The Maine privacy law—"An Act to Protect the Privacy of Online Customer Information"—focuses entirely on user data collected by Internet Service Providers (ISPs).
- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 which protects healthcare patient data.
- The Gramm-Leach-Bliley Act (GLBA) and the Fair and Accurate Credit Transactions Act (FACTA) which are directed at financial institutions.
- The Payment Card Industry Data Security Standard (PCI DSS) which applies to companies who accept credit card payments.
- The Family Educational Rights and Privacy Act (FERPA) legislation that protects the privacy of students by ensuring their education records are protected.

Australia

In February 2018, Australia's Privacy Amendment Act 2017 became effective, introducing the Notifiable Data Breaches Scheme. This scheme affects those under the Australian Privacy Act and requires them to take steps to secure certain categories of personal information.

With so many tightened data security requirements, companies are taking steps to develop more structured and formalized ITAD programs that are compliant with industry and privacy legislation and corporate risk management programs.

Global E-Waste Legislation

Legislation governing how e-waste is disposed of is inconsistent regionally and globally. Batteries, toner, ink, mercury bulbs and leaded glass from CRT monitors are common items requiring special handling when recycling electronics.

There have been significant industry issues with e-waste being illegally exported and dumped in developing countries causing human health and environmental issues. With the patchwork of inconsistent legislation, most companies take their own proactive stance in auditing vendors to ensure e-waste disposal is managed responsibly.

Evaluating Regulatory and Corporate Requirements

Regulatory compliance efforts can be further complicated when companies operate in multiple locations and face regulations that vary by country. For global ITAD, questions that typically come up include:

- What industry regulations need to be considered in each country regarding data privacy?
- Is there legislation regarding e-waste disposal?
- What changes on the horizon may affect how you dispose of e-waste?
- Are there any industry regulatory changes in the countries you operate, that impact your ITAD program?

Corporate Compliance

Corporate Management Considerations

Corporate risk management, business continuity, and data security policies can all impact your global ITAD program. A data destruction plan for media storage devices is critical when removing IT equipment and electronic assets from your live environment. This should reflect the same risk protection as outlined in your corporate data security policies.

Looking Back

IT asset disposition or “ITAD”, is a relatively new term. Historically, disposing of retired IT equipment was a financial calculation. Considerations focused on what,

- You paid for the equipment,
- You could resell your equipment for, and
- Someone would pay to recycle this equipment.

There were few additional considerations in most cases.

As data risks became more publicized and data threats more intimidating, companies began dedicating resources to ensure data destruction of information stored on retired IT assets. Companies have a vested interest in protecting confidential corporate information such as trade secrets, sales records, copyright and intellectual property, as well as customer data.

Global companies often face the challenge of consistently managing data destruction processes from country to country at smaller offices with remote employees.

On top of managing inventory, these global companies must also consider changes to data bearing devices over time. For instance, it took several years for all-in-one copiers and printers to be recognized as “data bearing devices” after they were equipped with hard drives to support electronic document storage. As our devices today become “smarter”, regular reassessment of data risks on retired IT assets and equipment will be critical.



After removing data bearing assets from your live environment, it is important to have a plan in place to ensure all data is destroyed.

Operations

Overview of an ITAD Program

Companies are taking a closer look at e-recycling and ITAD vendor's infrastructure. Having a better understanding of their ITAD and data destruction services will help ensure their corporate interests are protected and are compliant with relevant regulations.

Fragmented ITAD and Computer Recycling Programs

Some large enterprises manage different programs at each company location. It has been common for IT equipment disposal programs and plans to be managed separately but seldom has this task been part of anyone's job description nor provided in any formalized manner.

Data security was previously not as much of a primary consideration, and many times, there was no documentation of how equipment was disposed of and how data was destroyed. This fragmented opaque situation is no longer acceptable today.

Know What You Have — Operational Challenges for Multi-site Locations

The first obstacle many companies face in trying to manage a global ITAD program is a black hole of information. It can be difficult to assess what assets you have, where they are located and how each location handles removing IT assets from your live environment.

You cannot manage what you cannot measure.

Common challenges include:

- Ad-hoc approach at each facility,
- Inconsistent and undocumented processes,
- Undefined job description/ownership,
- No central control or reporting,
- Lack of training, and
- Multiple vendors (and multiple ways of doing things).

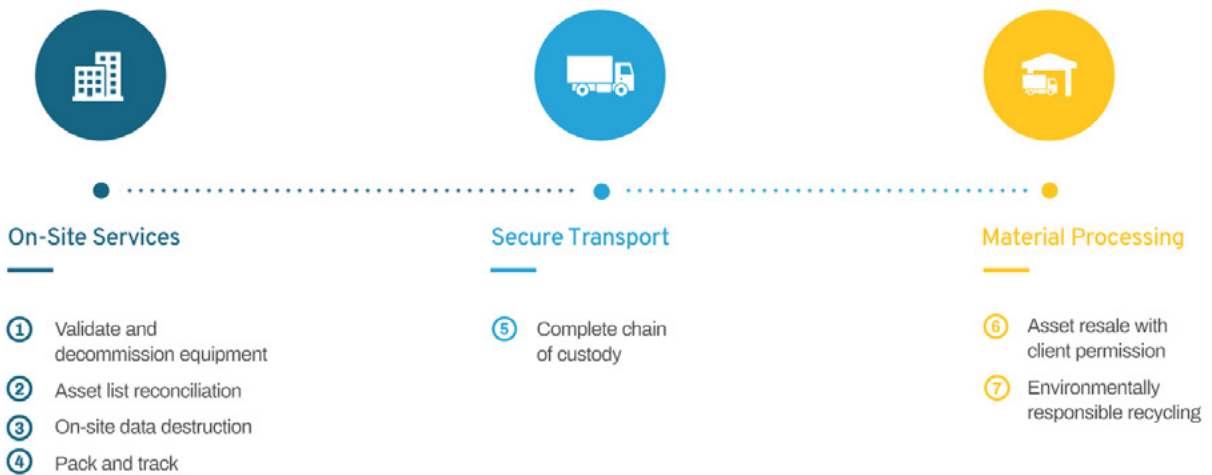
Vendor Selection

Global Data Privacy Regulations

The ITAD services required at each location will vary by client. In general, services offered by industry providers are categorized by location, either at the:

- Client's location (on-site services), or
- Vendor facility (off-site services).

Moving IT assets between two locations is also important for full accountability, especially for any data bearing devices. This diagram provides an overview of the structure of a typical ITAD program.



PORTAL FOR ASSET TRACKING, REPORTING AND CERTIFICATE OF DATA DESTRUCTION

On-site ITAD services (at client location) include:

- Decommissioning of IT assets
- Secure asset storage (between vendor pickups)
- Data destruction
- Inventory reconciliation (verification of make, model, serial number and asset tag, cross-referenced to internal lists)
- Packing of IT assets

It is important to know the correct transport service is provided to ensure chain-of-custody is defined, known and consistent with the risk associated with assets to be transported.

Off-site services (at service provider location) includes:

- Data destruction (if not done at client location)
- Resale of IT assets
- Parts harvesting (if applicable)
- Recycling
- Reporting

At a high level there are other vendor qualifications and capabilities to consider. To ensure credibility of the business you should consider the company size, longevity, number of employees and understand what percent of their business is dedicated to ITAD services.

When it comes to execution, you can ask yourself these questions.

- Do they have the infrastructure to support a global program?
- Does their footprint align to our footprint?
- How do they “fill in gaps” for services they do not provide directly?
- Can they demonstrate they can provide systematic and secure support?
- Can they support our data destruction requirements?
- Are they familiar with country regulations for handling data? E-waste? Billing?
- Do they operate to industry standards?

Global ITAD RFP Guide

We have seen many companies ask these types of questions through a Request for Information, prior to issuing a more detailed Request for Proposal (RFP). To get started building your custom RFP, best fit for your needs, check out the template we created to help companies like you.

Download our Global ITAD RFP Template Now
www.simslifecycle.com/reuse/itad/rfp-offer/



Contact us:

www.simslifecycle.com/contact