Keeping Compliant: The Benefits of a Formal IT Asset Disposition Policy

Having an ITAD plan has become a crucial priority, according to IT leaders in a new IDG Research Services survey

As organisations continue to produce, manipulate, and store data, the responsibility intensifies to properly manage and maintain it. Meeting ever-changing compliance regulations and security requirements are now part of daily IT operations.

At the same time, technology continues to advance, causing organisations to upgrade their IT assets and decommission old ones. Yet how companies handle IT asset disposition (ITAD) can play a significant role in determining the overall effectiveness of the IT organisation's ability to adequately protect the business.

The Case for a Formal ITAD Policy

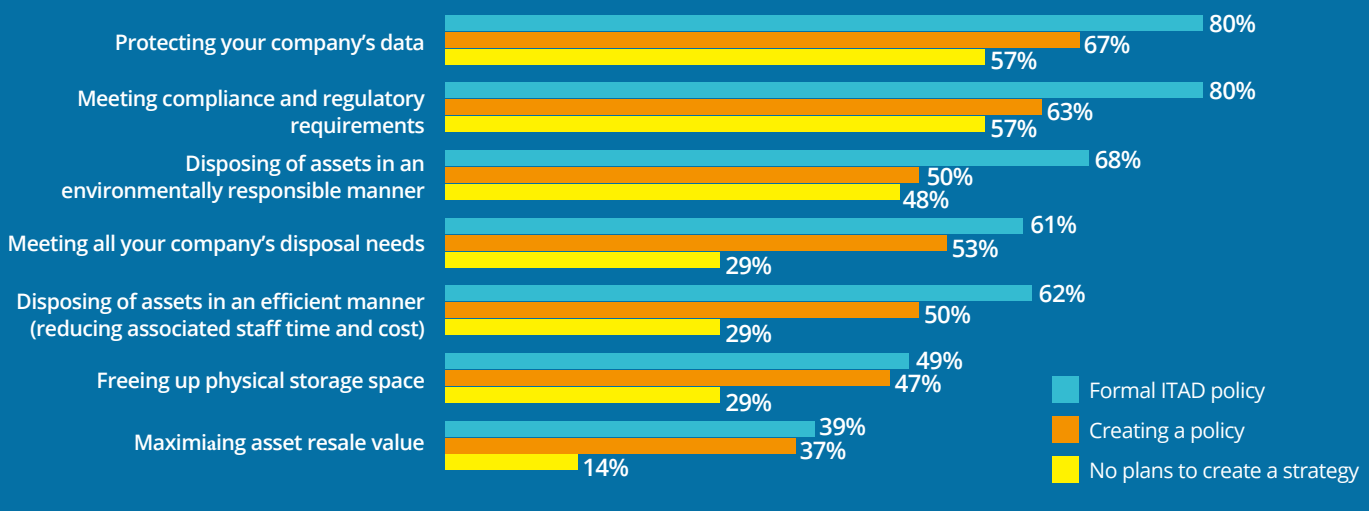
ITAD is a predetermined process that organisations utilise to properly decommission and dispose of their entire array of IT assets. A proper plan for ITAD includes the need to control data on IT equipment throughout its use, internal transfer, and disposal.

There are two primary reasons why having a formal ITAD policy makes sense. First, it's important to consistently track IT assets and ensure efficient use throughout their usable life. The amount of capital invested into these assets over time justifies ensuring that the business is getting the most return on its investment, which includes disposition.

> *Those companies with a formal ITAD policy in place are more than twice as effective in maximising resale value of old IT assets, according to IDG Research Services.*

The second reason — and often the driving force behind developing a formal ITAD plan — is the ability to effectively ensure that the organisation is complying with a growing number of regulations and compliance issues. IT assets are increasingly subject to both environmental and data privacy regulations at all levels of government, both in the U.S. and overseas. Having a formal and enforceable policy in place plays a pivotal role in standardising practises across the organisation.

FIGURE 1. Why ITAD Policy Works: Areas of Effectiveness



A global survey conducted in March by IDG Research Services among 311 IT leaders reveals that enterprises are far more effective in protecting data when a formal ITAD policy is in place (see Figure 1). Specifically, 80% of respondents with ITAD in place cite effectiveness versus 57% without a formal plan in place. The same statistics surface when comparing how well companies are able to meet compliance and regulatory requirements.

Most IT leaders recognise the value of having an ITAD plan, with almost two thirds (64%) placing a critical or high priority on it, and 62% saying its importance has increased over the past two years.

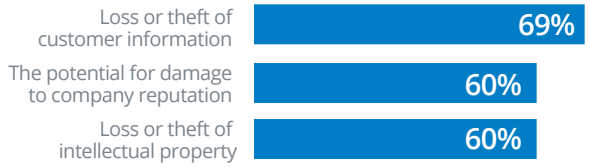
The significance of ITAD is even more pronounced among senior leadership. For example, 78% of VP titles and above cite IT asset disposition as a critical or high priority at their organisations, compared to 57% of respondents at the manager level. This difference suggests those in executive business positions are more familiar with and concerned about the risks of not having an ITAD policy, as discussed later in this paper.

There are also differences to note when comparing respondents among various geographical regions. For instance, the change in importance of ITAD strategy is most prominent in APAC, where 75% say the need has increased over the past two years versus 63% in EMEA and only 50% in the U.S. Potential reasons for these differences include varying age of IT assets, the regulatory landscape in each region, and the fact that many companies in the U.S., for example, may already have an ITAD policy in place (60% of U.S. respondents cite having an ITAD policy for two years or more, versus 47% in EMEA and 44% in APAC).

The Consequences of a Lack of ITAD Policy

There are compelling reasons for having an ITAD policy. IDG survey respondents cite the need to secure sensitive data, meet data compliance and environmental regulations, and have a consistent, secure chain of custody. In addition, they are motivated by the rapid growth in the number of mobile and IoT devices they have to protect and manage.

Respondents also acknowledge the risks of not having an ITAD plan. Perhaps the most significant problems surround the potential for inadvertent data loss:



The possibility of punitive fines and criminal charges surface as concerns across the board among survey respondents. That said, both of these factors are more prominent worries in APAC compared with U.S. and EMEA, which is likely due to that region's current regulatory landscape. The ongoing trend to clamp down on data protection issues is quite prominent. Some of the key developments include:

- According to the Hogan Lovell's Asia Pacific Data Protection and Cyber Security *Guide 2017,* Japan's Personal Information Protection Commission, tasked with supervising enforcement and application of amendments to the Act on the Protection of Personal Information, is now active.
- The Philippines appointed its National Privacy Commission in March 2016, which was closely followed by the introduction and passage of implementing rules and regulation for the country's first comprehensive data privacy law, the Data Privacy Act of 2012.
- Australia has passed amendments to the Privacy Act 1988, imposing a mandatory breach notification requirement.
- China adopted the Cyber Security Law in November 2016, to accompany the recently enacted National Security Law and Anti-Terrorism Law.
- In South Korea, a recent amendment introduces punitive damages as well as holding senior officers accountable for breaches, including being personally exposed to penalties.

Likewise, companies operating within Europe must conform to European Union legislation or face penalties when they fail to comply with waste electrical and electronic equipment (WEEE) directives.

Even when an organisation operates solely inside the

U.S., the regulatory landscape has become quite complex with many states requiring compliance with their own environmental standards, in addition to federal regulations. Specifically, 25 states currently have legislation in place dictating how organisations must dispose of or recycle e-waste.

In addition, various industries in the U.S. face unique compliance regulations including the Health Insurance Portability and Accountability Act (HIPAA) for those companies within health care, and the Graham-Leech-Bliley Act for the financial services industry.

The bottom line is that regional and industry differences can and should guide policies and procedures regarding ITAD.

Building a Policy through Best Practices

Developing, deploying, and maintaining a formal ITAD policy should be a priority for all organisations. And considering the potential consequences of data loss and fines, the process must involve more than simply downloading a boilerplate policy. Here are best practises to follow:

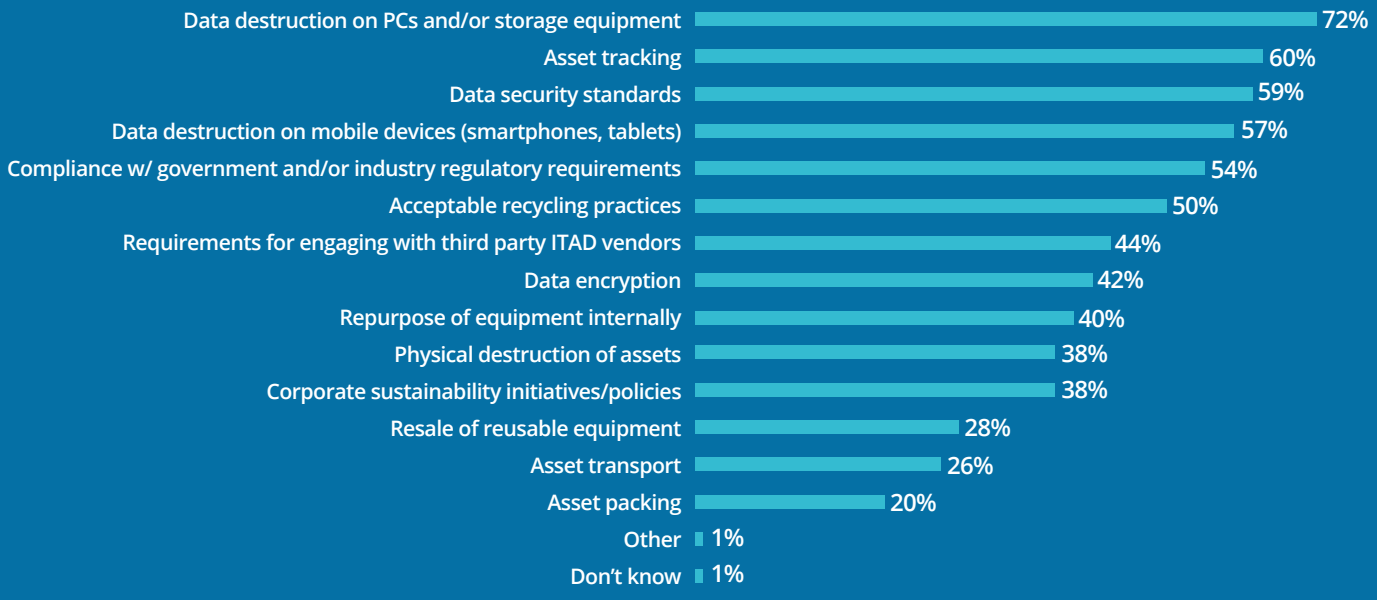
1. Start with a framework. While no one plan fits all, there are several components that organisations need to include in a well-crafted ITAD plan. Take it from IT leaders: As seen in Figure 2, which reflects those companies that have an ITAD plan in place, the key to success is to start with a solid framework including data destruction, asset tracking, data security standards, and regulation compliance.

2. Think and act outside of IT. Taking a big-picture approach means stepping outside the vacuum of IT. The best policies effectively incorporate the viewpoints of multiple stakeholders. This means garnering input from key personnel within procurement, IT, finance, facility, legal, environmental health and safety, and security.

When organisations fail to involve a diverse group of stakeholders, it becomes easy to overlook dimensions that could ultimately have negative repercussions for the whole company. Multiple perspectives yield a holistic approach to ITAD, which also results in facilitating buy-in from all of the areas within the enterprise.

Active involvement further provides an opportunity to adequately explain why the organisation is embracing a formal policy, as well as the significant role each employee plays.

FIGURE 2. Aspects Addressed by Companies with a Formal ITAD Policy



3. Incorporate regional differences. Regional differences can in many instances boost policy complexity, especially for large multinational organisations. Sometimes these geographical distinctions conflict, making the ability to have one comprehensive policy all the more challenging.

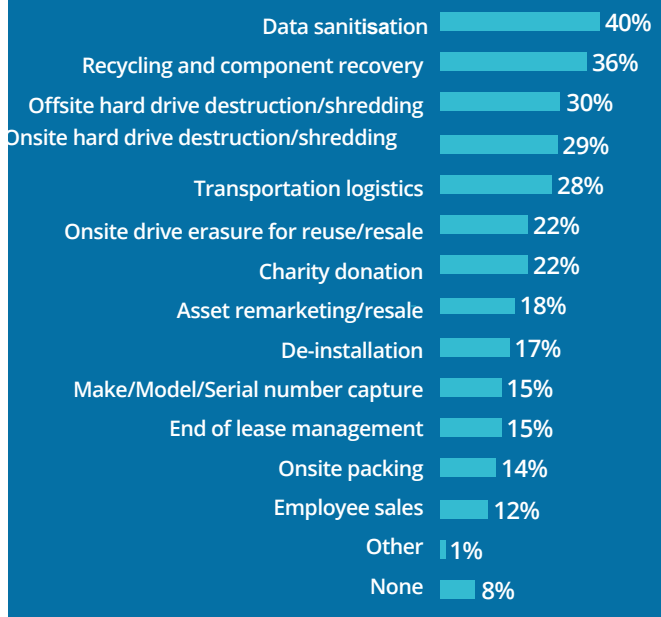
To accommodate various jurisdictions, it makes more sense to build one core policy that aligns with the business strategy, and then make modifications according to geographical operations or divisions.

4. Address potential risks. A key element of involving multiple stakeholders is to make sure that all departments understand the significance of having a living plan that strategically guides the organization through the IT lifecycle. It is equally important to address the consequences should people fail to comply with the formal plan. Because data security and resource protection are critical, employees that do not adhere to the foregoing policy should know that there is the potential for disciplinary action – i.e., termination of employment. In addition, any employee who becomes aware of a violation should be encouraged to report the issue in a timely manner.

5. Seek expert assistance. Working with a third-party vendor with experience in developing ITAD policies provides the business with a starting framework for success that's rooted in proven best practices. For instance, an experienced partner understands how to navigate the regulatory landscape, including the importance of keeping a close eye on upcoming legislation that could affect successful plan development and maintenance. Also, an expert partner can guide a company through potential risks, while offering strategies to effectively mitigate them.

Of course, policy development is only the first step. There are numerous roles a partner can play long after an ITAD policy is put in place — from data sanitisation to end-of-lease management (see Figure 3). It's interesting to note that IT leaders who already have a formal ITAD policy in place at their organizations are more likely to stick with a single third-party provider that handles all these functions and provides a comprehensive, centralising policy and strategy rather than multiple vendors.

FIGURE 3. Organisations Leverage Third Party for Many ITAD Aspects



Bottom Line

As the data threat landscape continues to evolve and regulations compound, it's likely that having an ITAD policy will continue to increase in importance. For those companies that are operating without one or are disposing of IT assets on a piecemeal basis, the risks to the business will also increase.

Visit *Iron Mountain* and discover how its Secure IT Asset Disposition solution can help:

- Build and manage your IT asset disposition practices with a proven, certified process
- Tailor the program to align with your objectives and compliance requirements
- Meet sustainability initiatives, while complying with internal and external regulations