


End of Life
 $=$
 End of Responsibility
 Aaron Zeper




iaitam.org | Peace, Love & Asset Management | ACE 2022

1



End of Life
 \neq
 End of Responsibility
 Not Quite



iaitam.org | Peace, Love & Asset Management | ACE 2022

2



Introductions



CEO of an ITAD company – R2, NAID AAA, B Corp
 Father of 3 and an ASU grad
 IT Services Industry for 22 years
 Worked large and small companies in DC Services, Software
 Asset Management, and Telecom Expense Management



iaitam.org | Peace, Love & Asset Management | ACE 2022

3




Audience Calibration

Who is responsible?

iaitam.org | Peace, Love & Asset Management | ACE 2022



4



The Facts

\$1,200,000

A \$1.2 Million Photocopier Mistake: Health Plan Settles with HHS in HIPAA Breach Case

disclosed the protected health information of up to 344,579 individuals when **returned multiple photocopiers to leasing agents without erasing the photocopier hard drives.**

iaitam.org | Peace, Love & Asset Management | ACE 2022



5



Agenda

- 01 Types of Responsibility
- 02 End of Life Process
- 03 Some Government Rules
- 04 Scary Results
- 04 Comfort Levels
- 05 Questions
- 06 Your Checklist (Handout)

iaitam.org | Peace, Love & Asset Management | ACE 2022



6




Responsibility



iaitam.org | Peace, Love & Asset Management | ACE 2022

7



What Does Responsibility Mean

Answerable, or accountable for.
Something within one's power, control, or management

Types of Responsibility

- Legal
- Moral
- Professional
- Social
- Environmental
- Corporate
- Etc.



iaitam.org | Peace, Love & Asset Management | ACE 2022

8



Focus

Legal – what you **MUST** do
Social – what you **COMMIT** to do,
From the lens of your Corporate entity

*Note: Environmental responsibility spans across both

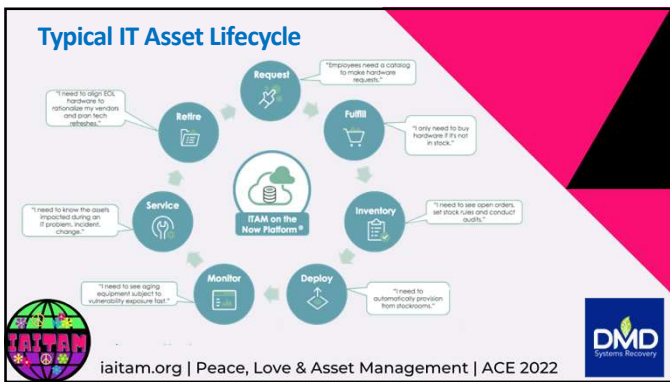


iaitam.org | Peace, Love & Asset Management | ACE 2022

9



10



11




12

What Does EOL Mean


The point at which the asset no longer serves its intended purpose for your organization and is removed to the point that you no longer have any remaining responsibility, and this includes both your specific legal and social responsibilities

The Big Question:

Does the current way you think about End of Life include the end of all of your responsibilities?



iaitam.org | Peace, Love & Asset Management | ACE 2022



13

Quick Break and Stretch



iaitam.org | Peace, Love & Asset Management | ACE 2022



14

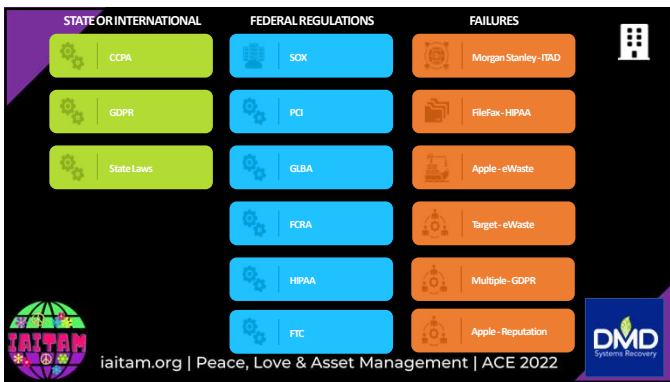
Value Assessment



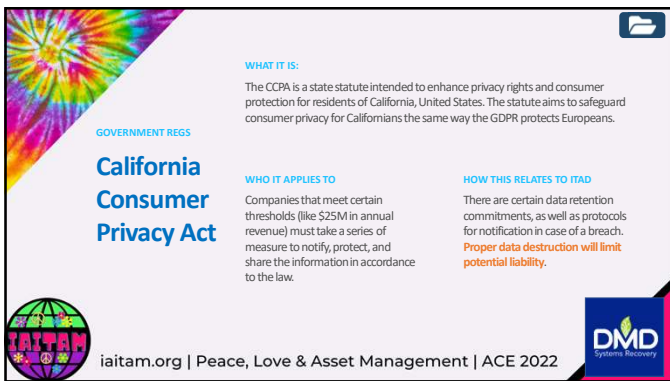
15



16



17



18

Data Processors and Data Controllers – CCPA and GDPR

GOVERNMENT REGS

WHAT IT IS:
It is not possible to relieve either party of their responsibilities under the GDPR. If a data subject's personal data is processed unlawfully, they have a legal right to pursue compensation from a data controller.

A DPA can't relieve a data controller of its liability to a data subject or a Data Protection Authority, even if an incident is clearly the data processor's fault.

HOW THIS RELATES TO ITAD
Unlimited liability and indemnification do NOT absolve you of your responsibility.

iaitam.org | Peace, Love & Asset Management | ACE 2022

DMD Systems Recovery

19

State Laws

e-waste Laws
Currently exist in 25 states

Data Protection Laws
Currently exist in 35 states

iaitam.org | Peace, Love & Asset Management | ACE 2022

DMD Systems Recovery

20

Sarbanes-Oxley

GOVERNMENT REGS

WHAT IT IS:
The Sarbanes-Oxley Act, also called Sarbanes-Oxley, Sarbox or SOX, is a 2002 United States federal law that set new or expanded requirements to protect the public from fraudulent or erroneous practices by corporations and other business entities. The goal was to increase transparency and require a formalized system of checks and balances in a company.

ACTUAL LANGUAGE
SOX compliance requirements include formal data security policies that are communicated and enforced. The data security strategy must protect all financial data stored and utilized.

HOW THIS RELATES TO ITAD
Companies governed by SOX must secure their financial data throughout the company and throughout that data's existence. Proper disposal is a legal requirement.

iaitam.org | Peace, Love & Asset Management | ACE 2022

DMD Systems Recovery

21



WHAT IT IS:

The Payment Card Industry Data Security Standard, PCI DSS, or PCI for short is a set of requirements developed to ensure the maintenance of a secure environment for all companies that process, store, or transmit credit card information.

GOVERNMENT REGS

PCI DSS

WHO IT APPLIES TO

This **applies to every company regardless of volume**. If you use a third-party processor for two transactions a month, you must comply.



HOW THIS RELATES TO ITAD

If you have any credit card information, **you are responsible for adherence for the life of the data**, making responsible destruction an important risk mitigation strategy.



iaitam.org | Peace, Love & Asset Management | ACE 2022

22



WHAT IT IS:

The GLBA is also known as the Financial Services Modernization Act of 1999. The act requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.

GOVERNMENT REGS


Gramm-Leach-Bliley Act

WHO IT APPLIES TO

Financial institutions are companies that offer consumer financial products or services like loans, financial or investment advice, or insurance.



HOW THIS RELATES TO ITAD

Companies this impacts must be consistent with the **FTC's Disposal Rule**, which includes the **erasure of media or hardware that contains customer information**.



iaitam.org | Peace, Love & Asset Management | ACE 2022

23



WHAT IT IS:

The Fair Credit Reporting Act (FCRA) is U.S. Federal Government legislation enacted in 1970 to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies.

GOVERNMENT REGS

Fair Credit Reporting Act


WHO IT APPLIES TO

Surprisingly, more companies than you think, must comply. This includes Consumer Reporting Agencies (CRAs) like credit bureaus, companies who report information to the CRAs like financial institutions, and **any company who uses credit reports including in a hiring procedure**.

HOW THIS RELATES TO ITAD

All companies with this personal data have legal obligations to **protect this sensitive information until its disposal**.

NOTE: There was an amendment, Fair and Accurate Credit Transaction Act (FACTA) that stipulates requirements for information privacy, accuracy and disposal.



iaitam.org | Peace, Love & Asset Management | ACE 2022

24



Health Insurance Portability and Accountability Act

GOVERNMENT REGS

WHAT IT IS:
HIPAA is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

WHO IT APPLIES TO
Organizations that must comply with HIPAA as Covered Entities are health care providers, health plans, and health care clearinghouses. Additionally, any individual or entity that performs functions on behalf of a HIPAA-covered entity and involves the use of protected health information is considered a HIPAA Business Associate and must comply.

HOW THIS RELATES TO ITAD
Companies that are a Covered Entity or a Business Associate are legally obligated to protect the health information, which persists until the data is eliminated.

iaitam.org | Peace, Love & Asset Management | ACE 2022

25



FTC Disposal Rule

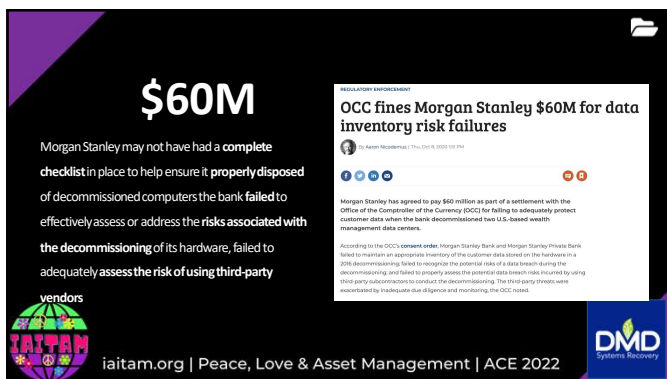
GOVERNMENT REGS

WHAT IT IS:
Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

WHAT IT SPECIFIES
Due diligence and monitoring compliance with a contract with another party engaged in the business of record destruction (consumer information). Due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security procedures, or taking other appropriate measures.

iaitam.org | Peace, Love & Asset Management | ACE 2022

26



\$60M

Morgan Stanley may not have had a complete checklist in place to help ensure it properly disposed of decommissioned computers the bank failed to effectively assess or address the risks associated with the decommissioning of its hardware, failed to adequately assess the risk of using third-party vendors

OCC fines Morgan Stanley \$60M for data inventory risk failures

REGULATORY ENFORCEMENT


By Aaron Moskowitz | The Week, 2022-03-04

Morgan Stanley has agreed to pay \$60 million as part of a settlement with the Office of the Comptroller of the Currency (OCC) for failing to adequately protect customer data when the bank decommissioned two U.S.-based wealth management data centers.

According to the OCC's consent order, Morgan Stanley Bank and Morgan Stanley Private Bank failed to maintain an appropriate inventory of the customer data stored on the hardware in a 2014 decommissioning, failed to recognize the potential risks of a data breach during the decommissioning, and failed to properly assess the potential data breach risks incurred by using third-party subcontractors to conduct the decommissioning. The third-party vendors were inadequately vetted due to a lack of diligence and monitoring, the OCC noted.

iaitam.org | Peace, Love & Asset Management | ACE 2022

27



aitam.org | Peace, Love & Asset Management | ACE 2022

Consequences for HIPAA violations don't stop when a business closes

A receiver appointed to liquidate the assets of Filefax, Inc. has agreed to pay \$100,000 out of the receivership estate to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Filefax, located in Northbrook, Illinois, advertised that it provided for the storage, maintenance, and delivery of medical records for covered entities. Although Filefax shut its doors during the course of OCR's investigation into alleged HIPAA violations, it could not escape its obligations under the law.

On February 10, 2015, OCR received an anonymous complaint alleging that an individual transported medical records obtained from Filefax to a shredding and recycling facility to sell on February 6 and 9, 2015. OCR opened an investigation, which confirmed that an individual had left medical records of approximately 2,150 patients at the shredding and recycling facility, and that these medical records contained patients' protected health information (PHI).


OCR's investigation indicated that between January 28, 2015, and February 14, 2015, Filefax impermissibly disclosed the PHI of 2,150 individuals by leaving the PHI in an unlocked truck in the Filefax parking lot, or by granting permission to an unauthorized person to remove the PHI from Filefax, and leaving the PHI unprotected outside the Filefax facility.

"The careless handling of PHI is never acceptable," said OCR Director Roger Severino. "Covered entities and business associates need to be aware that OCR is committed to enforcing HIPAA, regardless of whether a covered entity is opening its doors or closing them. HIPAA still applies."


\$100K

an individual transported medical records to a shredding and recycling facility...**left medical records of approximately 2,150 patients with PHI... in an unlocked truck outside the facility**

Although Filefax shut its doors, it **could not escape its obligations under the law**



28



aitam.org | Peace, Love & Asset Management | ACE 2022


Apple to pay \$450,000 after allegations of hazardous waste violations

Apple Inc. has agreed to pay \$450,000 as part of a settlement with the California Department of Toxic Substances Control (DTSC) regarding allegations of hazardous waste violations at two electronic waste shredding facilities that the tech firm operated.

The settlement follows a 2015 investigation by DTSC into Apple's operations at two e-waste shredding facilities in California. The investigation found that Apple had violated DTSC's hazardous waste handling and disposal regulations. As part of the settlement, Apple agreed to pay the \$450,000 fine and implement various safety and compliance measures to prevent future violations.

\$450K

A settlement with the California Department of Toxic Substances Control, which alleged it found **hazardous waste violations at two electronic waste shredding facilities** that the tech firm operated



29



aitam.org | Peace, Love & Asset Management | ACE 2022

\$7.4M

California's 2003 Electronic Waste Recycling Act mandates businesses to **dispose all their hazardous e-wastes, comprising of LCD TVs and laptops, computers and other fluorescent cathode ray tube powered devices, including miscellaneous electronic devices like circuit boards and batteries... properly.**

B TARGET TO PAY A \$7.4 MILLION FINE FOR ILLEGALLY DEPOSITING E-WASTE IN GULF TRASH

Target Inc. has been charged with depositing hazardous waste and other electronic waste and medical waste in the trash for four years.

The Santa Clara County District Attorney's Office has confirmed that Target has agreed to a \$7.4 million civil penalty for depositing hazardous waste and other electronic waste in the trash for four years.

California's 2003 Electronic Waste Recycling Act requires different regulations and obligations for recycling e-waste. The law mandates that businesses must dispose of their hazardous waste, including LCD TVs and laptop computers and other electronic devices, in a certified e-waste recycling facility. The law also requires businesses to maintain records of their e-waste disposal and to provide information to the public about their e-waste disposal practices.

The waste included items such as electronic devices, power tools, computer monitors, light bulbs, and medical waste including syringes and other sharps and protected pharmaceuticals as well as confidential information from customers.

Last year, Target faced a class-action lawsuit in federal court for allegedly mismanaging e-waste. Target had agreed to a \$1.5 million settlement with the plaintiffs, but the settlement was later overturned by a federal judge. The judge ruled that the settlement was not in the best interests of the plaintiffs and that Target should be held accountable for its e-waste disposal practices.



30

[illegible][illegible]




What are examples of Social Responsibility?




iaitam.org | Peace, Love & Asset Management | ACE 2022




34

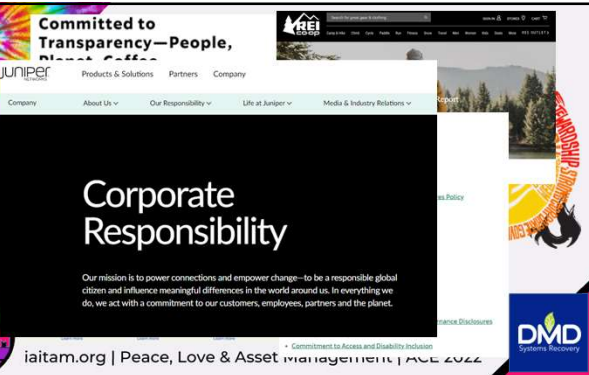


Committed to Transparency—People, Planet, Profit



iaitam.org | Peace, Love & Asset Management | ACE 2022





35



Better yet, what are your company's social commitments?



iaitam.org | Peace, Love & Asset Management | ACE 2022



36



aitam.org | Peace, Love & Asset Management | ACE 2022

Social / Corporate

Corporate Values
What we stand for

You CAN & DO get to add your own

WHAT IT IS:
Impacts so many things, including:

- Hiring
- Retention
- Reputation
- Customer Contracts and Terms
- Press Coverage
- How customers think of you

HOW THIS RELATES TO ITAD
Data Security (breaches)
Privacy
Environmental Commitments



DMD
Systems Recovery

37



aitam.org | Peace, Love & Asset Management | ACE 2022

Mini Recap



DMD
Systems Recovery

38



aitam.org | Peace, Love & Asset Management | ACE 2022

What We've Covered

Types of Responsibility

- Legal examples
- Social

End of Life

- Definition and Consideration

Legal Responsibility

- Environmental
- Data

Social Responsibility

- Definition and Your Commitments



DMD
Systems Recovery

39

What Should I Do?



iaitam.org | Peace, Love & Asset Management | ACE 2022



40

What is the Big Mistake?



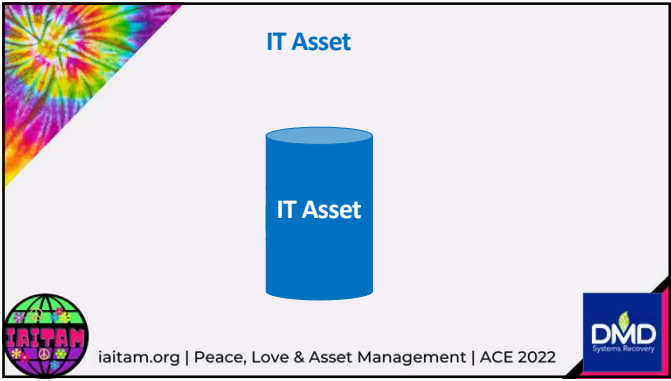
iaitam.org | Peace, Love & Asset Management | ACE 2022



41



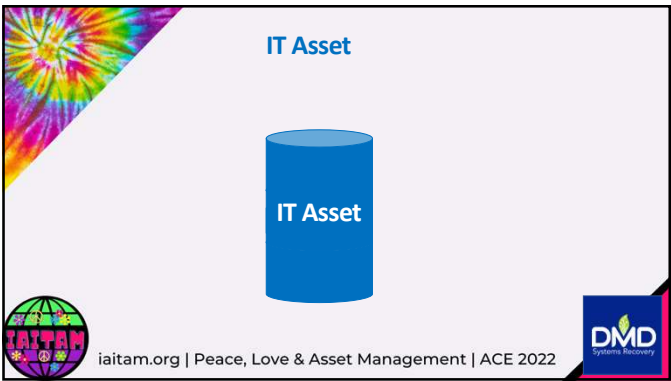
42



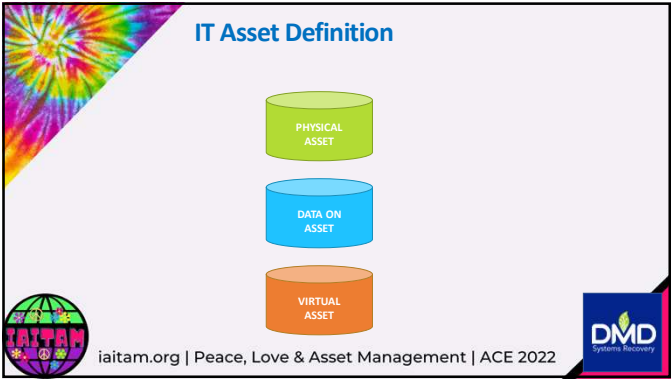
43



44



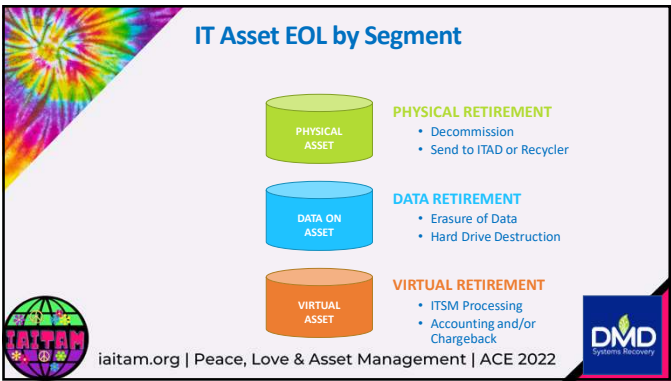
45



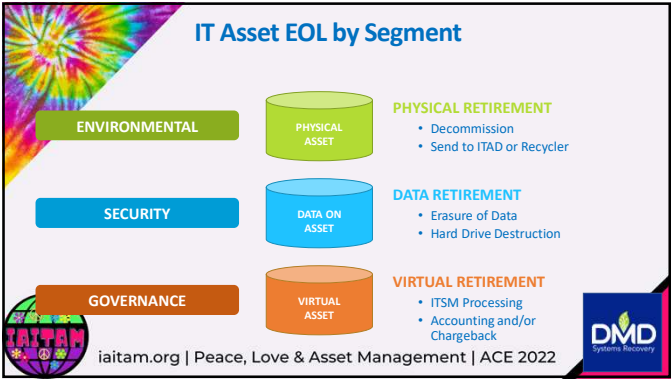
46



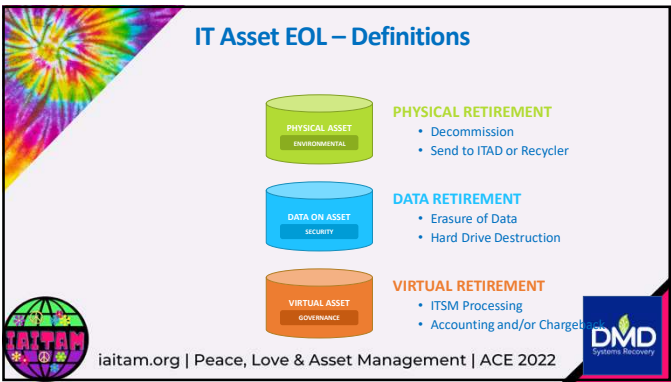
47



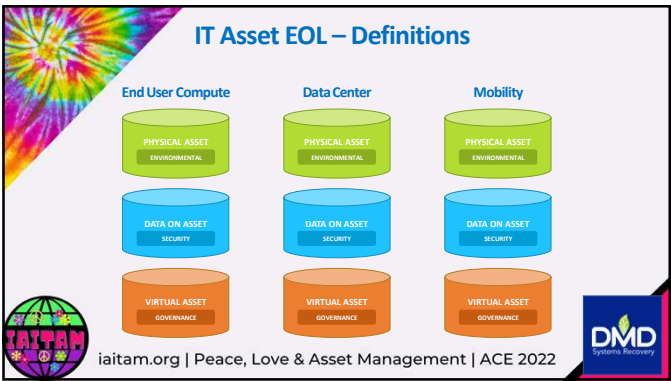
48



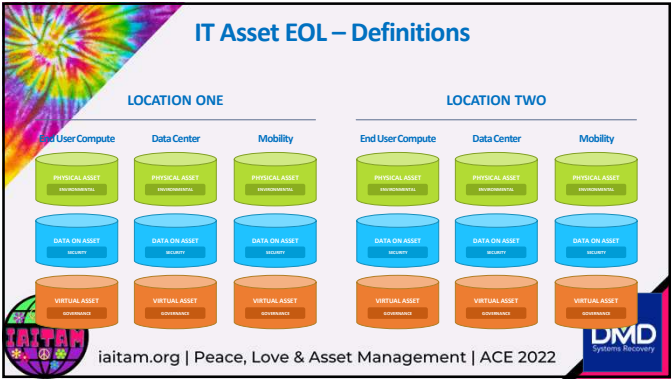
49



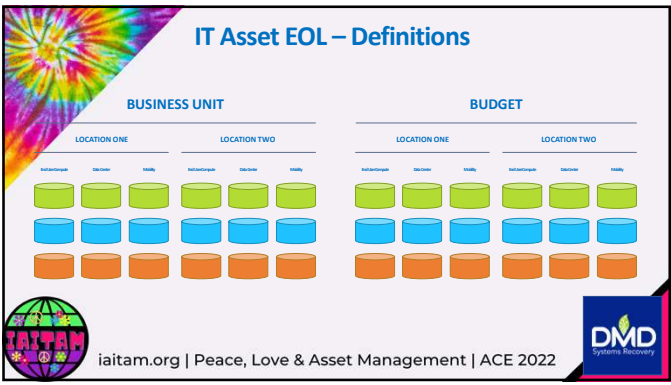
50



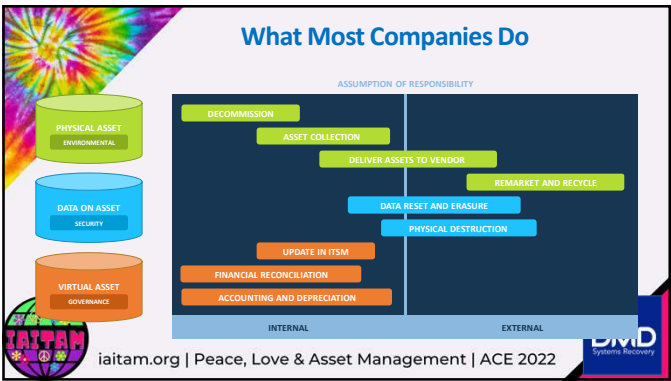
51



52



53



54



55



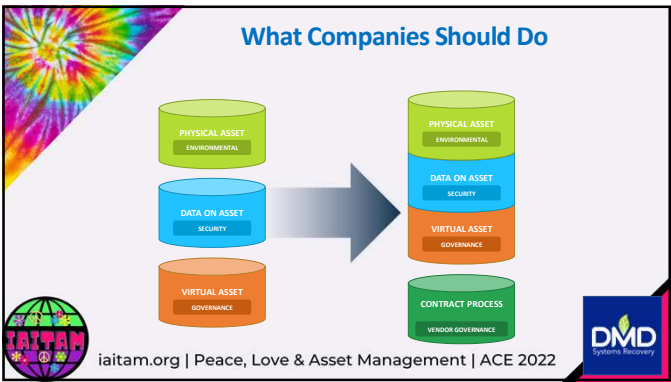
56



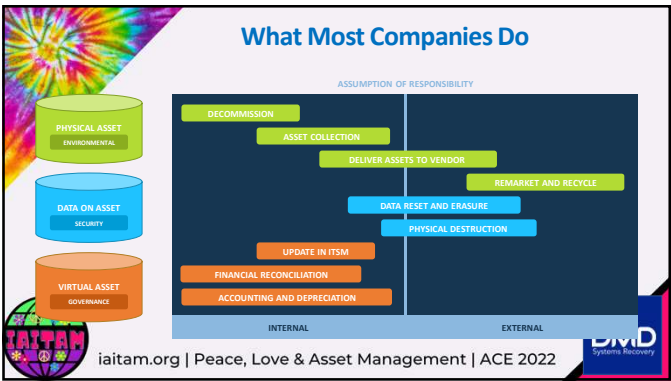
57



58



59



60



EOL Comfort Levels


	Acceptable	Proficient	Excellent
PHYSICAL ASSET ENVIRONMENTAL	<ul style="list-style-type: none">Certified by 3rd PartyHazardous Waste PolicyState Law Adherence	<ul style="list-style-type: none">Impact or Emission Reduction ReportingReuse First Policy	<ul style="list-style-type: none">Alignment of Sustainability Values – both organization and vendor
DATA ON ASSET SECURITY	<ul style="list-style-type: none">Certified by 3rd PartyCompliant Standard	<ul style="list-style-type: none">Certificates of Destruction by AssetCertified Facility	<ul style="list-style-type: none">Wipe data by AssetOnsite OptionsRemote PurgeAlignment w/ Org Policy
VIRTUAL ASSET GOVERNANCE	<ul style="list-style-type: none">ContractInsuranceIndustry Specific	<ul style="list-style-type: none">Chain of CustodyContractual SLAsIndemnity DocumentationDocumented Procedures	<ul style="list-style-type: none">Governance AssistanceSupplier Closure PlansInsuranceStandard terms for all locations & assets

COMFORT LEVEL

iaitam.org | Peace, Love & Asset Management | ACE 2022



61



Recap

iaitam.org | Peace, Love & Asset Management | ACE 2022



62



What We've Covered

- Types of Responsibility**
 - Legal & Social
- End of Life**
 - Definition and Consideration
- Legal Responsibility**
 - Environmental & Data
- Social Responsibility**
 - Definition and Your Commitments
- Three Segments of an IT Asset**
 - Definition, Complexity and Steps
- The Path to Comfort**
 - Three levels and a Checklist

iaitam.org | Peace, Love & Asset Management | ACE 2022



63

ITAD Solutions
THREE CRITICAL FACTORS SOLVED SYNCHRONOUSLY

PHYSICAL ASSET
ENVIRONMENTAL

DATA ON ASSET
SECURITY

VIRTUAL ASSET
GOVERNANCE

RESULT IN:
Complete Responsibility

iaitam.org | Peace, Love & Asset Management | ACE 2022

64

Questions

iaitam.org | Peace, Love & Asset Management | ACE 2022

65

I've indemnified my liability by assigning it to my vendor. What is my risk?

iaitam.org | Peace, Love & Asset Management | ACE 2022

66



What is the FTC Disposal Rule?

What it is:
Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

What it specifies:
Due diligence and monitoring compliance with a contract with another party engaged in the business of record destruction (consumer information). Due diligence could include **reviewing an independent audit** of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from **several references** or other reliable sources, requiring that the disposal company be **certified by a recognized trade association** or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures.

iaitam.org | Peace, Love & Asset Management | ACE 2022



67



When You Get Home

iaitam.org | Peace, Love & Asset Management | ACE 2022



68



EOL Responsibility Checklist

Acceptable	Proficient	Excellent
Environmental <ul style="list-style-type: none"> ISO 14001 or equivalent Certification (not membership) Hazardous Waste Confirmation 	Environmental <ul style="list-style-type: none"> Impact or Emission Reduction Reporting Reuse First Policy 	Environmental <ul style="list-style-type: none"> Alignment of Sustainability Values (organizational & vendor)
Security <ul style="list-style-type: none"> ISO 27001 or FIPS 140-2 Certification (not membership) NOT Standard 800-88 R1 or DoD 5252.02 M 	Security <ul style="list-style-type: none"> Certificates of Destruction by Asset Certified Facility ISO 27001 or equivalent 	Security <ul style="list-style-type: none"> Wipe Logs by Asset Onsite Purge Remote Purge Alignment of Organizational Security Policy
Governance <ul style="list-style-type: none"> Insurance ISO 9001, ISO 14001, ISO 27001, etc. Industry Specific HIPAA, FCRA, GLBA, SOX, etc. Contract Terms & Conditions 	Governance <ul style="list-style-type: none"> Chain of Custody Inventory Documentation Disclaimer Contractual SLAs Insurance Documented Procedure by Compliance Standard HIPAA, FCRA, etc. 	Governance <ul style="list-style-type: none"> Supplier Closure Plans Corporate Governance Assistance Reporting current and historical Insurance ISO 9001, ISO 14001, ISO 27001, etc. ISO 27001 (aligned to average breach cost)


Low Comfort Level High

Each industry and company has environmental, security, and compliance criteria for IT Asset Disposition. The criteria ranges from highly mandated to socially committed to organization preference. You should work with your provider to ensure compliance with your stated and desired responsibility with specific services, methods, and outcomes that result in a standardized contract with defined terms and SLAs for all locations and all assets.

877.777.6651 | INFO@DMDSYSTEMS.COM | WWW.DMDSYSTEMS.COM



69



Happy to Help

Aaron Zeper
zeper@dmdsystems.com
480.363.2510 (cell)



iaitam.org | Peace, Love & Asset Management | ACE 2022

