Value-4IT

GSE UK Conference 2014: Session HE

Compliant z/OS Data Life Cycle Processes: Storage & Security Management Interaction

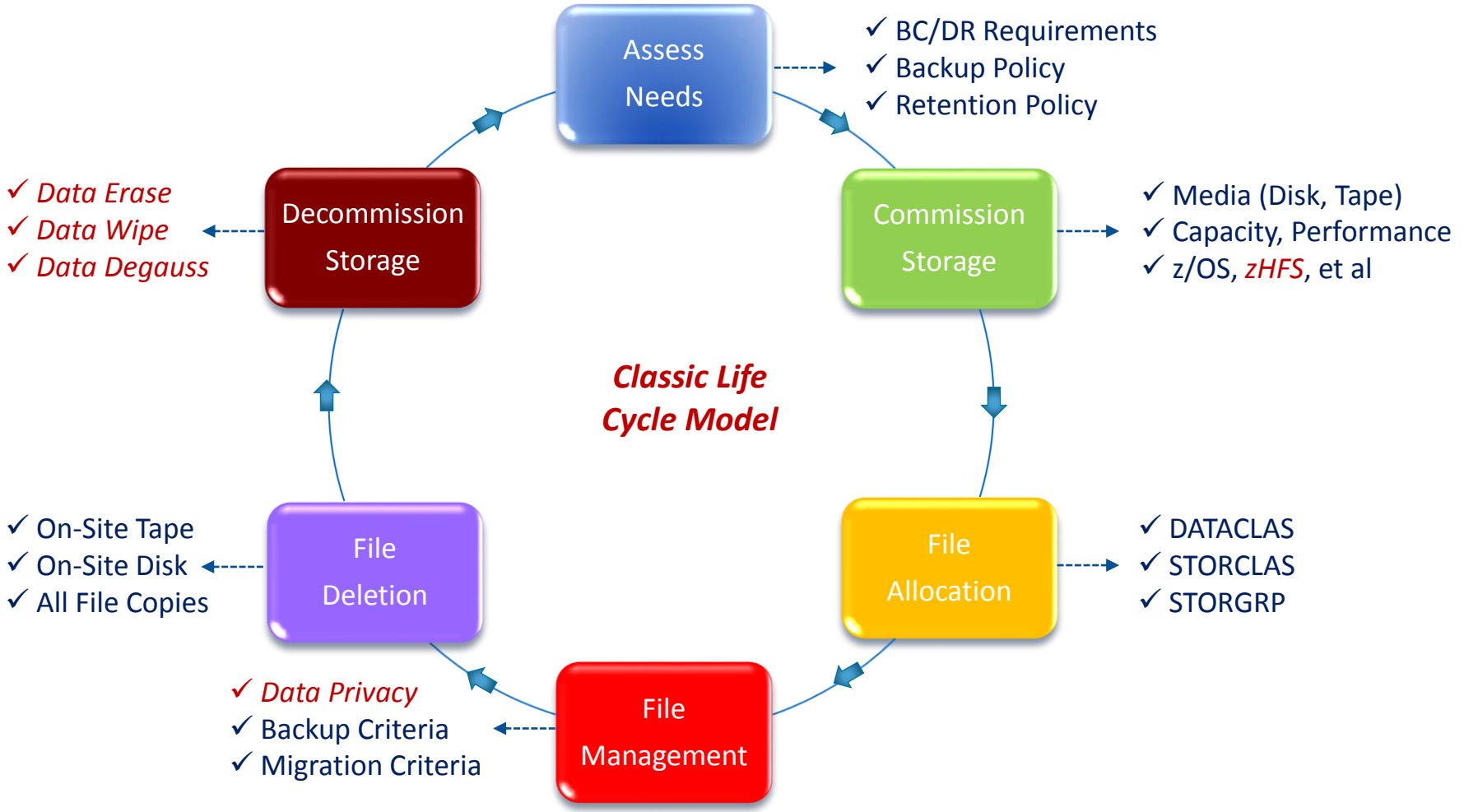
Michael W. Moss (mossmw@value-4it.com)

Introduction - Agenda

- Simple File-Storage Management Lifecycle
- High Availability & 3rd Party DR Configurations
- Regulatory Compliance: Data Protection Act, ISO 27001, PCI-DSS…
- Safeguarding Business Data Security: A Living Process
- z/OS: External Security Manager (ESM) Interaction
- STIG (Security Technical Implementation Guide) Checklists
- z/OS Storage: Data Sanitization & Media Destruction Examples
- z/OS Storage: Tape & Disk Sanitization Observations
- z/OS Storage: Disk Data Set Erase-On-Scratch (EOS)
- Data Sanitization: Is Wiping With Binary Zeroes Enough?
- z/OS Storage: Data Privacy - The Application Test Bed
- UNIX System Services (USS) - Who Manages Data Access?
- Regulatory Compliance & Data Sanitization – Web Links

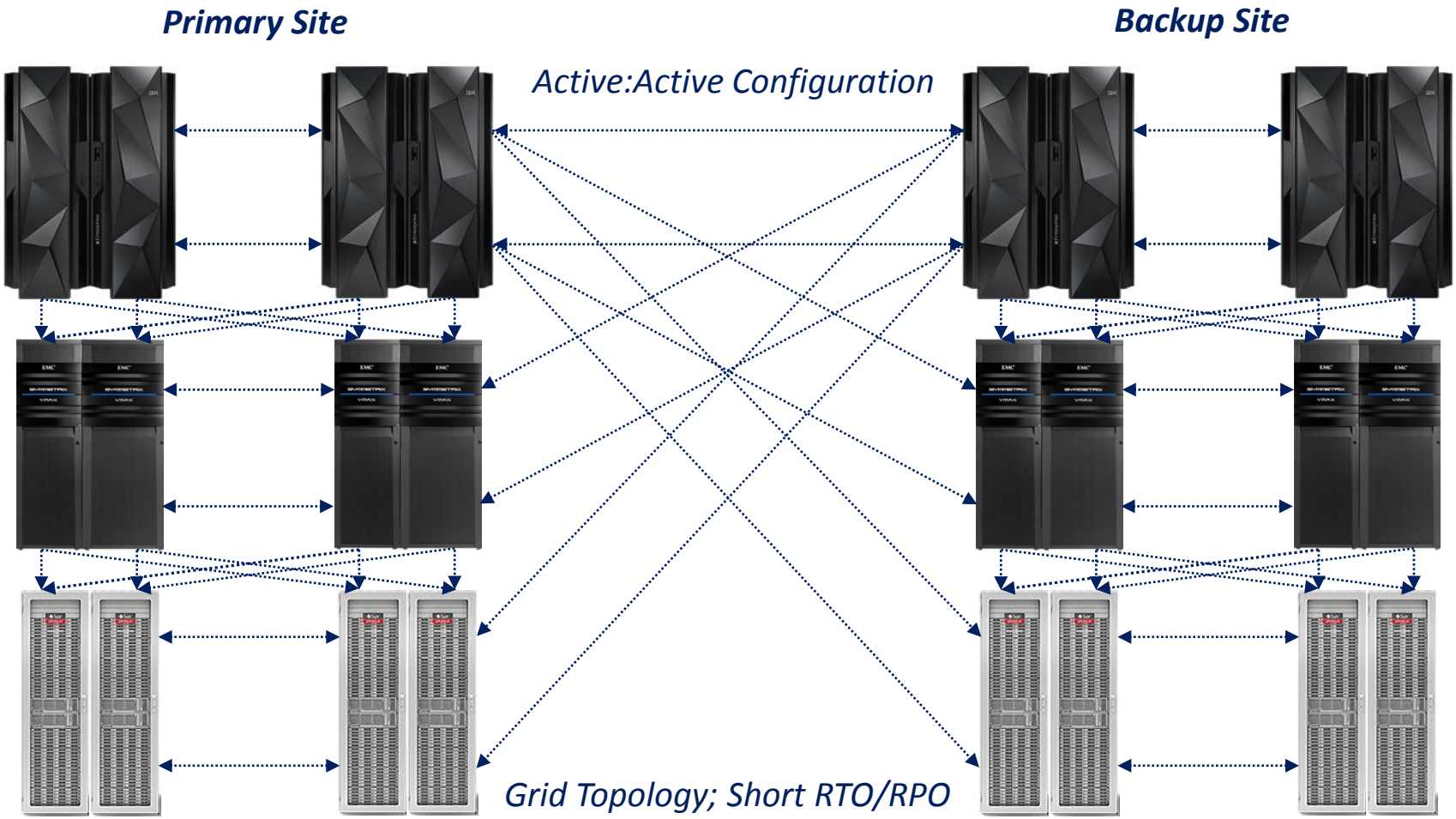
Disclaimer: Primarily this presentation is for "data at rest"

Simple File-Storage Management Lifecycle



A classic & simple process; but is it really that straightforward?

High-Availability Data Centres: A Secure Utopia?



Storage media & thus data remain in the Data Centre; always?

3rd Party DR Service Provision: An Ad-Hoc Event…

Customer Site

3rd Party Site

System Data could be periodically shipped (I.E. when changed), to maintain an active customized LPAR for rapid DR activation

All secondary data copies could be shipped directly to 3rd party site

We trust our 3rd party suppliers to always safeguard our data!

Regulatory Compliance: Common UK Requirements

The Data Protection Act 1998: For Information Security the Seventh Data Protection Principle states "Appropriate technical & organisational measures shall be taken against unauthorised or unlawful processing of personal data & against accidental loss or destruction of, or damage to, personal data. You will need to:"

- *Design & organise your security to fit the nature of the personal data you hold & the harm that may result from a security breach;*
- *Be clear about who in your organisation is responsible for ensuring information security;*
- *Make sure you have the right physical & technical security, backed up by robust policies & procedures & reliable, well-trained staff; &*
- *Be ready to respond to any breach of security swiftly & effectively.*

There is no "one size fits all" solution to information security. The security measures that are appropriate for an organisation will depend on its circumstances, so you should adopt a risk-based approach to deciding what level of security you need.

Computer security is constantly evolving, & is a complex technical area. Depending on how sophisticated your systems are & the technical expertise of your staff, you may need specialist information-security advice that goes beyond the scope of this Guide. A list of helpful sources of information about security is provided (There is an international standard for information security management. A detailed look at ISO 27001; includes an audit & certification scheme…)

A common business requirement, without specific compliance!

Regulatory Compliance: A Common Business Standard

ISO 27001 security

ISO/IEC 27001: International standard for information security management. It outlines how to put in place an independently assessed & certified information security management system. This allows you to more effectively secure all financial & confidential data, so minimizing the likelihood of it being accessed illegally or without permission.

Data: Category	Example Documents/Reports	Distribution	Destruction/Disposal
Internal: Proprietary	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate & inconvenient. Disclosure to anyone outside the company requires management authorization.	Electronic: Use internal Email system. Encryption is required for transmission to external Email addresses.	Electronic data: Erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.
Confidential: Restricted	Highly sensitive or valuable information, both proprietary & personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager.	Electronic: Use internal Email system only. Encrypt data.	Electronic data: Erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.

A common UK standard, required by many businesses to trade!

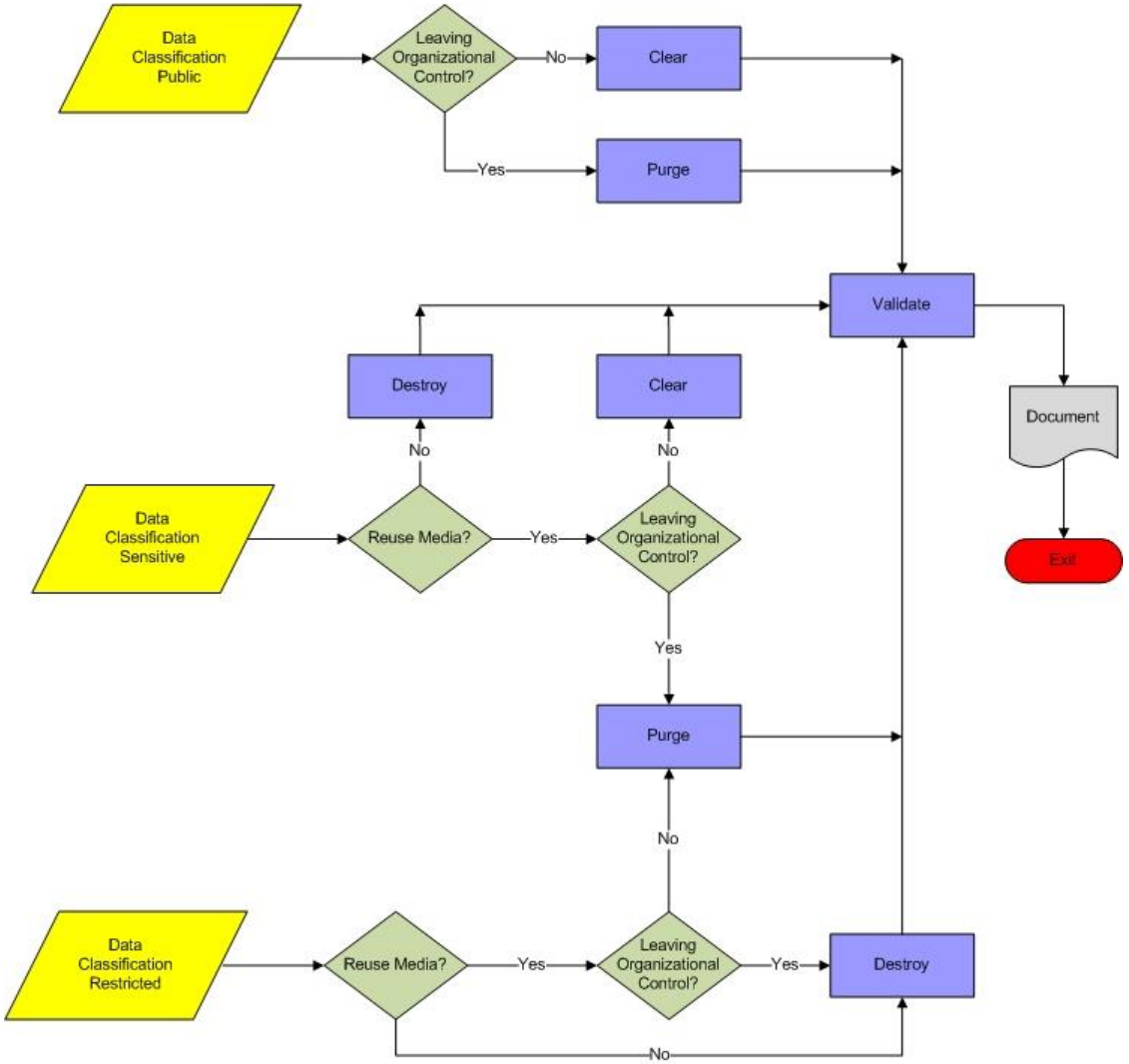
Regulatory Compliance: Data Sanitization Flowchart

Data Classification

Public: Web, Adverts, Brochures, et al
Sensitive: SLA, Intranet, Policies, Contact, etc.
Restricted: Proprietary, HR, PIN/VPN, etc.

Reuse Media?

A key data sanitization decision is whether media will be reused or recycled. Tape is often reused to conserve & optimize resources. If media is not intended for reuse either within or outside of the organization due to damage or other reasons, the simplest & most cost-effective method of control may be Destroy.



Validate (QA Check)

Process due diligence & sanity check. Verify internal & external 3rd party data sanitization & disk/tape storage media destruction.

Organizational Control

A factor influencing a sanitization decision is who has control & access to the media. This aspect must be reviewed when media leaves organizational control. Media control may be transferred when storage media is returned from a leasing agreement or is being donated or resold/reused outside of the organization.

Regulatory Compliance: A Common Financial Standard

PCI-DSS: The Payment Card Industry Data Security Standard was developed to encourage & enhance cardholder data security & facilitate the broad adoption of consistent data security measures globally. PCI-DSS provides a baseline of technical & operational requirements designed to protect cardholder data. PCI-DSS applies to all entities involved in payment card processing that store, process or transmit cardholder data (CHD) &/or sensitive authentication data (SAD).

Requirement	Testing Procedure	Guidance
3.1 Keep cardholder data storage to a minimum… ▪ Secure Deletion… ▪ Specific Retention… ▪ Periodic Cleanup…	▪ Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons ▪ Coverage for all storage of cardholder data ▪ A quarterly process for identifying & securely deleting stored cardholder	A formal data retention policy identifies what data needs to be retained…so it can be securely destroyed or deleted as soon as it is no longer needed. The only cardholder data stored after authorization is the primary account number (unreadable PAN), expiration date, cardholder name, & service code.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program (in accordance with industry-accepted standards for secure deletion), or by physically destroying the media.	Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).

A global standard for most companies trading with consumers.

Regulatory Compliance: US Government Example

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST: The National Institute of Standards Media Sanitization guidelines states "Several different methods can be used to sanitize media. Several of the most common are provided. The selected method should be assessed as to cost, environmental impact, etc., & a decision should be made that best mitigates the risks to an unauthorized disclosure of information".

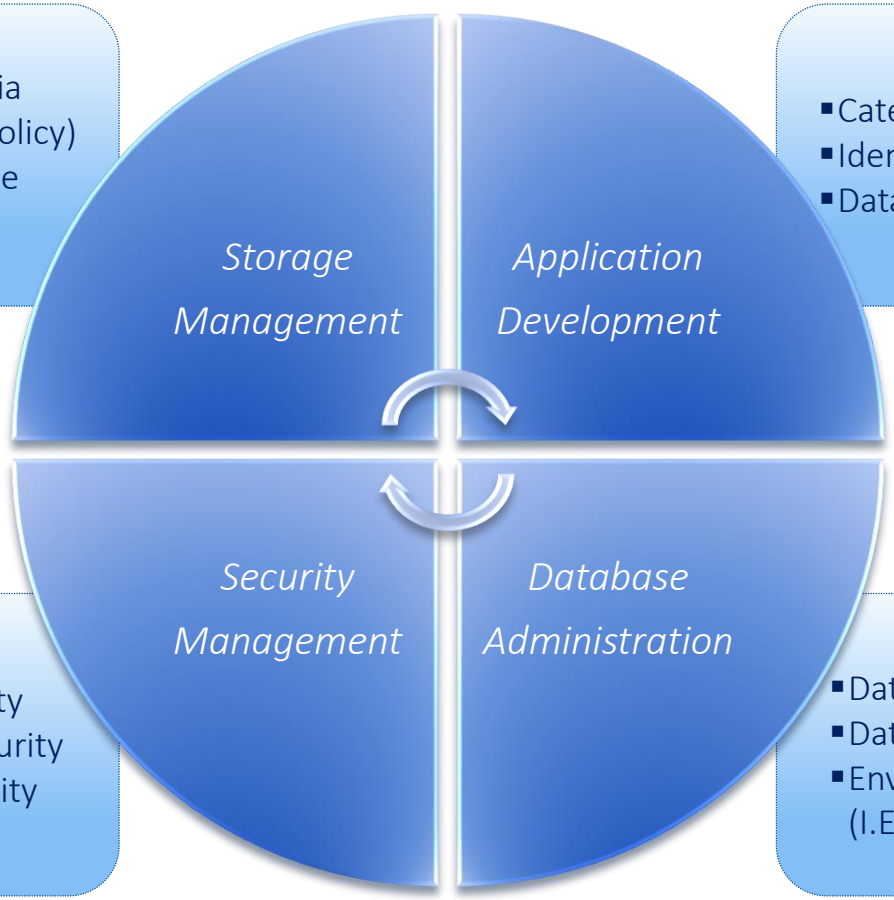
Action	Description
Reel & Cassette Format Magnetic Tapes	
Clear	Re-record (overwrite) all data on the tape using an organizationally approved pattern, using a system with similar characteristics to the one that originally recorded the data.
Purge: Destroy	Degauss the magnetic tape in an organizationally approved degausser: Incinerate by burning the tapes in a licensed incinerator or Shred.
ATA Hard Drives	
Clear	Overwrite media via validated overwriting tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge	ATA Sanitize or ATA Secure Erase or Cryptographic Erase or Degauss or disassemble the hard disk drive & Purge the enclosed platters with an organizationally approved degaussing wand.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

A detailed technical standard & associated ~50 page guide…

Safeguarding Business Data Security: A Living Process

- Allocate storage media
- Data management (policy)
- Decommission storage (data & media)

- Categorize data (business)
- Identify data retention
- Data privacy classification



CISO/CSO/CIO, CTO must support/drive this process!

Engage the company DPO (Data Protection Officer)!

- Storage media security
- Data interchange security
- File/File system security

- Data retention processes
- Data privacy processes
- Environment allocation (I.E. Test, Dev, Prod, et al)

Requires organizational collaboration & management support!

z/OS: External Security Manager (ESM) Interaction

What comes first; the data, the storage or the security policy? In the commercial world, of course the data came first & IT allowed data to be stored electronically. In 1964, what we know as the IBM Mainframe was introduced. In 1976, the first ESM was introduced, RACF, with User identification/verification & Data set authorization checking. In 1977, RACF included TAPE & DASD Volume protection. In 1985, DASD erase-on-scratch; in 1988, DFSMS (STGADMIN Facility Class) support & in 1994 OpenEdition MVS (USS) support. Not far behind, were the CA ESM solutions, ACF2 & Top Secret. Therefore, it could be ~20 years since we last implemented any major storage security function… We can refer to a plethora of technical manuals, ESM, DFSMS, Tape/Database/Report Management, et al, for security settings, but are there any best practices?

The National Institute of Standards & Technology (NIST) Defense Information Systems Agency (DISA) provides a comprehensive set of Security Technical Implementation Guides (STIG) for z/OS & the 3 External Security Managers, namely ACF2, RACF & Top Secret.

These documents provide procedures for conducting a Security Readiness Review (SRR) to determine compliance with the requirements. The SRR guide focuses on the IBM z/OS Operating System (OS) & how the ESM interacts with the operating system. Additionally, this checklist ensures the site has properly installed & implemented the ESM component for z/OS & that it is being managed in a secure, efficient & effective manner, by procedures outlined in the checklist.

Storage/Security managers might consider an ESM STIG review

STIG (Security Technical Implementation Guide) Checklists

The STIG guides provide a comprehensive review at the Operating System level, including storage management interaction. There are also a limited number of software product specific STIG guides, where the following table provides a cross-reference of "storage management" solutions:

ESM: Software Product	*CA ACF2*	*IBM RACF*	*CA Top Secret*
Full z/OS Operating System (Including DFSMS, Tape & Disk)	✓	✓	✓
BMC Control-D (Report Management Includes Disk/Tape Storage)	✓	✓	✓
CA 1 Tape Management	✓	✓	✓
CA Vtape Virtual Tape System	✓	✓	✓
IBM Transparent Data Migration Facility (TDMF)	✓	✓	✓
Innovation FDR (Fast Dump Restore)	✓	✓	✓
Rocket Catalog Solution (CSL)	✓	✓	✓
The Full z/OS Operating System review is by far the best checklist, providing a comprehensive & detailed review of storage management security resources. The other storage software product checklists are good, but the limited number of guides is disappointing. Ideally, the ISV (E.g. ASG, BMC, CA, IBM, et al) should commit to preparing STIGs for all their products, providing full coverage of best practices for all z/OS software products.			
Note: Download ESM DISA STIGs @ http://iase.disa.mil/stigs/os/mainframe/Pages/zOS.aspx			

STIGs are designed to pass a Security Readiness Review (Audit)!

z/OS Storage: Data Sanitization & Media Destruction

Whatever regulatory compliance standard(s) apply to your organization, ultimately a decision needs to be made as to what data sanitization (clean/erase/purge) & subsequent storage destruction processes are deployed. To some extent, from a regulatory compliance viewpoint, there is a modicum of flexibility as to how an individual organization implements these processes. *However, recognizing that only data differentiates one business from another, the value of that data is arguably priceless. Therefore one must draw one's own conclusions as to what extent data is sanitized, once the storage media it resides on, is finally decommissioned from the business.*

Data Sanitization (Clean/Erase/Purge) Examples	*Safeguarding Business Data Observations*
Disk (DASD, VTL cache) technology refresh (E.g. End of lease, Asset disposal)	*Will disks be sold onto the 2nd user market?*
Disk/tape reuse by another company group member	*Some compliance standards require "separate entity" reporting & thus "resource sharing" is questionable*
Tape (cartridges) failure or end-of-life replacement	*Will tapes be sold onto the 2nd user market?*
Cold site Disaster Recovery (DR) test at 3rd party site	*Is all data, disk & tape "sanitized" ASAP following the DR test? Which party performs this process?*
When disks/tapes are moved to another location for permanent or interim reuse	*Should storage media be sanitized before transit from one site to another (new data copy already active)*

Is in-house z/OS full data sanitization optional or mandatory?

z/OS Storage: Data Sanitization – IBM Standard Utilities

From a simplistic viewpoint, IBM does provide function in their standard utilities to erase data. One must draw one's own conclusions as to the sanitization (erase) techniques used & the speed & resource efficiency of these utilities. In essence, these standard IBM utilities are not designed for mass or specialized processing, just for general day-to-day & periodic activities.

Data Erase Activity	*ICKDSF*	*DITTO*
Disk track erase (Overwrite data via n cycles)	*TRKFMT ERASEDATA (Max 10 Cycles) IBM & National Computer Security Centre (NCSC) approved pattern.* *Issue: Slow; data access possibility?*	*Limited console originated Disk Track Edit (DTE) command. No pre defined data patterns, no batch interface.* *Issue: Slow, unusable, unsecure.*
Full disk volume media (track) initialize (Medial Initialization)	*INIT VALIDATE NOCHECK rewrites the home address & record 0 for the entire disk volume.* *Issue: Data easily accessible.*	*N/A*
Full tape erase (remove VOLSER information & data)	*N/A*	*ERT (Erase Tape), function writes 2 tape marks (header), erases the remainder of the tape via data security erase I/O command.* *Issue: Slow; data access possibility?*

Data sanitization is possible, but usability & data access issues!

z/OS Storage: Data Sanitization – Several ISV Options

Based on a notion that *"if you torture the data long enough it will confess"*, where standard z/OS utilities offer limited function; the 3rd party ISV market place offers specialized software for compliant data sanitization, for example:

Data Erase Activity	*Dino-Software XTINCT (Disk & Tape)*	*INNOVATION FATS (Tape) FDRERASE (Disk)*	*NewEra Software Fast DASD Erase for z/OS*
Disk track erase (Overwrite data via n cycles)	*Overwrites every track & all addressable locations with binary zeroes or a character, its complement, then a random character (multiple passes per track).*	*Overwrites every track with a single track-length record consisting of binary zeroes, or a user specified pattern (3 to 8 passes per track).*	*Overwrites every track with a single track-length record consisting of binary zeroes & a random byte, or a user specified pattern (multiple passes per track).*
Full disk volume media (track) initialize (Medial Initialization)			
Full tape erase (remove VOLSER information & data)	*Securely erase some or all tape data. DSIINIT function erases all tape volumes for a multiple volume data set.*	*Securely erase some (residual beyond EOT marker) or all tape data. ~20 Minutes (3590).*	*N/A*
Each individual organization must decide whether they will sanitize disk & tape storage media before it leaves their secure premises or following an off-site DR test. Similarly, each organization must decide which regulatory compliance standard(s) they're conforming with, or to acknowledge & document any risk(s), if any are identified.			

A modicum of software delivers optimized & increased function

z/OS Storage: Tape Data Sanitization - Installed Software?

Potentially data sanitization function might be incorporated within an ISV software solution deployed. The following table provides a non-exhaustive list of example utilities:

Data Erase Activity	*Full tape erase (remove VOLSER information & data)*
CA 1	*CTSDEU utility erases residual data after new data has been written to the tape. TMSTPPRO utility erases entire volume using the Data Security Erase (DSE) function; TMSTPPRO runs as an STC (pseudo) & does not produce a report (auditability).*
CA TLMS	*CTSDEU utility erases residual data after new data has been written to the tape. CTSDEU can also be used to erase a scratch tape with BLP processing, which equates to a complete volume erase operation.*
IBM DFSMSrmm	*EDGINERS ERASE: DSE exploits tape drive hardware capability to erase volume data; SHRED specifies that the encrypted volume Data Key should be made unusable; SHREDDSE makes encrypted Data key unusable, erasing (DSE) non-encrypted data.*
Rocket Tape/Copy	*Erase Tape Utility erases all data on one or more tapes. The data can be erased from either the physical load point, or from after the VOL1 label, erasing data to the end of the physical tape using the Data Security Erase (DSE) function.*
The Data Security Erase (DSE) function is hardware based, writing random data for 3490 & 3590 drives. For tape reuse, a DSE function erases all of the data, without damaging the servo tracks. Degaussing the tape erases servo tracks, making the cartridge unusable. Most current z/OS tape software products should provide a DSE utility!	

Do you have an auditable & fast tape data sanitization tool?

z/OS Storage: Disk Data Sanitization – Encryption?

What data should you encrypt is just as important as what data should you not encrypt? Encrypt everything that you can & still be able to recover data in event of a disaster is desirable. As long as system data can be separated from application data, encrypting everything with no performance impact is easier than choosing which data falls into which legislation for encryption & trying to keep current on the dynamic data privacy rights rules & regulations.

The encryption solution deployed should not negatively affect your storage environment & the applications that depend on it. Ideally an encryption solution that does not degrade application performance or jeopardize your disaster recovery plan is required. You also need the assurance that encryption does not cause any data loss & that all the appropriate measures are taken to protect & safeguard the associated encryption keys.

Ideally the zSeries disk encryption solution deployed utilizes disks that have hardware based encryption, performing symmetric encryption & decryption of data at full disk speed with no impact on performance, usability, scalability, availability, et al. Key management is of vital importance, utilizing asymmetric key encryption; using one key for encrypting (public key) & one key (private key) for decrypting data. Supplementing this approach with digital signatures, safeguarding the exchange of data with a secure verification process. Furthermore & of paramount importance, at least two sets of keys are maintained (E.g. DR System, Powered On System, et al), so keys & moreover data are never rendered unusable…

Full z/OS disk encryption is the utopia; it might take some time!

z/OS Storage: Disk Data Sanitization – IHV Subsystems

Data At Rest Encryption (DARE) is a function provided by all major Mainframe disk ISV's, namely EMC, HDS (HP OEM) & IBM. The overriding objective is seemingly subsystem level protection, theoretically safeguarding data access when a Hard Disk Drive (HDD) is removed from the disk subsystem; either for replacement due to failure, or the entire disk subsystem leaving the Data Centre as part of an asset disposal/end of lease/technology upgrade activity:

Disk Subsystem: Function	*EMC Symmetrix VMAX*	*Hitachi USP V/VM + VSP*	*IBM DS8000 (DS8870)*
DARE: Subsystem Level	✓	✓	✓
DARE: Internal Drive Level	✗	✓	✗
Key Management	*RSA Key Manager (RKM)*	*SafeNet Key Management* *Integrated Key Management*	*IBM Security Key Lifecycle Manager (ISKLM)*
Encryption Algorithm(s)	*AES-256 (XTS)*	*AES-256 (XTS)*	*AES-256 (XTS)*
FIPS 140-2 Certified	*Drives:* ✓ *Keys:* ✓	*Drives:* ✗ *Keys:* ✓	*Drives:* ✗ *Keys:* ✓
Availability Information	*Enginuity 5875 (New): No RPQ/Upgrade*	*Contact HDS*	*LMC Level 7.6.3.xx.xx: Features 1751/5xxx/6xx5x*

Over time, is key management the only differentiation factor?

z/OS Storage: Disk Data Set Erase-On-Scratch (EOS) Usage

To physically erase security-sensitive data at the time the data set extents are scratched, RACF & DFSMS provide an erase-on-scratch facility. Erase-on-scratch ensures that when the data set is scratched (deleted or released for reuse), it cannot be read by any program running under control of an IBM operating system. It enables you to protect both single & multivolume DASD data sets.

With the erase-on-scratch facility, you can designate that specific data sets with a particular security level or that all data sets should be physically erased when the data set is deleted or when some of the space that was allocated to the data set is released. During this process, RACF (ACF2, Top Secret) tells DFSMS that data erasure is required.

The erase-on-scratch facility provides a defence against two types of attacks:

- It protects against an attempt to read residual data. This means that no one can allocate a new data set at the same location, open it for input, & read your data. This requires no exotic tools or insider knowledge & can be done quite easily using JCL & an IBM-provided utility such as IEBGENER.
- It defends against an attempt to read data by acquiring physical access to a device & attempting to read its data directly.

Historically, DASD performance might have been a consideration if System-Wide EOS was implemented (I.E. RACF SETR ERASE(ALL), ACF2 AUTOERASE ERASEALL or Top Secret AUTOERASE(ALL)), but modern DASD subsystems have eradicated this CPU & I/O overhead.

Erase-On-Scratch (EOS) is an option/supplement to encryption.

z/OS Storage: Erase-On-Scratch (EOS), ISV Software Usage

DFSMShsm SETSYS ERASEONSCRATCH|NOERASEONSCRATCH:

- ERASEONSCRATCH specifies that DFSMShsm requests SAF for the erase status of the user's data set when backup versions & migration copies are scratched from DFSMShsm-owned DASD volumes. The data set is deleted, & if RACF indicates erase-on-scratch, the DASD residual data is overwritten by data management.
- NOERASEONSCRATCH specifies that DFSMShsm does not request SAF for the erase status of the user's data set when backup versions & migration copies are scratched from DFSMShsm-owned DASD volumes. The data set is deleted but the DASD residual data is not overwritten by data management.

NB. Copies (Backup & Migration) of data also require EOS actions; not just original data set!

INTERCHIP RealTime Defrag (RTD):

- Track erase is controlled by the Volume Level SET parameter ERASE (I.E. Overwrite with binary zeroes, up to 15 tracks per I/O instruction for efficiency).
- By default, tracks are erased based on RACF & Catalog definitions.
- Specifying ERASE=ALWAYS will result in erasing any tracks freed by an RTD operation (RELEASE, COMBINE, or DEFRAG) without reference to SAF or VSAM Catalogue settings.
- ERASE=ALWAYS also supports OEM DASD Dynamic Provisioning (E.g. EMC VMAX, HDS VSP), which require tracks to be erased (I.E. binary zeroes) in order to perform space reclamation.

This dramatically reduces system overhead associated with free space reclamation activities.

Safeguard EOS for all data & maintain system performance…

Data Sanitization: Is Wiping With Binary Zeroes Enough?

From a regulatory compliance viewpoint, sanitizing disk & tape storage media with one or several passes of binary zeroes is seemingly good enough, for example:

ISO 27002	*PCI-DSS*	*NIST*
Erase or degauss magnetic media. Send media to specialist 3rd party for appropriate disposal.	*Secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).*	*At least a single pass with a fixed data value (E.g. binary zeroes). Shred, Disintegrate, Pulverize or Incinerate.*

Arguably overwriting data just once is not usually good enough to prevent data recovery, instead it is recommended that a minimum of three passes are made writing alternating zero & one patterns over the data & then further passes with random data. Data sanitization in combination with disk drive encryption & in-built Hard Disk Drive (HDD) Secure Erase (SE) functions, provides a comprehensive & evolving solution. Finally, let's review the sanitization method risk hierarchy:

Data/Media Action	*Security*	*Duration*	*Observations*
File deletion; Volume initialization	*Poor*	*Seconds*	*Only removes pointers; data remains intact*
File Erase-On-Scratch (EOS)	*Medium*	*On-Going*	*Data overwritten with binary zeroes (1 pass)*
File-Volume Sanitization	*High*	*Minutes*	*Data overwritten with several patterns & passes*
File-Volume Encryption	*Very High*	*On-Going*	*AES-256 (XTS)+ Data At Rest Encryption (DARE)*
Encrypted Volume Disposal	*Very High*	*Seconds*	*Change & destroy in-drive encryption key*

Data lives for years; you can't securely destroy it in seconds!

z/OS Storage: Data Privacy – The Application Test Bed

The UK Data Protection Act 1998 states *"Personal data means data which relates to a living individual who can be identified"*. Similar data protection/privacy regulations are described within Directive 95/46/EC of the European Parliament, The Human Rights Act 1998 (Article 8) & Privacy & Electronic Communications Regulations (PERC). Put another way, data privacy applies!

There are numerous examples of personal data that are readily stored in customer, personnel, supplier, user, et al, data sources, maintained for application processing. The following table lists some common examples, with broad categorization:

Contact	*Financial*	*Government*	*Miscellaneous*
Gender-Title	*Account Number*	*NI Number*	*User-Userid-Password*
Name-Forename-Surname	*Sort Code*	*Date Of Birth*	*Membership Number*
Address-Post Code	*Debit-Credit Card Number*	*Marital Status*	*Security Question Responses*
Phone-Landline-Mobile	*CV2-Signature Code*	*Employer-Job Title*	*Social Media Accounts*
Email	*PIN Code*	*Tax-PAYE Number*	*Passport, Driving License, et al*
Why is data privacy an issue? How many of these commonly stored personal data fields are required for identity theft? Sometimes data security is more than securing the file (data set) entity; we have to safeguard against the "insider threat" where snippets of data are more than enough to generate significant data breaches…			

Creating application test beds from production data is how easy?

z/OS Storage: Data Privacy – A Safe Application Test Bed

It might not be prudent, just considering one aspect of application test bed creation, namely data privacy. Ideally this process should evolve & be optimized to generate several business benefits:

Secure: Data Privacy	*Coverage: Testing*	*Size: Fit-For-Purpose*
Formulated encryption	*Precision; meeting all test conditions*	*Extract/load production sub-sets*
Translation with meaningful rules	*Discrete data package*	*Maintain database relationship*
Ageing while maintaining integrity	*Simple creation of clean test beds*	*Size data for specific test scenario:* ✓ *Unit/Code (Minimal)* ✓ *System/Integration (Medium)* ✓ *Acceptance (Medium-Full)* ✓ *Stress (Full+)*
Mask partial/sensitive fields	*Customization for specific testing*	
Generate fictitious/accurate data	*Allow for application evolution*	
Secure & Compliant Data	***Simplified & Optimized Testing***	***Optimized CPU & Storage Usage***
Format-Preserving Encryption (FPE): Data retains its original format, on a character-by-character basis, so that encrypted data "fits" in existing fields, eliminating the need for database & application schema changes.		
Hashing: Allow data within a field to be passed as input to a "black-box" algorithm. The output of the algorithm produces an access method (row pointer or key).		
Masking (obfuscation): A process of hiding original data with random characters or data.		
Translation: Utilize existing values stored within files, translating as replacements to sensitive data values.		

Applications & related data are the business; let's keep them safe!

z/OS Storage: Data Privacy – Application Test Bed Tools

There are a plethora of ISV tools that assist with the creation of application test beds, with data privacy as a feature. These tools include, but are not limited to:

ISV	*Product Name*	*Brief Description*
CA	*LISA Datafinder*	*Quickly discover & mask sensitive data/messages with consistent, realistic values, in-situ or 'in-flight', using native database or z/OS utilities.*
Compuware	*File-AID*	*Includes a workbench that assists in the creation & management of privacy specifications, allowing users to define, update & manage privacy criteria in a commonly shared repository.*
Direct Computer Resources	*DME (Data Masking Express)*	*Protect Personally Identifiable Information (PII) or sensitive/confidential information that might otherwise be compromised during application testing, off-shoring or in the unfortunate event of a data breach.*
IBM	*InfoSphere Optim Data Privacy*	*Mask confidential data on demand in applications, databases & reports based on business policies to protect data privacy.*
Informatica	*Persistent Data Masking*	*Minimizes risk of data breaches by masking development environments created from production data regardless of database, platform, or location.*
Micro Focus	*Data Express*	*Manage the test data environment; improving test results, lowering testing costs, securing customer data from loss or misuse & enable accelerated delivery & privacy compliance.*

Optimize the application testing process, while keeping data safe!

UNIX System Services (USS) - Who Manages Data Access?

Unlike z/OS DASD storage, where Storage & Security Management roles are clearly defined, this is not necessarily the case with USS (OMVS). As most USS requirements originate with the installation of software, it's typical for a z/OS Systems Programmer to install the software, while allocating the associated z/OS HFS/zFS file system. Complications can occur, as there are significant differences between z/OS & UNIX security management disciplines, which could introduce significant exposures (I.E. Multiple UID(0) Entries, Orphaned Access Control Lists, Duplicate UID/GID, et al).

More recently with the introduction of z/OS 2.1, the default OMVS segment support is no longer provided regardless of whether the BPX.DEFAULT.USER profile is defined in the FACILITY class. z/OS UNIX users or groups must have OMVS segments that are defined for user & group profiles with unique UIDs & GIDs. Put another way, a z/OS 2.1 upgrade requires the BPX.DEFAULT.USER profile to be removed & for all users without an OMVS segment be identified & remediated, as they will be unable to run any UNIX systems services! This subject matter is extensive, while there are several good resources available to at least make a start:

Vanguard: Replacing BPX.DEFAULT.USER	*www.go2vanguard.com/webinars/Replacing_BPX_DEFAULT_USER.pdf*
UK GSE: z/OS UNIX needs fixing	*http://racf.gse.org.uk/content/content_download.php?attachid=39*
IBM Tool: Find & remove orphaned UID/GID	*ftp://ftp.software.ibm.com/eserver/zseries/zos/racf/irrhfsu*

20 years of USS; maybe the z/OS 2.1 upgrade helps us get it right!

UNIX System Services (OMVS): Typical Data Security Exposures

Because of the differences between UNIX & z/OS security processes, what might be a limited exposure for z/OS, can be a significant exposure for OMVS. The most common exposures identified from numerous global Vanguard Security Audit reviews are listed:

Scenario Description	*OMVS Data Security Exposure*
UID(0) privilege assigned to human users	*UID(0) is superuser (do anything) privilege; Any human user can modify the contents of any OMVS zFS/HFS files, directories, or permissions*
Non-unique GID values assigned to RACF groups	*Group ownership and access to UNIX files is based on the GID number, exposing OMVS zFS/HFS files and directories to unintended access*
OMVS zFS/HFS executable files with setuid permission	*An executable file with setuid permission allows the executable to run with the authority of the file owner rather than the authority of the user, allowing escalation of the user's access rights*
Broken symbolic links in OMVS zFS/HFS are treated as a path to a file or directory that no longer exists	*If any directories with "like" names are created this could expose that data, providing a direct link to this data, bypassing any directory structure security*
OMVS zFS/HFS files with world-writable RWX attributes	*Any OMVS user could modify the contents of and file with world-writable RWX attribute*
Files with an unknown owner (UID) or Group(GID) – I.E. Orphaned files	*Access to orphaned files may be inhibited by other than UID(0), affecting processes for which access is required*

Remember z/OS USS data; it's not always just software libraries!

Summary: Keeping z/OS Data Secure From Cradle To Grave

Accidents happen! As IT professionals with a Mainframe heritage it's incumbent on us all to safeguard that our valuable business data is secure, from cradle to grave. Since DFSMS (1988) data creation & management has largely stayed the same for several decades or more. What has changed is the amount of data stored & the ever increasing requirement to safeguard our business data.

Objective	*Personnel/Teams*	*Observations*
Collaboration	*CxO, DPO, Applications, Security, Storage, Systems, Database*	*Identify sensitive business data; optimize applications testing with data privacy techniques*
Proactive Data Sanitization	*Security, Storage, Systems*	*Securely (EOS) erase data (CKD tracks, files, volumes) ASAP; don't wait for the compelling event (disposal)*
Proactive Data At Rest Encryption	*Security, Storage, Systems*	*Deploy disk drive/subsystem encryption techniques ASAP, complementing data sanitization processes*
Achieve/Surpass Compliance	*CxO, DPO, Security, et al*	*Don't just achieve regulatory compliance; surpass these vanilla rules & safeguard your business data!*

Don't just comply or imitate others; be the best that you can be…

Regulatory Compliance & Data Sanitization – Web Links

Description	Web Link
Data Protection Act 1998	http://ico.org.uk/for_organisations/data_protection/security_measures
ISO/IEC 27001	http://www.iso27001security.com/ISO27k_Information_classification_matrix.xlsx
PCI-DSS v3.0	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
NIST Media Sanitization Guidelines (800-88)	http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
ACF2, RACF, Top Secret DISA STIGs	http://iase.disa.mil/stigs/os/mainframe/Pages/zOS.aspx
OMVS HFS/zFS Orphaned GUI/UID Find/Remove Tool	ftp://ftp.software.ibm.com/eserver/zseries/zos/racf/irrhfsu
RACF System's Programmers Guide: Erase-On-Scratch	http://pic.dhe.ibm.com/infocenter/zos/v1r13/index.jsp?topic=%2Fcom.ibm.zos.r13.icha200%2Feos.htm
z/OS DFSMS Using Data Sets: Erasing DASD Data	http://pic.dhe.ibm.com/infocenter/zos/v1r13/index.jsp?topic=%2Fcom.ibm.zos.r13.idad400%2Ferasrd.htm
z/OS DFSMS Using Data Sets: Erasing Tape Data	http://pic.dhe.ibm.com/infocenter/zos/v1r13/index.jsp?topic=%2Fcom.ibm.zos.r13.idad400%2Fertape9.htm
ICKDSF User's Guide: Erasing a DASD Volume	http://pic.dhe.ibm.com/infocenter/zos/v1r13/index.jsp?topic=%2Fcom.ibm.zos.r13.ickug00%2Fcsd.htm

Disclaimer: Links OK @ November 2014; no endorsement applies