



Education

Implementation Practices for the Archiving and Compliance Infrastructure

Gary Zelman, Network Appliance
WW Practice Director
Co-chair 100 Year Archive and ILM PS

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
 - ◆ Any slide or slides used must be reproduced without modification
 - ◆ The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.

Archiving and Compliance Infrastructure: The Cornerstone of Enterprise Data Management

Enterprise data management strategies that include information archiving capabilities provide companies with a full-lifecycle approach for managing data.

- ◆ The drivers that compel an organization to look for an archive solution
- ◆ How to approach a project to deploy a winning solution

The tutorial teaches basic principles for managing data as well as how to plan an archiving strategy that will meet your organization's requirements, drive business value and enable the organization to:

- ◆ Manage explosive data growth
- ◆ Aligning performance and service levels for timely information access
- ◆ Support data retention compliance requirements and effective storage strategies.
- ◆ Improving data management to eliminate redundancies and simplify the IT infrastructure.

It will end with a view of the benefits to be derived through Archiving Infrastructure

- Introduction to Data Management & Archiving
- Why Compliance Archiving has changed
- Compliance Archiving Infrastructure
- Implementation Practices and Steps

Setting an Effective Archive Strategy

➤ Archiving

- ◆ How to save, protect and preserve

➤ Records Management

- ◆ What must be saved and for how long

➤ An effective archive strategy will be the most far-reaching decision you will make.

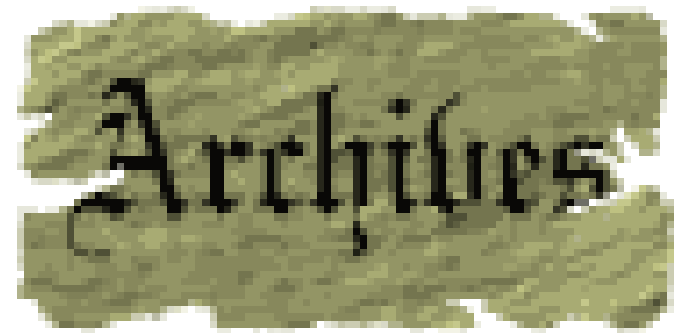
- ◆ Affect the outcome and speed of legal cases and regulatory inquiries
- ◆ Save your company fines & legal fees
- ◆ Determine ability to recover from an outage or disaster
- ◆ Improve application performance and costs
- ◆ Improve productivity for all of your company's employees.

**Compliance
Events**

**Regulatory
Inspection**

Litigation

- Understanding the roles of records managers and archivists
 - ◆ Records manager
 - Manage large quantities of institutional records
 - many will eventually be destroyed
 - ◆ The archivist
 - Preserves relatively small quantities of records deemed important enough to be retained for an extended period.
 - Preserve and makes the records accessible for use, and these archival records can be used for research.



What's Driving Data Growth?

- ▶ Transaction processing:
 - ◆ Customer facing eCommerce applications
 - ◆ ERP/CRM
 - ◆ Supply chain applications
- ▶ Business Process
 - ◆ Claims, Mortgages, e-Government
- ▶ Ad Hoc/ Casual
 - ◆ Email/PST, Office Automation
- ▶ On the horizon
 - ◆ Voice mail
 - ◆ Voice conversations
 - ◆ Video
 - ◆ Video conferences
 - ◆ Audio and Video (WebEx)



What drives archiving

Regulatory Retention	HIPAA, SOX, GLB, NASD etc.
IT Efficiency	Storage, Backup, Performance, Capacity Planning
Legal Preservation	Legal process, Discovery Costs, Discovery speeds, Search
Knowledge Management	Classification, Data mining and sharing, Improved information access
Digital Information Creation	Email, RDBMS, Office Automation, Policies, IP, Records born Digital, Processes

What hampers archiving

Collaboration	Lack of collaboration between key organizations and executive support
ROI not well understood	ROI not understood or planned
Emerging technologies not well understood	Classification, Compliance workflow and legal process not well understood
Understanding approach	Not clear stepped approach to building an archive
Physical & logical migration issue	Management of Storage media longevity Application and operating system obsolescence

Data Management Practices ?

Advanced Practice



Best Practice



Common Practice



Base Practice

Business Processes



Archival



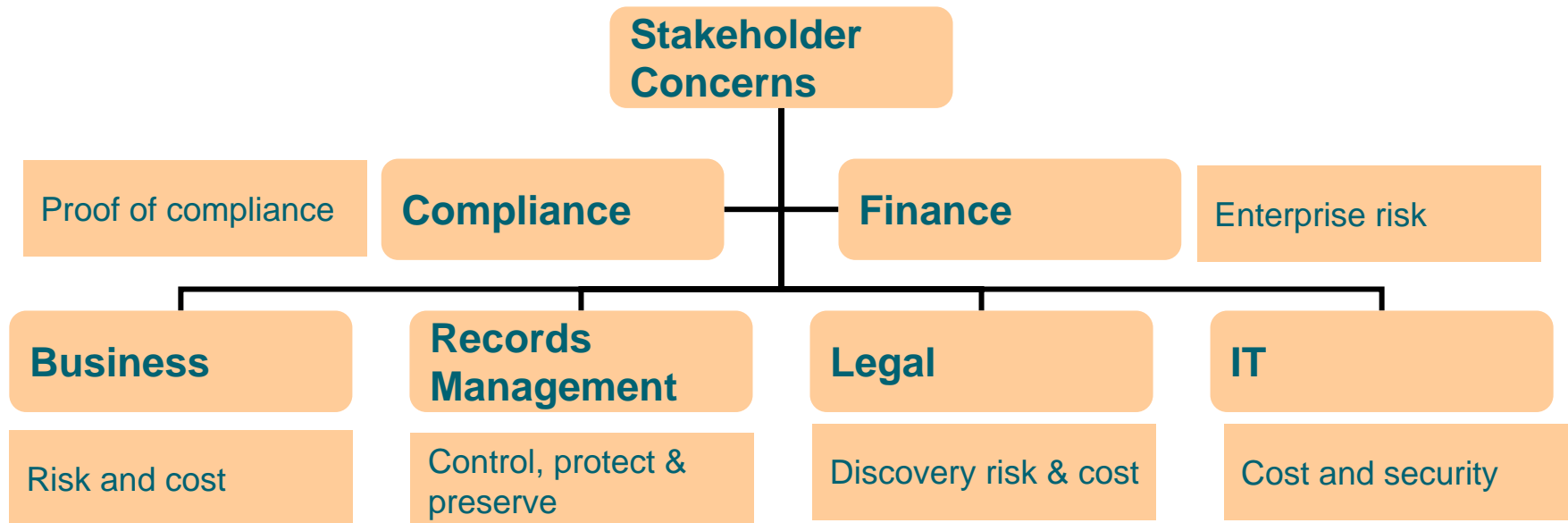
Add Primary Disk



Tape-Backup

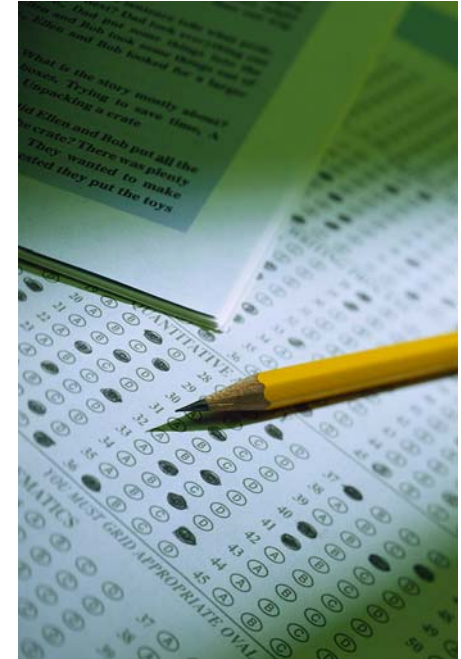


Why Compliance Archiving has changed? **SNIA**



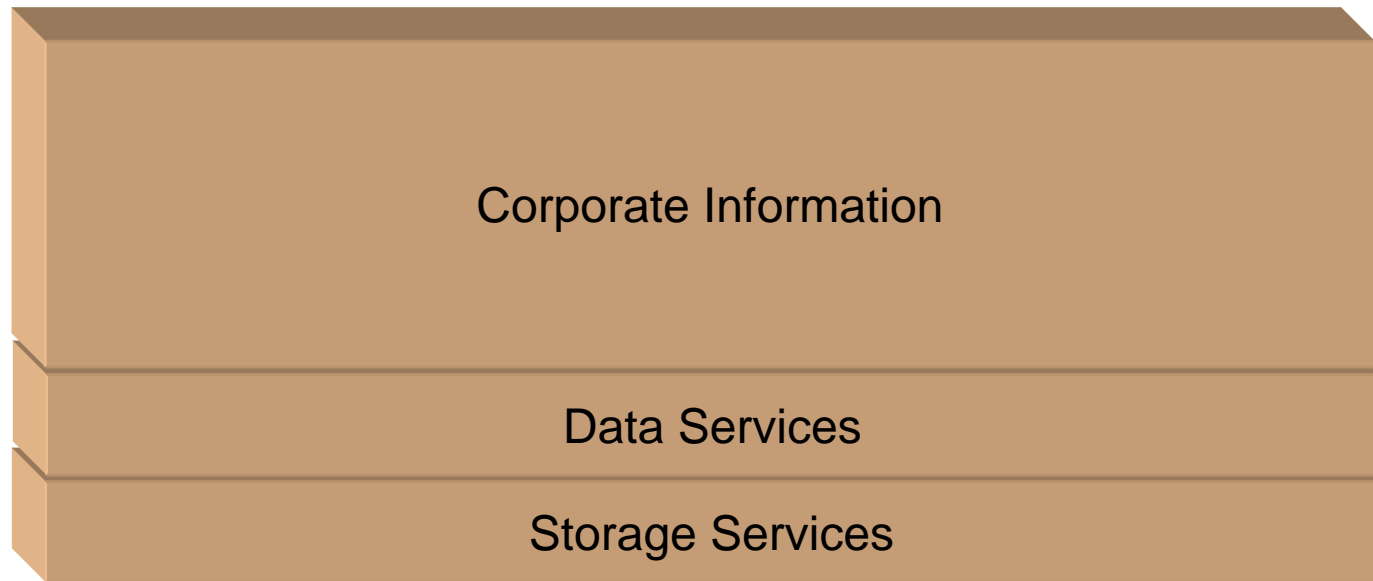
Compliance Readiness Test

1. Do you have an archival policy for books and records?
2. Do you separate retention periods per data types?
3. Do you have compliant non-destructive media in place?
4. Do you have an archival policy for email and IM and files?
5. Are the email and IM and files archival policies explicit per groups?
6. Do you have a supervisory review process for communications?
7. Do you have checks and balances for all of the above?
8. Do you have a regular records recovery, including audit logs, test?
9. Is all your compliant data readily accessible online for reconciliation business functions?
10. Is Sr. Management (CEO, CIO, CFO, CCO) actively involved in the firms compliance and IT alignment strategies?



- ▶ >80 Leader
- ▶ >70 Excellent State of Readiness
- ▶ >50 Towing the line
- ▶ >30 High Risk
- ▶ >20 Strong ROI

- ▶ >80 Leader
- ▶ >70 Excellent State of Readiness
- ▶ >50 Towing the line
- ▶ >30 High Risk
- ▶ >20 Risk of Incarceration



Storage Services

Extended Capabilities

- ▶ **Data classification**
- ▶ **Data migration**
- ▶ **Data discovery**
- ▶ **Data permanence**
- ▶ **Data security**
- ▶ **Data privacy**

Core Capabilities

- ▶ **Optimized archiving architecture**
- ▶ **Replication**
- ▶ **Integration with archival & compliance applications**
- ▶ **Ability to meet long-term needs for scale, security, access, and cost**
- ▶ **Ability to deploy archive & compliance initiatives together**

Implementation Steps

Step 1



Structure project

Step 2



Develop policies & retention

Step 3



Select & define policies to archive system

Step 4



Select tool options

Step 5



Create archiving processes

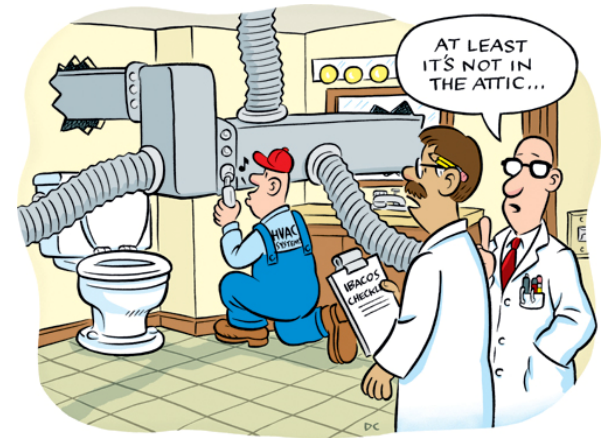
Step 6



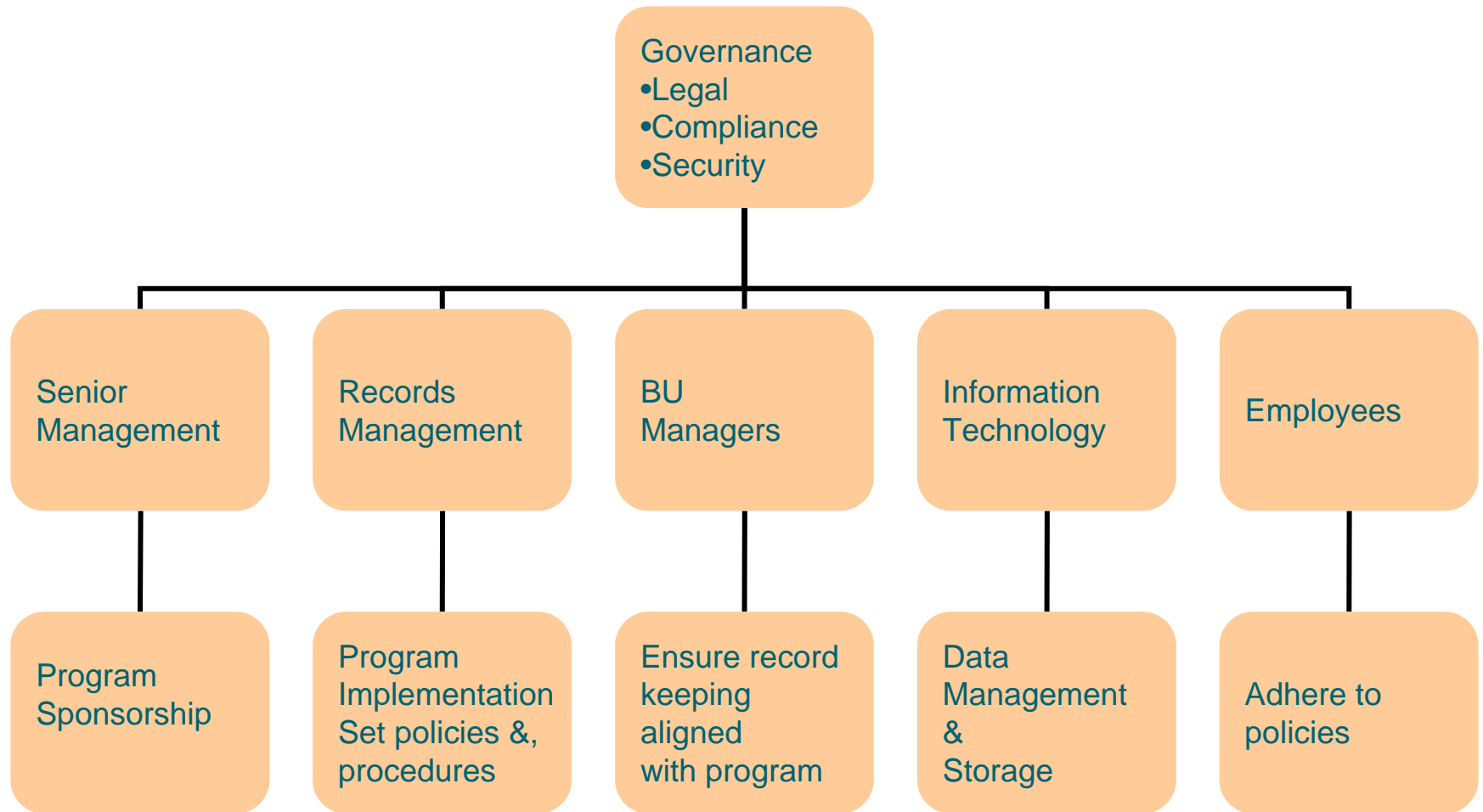
Calculate benefits & document

➤ Overarching Project Best practices

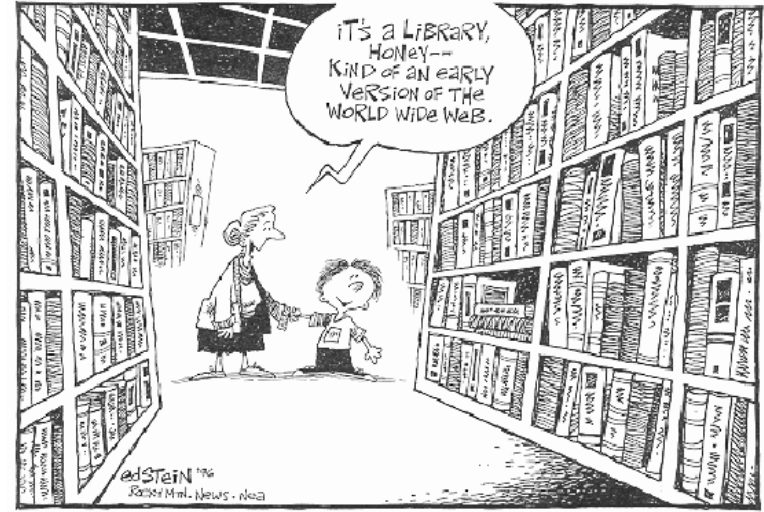
- ◆ Understand and interpret the relevant regulations correctly
- ◆ Involve all stakeholders
 - IT, LOB, Legal, RIM etc
- ◆ Archiving Policies
 - Revised to go electronic
 - Support reducing risk and cost
- ◆ Develop enterprise architectures



Roles & Responsibilities?



- Policies (IT owns Infrastructure, and the Business owns the data)
 - ◆ Litigation
 - ◆ Compliance
 - ◆ Business Operations
- Archiving Goals
 - ◆ Retention
 - › Scope
 - › Retention Periods
 - ◆ Security
 - › CIA
 - ◆ Service Delivery and Support
 - › Service levels
 - › Risk and cost reduction



Long-term preservation policy should:

- ▶ State that providing long-term preservation of authentic and processable information is a storage repository goal
- ▶ A description of the type of custody the storage repository will undertake, e.g. legal or physical
- ▶ A description of best practices to which the storage repository adheres
- ▶ Identify the circumstances under which migration activities will occur
- ▶ Explain the types of compliance audits that will take place
- ▶ Clarify the roles of storage repository personnel

Business Policies Translate To Archiving

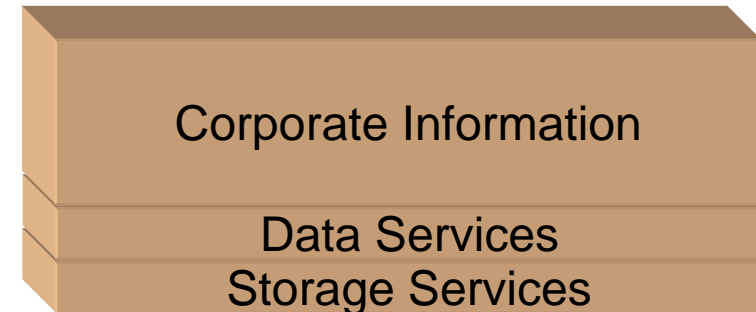
- Include all applications that manage regulated data
- Gain agreement among stakeholders on retention and retrieval:
 - ◆ LOB, RM, IT, Finance, Legal, Compliance, Security etc.
- Document your business policies:
 - ◆ Data types (Active, Inactive, Reference etc.)
 - ◆ Policies for Archiving, Viewing, Retrieving Objects
 - ◆ Policies for Compliance and Disposal
 - ◆ Policies for EDiscovery



Storage Service & Data Services

➤ Data Services

- ◆ Extend primary storage capacity
- ◆ Archive data on specific criteria
- ◆ Speed up backup and restore
- ◆ Retain a copy of data ensuring they are kept for the appropriate period of time to meet regulatory and legal retention requirements

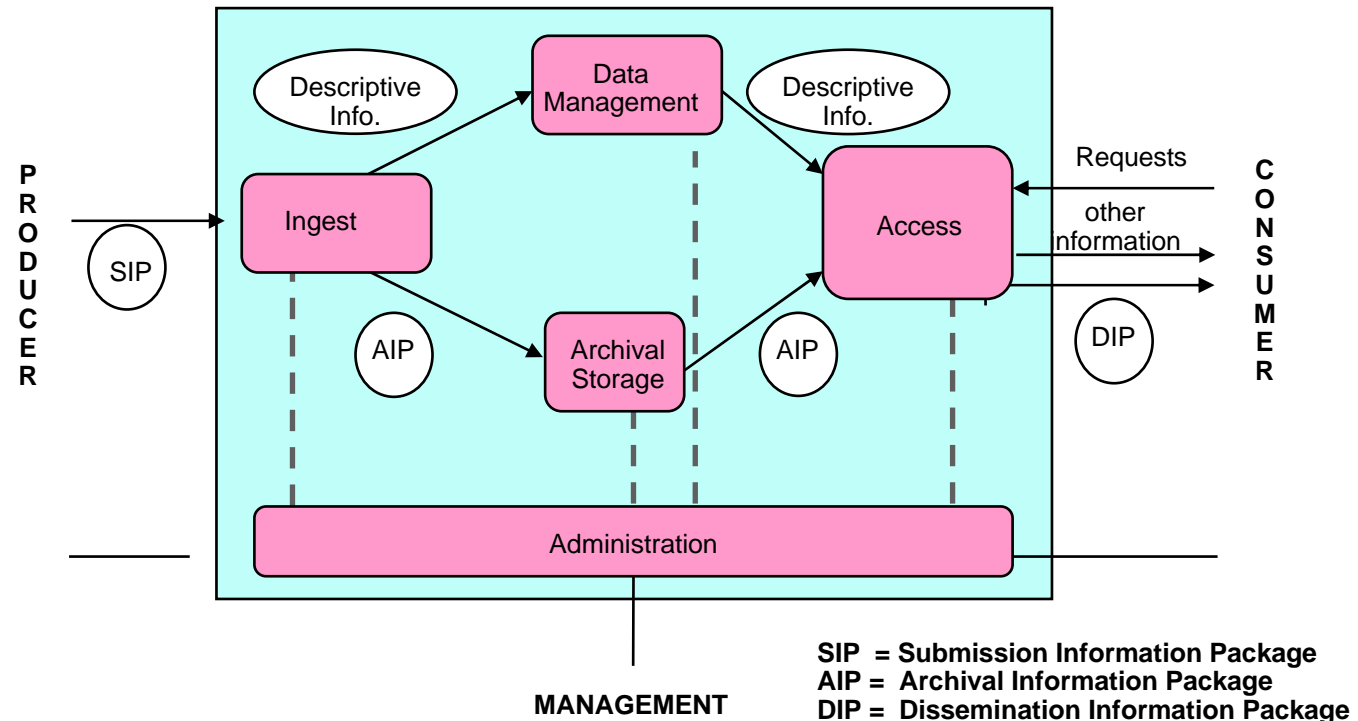


➤ Storage Services:

- ◆ High-performance, WORM storage protects data until a specified retention date.
- ◆ Easy data access and application integration.
- ◆ Flexible and Robust Compliant Data Protection
- ◆ Supports fully compliant replication
- ◆ Advanced Security Features: authentication, access controls, access restrictions, transmission encryption, and audit logs to protect confidential data.

OAIS Functional Entities

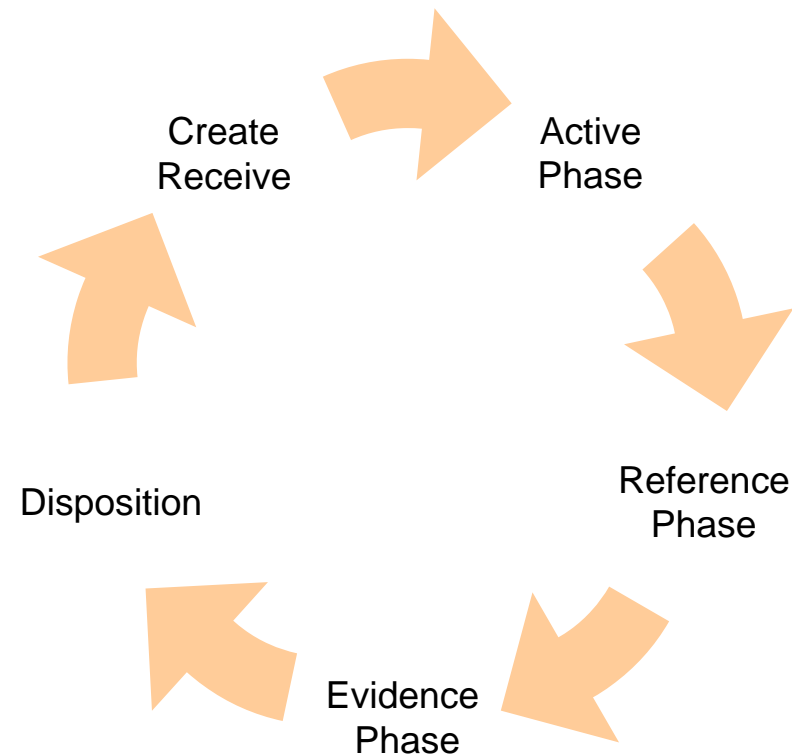
- OAIS is an ISO standard for preservation
- It provides
 - ◆ Fundamental ideas, concepts and a reference model for long-term archives



Integrate compliance with ILM

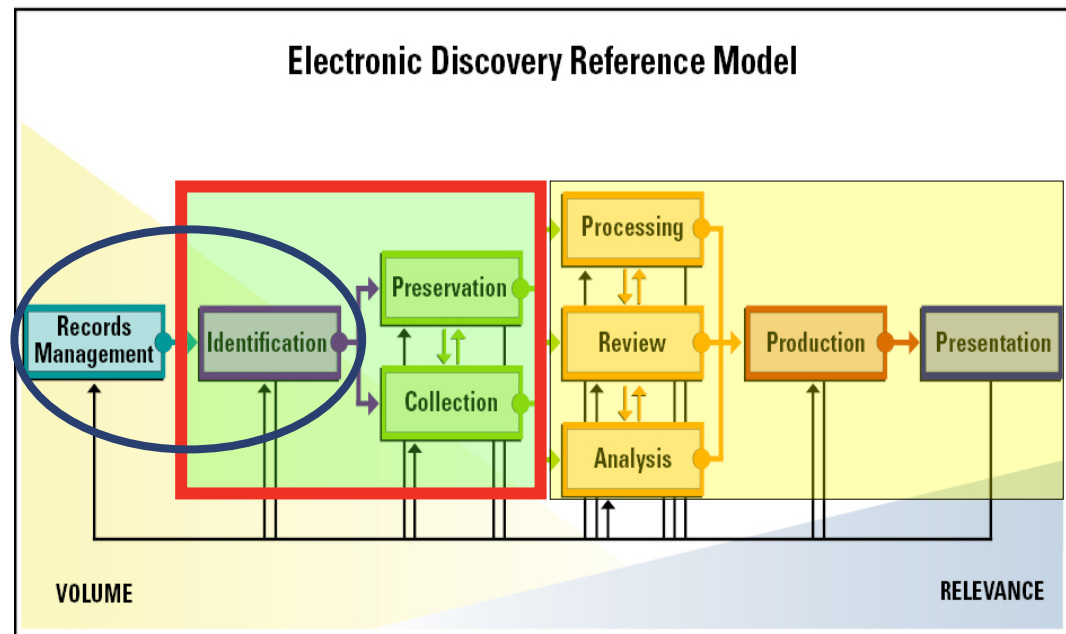
Facilitates Lifecycle Management & enables

- ◆ Managing data growth aligned with SLA's and operation cost and risk
- ◆ Optimizing application performance
- ◆ Enabling data retention compliance requirements until they expire
- ◆ Enabling legal discovery
- ◆ Enable records management
- ◆ Simplifying storage operations and IT infrastructure



Best practices for eDiscovery


- **Collect**
 - ◆ Acquire data Identified as potentially relevant, and export copies for further processing and review,
 - ◆ Preserve data integrity, preferably in native format, associated metadata, and chain of custody
- **Indexing**
 - ◆ Full text (Email and unstructured)
 - ◆ Searching using metadata
 - ◆ Plan for metadata and indexes
- **Proof of process**
 - ◆ Spoliation prevention
 - ◆ Audit trails
- **Disposition hold and legal hold**
 - ◆ Manage litigation holds



Reference: Socha Consulting LLC and Gelbmann & Associates

Records Management Processes

Information Strategies Underpinned By Policies

- Capture
- Register
- Classify
 - ◆ Content
 - ◆ Security, Access, & Functionality
 - ◆ Tools
 - > ICM
 - > Taxonomy, Thesaurus
- Assign Retention 
- Implement Disposition
- Monitor & Report

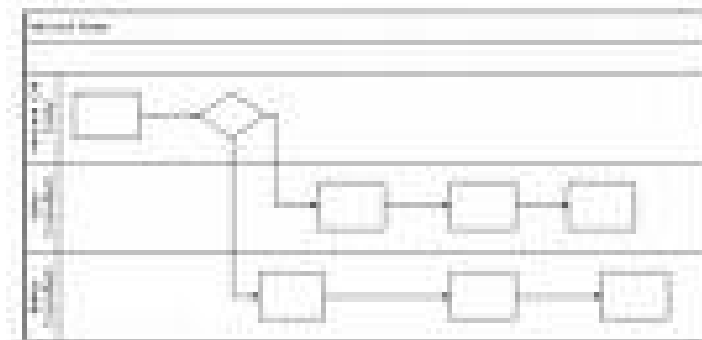
A retention schedule is a list of records for which pre-determined destruction dates have been established.

Three objectives:

1. disposal of those records which have completed their retention period
2. storage of records which have to be kept temporarily after they are no longer needed for current business
3. preservation of records which are of long-term or historic value

In practice the schedule will have dates varying from a few months to permanent retention

- ◆ Processes best practices
 - ◆ Consistent
 - ◆ Repeatable
 - ◆ Controlled
 - ◆ Documented
- ◆ Some Archive Processes
 - ◆ Archiving Viewing & Retrieving Objects
 - ◆ Compliance
 - ◆ Disposal
 - ◆ EDiscovery
 - ◆ Access
 - ◆ Storage Management
 - ◆ Others as needed and required by regulation



Digital Information Layers

- Manage the risk for storing electronic records with long term retention periods
 - ◆ Storage media longevity
 - ◆ Application and operating system obsolescence
- Preserve electronic records that must be kept for long periods of time:
 - ◆ Can be converted to PDF format
 - ◆ Designate electronic records for recurring migration forward as systems are upgraded or replaced
- Set review dates
 - ◆ Records' continuing value has a recurring evaluation

Application Layer

- ◆ Get the interpretation of the data
- ◆ Example: render a Word 3.0 document
- ◆ Diverse applications and data types

Data Layer

- ◆ Get the basic units (records/containers/objects)
- ◆ Example: OAIS AIPs
- ◆ Can it be standardized?

Bit Layer

- ◆ Get out the bits from the media
- ◆ Example: Linear Tape-Open (LTO) for tapes
- ◆ Maybe depends on media type

Risk Assessment should:

- Identify, quantify, and prioritize risks against pre-determined criteria set by the organization
- Include a systematic approach to estimate the magnitude of risks (risk analysis) against the significance of the risks (risk evaluation)
- Be performed periodically to address changes in security requirements and in the risk situation e.g., change in assets, threats, vulnerabilities

Calculate ROI

Areas of improvement	Yearly Total
Software savings	\$
Hardware savings	\$
IT administration savings	\$
Consumable savings	\$
Compliance search and retrieval savings	\$
eDiscovery search and retrieval savings	\$
Savings in compliance penalties	\$
Employee productivity gains	\$\$\$\$

- Start with business needs assessment
- Use best practices to guide
 - ◆ Policies
 - ◆ Processes
 - ◆ Architecture
- Create ILM policies and strategies
 - ◆ Reduce cost
 - ◆ Reduce risk

- Please send any questions or comments on this presentation to SNIA: trackdatamgmt@snia.org

**Many thanks to the following individuals
for their contributions to this tutorial.**

SNIA Education Committee

Gary Zasman – Network Appliance
Peter Mojica – AXS-One