

Storage Decisions

Hosted by STORAGE SearchStorage.com

How to build a compliant storage infrastructure

Meet new requirements with intelligent policy, processes and technology

Mike Casey

mcasey@contoural.com 

Storage Decisions

Hosted by STORAGE SearchStorage.com

Requirements Assessment: Start with the Business Needs

- **Business drivers – *what to save***
 - Compliance requirements
 - Litigation risks
 - Operational needs
- **Technical requirements – *how to save it***

Storage Decisions

Hosted by STORAGE SearchStorage.com

Compliance Requirements

- A patchwork of new and changing laws & regulations
- Don't focus exclusively on one regulation or requirement

Agency	Laws / Regulations	Industry	Records	Retention	Focus
SEC	Rule 17a-4 17 CFR 240.17a-3,4	Securities: Broker-Dealers	Trading Records	2-6 yr+	Integrity
SEC ...	Sarbanes-Oxley 17 CFR 240.13a	Public Corporations	Financial, Audit	5 yr+	Integrity
FDA	21 CFR Part 11, 21 CFR 11, GxP rules	Drugs, Medical Devices	R&D, Test, Mfg, etc.	3 yr+	Integrity
DHHS	HIPAA 45 CFR 164	Health Care, Insurance	Patient Health Info	10 yr+	Privacy, Security
Fed, OCC, FDIC ...	GLBA 12 CFR 30	Securities, Banking, Insur.	Customer Info	5 yr+	Privacy, Security

Storage Decisions

Hosted by STORAGE SearchStorage.com

New Rules: Moving From Scary to Safe

- **New laws, regulations and enforcement guidelines can be scary**
- **Key: Understand the common requirements!**
- **Agencies translate public policy goals into requirements for data retention and security**
- **Security objectives include integrity, confidentiality and availability**
- **Regulations prescribe capabilities to meet these goals – some general, some very specific**

Storage Decisions

Hosted by STORAGE SearchStorage.com

Example: HIPAA Security Rule

HIPAA Security Rule

45 CFR 164 -- Subpart C
Security Standards for the Protection of Electronic Protected Health Information

164.312 **Technical safeguards**

- (a) **Access control**, Implement technical policies and procedures... to allow access only to those persons or software programs ...
- (b) **Audit controls**, ...
- (d) Person or entity **authentication**..
- (e) Transmission security, ...
- (e)(2)(ii) **Encryption** ...

Security Technical Capabilities

- Authentication
- Access Controls
- Audit Logs
- Backup & recovery
- Media controls
- Data Permanence
- E-signatures
- Encryption
- Expungement

Storage Decisions

Hosted by STORAGE SearchStorage.com


Litigation Risks & Discovery Costs

- **Electronic documents – now a key focus of discovery**
- **Failure to keep and produce records can be expensive:**
 - **Bank of America fined \$10 M for failure to produce records (among other things)**
 - **Recovering email can be enormously costly**
 - **Cost to recover 250,000 e-mails from 5,000 backup tapes is US \$10M. CNI Research**
 - **Generally speaking, producing party pays costs**
- **Another risk: lost credibility, adverse judgments**
- **83% of lawyers say their corporate clients are not prepared to retrieve and turn over electronic files**

Storage Decisions

Hosted by STORAGE SearchStorage.com

Retention Policy: Keep or Delete?

Hurtful?  Helpful?

- **Inflection point: Litigation risk is moving from archiving inhibitor to archiving driver**
- **Attempts to delete adverse documents backfire**
 - **Usually the Problem is Not Having Documents**
- **Recommendation: Keep a complete, accessible archive of electronic documents & messages**

Storage Decisions

Hosted by STORAGE SearchStorage.com

Operational needs

- **Employees will save data, including e-mail, regardless of policy (they need it)**
 - **E-mail is a key productivity tool**
 - **A policy not followed is worse than no policy**
 - **One centrally managed archive is better than 1,000 PST files or 5,000 backup tapes**
- **A complete, accessible, secure business record protects corporate knowledge and IP**
- **Archiving improves service levels of production applications, and reduces server & storage costs**


Storage Decisions

Hosted by STORAGE SearchStorage.com

Why Do Compliance Projects Fail?

- **Fail to get agreement between business and technical people on policy objectives**
- **Focus on technology first**
- **Focus on a single regulation**
- **Not addressing litigation discovery issues**
- **Tactical silo solutions – no enterprise approach**


Storage Decisions

Hosted by **STORAGE** 

Engaging the Right Stakeholders

Business Perspectives	<ul style="list-style-type: none"> • CFO • General Counsel • Compliance Officer • Records Management 	<p>Are we in compliance?</p> <p>How will e-mail & e-docs affect liability?</p> <p>How does it impact litigation discovery?</p> <p>How do we ensure consistency?</p> <p>What is the risk/cost analysis?</p> <p>How does this fit into current RM Policy?</p>
Application Perspectives	<ul style="list-style-type: none"> • Application Administrator 	<p>Can I keep application server available?</p> <p>How do I manage discovery requests?</p> <p>How do I keep my SLAs?</p> <p>How do I avoid manual processes?</p>
Storage Perspectives	<ul style="list-style-type: none"> • Storage Administrators • System Administrators 	<p>How can I prevent e-mail from overwhelming storage?</p> <p>How do I manage capacity, backups, DR?</p> <p>Can this be handled consistently?</p> <p>How do I avoid manual processes?</p>


Storage Decisions

Hosted by **STORAGE** 

Engaging the Right Stakeholders, II

Business Perspectives	<ul style="list-style-type: none"> • CFO • General Counsel • Compliance Officer • Records Management 	<p>Are we in compliance?</p> <p>How will e-mail & e-docs affect liability?</p> <p>How does it impact litigation discovery?</p> <p>How do we ensure consistency?</p> <p>What is the risk/cost analysis?</p> <p>How does this fit into current RM Policy?</p>
------------------------------	--	---

Storage Decisions

Hosted by **STORAGE** 

Engaging the Right Stakeholders, III

Application Perspectives	<ul style="list-style-type: none"> • Application Administrator 	<p>Can I keep application server available?</p> <p>How do I manage discovery requests?</p> <p>How do I keep my SLAs?</p> <p>How do I avoid manual processes?</p>
---------------------------------	---	--

Storage Decisions

Hosted by STORAGE SearchStorage.com

Engaging the Right Stakeholders IV

Storage Perspectives	<ul style="list-style-type: none"> Storage Administrators System Administrators 	<p>How can I prevent e-mail from overwhelming storage?</p> <p>How do I manage capacity, backups, DR?</p> <p>Can this be handled consistently?</p> <p>How do I avoid manual processes?</p>
----------------------	---	---

Storage Decisions

Hosted by STORAGE SearchStorage.com

Compliance Initiatives: Key Steps

Example:
The bank examiner's view

Federal Financial Institutions Examination Council

Guidelines Establishing Standards to Safeguard Customer Information

to implement section 501(b) of the Gramm-Leach-Bliley Act of 1999

1. Risk assessment
2. Strategy development
3. Implementation of controls
4. Testing
5. Process monitoring and updating

Reference: FFIEC's IT Examination Handbook on Information Security

Storage Decisions

Hosted by STORAGE SearchStorage.com

Step One: Assessment

- **Involve management & cross-functional team**
- **Establish an effective process for assessment & policy development**
- **Assess risks and needs**
- **Understand compliance, litigation and operational requirements**
- **Also requires understanding of archiving and storage capabilities**

Step Two: Policy Development

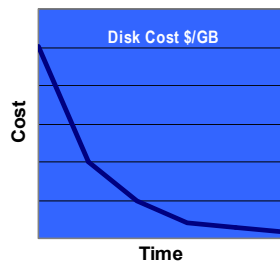
- Focus first on what to save, not how to save it
- Identify applications with regulated data
- Build consensus on retention & retrieval
 - Business owners, records management, applications, storage ... include CFO, legal, compliance, security
- Document the archival policy
 - Types of data (scope)
 - Retention periods (duration)
 - Archival processes
 - Compliance processes

Symptoms of Policy Confusion

- Waiting for requirements to come down from policy committee
- Focus on a single regulation
- Insistence on 90-day deletion policy
- Confusion about the need for WORM
- Inability to move forward (TCO fear)

Cost Implications

- Costs of Manual Record Processes are High
- Disk Storage Cost Decreasing Dramatically
- Nearline and Secondary Storage Even Less Expensive
- Good Archival Strategies Can Be Cost-Effective



Storage Decisions

Hosted by STORAGE SearchStorage.com

The New Records Management Paradigm

- Old view: save and delete
- New view: save and keep longer
- Recommendation:
 - Save more data, intelligently!

Storage Decisions

Hosted by STORAGE SearchStorage.com

Step Three: Implementation "How to Save It"

- Security objectives include integrity, confidentiality and availability
- Regulations prescribe controls to meet these goals – some general, some very specific
- Controls include administrative, physical and technical capabilities

Administrative Controls

Physical

Technical

Data

Storage Decisions

Hosted by STORAGE SearchStorage.com

Example: SEC Rule 17a-4

Books and Records Requirements
17 CFR 240.17a-4

17a-4 (f)(2) If electronic storage media is used ...

- (ii) The electronic storage media must:
 - (A) Preserve the records exclusively in a non-rewriteable, nonerasable format;
 - (B) Verify automatically the quality and accuracy of the storage media recording process;
 - (C) Serialize the original and, if applicable, duplicate units of storage media, and time-date ...
 - (D) Have the capacity to readily download indexes and records preserved on the electronic storage media as required by the Commission or the self-regulatory organizations ...

Security

Technical Capabilities

- Authentication
- Access Controls
- Audit Logs
- Backup & recovery
- Media controls
- Data Permanence
- E-signatures
- Encryption
- Expungement

Storage Decisions

Hosted by STORAGE SearchStorage.com

Technical Capabilities: Storage Technology Examples

- **Data integrity: Permanent, tamper-proof recording is an extra-strength capability for ensuring data integrity**
 - WORM functionality is specified by SEC Rule 17a-4, which applies only to broker-dealers
 - WORM may also prove useful in other cases, like SANs
 - Other capabilities – such as retrieval speed – may be more important. Assess your business needs!
- **Confidentiality: Privacy rules point to encryption as a safeguard for data at risk. Do that risk assessment!**
Expungement – secure, physical erasure – is an extra-strength capability for confidentiality – e.g., DoD 5015.2

Storage Decisions

Hosted by STORAGE SearchStorage.com

Compliance Enabler: Nearline Storage

- **Compliance is a catalyst for nearline storage deployment**
- **Organizations need to save more data, keep it longer, and access it quickly**
- **Intelligent storage policies and infrastructure can enable cost-effective compliance**
 - **Make compliance cost-neutral**

Storage Decisions

Hosted by STORAGE SearchStorage.com

Lessons Learned: Best Practices in Compliance

- **Save more, intelligently**
- **Build policy consensus before starting technical implementation**
- **Look at data first from an application viewpoint, not a block basis**
 - **Storage managers must talk with application owners!**

Storage Decisions

Hosted by STORAGE SearchStorage.com

Conclusions


- **Start with business needs assessment**
 - Compliance Requirements
 - Litigation Discovery
 - Operational Needs
- **Create an archive policy**
 - Include key stakeholders
- **Save more data, intelligently!**
 - Avoid silo effect when designing archive solutions
 - Deploy essential infrastructure, and extra-strength capabilities if needed
 - Move toward an enterprise data archive

Storage Decisions

Hosted by STORAGE SearchStorage.com

Questions?

- Ask the Expert
<http://searchstorage.techtarget.com/ateExperts/>
- Resources
 - www.searchstorage.com
 - www.snia.org/ssif/home
 - www.contoural.com
 - www.graycary.com
 - mcasey@contoural.com

contoural 

Storage Decisions

Hosted by STORAGE SearchStorage.com

Thank you.

Mr. Casey will be available in the Ask-the-Expert booth in the exhibit hall:
Monday 4-5 PM
