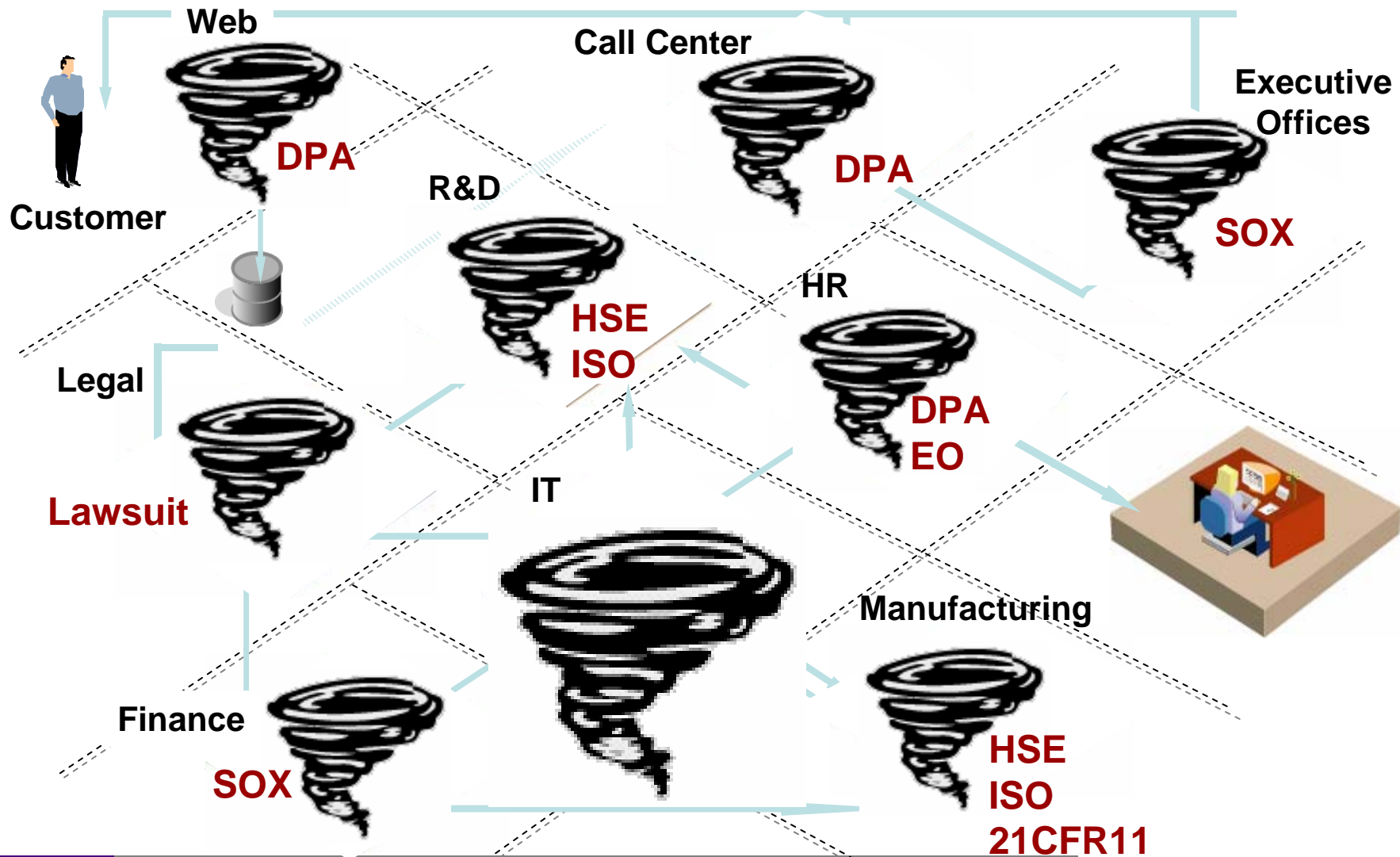


Solving Records Management Compliance Across The Enterprise

Mark Winstone

Sales and Marketing Director

Regulations affect all aspects of an organization



Commonality of Compliance Requirements



INTEGRITY



CONFIDENTIALITY



ACCESSIBILITY

	<i>Familiar</i>				<i>Emerging</i>			
	<i>GLBA</i>	<i>21CFR</i>	<i>PRO</i>	<i>SEC 17a-4</i>	<i>HIPAA</i>	<i>SOX</i>	<i>Basel II</i>	<i>DPA</i>
System Validation								
E-Signatures								
Retention Mgmt								
Authenticity								
Monitoring								
WORM								
Provisioning								
Protection								
Availability								
Authentication								
Encryption								
Disposition								
Access Control and Logs								
Timeliness								
Audit Trails								
Access, Query and Retrieve								
Report and Publish								
Copies								
Performance								

Documentum Enterprise Content Management

Create / Capture



Authoring and Collaboration

- Hundreds of integrations: Office documents, emails, photos, CAD drawings, xml
- Seamless & user friendly
- Collaborative workspaces



Scanned Images

- Scan & OCR
- Departmental & high volume
- Automatic batch separation
- Single & double-sided
- Advanced image enhancement
- File conversion



Manage



Library Services

- Automatic renditions & transformations
- Fully multi-lingual
- Workflow & lifecycle management
- Virtual document management
- Security and audit trails
- Full text, keyword and attribute searching



Deliver

Multi-Channel Delivery

- Publish to web
- Publish wireless
- Publish to print
- Syndicate/Distribute



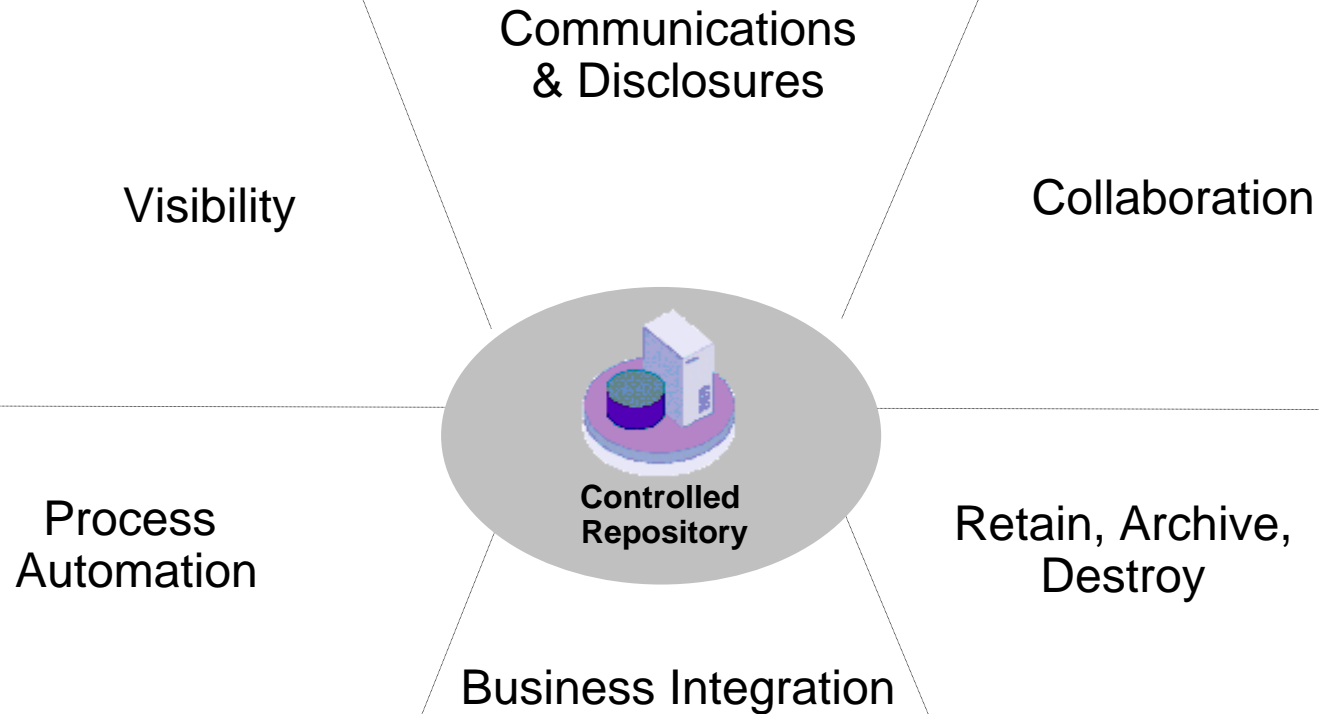
Archive

Records Management



- Retain
- Archive
- Dispose

Enterprise Compliance key Requirements



Documentum Enables Enterprise Compliance

Communications & Disclosures

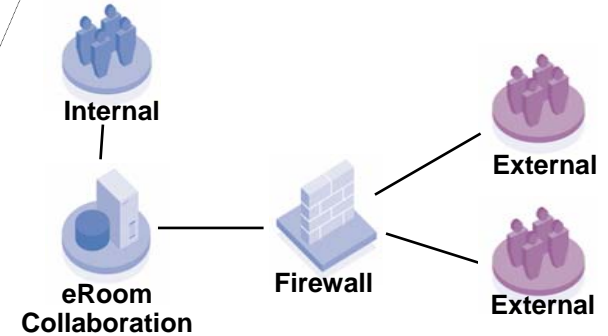
Collaboration

Visibility

Compliance Dashboard



Workflow Dashboard



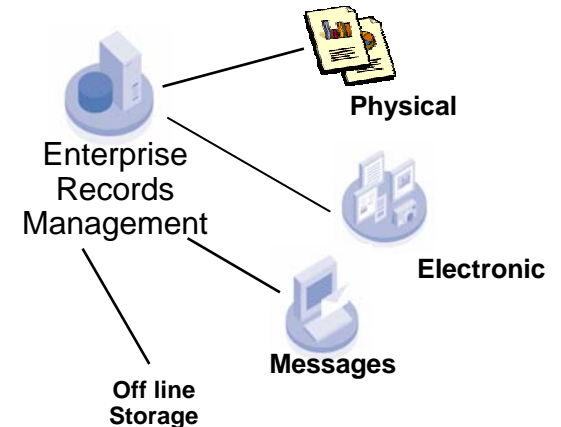
D5 Platform

Controlled Repository

Integrations

- ERP
- CRM
- SCM
- FMS
- Business Intelligence

Business Integration



Retain, Archive, Destroy

EMC² documentum

Intelligent Auto-tagging and Auto-categorization



Lifecycles Workflows



Version Management

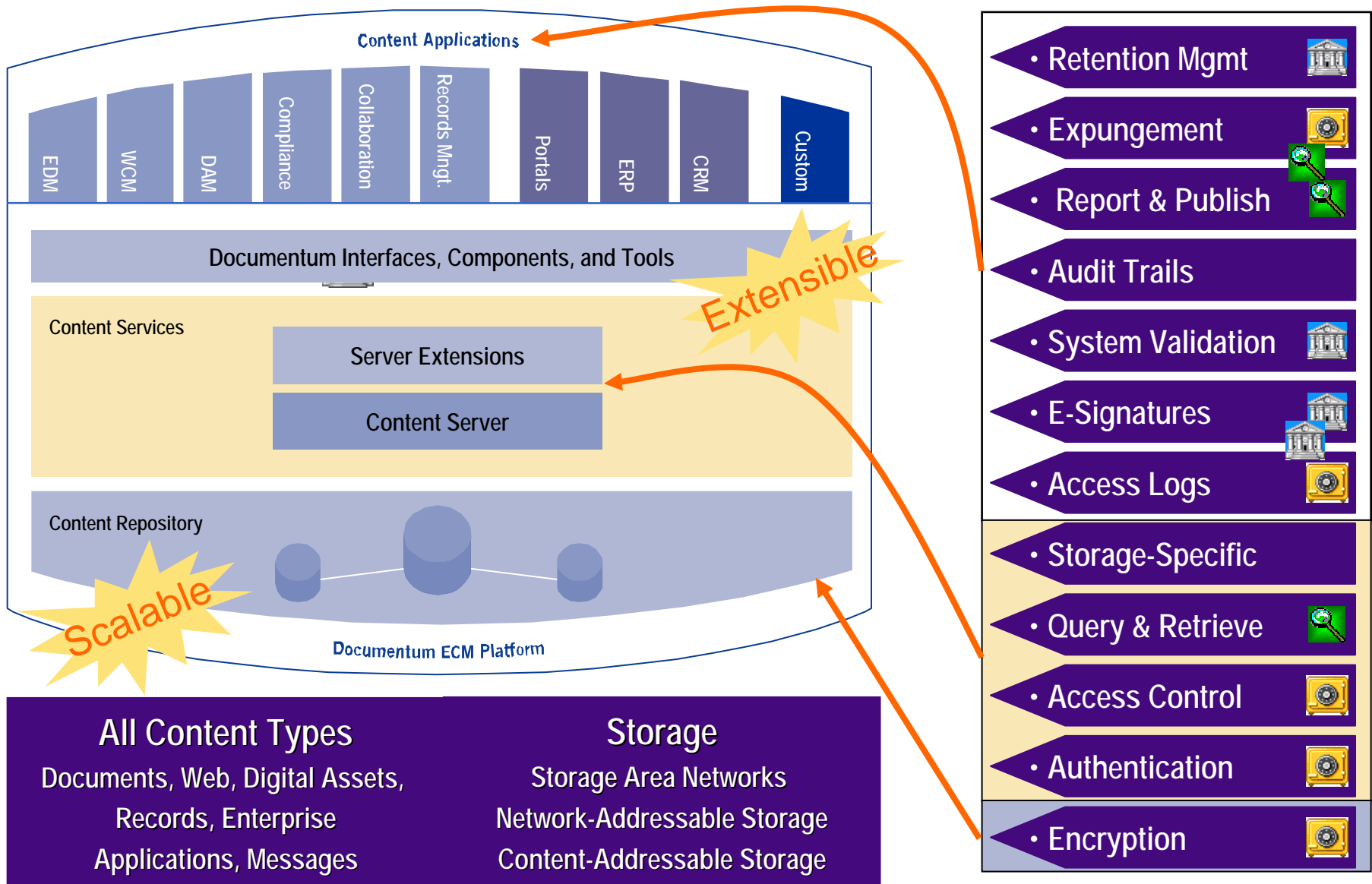


Process Automation

SynApps Solutions

Enterprise Compliance

EMC-Documentum *Platform for Compliance*



Sarbanes-Oxley

CROSS-INDUSTRY:
Publicly-Traded Firms
(and Pre-IPO Firms,
acquisition targets)

Laws & Regulations Enforce
Common Compliance Goals
for Records and Data:

• Integrity



• Confidentiality



• Transparency



Sarbanes-Oxley: SEC Rule 13a-15 (aka Section 404)

17 CFR 240.13a-15
General Rules and Regulations,
Securities Exchange Act of 1934

13a-15 Controls and procedures.

- (f) The term **internal control over financial reporting** is defined as a process ... to provide reasonable assurance regarding the **reliability of financial reporting** and the preparation of financial **statements for external purposes** in accordance with generally accepted accounting principles ...
- (1) ... maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
- (2) Provide reasonable assurance that **transactions are recorded** as necessary ...
- (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets

Specified
Capabilities

• Report & Publish



• Retention Mgmt



• Access Control



• Audit Trails






Data Protection Act

GEOGRAPHIES:

- Implements EU Directive
- UK Law – DPA

Laws & Regulations Enforce Common Compliance Goals for Records and Data:

- Integrity 
- Confidentiality 
- Transparency 

Data Protection Act (EU)

Data Protection Act 1998, Schedule 1 **THE DATA PROTECTION PRINCIPLES**

- 1. Personal data shall be processed fairly and lawfully ...
- 2. Personal data shall be obtained only for one or more specified and lawful purposes...
- 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose ...
- 4. Personal data shall be accurate and, where necessary, kept up to date.
- 5. Personal data processed for any purpose or purposes shall **not be kept for longer** than is necessary for that purpose or those purposes.
- 6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
- 7. Appropriate technical and organisational measures shall be taken against unauthorised or **unlawful processing of personal data** and against accidental loss or **destruction of, or damage to,** personal data.

Specified Capabilities

• Audit Trails 

• Retention Mgmt 

• Expungement 

• Access Logs 

• Access Control 

• Backup-Recovery 

HR - Compliance Requirements

- There are broadly three areas that HR professionals need to worry about.
- Data Protection
- Equal Opportunities
- Enforcing HR Procedures (e.g. Disciplinary)

DPA - HR Record Retention Requirements

Record	Statutory Retention Period
Accident Books	3 Years after last date of entry
Income Tax & NI	3 Years after fiscal year
Medical Records - Hazardous Substances	40 Years for date of last entry
Records relating to retirement benefits	6 Year from event date
Maternity/Sick Pay records calcs	3 Years
Wages/Salary	6 Years
Record	Recommended
Application forms/interview notes	1 Year
Assessments under H&S Regs	Permanently
IR Approvals	Permanently
Money Purchase details	6 Years
Paternal Leave	5 Years
Pension records	12 Years
Redundancy Details	6 Years
Senior Execs records	Perminently
Trade Union Agreements	10 Years
Time Cards	2 Years after audit

Source – Information Commissioners Office

Enterprise Compliance Example

IT Compliance Manager

Key Tasks

- IT Point person for compliance initiatives
- Oversees security practices

How they Work

- Attends meetings
- Coordinates regional eDiscovery efforts

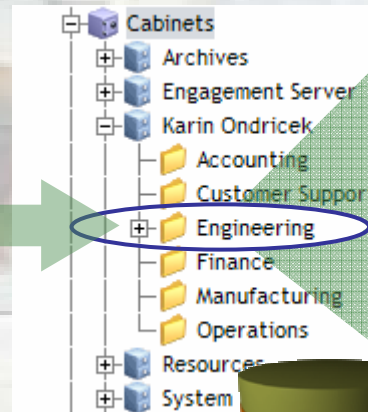
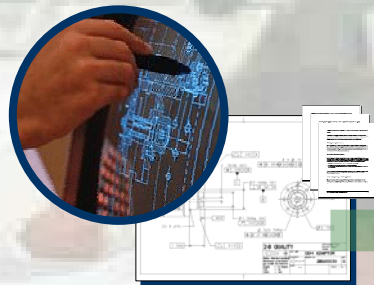
1: Must retain Engineering documents for 7 years after product ships.

Compliance Infrastructure

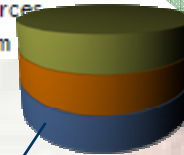
Engineering documents created/ completed.

Policies mapped to Engineering folders.

Retention policies ensure content locked down

A screenshot of a software interface for configuring a retention policy. The window title is 'New Retention Policy: Phases'. It has three tabs: '1. Create', '2. Info', and '3. Phases'. The '3. Phases' tab is active. There are four phase buttons: 'Active', 'Semi-Active', 'Dormant', and 'Final'. 'Semi-Active' is selected. Below the buttons, there is a 'Phase Name' field with 'Semi-Active' entered. Under 'Duration', there are three input fields: 'Years' with '1', 'Months' with '0', and 'Days' with '0'. At the bottom, there is a 'Cut-off Period' dropdown menu set to 'Disabled'. A blue circle highlights the 'Semi-Active' button and the 'Duration' fields.

Freeze Holds -
Digital Shredding -



Enterprise Compliance Example

IT Compliance Manager

Key Tasks

- IT Point person for compliance initiatives
- Oversees security practices

How They Work

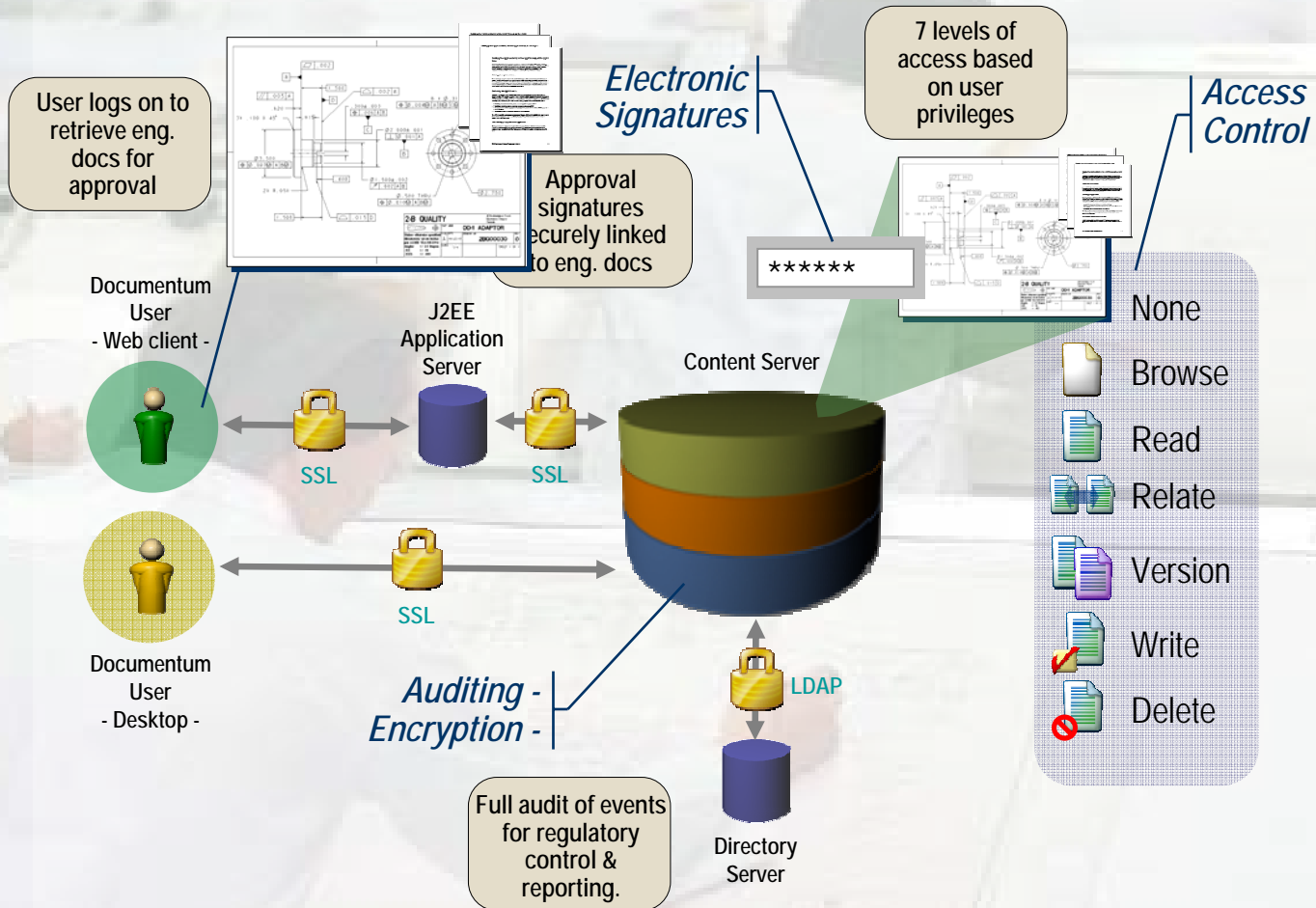
- Attends meetings
- Coordinates regional eDiscovery efforts

1: Must retain Engineering documents for 7 years after product ships.

Compliance Infrastructure

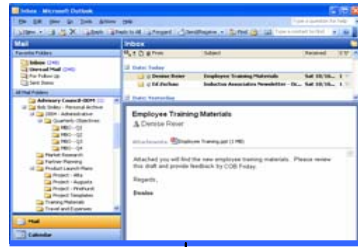
2: Ensure protection of intellectual property.

Secure Repository

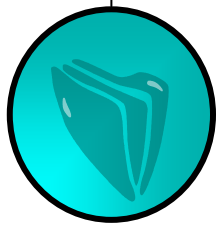


Organisation Technology Solutions

Not point solutions



Common Client Technology such as Outlook



Content Management

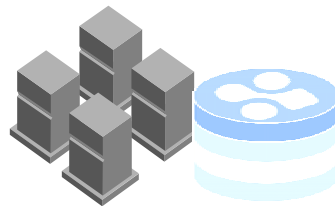


Records Management



Email Management

Optional Applications provide "layers" of functionality



Common Repository needs to be "Storage Aware"

Adding the capabilities of an Enterprise Content Management Platform...

Maturity Level

Characteristics of Compliance Maturity Levels

5. Enterprise Risk Management and Automated Compliance Processes

4. Integration with Operational Systems to Provide Automated Controls Monitoring

3. Integration of ECM and Business Process Management

2. Targeted Point Solutions

1. Ad Hoc Controls Monitoring Tools

- Document check-in/check-out, version control, audit trail, archiving of supporting documentation, collaboration
- Business process definition, workflows, automation

- Custom systems to address Sarbanes-Oxley Compliance
- Role-based functionality to provide data security
- Minimal functionality to support controls documentation repositories

- Controls stored in Excel, Word, etc.
- Minimal visibility into status and processes
- Inconsistent/manual approaches for addressing security of controls data