What Are the Regulators Really Expecting?

Information governance capabilities are a critical enabler to addressing regulatory concerns.

James K. Watson, Jr., PhD and Scott Swanson, CFE Doculabs, Inc.
About the Presenters

James K. Watson, Jr., PhD
CEO and Founder

Scott Swanson, CFE
Vice President and Practice Leader
IG from the Financial Service Global Risk and Compliance View

- Key issue: Risk Exposure, Legal, and Regulatory actions while Collaborating, Controlling, Safeguarding and remaining AGILE and PROFITABLE
- Document attrition (collections lost when employees leave, change roles, etc.)
- Compromise of confidentiality, integrity, and availability of critical internal or customer information — THE MORE YOU REQUIRE, THE MORE YOU ARE RESPONSIBLE FOR
- Non-compliance with records management policies or regulations
- Explosive e-discovery cost and risk; with “X”+ years of company-wide over-retention, just one significant litigation can severely impact the organization
- Conflicts, overlaps, and gaps
3 Enforcement Targets

• They will ASK
  – Enforce governance—Is it effective to dictate behavior?
  – Mitigate risk—Is it correlating to business operations?
  – Ensure compliance—Are the proper controls in place?

• They will SEEK
  – Dishonest behavior to the point of profit from unethicality
  – Naiveté
  – Inefficiency

• They will FIND
  – Documentation of communications, policies and procedures, activity
Quick Takes on Your Security and Compliance Situation

1. Most organizations are missing several pieces

2. Three types of missing pieces:
   1. **Directly** impact compliance
   2. **Necessary** or highly pragmatic enabling conditions for compliance
   3. Enable compliance, **positively impact** other requirements

3. Align compliance program with information management and governance
From Information Governance to Enterprise GRC

Information governance is the control of information to meet your legal, regulatory, and business risk requirements.
Case Study: Financial Institution Big Bills and Small Controls

**BACKGROUND**
- AML/BSA/OFAC/FRAUD AUDIT
- $XXB in revenue, XXXX employees
- Decentralized information models
- Poor governance, controls, policies, and procedures
- Frequent regulatory visits

**ENGAGEMENT**
- Gather and Review Documentation
- Assess relative health of organization’s AML/BSA programs
- Determine weaknesses and gaps
- Identify illicit activity

**RESULTS**
- 40% of the cost was in document capture and review
- Conclusions were worse than reality because there was no documented proof—only observable behavior
- Knowledge and information retention was poor and high risk for attrition or data loss
- Branches and affiliates were operating at rogue levels
- Poor information / data flows resulted in red flags across product lines and business units unwitting to AML and Fraud departments (FrAML model was recommended)
Why develop an integrated approach to risks such as Fraud and AML (FrAML)?

- Information sharing, storage, and governance frameworks were cornerstone to risk management and compliance.
Case Study: Financial Institution with Lacking or Delayed Information

Non-compliance and poor governance is no longer a cost of doing business. Lawsuits and prosecutions are targeting individuals. Where do you stand---on the stand?

HEADLINE EXAMPLE

- **KYC/CDD**: Arab Bank Ruling: If banks have a client, institutional relationship, or correspondent bank affiliation that is NOT on a screening list, but ends up being identified as an illicit relationship---witting or unwitting, they could face hefty civil settlements in addition to the federal penalties. Such discoveries will lead to additional investigations and likely more fines.

- **Cooperation**: SEC charged that Wells Fargo unreasonably delayed its production of documents and omitted key documents during the SEC’s investigation. The Chief of the SEC Enforcement Division’s Market Abuse Unit, stated that Wells Fargo's actions "improperly delayed our investigation and... interfered with our search for the truth.” A few weeks ago, this very issue was highlighted since [SEC/DOJ] "opinion is based on the perception of the investigators."
Case Study: Hot Mess- CDD/KYC, Governance, Fraud, AML, Sanctions
Case Study: They Showed their Compliance, and Saved

Everything must be documented and available for review. Delays are costly and set the tone for perceptions.

- Board Minutes
- Trainings
- Reviews
- Communications
- Programs
- Samples
- Policies and Procedures
What’s the Scope of Information Governance?

• **Good**: Information governance is the control of information to meet your legal, regulatory, and business requirements. (Robert Smallwood)
  
  — Great start because it's accurate and simple -- it avoids the trap of being a laundry list written in legalese.

• **Better**: Information governance is the control of information to meet your legal, regulatory, and business *risk* requirements.
  
  — IG doesn't address all your business demands -- its primary focus is on "defensive" business requirements as opposed to "offensive" business requirements.

  — IG’s primary focus should be on controlling the risks and costs (primarily risk-related costs) of your information.
Three Big IG Challenges for 2015

1. The digital landfill problem.
   - TBs or PBs
   - How do you sort through it and responsibly retain or dispose within your constraints?

2. The “systems of engagement” fragmentation problem.
   - How do you do IG on your dynamic, sometimes chaotic “systems of engagement”? They use social media, mobile devices, and the cloud.
   - Your problem has three parts:
     1. How do you meet your IG demands with your internal use of systems of engagement which you use for collaboration, interactive community building, etc.?
     2. How do you meet your IG demands with your use of external SOE beyond the firewall, with vendors and the public?
     3. How do you meet your IG demands in how you’re integrating your evolving SOE into your more mature systems of record, which help to run your core processes?

3. The discovery problem.
   - How do you prepare for and respond to regulatory audit, litigation and other discovery, given #1 and #2 above?
Plan and Manage IG with a Program Framework

1. Overall IG Program Strategy
2. IG Governance Team and Operations
3. IG Process Design and Implementation
4. Information Architecture
5. IG Architecture and Technology
6. IG Communications and Training

<table>
<thead>
<tr>
<th>IG Program Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Program Strategy</td>
</tr>
<tr>
<td>Information Architecture</td>
</tr>
</tbody>
</table>
The Assessment Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
<th>Key Components</th>
</tr>
</thead>
</table>
| Overall Program Strategy        | The overall vision and strategy for managing content at an organization. This strategy should address existing visions and strategies for enterprise content management (ECM), e-discovery, and records management (RM), and should address any gaps that may exist. This strategy should also establish general principles for the level of resources the organization will apply to the program at a high level. | • RM vision, strategy, and roadmap  
• ECM vision, strategy, and roadmap  
• A litigation readiness vision, strategy, and roadmap that addresses the RM and ECM strategies and any gaps  
• Principles for resources |
| Governance and Operations       | The governance structure and operational structure(s) for implementing the content management strategy. Includes roles, responsibilities, program governance metrics, policies, procedures, and guidelines. | • Governance structure (roles, responsibilities)  
• Operational structure (roles, responsibilities)  
• “Rules” (i.e. policies, procedures, and guidelines) for managing ESI (e.g. records management, e-discovery, etc.) |
| Information Organization        | The manner in which information is organized. This includes a content taxonomy or organizational hierarchy, a records plan and retention schedule, and a content map of the organization’s electronically stored information (ESI) and content repositories. | • Content taxonomy  
• Records retention plan  
• ESI-Repository Map |
| Process Design and Implementation| The overall processes used to support content management. These include the overall records/information lifecycle management process, as well as more specialized processes such as e-discovery. | • Discovery process  
• Record/information lifecycle management process |
| Architecture and Technology     | The tools and technologies that are used or leveraged for managing content and the architecture for how they fit together. This can include technologies and capabilities for ECM, records management, and email management, as well as specialist tools for areas such as e-discovery. | • Architecture strategy  
• ECM tools and capabilities  
• Records management tools and capabilities  
• Email management tools and capabilities  
• E-discovery tools and capabilities |
| Organizational Readiness        | The mechanisms used to educate the user community and improve compliance and adoption of the procedures and solutions that support proper content management. | • Communication plan/program  
• Training plan/program |
Maturity Curve

OVERALL PROGRAM STRATEGY
• No adequate strategy and roadmap even partially implemented; may be partially designed
• No perceived need for strategy to address ECM, RM, e-discovery (ED), and email management (EMM) at the enterprise level

GOVERNANCE AND OPERATIONS
• Governance and operational structure at most partially developed
• “Rules” – policies, procedures, guidelines – at most partially designed

INFORMATION ORGANIZATION
• No adequate taxonomy or retention plan even partially developed
• ESI-Repository Map at most partially developed (for most businesses)

PROCESS DESIGN AND IMPLEMENTATION
• Discovery processes not evaluated or even partially designed
• Information lifecycle management (ILM) processes not evaluated or even partially designed

ARCHITECTURE AND TECHNOLOGY
• Architecture strategy for core ECM, discovery, RM, and email management (where required) not even partially developed
• Adequate and consolidated technology portfolio not even partially implemented

ORGANIZATIONAL READINESS
• Communications and training strategy not even partially developed
• Organization is unprepared to implement ILM improvement program

OVERALL PROGRAM STRATEGY
• Developed and implemented strategy and roadmap
• Developed and implemented strategy addresses ECM, RM, ED and EMM at the enterprise level

GOVERNANCE AND OPERATIONS
• Governance and operational structure implemented and operational
• “Rules” – policies, procedures, guidelines – implemented and practiced

INFORMATION ORGANIZATION
• Developed and implemented taxonomy and retention plan, with methodology for further development and maintenance
• Developed and maintained ESI-Repository Map

PROCESS DESIGN AND IMPLEMENTATION
• Discovery processes evaluated, designed, implemented, monitored, and maintained
• ILM processes evaluated, designed, implemented, monitored, and maintained

ARCHITECTURE AND TECHNOLOGY
• Developed and implemented architecture strategy for core ECM, discovery, RM, and email management (where required)
• Implemented adequate and consolidated technology portfolio

ORGANIZATIONAL READINESS
• Developed and implemented communications and training strategy
• Organization is adequately prepared to implement ILM improvement program

Note: Bold blue text indicates characteristics that apply to ACME.
ACME has scored better than the peer group average in five of the six evaluation categories – a significant achievement, given the complexity of the ACME environment.

Top firms balance their programs so that no specific program categories are overemphasized or sacrificed relative to other aspects of a successful program (ACME is doing a good job of this).

The primary gap observed across the categories is the level of actual implementation that has been achieved.
Overall Program Strategy

Benchmark Scoring:

- **Strengths**
  - Strong organization based on federated model
  - Innovative approach to addressing transactional vs. functional records
  - Highly capable staff in place as managers and leaders

- **Rationale / Impact**
  - Ability to present a clear and comprehensive story at all levels of the organization
  - Program sustainability
  - Ability to project longer term costs and benefits

- **Recommended Actions**

- **Risks**
  - Ability to impact/manage supplier risk
  - Ability to maintain program momentum

Lowest Rating: 1

Benchmark Average: 2.7

ACME Score: 3.3

Target ACME Score: 4.0

Highest Rating: 5

- Benchmark Average
- ACME Score
- Target ACME Score
Information Management Capabilities in a Reference Model

ECM Presentation
- Capture
- E-forms
- User Interface

Process and Collaboration
- Collaboration
- Workflow
- Process Automation

Content Middleware
- Enterprise Search
- Taxonomy Management
- Document Comp/Publishing
- Document Security
- Information Rights Management
- E-discovery
- Document Exchange
- Integration
- Digital Signatures

Repository Management
- Document Management
- Document Image Management
- Web Content Management
- Digital Asset Management
- Technical Doc Management
- Output/Report Management
- Records Management
- Email Management
- Storage
Summary

• GRC programs and processes are inextricably linked to information governance

• Enforcers require you to **Prove not Explain**
Thank You

• James Watson, Jr PhD
  jwattson@doculabs.com
  312-881-1620

• Scott Swanson, CFE
  sswanson@doculabs.com
  312-659-3000