How to Plan and Implement
Your Information Governance Program

Doculabs’ Rick Tucker and Richard Medina
"How to Plan and Implement Your Enterprise Information Governance, Risk, and Compliance Program"

Most organizations in highly regulated industries are missing several components in their information governance program that are necessary to provide adequate, sustainable security, compliance, and risk reduction.

This session:

1. Describes and classifies the missing components
2. Shows how to incorporate them into your program
3. Explains how to implement them in a multi-year roadmap
Rick Tucker
Vice President at Doculabs

Rick Tucker has 17 years of experience in information management technologies, focusing on enterprise content management (ECM) technologies and their applications to business processes.

630-448-0616
rtucker@doculabs.com
@ricktucker88
www.linkedin.com/in/ricktucker
Richard Medina

Co-Founder and a Principal Consultant at Doculabs.

In my 23 years with Doculabs, I’ve consulted for organizations in a wide range of industries, including financial services, insurance, manufacturing, utilities, and government.

312-953-9983
rmedina@doculabs.com
www.linkedin.com/in/richmedinadoculabs
www.doculabs.com
Management Consulting

Objective

Enterprise Content Management (ECM)
Vision for Compliance

Culture of compliance

Proactive, Beyond mere letter of law

Audit ready

Sustainable

Effective

Demonstrable
So How Do You Get There from Here?
You Need a Compliance Program Framework
What’s the Minimum that a Compliance Framework Should Do?

1. What regulations and standards should we comply with?
2. Who is responsible for compliance?
3. What controls should be in place?
4. How do we monitor compliance?
But the Framework Should Do More

1. It must be “leak proof” for any regulatory audit, litigation, etc.
2. It must explicitly show how it follows the relevant regulations and standards (Federal, State, Industry)
3. It must be fulfillable
4. It must be clearly translatable into a Roadmap
5. It must be easily communicated and understood – so it must be as simple as possible while meeting the other necessary requirements
6. It must be aligned with your other enterprise objectives and initiatives to be effective and sustainable
7. Since your organization has other GRC obligations (IS, Legal, Business Continuity), it should fit into a general Framework and overall strategy that allows you to align and effectively address all such obligations
   - Different, unaligned “frameworks” and initiatives will fail
   - You should have a single GRC framework into which compliance, IS, and other current and future “defensive” programs can fit
Example #1: A Compliance Framework?

Figure 1—Information Security Program
Office Functional Inventory

Functional Elements:
- CISO
- Threat and Vulnerability Assessment
- Vulnerability Management and Incident Response
- Legal and Regulatory
- Strategy
- Policies, Procedures, Principles and Standards
- Business Continuity and Disaster Recovery
- Education and Communications
- Program Governance
- Architecture and Design
- Technology Capability and Evaluation
- Key Performance Analysis and Effectiveness
- Information Security Oversight Board

Organizational Interactions:
- Legal (Office of General Counsel)
- Vendor and Partner Management
- Privacy (Chief Privacy Officer and/or Privacy Office)
- Business Units
- Operations Linkage (IT, General Ops)
- Audit and Global Compliance
- Human Resource
- Change Management
- Physical Security
Example #2: A Compliance Framework?
Example #3: A Compliance Framework?

- **Governance, Risk & Compliance**
  - **IT Governance**
    - Governance Framework
    - Information Security Management
  - **Business Resilience**
    - Business Continuity Management
    - IT Disaster recovery planning
  - **Operational Risk**
    - IT Risk
    - Vendor Risk
    - Supply chain Risk
  - **Regulatory & Compliance**
    - Regulatory readiness
    - Audit & Assessment
    - Remediation

*Images and logos of ARMA Northern New Jersey, ARMA International, and ARMA Metro NYC Chapter.*
Example #4: A Compliance Framework?
Example #5: A Compliance Framework?
The Framework Should Address Roles and Regulations
It Should Allow Us to Drill Down in a Direct Way

<table>
<thead>
<tr>
<th>UNIT #1</th>
<th>UNIT #2</th>
<th>UNIT #3</th>
<th>UNIT #4</th>
<th>UNIT #5</th>
<th>UNIT #6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labor Laws</td>
<td>EEOC &amp; Workplace Guidelines</td>
<td>Confidential Business Information</td>
<td>SEC Guidance</td>
<td>PCI</td>
<td>Onboarding Credentialing Requirements</td>
</tr>
<tr>
<td>Onboarding Background Checks</td>
<td>Sexual Harassment Laws</td>
<td>Information Requests for Legal Investigations</td>
<td>GAPP, FASB Guidance</td>
<td>Business Continuity, Disaster Recovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOX</td>
<td>SOX</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contract Guidelines</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Records Management, Information Requests

“Other” Regulations and Standards

<table>
<thead>
<tr>
<th>HR</th>
<th>RCS</th>
<th>ERMD</th>
<th>ACCOUNTING / FINANCE</th>
<th>IT</th>
<th>OPERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Kickback Statutes</td>
<td>Governmental Payor Rules</td>
<td>HIPAA and HITECH Privacy and Security</td>
<td>Anti-Kickback Statutes</td>
<td>Physical Safeguards</td>
<td>Scope of Practice Requirements</td>
</tr>
<tr>
<td></td>
<td>External Audits</td>
<td></td>
<td></td>
<td>Administrative Safeguards</td>
<td>OIG Guidance for Continuous Sanction Checks</td>
</tr>
<tr>
<td></td>
<td>False Claims Act</td>
<td></td>
<td></td>
<td>Technical Safeguards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deficit Reduction Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACA ID of Overpayments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conflicts of Interest, Gifts and Business Courtesies

“In-Scope” Regulations and Standards

This is a healthcare organization example
The Framework Should Address Controls and Monitoring

- Overall Program and Framework Strategy
- Policies and Procedures
- Processes and Operations
- Information Technology and Information Management
- Physical Assets and Environment
- Human Resources and Roles and Responsibilities
- Metrics, Measurement, and Monitoring
- Communication and Training
Continuous Improvement Should be Inherent to the Design
The Compliance Framework
A Simple Outline of the Framework Components
The Primary Framework Components

1. Overall Program and Framework Strategy
2. Policies and Procedures
3. Processes and Operations
4. IT and Information Management
5. Physical Assets and Environment
6. HR and Roles and Responsibilities
7. Metrics, Measurement and Monitoring
8. Communications and Training

Information Governance Program Categories

- Overall Program and Framework Strategy
- Policies and Procedures
- Processes and Operations
- IT and Information Management
- Physical Assets and Environment
- HR and Roles and Responsibilities
- Metrics, Measurement, and Monitoring
- Communications and Training
Four Guiding Principles

Design the Framework to:

1. Align all areas of IG
2. Align IG with your overall organization
3. Directly address all IG requirements
4. Address those requirements’ necessary and enabling conditions
1. Overall Program and Framework Strategy

**Key Elements**

- Comprehensive organizational compliance strategy and roadmap that address and align all relevant areas of compliance and risk
- Strategy and roadmap align with other and overall objectives of the organization
- Compliance program is designed for continuous improvement
- Strategy and roadmap align with resources (including time, people, and money) and failure risk tolerance

**Primary Gaps**

- Lack of alignment in IG areas, between IG areas, and between IG and the “offensive” strategies and functions (“the business”)
- No Future State or Roadmap for compliance program that addresses necessary/enabling conditions for compliance
2. Policies and Procedures

**Key Elements**

- Establishes policy oversight, P&Ps, and efforts to set required standards, guidance, and enforcement to meet compliance and risk requirements
- Includes Code of Conduct and relevant P&Ps
- Addresses P&Ps relevant to information lifecycle management, including Information Security, Information Privacy, Records Management, Email, Social Media

**Primary Gaps**

- The scope and coverage of P&Ps are not clear, and they are poorly designed for authoring, updating, and implementing
- Most lack clear “crosswalking” understanding and documentation of all relevant regulations and P&PS to identify and address gaps and overlaps
- Many RM Retention Plans are unclear and can’t be effectively executed
3. Processes and Operations

**Key Elements**

- Includes processes relevant to compliance and ILM, from creation and ingestion of information through disposition
- Addresses clear lines of communication, procedure for raising concerns
- Includes incident management, the response and resolution of compliance incidents

**Primary Gaps**

- Lack defined processes for many areas of the information lifecycle, e.g. when information leaves the control of systems
- Many have “pockets” of well-managed processes -- but these processes are inconsistently applied
A Simple Process for Compliance Management

1. Understand the Risk and Regulatory Environment
2. Create and Maintain the Requirements Matrix
3. Perform Compliance Risk Assessment
4. Manage Obligations and Implementation
5. Measure and Monitor
6. Communications and Training
4. IT and Information Management

Key Elements

• Architecture strategy, standards, and portfolio for EIM, IG, RM, E-discovery, and other tools and capabilities
• Information architecture -- a content taxonomy, records retention schedule, and an ESI-repository map
• Technical security and access control, to restrict access for IS (info security)

Primary Gaps

• Effective approach for managing the system portfolio
• Some lack an advanced ECM system for high-risk and high value ESI
• Inconsistencies in content organization between and within departments; over-reliance on shared drives
• No good ESI-repository map or documented understanding of where the ESI resides
• Records retention plan is inadequate for ESI
Information Management Capabilities in a Reference Model

<table>
<thead>
<tr>
<th>Information Management</th>
<th>Information Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC</td>
<td>Controls and Policy Library and Response</td>
</tr>
<tr>
<td></td>
<td>IT Application Registry</td>
</tr>
<tr>
<td>Remediation and Exception Management</td>
<td>Privacy Management</td>
</tr>
<tr>
<td></td>
<td>Controls, Risk Evaluation and Compliance Dashboard</td>
</tr>
<tr>
<td>Records Management and Discovery</td>
<td>Records Plan Management</td>
</tr>
<tr>
<td></td>
<td>ESI Inventory</td>
</tr>
<tr>
<td></td>
<td>Retention and Destruction</td>
</tr>
<tr>
<td></td>
<td>Electronic Discovery</td>
</tr>
<tr>
<td>Information Security</td>
<td>Identity Management</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Authorization</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Isolation</td>
</tr>
<tr>
<td>Enterprise Content Management</td>
<td>Content Capture and Access</td>
</tr>
<tr>
<td></td>
<td>Process Management</td>
</tr>
<tr>
<td></td>
<td>Content Middleware</td>
</tr>
<tr>
<td></td>
<td>Repository Services</td>
</tr>
<tr>
<td>Enterprise Data Management</td>
<td>Master Data Management</td>
</tr>
<tr>
<td></td>
<td>Metadata Management</td>
</tr>
<tr>
<td></td>
<td>Data Quality Management</td>
</tr>
<tr>
<td></td>
<td>Data Architecture</td>
</tr>
</tbody>
</table>
ECM Capabilities in a Reference Model
5. Physical Assets and Environment

**Key Elements**

- Physical and environmental for physical protections of the data center, other secure processing areas, physical assets, and data from theft, damage, or loss
- Asset identification and classification for the inventory, accountability, responsibility, classification, and implementation of associated controls

**Primary Gaps**

- Many actually have relatively good comprehensive security for their physical environment, including e.g. controlling physical access, printer control, clean desk access
- Many have relatively good comprehensive IT asset security, including e.g. laptop, mobile device, and other IT asset control

![Information Governance Program Categories]

[Image of Information Governance Program Categories]

- Overall Program and Framework Strategy
- Policies and Procedures
- Processes and Operations
- IT and Information Management
- Physical Assets and Environment
- HR and Roles and Responsibilities
- Metrics, Measurement, and Monitoring
- Communications and Training

[Logos of ARMA Northern New Jersey, ARMA International, Long Island Chapter, ARMA Connecticut Chapter, and ARMA Metro NYC Chapter]
6. HR and Roles and Responsibilities

Key Elements

• Roles and responsibilities for the various GRC and IG sub-domains (info security, privacy, risk, etc.) – with clear separation of duty and authority
• Roles and responsibilities for the individual units
• Includes establishing the CCO (Chief Compliance Officer), CCC (Corporate Compliance Committee), and ensuring adequate program resources
• Includes workforce management and outsourcing, to govern the hiring, transfer, termination, and clearance processes for employees, contractors, and vendors

Primary Gaps

• Many have GRC and IG executive and managerial roles, but more need to be implemented and aligned
• Lack some skills necessary for the next stages of GRC – e.g. information architecture and ECM strategy and implementation
• Lack incident, breach, and “see something say something” reporting system with all necessary pieces in place (hotline, clear non-retaliation policy, clear reporting chain)
7. Metrics, Measurement and Monitoring

Key Elements

- Key objectives and measures of program success, and the tracking of defined metrics within the program for reporting
- Internal compliance and security audits to provide assurance that controls are adequately designed and operating
- Defines what is logged, monitored, analyzed, reported, and the alert levels to trigger for incident response

Primary Gaps

- Program is not aligned so significant gaps and overlaps in most areas are not measured or monitored
- Program not designed for continuous improvement, based on effective tracking and monitoring
8. Communications and Training

**Key Elements**

- Communication plan and program
- Training plan and program
- The planning, procedures, documentation, and implementation of compliance and security awareness and related training for the workforce, partners, and contractors

**Primary Gaps**

- Most lack an enterprise IG training plan
- Many have relatively good communications and training for some high risk areas – e.g. physical environment and IT security
- But lack training in many areas for consistent, effective methods (e.g. search and findability, reports requesting and use, almost ALL areas of information lifecycle management)
- No clear plan for communication and training on the compliance program in general, and, more specifically, the enabling/necessary information management areas
- Many users unaware of the relevant information management policies and guidelines; performing what they believe is the “right thing to do”
So How Do We Start?
Next Steps

1. Don’t get overwhelmed
   – Break the big problem into smaller problems
2. **Assess** your risks, regulations, and requirements
   - Direct and enabling
   - You may need to prioritize and focus on “in-scope” subset
   - Organize by **Responsible Units**

### Responsible Units

<table>
<thead>
<tr>
<th>UNIT #1</th>
<th>UNIT #2</th>
<th>UNIT #3</th>
<th>UNIT #4</th>
<th>UNIT #5</th>
<th>UNIT #6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADA</td>
<td>Malpractice Laws</td>
<td>IRS Tax Reporting and Filing Guidance</td>
<td>NIST Cyber Security Guidance</td>
<td>Licensing Board Imposed Sanctions</td>
<td></td>
</tr>
<tr>
<td>Labor Laws</td>
<td>Confidential Business Information</td>
<td>SEC Guidance</td>
<td>PCI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEOC &amp; Workplace Guidelines</td>
<td>Information Requests for Legal Investigations</td>
<td>GAPP, FASB Guidance</td>
<td>Business Continuity, Disaster Recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Onboarding Background Checks</td>
<td>SOX</td>
<td>SOX</td>
<td></td>
<td>Onboarding Credentialing Requirements</td>
<td></td>
</tr>
<tr>
<td>Sexaul Harassment Laws</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### “Other” Regulations and Standards

<table>
<thead>
<tr>
<th>HR</th>
<th>RCS</th>
<th>ERMD</th>
<th>ACCOUNTING / FINANCE</th>
<th>IT</th>
<th>OPERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Kickback Statutes</td>
<td>Governmental Payor Rules</td>
<td>HIPAA and HITECH Privacy and Security</td>
<td>Anti-Kickback Statutes</td>
<td>Physical Safeguards</td>
<td>Scope of Practice Requirements</td>
</tr>
<tr>
<td></td>
<td>External Audits</td>
<td></td>
<td></td>
<td>Administrative Safeguards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>False Claims Act</td>
<td></td>
<td></td>
<td>Technical Safeguards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deficit Reduction Act</td>
<td></td>
<td></td>
<td></td>
<td>OIG Guidance for Continuous Sanction Checks</td>
</tr>
<tr>
<td></td>
<td>ACA ID of Overpayments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### “In-Scope” Regulations and Standards

| Conflicts of Interest, Gifts and Business Courtesies |  |  |  |  |  |

This is a healthcare organization example.
3. Use a comprehensive IG framework  
   – For your immediate and future IG requirements
Next Steps

4. Think Alignment
   – Of your IG areas
   – Of IG with your organization
Next Steps

5. **Contact us** with any questions

Richard Medina, Doculabs  
312-953-9983  
rmedina@doculabs.com

Rick Tucker, Doculabs  
630-448-0616  
rtucker@doculabs.com
Thank You