Closing the Regulatory Compliance Loop with SAP Regulation Management and SAP Process Control

James Rice
Greenlight Technologies
In This Session

- Regulations are simply a part of doing business in today’s world, but staying current with regulatory changes and ensuring organizational compliance is anything but simple.

- Attend this session to delve into the intricacies of this practice and learn how to close the regulatory compliance loop with SAP Regulation Management and SAP Process Control. Attendees will learn to:
  - Consolidate regulatory feeds in a single authoritative source for alerts and requirements
  - Leverage SAP Process Control to automate controls testing and extend continuous monitoring of controls’ effectiveness across operational, financial, and IT systems
  - Demonstrate end-to-end auditability of regulatory compliance
What We’ll Cover

- Discuss the problem
- Describe the evolution of compliance solutions
- Define regulation management as a process
- Manage regulatory intake
- Ensure compliance through control monitoring
- Evidence and Report on compliance status
- Wrap-up
Top Risk for Most Organizations

“Regulatory Change and heightened regulatory scrutiny – This risk continues to represent the top overall risk for the third consecutive year for most organizations”

– Executive Perspectives on Top Risks for 2015, Key Issues Being Discussed in the Boardroom and C-Suite
Challenge in Managing and Responding to Regulatory Compliance

- Customers need the ability to:
  - Capture new and changing regulatory mandates
  - Monitor compliance with regulatory mandates and internal policies
  - Establish accountability and unify regulatory requirements across key stakeholders
  - Leverage existing compliance and control activity to satisfy new and changing regulations
  - Align regulatory requirements with internal control activities and operations
  - Automate execution and testing of controls across enterprise systems
What We’ll Cover

- Discuss the problem
- Describe the evolution of compliance solutions
- Define regulation management as a process
- Manage regulatory intake
- Ensure compliance through control monitoring
- Evidence and Report on compliance status
- Wrap-up
Point Solutions

- Companies have one or more point solutions in place
  - Standalone “silos” with a singular purpose

- Regulatory Compliance obligations have resulted in the exploration of compliance outputs from operational toolsets

- These tool sets were never designed as singular compliance-driven solutions
  - That is changing as compliance solutions are in high demand at companies and vendors see opportunity to address compliance
Document Management

- Document Management
  - Compliance audits were documentation/evidence-focused
  - Still manually dependent to populate the solution

- SharePoint
  - Still manual but can incorporate calendar notifications and task management
  - Easy to deploy
  - Data integrity concerns
  - Non-sustainable
Why GRC?

• Granularity in regulatory requirements makes a manual approach non-sustainable
• Pro-active vs. re-active
• Enterprise layer to manage/integrate point solution outputs
• Workflow automation
• Self-assessment functionality
• Detection and mitigation automation through workflows
• Controls testing and design
• Forces consistency in data
• Correlate and manage Big Data
The Evolution of Compliance Solutions

“I don’t have time to do this compliance stuff AND my day job!”

- Companies should never have to hear this complaint again if:
  - Sound operational-driven Processes and Controls are in place that “Bake In” Compliance
  - GRC technology is being leveraged to sustain and enforce controls and processes
What We’ll Cover

• Discuss the problem
• Describe the evolution of compliance solutions
• Define regulation management as a process
• Manage regulatory intake
• Ensure compliance through control monitoring
• Evidence and Report on compliance status
• Wrap-up
Content and Notification

- Intake Global, Federal, State/Local changes
- Monitor regulatory news
- Examine industry compliance breaches

Change Management

- Assign ownership and manage change
- Assess impact to business
- Align requirements to risks, policies and controls

Risk, Policy, and Control

- Assess and manage risks
- Maintain policies and controls
- Develop plans to test and monitor controls

Continuous Monitoring

- Aggregate for KRI & KPI monitoring
- Align with business objectives
- Automate control testing activities

Issue Management

- Identify and manage issues
- Implement remediation plan
- Prioritize by impact on business objectives

End to end Reporting

- Visualize end-to-end traceability
- Report to executive, business & compliance stakeholders
- Communicate the impact to the business

Regulatory Content Is the Tip of the Iceberg
### Regulation Management Process

1. **Regulatory Mandates**
   - Capture, intake and reporting of regulations
   - Leverage publicly available content & subscriptions from UCF, LexisNexis, Thompson Reuters, etc.
   - Regulatory alerts and monitoring

2. **Requirements**
   - Version control and gap analysis for periodic guidance documents
   - Delta change management
   - Reports and dashboards

3. **Collaboration**
   - Central repository for regulatory / policy content & requirements
   - Comment and interact from start to finish
   - Share and review best practices

4. **Workflow**
   - Dynamic, multi-threaded workflow capabilities
   - Review all or part of citations, requirements or controls at any time

5. **Control Definition**
   - Best practice control mapping & content creation
   - Unified control framework for all regulatory agencies
   - Map controls back to citations

4. **Control Management**
   - Manage, monitor and test controls
   - Execute control tests against operational systems & business applications

5. **Compliance Reporting**
   - Capture, store and import report results
   - Manage and maintain findings & evidence
Regulation Management Pillars

**Regulations & Policies**
- Intake and change management
- Identify and address compliance gaps in meeting new or changing requirements
- Engage business stakeholders

**Analytics**
- Assess the impact of regulatory risk & compliance
- Analyze policies, regulations and processes in the context of material exceptions
- Dashboard and detailed reporting for compliance

**Integrations**
- Integrate across multiple operational and financial data sources
- Data to decision aggregation
- Discovery, correlation, and normalization of disparate data
Key Considerations

- Big bang approach is NOT required
  - Where to start? It depends on your requirements!
    - Regulatory change?
    - Monitoring compliance across various business units?
    - Internal and external reporting?

- Change management is a MUST have
  - Executive level support to drive adoption and support

- Already have a content provider?
  - That’s a great start, but remember that’s just the tip of the iceberg!
What Can a Solution Provide to Your Business?

- Defensible and sustainable compliance
  - Proactively monitor regulatory compliance
  - Standardized processes
  - Enable transparency and auditability for enterprise regulatory compliance processes
- Reduce cost of compliance
- Reduce risk of control inefficiencies
- Operational autonomy for the business
What We’ll Cover

- Discuss the problem
- Describe the evolution of compliance solutions
- Define regulation management as a process
- Manage regulatory intake
- Ensure compliance through control monitoring
- Evidence and Report on compliance status
- Wrap-up
Challenges in Managing Regulatory Change
Unified Regulatory Change Management

SAP Regulation Management by Greenlight

Business

IT

Compliance

Audit

Legal

Unified Control
Banking Example

- Regulatory Requirements
  - PCI DSS
  - Gramm Leach Bliley Act (GLBA)
  - State-Based Consumer Privacy Laws
    - MA CMR 17
    - CA SB 1386
- Universal Control
  - Instead of three controls that are compliance-driven, now you have one control that is security-driven where compliance is a natural byproduct
  - Requirements to protect the security, integrity, and confidentiality of consumer non-public information
    - Access controls (who has access rights to customer data)
    - Activity controls for auditing of privileged users (who actually accessed customer data and what did they do)
    - Segregation of duties controls that prohibit a conflict of interest (keeping users from one side of the bank from being able to see account information on bank customers)
Utility Example

- Regulatory Requirements
  - Critical Infrastructure Protection (NERC)
    - Critical Asset Identification
  - SANS Top 20 Critical Controls (NIST)
    - Control 1: Inventory of Authorized Devices & Control 2: Inventory of Authorized and Unauthorized Software
  - ISO 27002 Section 7
    - Responsibility of Assets & Ownership and Accountability
  - Sarbanes-Oxley (SOX)
    - Risk Assessment & Event Identification

- Universal Control
  - Asset Identification that includes ownership and accountability to the asset
  - Instead of 4 controls that are compliance-driven, now you have one control that is operations-driven where compliance is a natural byproduct
Life Sciences Example

- Regulatory Requirements
  - FDA
    - Pharma Serialization
    - Drug Supply Chain Security Act (DSCSA)
  - State & Local Regulations
    - California
    - Florida
- Universal Control
  - Instead of multiple controls that are compliance-driven, now you have one control that is operations-driven where compliance is a natural byproduct
### Unified Regulatory Control Framework

<table>
<thead>
<tr>
<th>ISO 17799 2005</th>
<th>Cobit 4.0</th>
<th>SOX</th>
<th>PCI</th>
<th>CIP</th>
<th>NIST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1: Risk Assessment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 Assessing Security Risks</td>
<td>Plan and Organize:</td>
<td>• PO9 Assess and Manage IT Risks</td>
<td>• Risk Assessment</td>
<td>• 002 – Critical Cyber Asset Identification</td>
<td>Control 1: Inventory of Authorized and Unauthorized Devices</td>
</tr>
<tr>
<td></td>
<td>Monitor and Evaluate</td>
<td>• ME1 Ensure Regulatory Compliance</td>
<td>• Objective Setting</td>
<td></td>
<td>Control 2: Inventory of Authorized and Unauthorized Software</td>
</tr>
<tr>
<td></td>
<td>• ME2 Provide IT Governance</td>
<td>• ME3 Ensure Regulatory Compliance</td>
<td>• Event Identification</td>
<td></td>
<td>Control 4: Continuous Vulnerability Assessment and Remediation</td>
</tr>
<tr>
<td>1.2 Treating Security Risks</td>
<td>Plan and Organize:</td>
<td>• PO9 Assess and Manage IT Risks</td>
<td>• Risk Response</td>
<td>• 002 – Critical Cyber Asset Identification</td>
<td>Control 1: Inventory of Authorized and Unauthorized Devices</td>
</tr>
<tr>
<td></td>
<td>Determine risk treatment options; Apply appropriate controls, accept risks, avoid risks or transfer risks to other parties</td>
<td>Monitor and Evaluate</td>
<td>• Event Identification</td>
<td></td>
<td>Control 2: Inventory of Authorized &amp; Unauthorized Software Critical Controls 3-4: Security Configurations for Network Devices such as Firewalls, Routers, and Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ME1 Monitor and Evaluate IT Performance</td>
<td></td>
<td></td>
<td>Critical Control 18: Incident Response and Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ME2 Monitor and Evaluate Internal Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Section 2: Security Policy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Information Security Policy</td>
<td>Plan and Organize:</td>
<td>• PO1 Define a Strategic IT Plan</td>
<td>• Internal Environment</td>
<td>• 003 – Security Management Policies</td>
<td>Critical Control 15: Controlled Access based on need to know</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PO4 Define the IT Processes, Organization and Relationships</td>
<td>• Objective Setting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PO6 Communicate Management Aims and Direction</td>
<td>• Risk Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PO7 Manage IT Human Resources</td>
<td>Maintain an Information Security Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12. Maintain a policy that addresses information security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Section 3: Organization of Information Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1 Internal Organization</td>
<td>Deliver and Support:</td>
<td>• DS3 Ensure Systems Security</td>
<td>• Internal Environment</td>
<td>• 003 – Security Management Control</td>
<td>Critical Control 15: Controlled Access based on need to know</td>
</tr>
<tr>
<td></td>
<td>A management framework should be established to initiate and control the implementation of information security within the org</td>
<td>• Control Activities</td>
<td>• Information and Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DS5 Ensure Systems Security</td>
<td>Maintain an Information Security Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2 External Parties</td>
<td>Plan and Organize:</td>
<td>• PO9 Manage Quality</td>
<td>• Internal Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To maintain the security of information and information processing facilities that are accessed, processed, communicated to, or managed by external parties</td>
<td>Deliver and Support:</td>
<td>• Risk Assessment</td>
<td>• 003 – Security Management Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DS1 Define &amp; Manage Service Levels</td>
<td>• Control Activities</td>
<td>12. Maintain a policy that addresses information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DS2 Manage Third-Party Services</td>
<td>• Information and Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DS3 Ensure Systems Security</td>
<td>• Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maintain an Information Security Policy</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Source: SAP
Demo: Regulatory Intake
What We’ll Cover

- Discuss the problem
- Describe the evolution of compliance solutions
- Define regulation management as a process
- Manage regulatory intake
- Ensure compliance through control monitoring
- Evidence and Report on compliance status
- Wrap-up
Realizing Benefits of Control Optimization & Automation

Transform the compliance model to continuous control monitoring reduces cost, increases scope and lowers the financial risk exposure

**Control Cost Reduction**
- Eliminates redundancy
- Reduces # of key controls

**Automated Controls**
- Configurable controls
- Automated monitoring
- 100% of total population
- Business processes, SOX/SOD, IT general controls, application security controls, etc.

**Manual Controls**
- Controls relying on significant manual intervention
- Rely on data from source systems
- Customer and/or Shared Service

---

**Optimizing controls:**
- Eliminates redundancy
- Reduces # of key controls

**Automating manual activities:**
- Increases efficiency
- Improves compliance
- Lowers risk profile

**Balancing control mix:**
- Reprioritizes FTE activity
- Lowers total cost of ownership
Utilities Example

- Regulatory Requirements
  - Basel III – Liquidity Standards
    - Liquidity coverage ratio
    - The liquidity coverage ratio (LCR) will require banks to have sufficient high-quality liquid assets to withstand a 30-day stressed funding scenario that is specified by supervisors

- Controls
  - Identify High Quality Liquid Assets Details
  - Identify Expected Cash Outflows details
  - Identify Expected Incoming 30-Day Cash Flows details
  - Identify Total Asset value based on Asset class for HQLA
  - Identify Total Expected cash outflows based on Account Type
  - Identify Total Expected cash Inflows
  - Calculation of Liquid Coverage Ratio
Utilities Example (cont.)

• Regulatory Requirements
  - CIP, NIST, etc.
    - 24/48 hour de-provisioning to critical infrastructure
  - Sarbanes-Oxley (SOX)
    - User access reviews

• Controls
  - HR termination/position based revocation of user access
  - Enterprise de-provisioning
  - Audit reporting
Demo: Control Monitoring
What We’ll Cover

- Discuss the problem
- Describe the evolution of compliance solutions
- Define regulation management as a process
- Manage regulatory intake
- Ensure compliance through control monitoring
- Evidence and Report on compliance status
- Wrap-up
Reporting Up the Value Chain

- Link to business impact
- Manage accountability to KPIs and KRIIs
- Measure against best practices & evidence compliance with regulations
- Automate testing of key controls
- Provide exception-based monitoring of events
- Analyze policies, regulations and processes in the context of material exceptions
- Multiple operational and financial data sources
- Data to decision aggregation
- Discovery, correlation, and normalization of data
How to Report Strategically

- Highlight events in business context
- Tie to Key Performance and Risk Indicators
- Measure against industry best practices and frameworks
- Link to Internal Risks, Policies, and Controls
- Correlate events and exceptions; automate tests of control

Operational Solutions & Business Landscape

Technical Solutions & IT Landscape

Integration Platform

Technical Solutions

Operational Solutions & Business Landscape

Integration Platform
1. Why Cyber Security?
   - Reputational risk
   - Fines, penalties and “make it right” costs
   - Increased importance of Information Technology
   - Growth of e-commerce

2. Business Impact
   - Data Privacy
   - Infrastructure reliability
   - Data Quality and Integrity
   - Security
   - Accountability

3. Technology Trends
   - Mobile Workforce
   - Cloud Computing
   - Big Data
   - Internal & external user communities

4. Regulatory Pressures
   - New and expanding Federal Regulations
   - Overlap with industry specifics requirements

How can SAP Regulation Management help?
1. Stay current on new and changing regulatory mandates
2. Align compliance requirements with internal control activities
3. Automate evidentiary data collection and reporting
Demo: Reporting
What We’ll Cover

- Discuss the problem
- Describe the evolution of compliance solutions
- Define regulation management as a process
- Manage regulatory intake
- Ensure compliance through control monitoring
- Evidence and Report on compliance status
- Wrap-up
SAP Solutions for Governance, Risk and Compliance

- **SAP GRC Core**
  - SAP Risk Management
  - SAP Process Control
  - SAP Access Control

- **GRC Solution Extensions**
  - SAP Access Violation Management by Greenlight
  - SAP Regulation Management by Greenlight
  - SAP Dynamic Authorization Management by NextLabs

- **Native HANA Applications**
  - SAP Fraud Management
  - SAP Audit Management

Source: SAP
SAP Regulation Management by Greenlight

- Demonstrate end-to-end auditability of regulatory compliance
- Align compliance requirements with operational activities and automate testing of controls
- Establish accountability and unify requirements and controls across operations and compliance stakeholders
- Maintain a single authoritative source for regulatory alerts and mandates intake
- Identify and address compliance gaps in meeting new or changing regulatory requirements

Source: SAP
SAP Value Proposition

• Limited hardware cost
  • Can be installed on planned corporate SAP GRC infrastructure

• Content from multiple data sources
  • Thomson Reuters, internal/external legal, audit, SIs, etc.
  • Global, federal, state, and local publicly available data
  • Single source for all content, not just content provided by a single provider
SAP Value Proposition (cont.)

- Out-of-the-box integration with SAP GRC
  - Part of the SAP GRC portfolio with Process Control, Risk Management, etc.
  - SAP Regulation Management is the recommended architecture to integrate non-SAP solutions with SAP GRC
- Control automation is included
  - Eliminates manual work required by integrating regulations, requirements and controls with operational/business applications and IT systems
Where to Find More Information

- Greenlight Technologies Cyber Resource Center
  - [www.greenlightcorp.com/resources/](http://www.greenlightcorp.com/resources/)

  - [www.goo.gl/UKnp3G](http://www.goo.gl/UKnp3G)

- Governance, Risk, and Compliance (SAP GRC) on SCN
  - [http://scn.sap.com/community/grc](http://scn.sap.com/community/grc)
7 Key Points to Take Home

- Granularity in regulatory requirements makes a manual approach non-sustainable
- Collect and correlate content from multiple providers and/or publicly available sources
- Move towards a pro-active vs. re-active state of regulatory compliance and reporting
- Ensure enterprise-wide integration with point solution outputs
- Identification, detection, and mitigation automation through workflows drives the process
- Enforce requirement and control rationalization
- Force consistency in data and correlate and manage Big Data
Your Turn!

Questions?

How to contact me:
James Rice
jrice@greenlightcorp.com

Please remember to complete your session evaluation
Disclaimer

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.