GRC Program
Best Practices & Lessons Learned

Steps to Establishing and Maturing a GRC program

Carl Sawicki, American Express
Kathleen Randall, RSA Archer
Abstract

In today’s world, few organization’s contest the value of a GRC tool to increase the efficiency and effectiveness of their programs. But getting budget approval, organization buy-in and executing on a successful implementation can be daunting tasks to take on.

How do you measure the cost and ROI of an implementation, so that you can present the case to management?

How do you identify the maturity and design of your GRC program, and plan on an appropriate GRC implementation given your current state?

This presentation will guide you through these questions to help you determine if what it takes to have a successful GRC implementation at your organization.
Today’s Speakers

Carl Sawicki

American Express, Director of Technical Delivery

- Carl is responsible for delivering technical solutions that have a focus around the areas of Operational Risk and Information Security for American Express. With his 33 years of experience in various technical roles and 23 of those years at his current company, Carl works with a variety of business partners across the enterprise to deliver solutions and support their needs for GRC (Governance, Risk & Compliance).

- With the ever changing landscape of complex regulatory demands for the Financial & Banking Industry, Carl and his team have to be ready to understand, support and deliver to this demand with a variety of GRC platforms and custom solutions that he is responsible for.

Kathleen Randall

RSA Archer, Senior GRC Account Manager

- As a Senior Account Manager specializing in the RSA Archer eGRC product suite, Kathleen is responsible for managing Archer’s strategic customer accounts located in the southwest U.S. region. Kathleen has domain expertise in risk, audit, compliance and security domains, and has earned the CISSP, CISA, and GSNA designations. Prior to joining RSA, Kathleen was a part of the Deloitte & Touche’s Enterprise Risk Services group. She has led enterprise risk assessments, internal audit projects, and global risk and audit assessments for Fortune 500 organizations. She was also formerly the Regional Director of ControlPath, a GRC software solution acquired by Trustwave, responsible for channel and direct sales.

- Kathleen has served as a SANS course reviewer and course contributor, and has spoken several ISACA and IIA events.
Today’s Agenda

Implementation Opportunities
Where you are now?

Ideal State Definition
Where you want to go?

Next Steps
Recommendations to get you there
Maximizing Return

What to Consider

- Implementation
- Set Requirements and Design
- Key Stakeholders Engaged
- Define Process, Content & Infrastructure
- Program Strategy
What is GRC Tool Implementation ROI?

Implementation ROI =

- Project definition
- View of implementation plan (short-run VS long-run)
- Cross-domain strategy
  - Technology
- Bridging people, process and technology
  - Program Sponsorship

+ Implementation Costs
GRC Tool ROI Spectrum
Where do you see your organization?

**Basic**
- Use-cases identified

**Customer Profile**
- Focused use-cases
- Single domain
- Largely compliance focused

**Defined**
*All "Basic" elements plus...*
- Current state objectives and use-cases identified
- Processes identified
- Requirements documented
- Implementation plans developed
- Implementation team identified

**Customer Profile**
- Use-cases largely align to “out-of-the-box”
- Single domain
- Largely compliance focused

**Foundational**
*All "Defined" elements plus...*
- Forward-looking objectives set and coordinated
- Integrated, streamlined processes and content for a single domain
- Scalable infrastructure plan
- Key stakeholders trained

**Customer Profile**
- Mix of “out-of-the-box” as well as unique use-cases
- Single domain
- Compliance and risk focused

**Leading**
*All “Foundational” elements plus...*
- eGRC vision, scope, and strategy considered
- Enterprise-wide adoption
- Integrated, streamlined processes and content across domains
- Understanding of business risk
- Complete content taxonomy and visibility
- Fully enabled stakeholders

**Customer Profile**
- Many unique and/or industry specific use-cases
- Multiple domains
- Governance, risk and compliance focused
GRC Tool ROI Spectrum
Moving from Basic to Defined Implementation: Return Drivers

Implementation ROI = [Project definition, View of implementation plan (short-run VS long-run), Cross-domain strategy, Technology, Bridging people, process and technology, Program sponsorship] + Implementation Costs

Return Drivers
✓ Project definition
✓ View of implementation plan (short-run versus long-run)
✓ Ability to bridge people, process and technology
✓ Technology leverage
✓ Cross-domain strategy
✓ Program consideration
GRC Tool ROI Spectrum
Moving from Basic to Defined Implementation: Recommended Steps

Step 1: Align current state use cases
Step 2: Identify process and content
Step 3: Develop implementation project plans
Step 4: Identify implementation team
GRC Tool ROI Spectrum

Moving from Defined to Foundational Implementation

Return Drivers

- Project definition
- View of implementation plan (short-run VS long-run)
- Ability to bridge people, process and technology
- Technology leverage (full suite of modules)
- Cross-domain strategy
- Program consideration

Implementation ROI = [Project definition, View of implementation plan (short-run VS long-run), Cross-domain strategy, Technology, Bridging people, process and technology, Program sponsorship] + Implementation Costs
GRC Tool ROI Spectrum

Moving from Defined to Foundational Implementation

**Step 1:** Identify future state use-case and objectives across domains

**Step 2:** Document, benchmark and optimize process and content for a single domain

**Step 3:** Evaluate success metrics

**Step 4:** Introduce convergence of processes

**Step 5:** Engage & alignment of stakeholders to program vision
GRC Tool ROI Spectrum
Moving from Foundational to Leading Implementation

Implementation ROI = [Project definition, View of implementation plan (short-run VS long-run), Cross-domain strategy, Technology, Bridging people, process and technology, Program sponsorship] + Implementation Costs

Return Drivers
- Project definition
- View of implementation plan (short-run VS long-run)
- Ability to bridge people, process and technology
- Technology leverage (full suite of modules)
- Cross-domain strategy
- Program stakeholders
GRC Tool ROI Spectrum
Moving from Foundational to Leading Implementation

**Step 1:** Formalize eGRC program (Framework, Vision, Scope)

**Step 2:** Document, benchmark and optimize process and content for multiple domains

**Step 3:** Identify data gaps and consolidate siloes of information (common taxonomy)

**Step 4:** Fully enable and align stakeholders... continuously reviewing
GRC Tool GRC Maturity Spectrum

What’s next?

Risk Identification & Reaction
- Silo’d, fragmented information
- “Get it done” mentality
- No/minimal dedicated resources

Risk Awareness & Anticipation
- Efficiency and automation
- Basic governance and strategy
- Increased accountability
- Key risk appetites known

Risk Integration & Collaboration
- Continuous monitoring and improvement
- Enterprise objectives set and coordinated
- Complete content taxonomy and visibility
- Integrated, streamlined processes

GRC Optimization & Intelligence
- Risks identified
- Risk posture understood
- Aggregated, prioritized view managing key performance indicators
- Active governance
- Automated, integrated systems

© Copyright 2013 EMC Corporation. All rights reserved.
Questions? Comments?

Carl Sawicki
carl.a.sawicki@aexp.com
602.766.7338

Kathleen Randall
Kathleen.randall@rsa.com
310.318.4883