GRC
SUMMIT 2023
MIAMI, JUNE 14 & 15
Hosted by MetricStream

American Fidelity - Journey

Tice Morgan

Agenda

- Organization Overview
- GRC Needs
- GRC Program
- GRC Challenges and Opportunities
- GRC Approach
- Ecosystem and Deployment
- Key Learnings and Best Practices
- Business Value and Realized Benefits
- Audience Questions and Discussion

American Fidelity Overview

- In 1960, C.W. and C.B. Cameron founded American Fidelity Assurance Company based on a fundamental belief: The most important asset anyone has is their ability to work and earn a living.
- American Fidelity specializes in the education, public sector, automotive and healthcare industries with products like group and individual life, health and annuity services as well as other financial security products and services.
- Since 1960, American Fidelity has built our business on a commitment to our customers, and we have strived for excellence and innovation in the financial and insurance industry. This foundation has allowed us to repeatedly earn recognition and accolades from industry and rating organizations.
- Our proudest achievement is the rating of “A+” (Superior)[1] by AM Best, a recognition we have earned since 1982. This award represents our commitment to reliability and stability.

GRC Needs

- Address a variety of organizational compliance needs
- Easily communicate and manage compliance objectives
- Ensure proper ownership and visibility to control activity
- Introduce consistent reporting and self-service capabilities
- Near real time visibility into compliance
- Automation and workflow components for efficiency
- Central source for majority of IT controls and compliance

GRC Program

- Leverage two main modules for our GRC program today
  - IT Compliance and TPRM
- Business specific regulatory challenges and obligations
  - Model Audit Rule
  - SEC
  - FINRA
  - HIPAA
  - Bermuda Monetary Authority
  - States and Privacy
- Hybrid compliance framework that leverages HITRUST and NIST CSF

GRC Challenges and Opportunities

- Articulating the challenges currently faced
- Changing the organizations approach and culture are key
- Developing collaborative and inclusive feedback loops
- Demonstrating the efficiency and automation wins
- Establishing confidence in the program with transparency
- Identifying information sources and responsible parties
- Keeping it simple and starting things out small

GRC Approach

- Identify what we are doing today and where it applies
- Investigate any compliance gaps and regulatory deliverables
- Indicate who is doing what and who should be doing what
- Establish a committee or function and key stakeholders
- Develop a rhythm and cadence
- Outline a concise strategy but allow for flexibility
- Extrapolate a reasonable timeline and ensure resourcing
- Evaluate every so often to ensure agility and need

Ecosystem and Deployment

- MetricStream Product Areas:
  - Started with TPRM
    - Adapt our manual assessments into components that ease reporting
    - Enable limited automation and categorization to prioritize assessment activity and frequency
  - IT Compliance is a more long-term strategy for our organization
    - Move our control documentation to the platform
    - Ensure that we have our assets, processes, compliance areas and self assessment activity well defined
    - Implement a workflow approach through automation
- Deployment – What worked well, what didn’t
  - Roadmap for deployment was too aggressive and required some adjustments that continue to this day
  - Foundational activities for the platform itself: Libraries and data sources were challenging for us in the beginning
  - Balancing our current compliance programs and timing of those around the implementation elements
- Implementation Rollout Strategy and Tactics:
  - Organizational awareness and training
  - Increment small updates and enhancements as the program matures
  - Solicit feedback from the user community and provide resources and documentation

Key Learnings and Best Practices

- Key Learnings:
  - Keep your program simple and implement small enhancements
  - Explain, educate, collaborate and then automate
  - Showing we are attempting to manage and leveraging a tool gets us partly there
- Best Practices:
  - Understand the mechanics of the business process(es) being assessed
  - IT general controls should follow an 60-20-20 rule generally
  - Don’t shortcut a control if the process isn't clearing defined
  - Make sure you have the appropriate parties involved
  - Identify key source systems and reporting requirements
- The Road Ahead:
  - Better documentation, especially around processes
  - Incorporation of documentation and attributable workflows to keep GRC data current
  - Expanding control activities to other areas and compliance improvement

Business Value and Realized Benefits

- **American Fidelity – a different opinion**
- Afforded us an ability to tailor a question and procedure approach to assessments
- Process development considers control and evidence considerations
- Enhanced the ability to quickly respond to spot checks or out of band requests
- Facilitates continuous control monitoring for frequent compliance activity
- Identify issues quickly before the auditors come in
- Reduce overall control expectations and re-use

GRC
SUMMIT 2023
MIAMI, JUNE 14 & 15
Hosted by MetricStream

EXPERIENCE
the Power of Connection

Audience Questions and Discussion

Thank You!