IT Risk Management Life Cycle and enabling it with GRC Technology

Debbie Lew (debbie.lew@ey.com), Senior Manager, E&Y
Steven Jones (steven.jones@ey.com), Senior Manager, E&Y
Overview

1. What is risk management? Common understanding
2. IT risk management life cycle
3. Key components of an IT risk management program
4. Resources and enablers for IT risk management
5. What does technology enablement mean?
6. Industry perspective
7. Business drivers
8. Trends and challenges
9. Risk process implementation
10. GRC technology implementation considerations
11. Value considerations
What is risk management?

Is the identification, assessment, and prioritization of risks (as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

As per Wikipedia
What are your challenges with IT risk management in your organization?
Industry Perspective

- Risk management, regulatory, and compliance requirements are increasingly complex and intrusive (especially for financial services institutions) and have become a growing operational and financial burden. These requirements are not optional and must be addressed.

- Institutions have often approached the requirements in silos, leading to the creation of multiple risk governance processes, methods and infrastructure.

- Typical control functions are experiencing scope “creep” due to a combination of external and internal pressures. High expectations have blurred the lines of authority and responsibility among the control units.

- Cost reduction imperatives are limiting the ability of risk management functions to keep pace with business growth.

- Lines of business are experiencing “risk management process fatigue.” Significant amounts of time and money are spent complying with risk requirements, which can be further burdened by multiple requests and duplicative efforts.

- Boards of directors and senior management are demanding more comprehensive, consolidated, and actionable governance, risk and compliance information.
Risk management lifecycle

Establish Risk Context & Governance

Identify Value Drivers

Develop consistent risk taxonomy and risk repository and align relevant risks with value drivers (strategies, objectives, initiatives)

Monitor & Report

Frequently monitor effectiveness of risk response (e.g., controls) and report on results

Identify Risks

Define consistent assessment criteria based on risk appetite and tolerances and assess relevant risks

Assess Risk Response

Conclude on preliminary effectiveness of risk response and develop action plan for monitoring

Assess Risks

Define appropriate risk response strategy (i.e., acceptance, mitigation, avoidance, transfer, etc.)

Risk Management Components

Risk Culture
Policy & Mandate
Infrastructure & People
Methods & Practices
Information & Technology

Develop Risk Response

Follow us @ISACA_News
#NACACS
IT risk management program—What is it?

• IT risk governance and strategy, and the supporting organization, resources and components used to establish an effective, operational and sustainable IT risk management program

• **Components can include:**
  – Defined business drivers that align to Risk Strategy, Charter and Reporting on critical success factors
  – Define regulatory requirements and industry standards for adherence
  – Charter that reflects mandate for IT risk management program, risk principles and governance structure for operating the program
  – IT risk management strategic plan that defines program objectives, business drivers alignment, critical success factors and measurements, risk governance structure, risk management processes, roles and responsibilities, risk appetite and tolerance guidance, strategic and tactical initiatives, timelines and work effort for design and implementations, interdependencies with other functional operations – ERM/ORM, Security, BCM, Compliance, SOX, etc.
  – Defined risk management policies and standards
  – Defined and documented taxonomy
  – Defined IT Risk & Control Framework – Process/Risk/Control Model
  – Rating, scoring and weighting model or quantification model
  – Risk identification process – internal and external data mining for trends, analysis and classification
  – Risk profiling attributes and process
**Business case and value of an IT Risk (GRC) Management Framework**

- Effective, documented response to numerous regulatory/industry/audit/compliance requirements
- Lower cost
  - Repeatable processes and risk based technology decisions produce 8-12% cost savings
  - *Average from various sources including Gartner, Forrester, and the Risk Management Association*
- Reduce siloed and duplicative efforts
- Lines of business/functions experiencing “assessment fatigue”
- Consistent controls and consistent testing strategy focused just on higher risk areas deemed key for the organization
  - Better allocation of technology spend and resources
- Defensible, risk based decisions to properly allocate technology spend to highest risk areas
- Manage unknown risk
  - Quickly identify new risks and quantify cost of exposure through consistent processes (new systems, new technologies)
  - Enable go-to-market for new ventures, emerging technologies, and business products
- System stability/performance
  - Reduce system failures with risk based approach to system and architecture investments – e.g., identification and categorization of failure trends and issues with systems allowing risk ranked remediation across the enterprise
Resources & Enablers

Risk IT Framework and Practitioner’s Guide
COBIT5 Framework and supporting products
Risk IT is a framework based on a set of guiding principles and featuring business processes and management guidelines that confirm these principles.

Risk IT framework is to be used to help implement IT governance.

Organisations that have adopted (or are planning to adopt) CobiT as their IT Governance framework can use Risk IT to enhance risk management.
Risk IT Framework

Risk Governance
- Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

Integrate With ERM

Establish and Maintain a Common Risk View

Make Risk-aware Business Decisions

Risk Response
- Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

Articulate Risk

React to Events

Manage Risk

Business Objectives

Communication

Risk Evaluation
- Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Collect Data

Maintain Risk Profile

Analyze Risk
COBIT 5

- The COBIT 5 governance or management practices are equivalent to the Risk IT processes.
- The COBIT 5 activities are equivalent to the Risk IT management practices.
- COBIT 5 follows the same goal and metric concepts as Risk IT, but these are renamed enterprise goals, IT-related goals and process goals reflecting an enterprise level view.
- COBIT 5 provides RACI charts describing roles and responsibilities in a similar way to Risk IT.
- Future enabler includes COBIT 5 for Risk.
Principle 1. Meeting Stakeholder Needs

- Enterprises exist to **create value** for their stakeholders.
## Enabling Process APO12 – Manage Risk

<table>
<thead>
<tr>
<th>APO/2 Manage Risk</th>
<th>Area Management Domain: Align, Plan and Organise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Description</strong></td>
<td>Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.</td>
</tr>
<tr>
<td><strong>Process Purpose Statement</strong></td>
<td>Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.</td>
</tr>
<tr>
<td><strong>The process supports the achievement of a set of primary IT-related goals:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IT-related Goal</strong></td>
<td><strong>Related Metrics</strong></td>
</tr>
<tr>
<td>02 IT compliance and support for business compliance with external laws and regulations</td>
<td><strong>Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of IT-related non-compliance issues reported to the board or causing public concern or embarrassment</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of non-compliance issues relating to contractual agreements with IT service providers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Coverage of compliance assessments</strong></td>
</tr>
<tr>
<td>04 Managed IT-related business risk</td>
<td><strong>Percent of critical business processes, IT services and IT-enabled business processes covered by risk assessment</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of significant IT-related incidents that were not identified in risk assessment</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Percent of enterprise risk assessments including IT-related risk</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Frequency of update of risk profile</strong></td>
</tr>
<tr>
<td>06 Transparency of IT costs, benefits and risk</td>
<td><strong>Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Percent of IT services with clearly defined and approved operational costs and expected benefits</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information</strong></td>
</tr>
<tr>
<td>10 Security of information, processing infrastructure and applications</td>
<td><strong>Number of security incidents causing financial loss, business disruption or public embarrassment</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of IT services with related security requirements</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Time to grant, change and remove access privileges compared to agreed-on service levels</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Frequency of security assessment against latest standards and guidelines</strong></td>
</tr>
<tr>
<td>13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards</td>
<td><strong>Number of programmes/projects on time and within budget</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Percent of stakeholders satisfied with programme/project quality</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of programmes needing significant rework due to quality defects</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cost of application maintenance vs. overall IT cost</strong></td>
</tr>
</tbody>
</table>

## Process Goals and Metrics

<table>
<thead>
<tr>
<th>Process Goal</th>
<th>Related Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. IT-related risk is identified, analysed, managed and reported.</td>
<td><strong>Degree of viability and recognition in the current environment</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of key events with key characteristics captured in repositories</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Percent of audits, events and trends captured in repositories</strong></td>
</tr>
<tr>
<td>2. A current and complete risk profile exists.</td>
<td><strong>Percent of key business processes included in the risk profile</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Completeness of attributes and values in the risk profile</strong></td>
</tr>
<tr>
<td>3. All significant risk management actions are managed and under control.</td>
<td><strong>Percent of risk management proposals rejected due to lack of consideration of other related risk</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of significant incidents not identified and included in the risk management portfolio</strong></td>
</tr>
<tr>
<td>4. Risk management actions are implemented effectively.</td>
<td><strong>Percent of IT risk action plans executed as designed</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of measures not reducing residual risk</strong></td>
</tr>
</tbody>
</table>
When you hear the term, GRC, what does it mean to you and your organization?
What does GRC technology enablement mean?
Technology enablement

The development of business aligned requirements to drive the use of technology to design, enhance, implement and operationalize Governance, Risk and Compliance processes

• Organizations that use technology to enable their GRC processes have the potential to reduce the cost of risk management, enhance compliance and audit, streamline reporting, better manage risk, and deliver insight for better decision making. By enabling technology, companies can build an effective foundation that allows them to build efficiency, integrity and consistency into their processes:
  
  – Data mapping to identify critical relationships between corporate objectives, risks and controls;
  – Workflow to optimally coordinate activities across multiple layers of the organization;
  – Decision support necessary for planning and reporting;
  – Management of risks from identification, to assessment and treatment;
  – Model multiple risk hierarchies and integrate risk intelligence with other asset and risk information systems;
  – Understanding the holistic IT Process, Risk and Control environment in place within an organization; and
  – Reporting, monitoring and dashboarding of risk (inherent risk, residual risk and key risk indicators) across the IT environment.
Governance, Risk & Compliance tool space

OpenPages, Oracle, Paisley, ProcessUnity, Archer Technologies, MetricStream, B Wise, Axentis Enterprise, R-sam, Algorithmics, MODULO, bringa, Agiliance
Business drivers for technology enablement
Business drivers

• Increasingly complex and updated risk management, regulatory and compliance requirements, and Board and shareholder expectations
  – Pending Dodd Frank legislation
  – An increased pressure to comply with NIST
  – Regulatory updates across FFIEC and BITS
  – PCI DSS v2.0

• Duplication of risk governance processes, methods and infrastructure
  – Too many siloed assessments across functional areas of technology
  – Non aggregated reporting across multiple sources of risk intelligence
  – Inconsistent risk taxonomies

• Control functions experiencing scope “creep” and high expectations have blurred lines of authority/responsibility amongst control units
  – Duplication of controls across multiple IT units
  – Multiple shared controls that could be condensed
  – Driving towards control convergence and automated control monitoring through GRC technology

• Cost reduction imperatives are limiting the ability of risk management functions to keep pace with business growth
  – IT risk management requirements have increased while pressure is faced across available budget and head count
Business drivers (cont.)

• Lines of business are experiencing “risk management process fatigue” due to the amount of time and money spent complying with risk requirements
  – Repeat and overlapping assessments over functional areas of technology
  – Time commitment required to follow organizational risk management processes is placing a burden on the first line of defense
  – Non-prioritized approach to risk mitigation leading to potential improper allocation of funds

• Management is demanding more comprehensive, consolidated, and actionable governance, risk and compliance information
  – Reporting of risk management activity and outcomes across multiple hierarchies is a challenge for IT risk functions
  – Organizations are facing challenges when attempting to incorporate risk intelligence across the organization

• Mergers & Acquisitions
  – Multiple risk programs requiring consolidation and aggregation
  – IT risks inherited from legacy environments
Most companies have taken a very siloed approach to risk and compliance management which creates multiple redundancies and extensive inconsistency in how risks are assessed and managed.
Trends and challenges
Key issues and trends facing GRC tools

- Lack of a GRC strategy, vision and holistic business and functional requirements can lead to incorrect tool selections, over-budget implementations of GRC tools, or misuse of GRC technology.
- There is a continued evolution and broader use of technology for GRC across IT.
- There has been a recent entrance of software “heavyweights” into the GRC market.
- GRC tools are being leveraged for business process management and assessment rules engines along with continuous auditing, monitoring and control testing.
- GRC vendors are developing relationships with other application vendors (competitors and complementary products) to extend the range of the software. Others have been acquired to combine product offerings into larger, more comprehensive packages.
Key issues and trends facing GRC tools

- A lack of governance and accountability for GRC tools can limit the return on investment from a GRC solution. Ownership of GRC technology is crucial to driving consistency in methodology, reporting and presentation.
- Many organizations are designing a holistic GRC technology ecosystem to achieve holistic risk intelligence across the enterprise.
- There are multiple regulatory environments that can be covered by GRC tools, and not one GRC vendor provides content to cover all the environments.
- There is increased board liability as it pertains to IT risk.
- Organizations are looking at leveraging GRC technology to facilitate a central corporate policy management portal.
- There is outsourcing of compliance monitoring for the internal and external business environments.
- Consulting firms are either tool agnostic or they are not. Many firms have strategic relationships with GRC vendors that may skew their perspective.
Current state limitations

• **Definition of GRC**
  – The definition of GRC differs from client to client and vendor to vendor, leading to an inability to standardize GRC requirements and guide future development.

• **Isolation of financial risk management functionality** from mainstream GRC solutions

• **No single solution available**
  – All solutions perform well for certain aspects of GRC, but no one solution provides a complete holistic solution for all GRC requirements.

• **Immature dashboarding and metrics**
  – Not all tools provide web-enabled reporting and dashboards.
  – Non-financial RM tools do not provide advanced charting capabilities to address complex risk scenario analysis.

• **Virtually nonexistent global regulatory content**

• **Inconsistent framework mapping and content**

• **Assessment methodology**
  – Only a select few tools allow for logic-based assessments (questionnaires, surveys, etc.), which integrate business workflow and risk calculations driven by assessment results.
  – Risk control library management is not integrated into assessments to drive risk convergence.
Key issues & trends facing GRC tools...no silver bullet!

**Issues**
- No silver bullet
- Non-standard definition of GRC hampers ability to define future state and drive requirements
- Multiple regulatory environments
- Increased board liability
- Many of the systems currently in use were developed for a specific function or sector need. These vendors are challenged with finding alternative uses for their applications
- Immature dashboards and metrics
- Immature capabilities to gain real-time data feeds
- Inconsistent framework mapping
- Configuration flexibility
- Assessment methodology and maturity
- Initiative should be a directive from executive management with agreement from all key stakeholders

**Trends**
- Continued evolution and broader use of technology for GRC
- Entrance of software “heavyweights” into GRC market
- Architecting a holistic GRC technology ecosystem
- Integration of web services to enable risk and regulatory intelligence
- Implementation of a central corporate policy management portal
- Use of business process management and rules engines along with continuous auditing, monitoring and control testing
- Outsourcing of compliance monitoring for the internal and external business environments
- Acquisitions and alliances are forming to extend or enhance product offering

Market issues are driving product trends
What are your challenges (anticipated) in selecting, configuring and implementing GRC technology?
GRC tool implementation challenges

- Functional requirements along with organizational and process convergence should be defined prior to tool selection by performing a feasibility study.
- Organizations purchasing a solution, and then attempting to converge the risk organization and processes contains many challenges.
- Maturity of vendor solutions is not where it needs to be to meet all GRC functional requirements.
- A lack of understanding of how other business tools can integrate into GRC solutions and of future GRC state requirements still exist.
- Many organizations will need to customize their selected GRC tool or change their current methodologies, business processes, and hierarchies to have a successful GRC tool implementation.
- Content management decision – if aligning to leading practices, frameworks, and regulations, a decision needs to be made to determine if you will rely on a vendor to provide and manage content going forward or will it be customized and managed by the client.
- Timeframes for implementation is often underestimated – most organizations take between 12 - 24 months for successful implementation and for operational competencies to be realized.
- GRC tool cost is often underestimated due to improper calculating of customization or functional and process modifications that will be needed by the firm.
- Lack of experience and knowledgeable resources that are dedicated to GRC tool implementation.
- Vendor support and experience at business aligned deployments is limited.
Customization vs. configuration

- A key consideration when analyzing GRC solutions is the concept of customization vs. configuration. These are two very distinct terms, and have significant impact on a GRC solutions ability to meet or exceed business and functional requirements.
  - Configuration refers to the process of altering a GRC solution by making basic changes to the “out of the box” capability to meet business requirements. This process will not greatly enhance a GRC solutions’ functionality. Examples of configuration include:
    - Changing colors
    - Changing field properties (i.e., text, number, length, etc.)
    - Adding fields
    - Creating basic calculations
  - Customization refers to the process of altering and enhancing a GRC solution by making advanced changes to the “out of the box” capability to meet business requirements. This process can greatly enhance a GRC solution’s functionality. Examples of customization include:
    - Building custom business workflow
    - Using JavaScript or HTML to enhance the functionality of the GRC solution
    - Using advanced calculations and logic
    - Integrating data from multiple systems and sources
What’s the right balance for your organization?

GRC solution cost balance

Need to increase cost to achieve balance
## GRC tool functional coverage

<table>
<thead>
<tr>
<th>Governance</th>
<th>Financial risk</th>
<th>Risk management</th>
<th>Metrics, presentation and reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy management</td>
<td>Scenario analysis</td>
<td>Risk profiling</td>
<td>Dashboards</td>
</tr>
<tr>
<td>Standards</td>
<td>Risk modeling</td>
<td>Risk assessment</td>
<td>Ad-hoc reporting</td>
</tr>
<tr>
<td>Procedures</td>
<td>Financial risk impact analysis</td>
<td>Risk identification</td>
<td>Notifications</td>
</tr>
<tr>
<td>PRC framework</td>
<td></td>
<td>Risk analysis</td>
<td>User interface</td>
</tr>
<tr>
<td>Asset and hierarchy management</td>
<td></td>
<td>KRI</td>
<td>Statistical analysis</td>
</tr>
<tr>
<td>Process accountability</td>
<td></td>
<td>Threat and vulnerability management</td>
<td>Historical trending</td>
</tr>
<tr>
<td>Data management</td>
<td></td>
<td>Information security</td>
<td>Triggered calculations</td>
</tr>
<tr>
<td>Awareness training</td>
<td></td>
<td>BCP/DR</td>
<td>Audit tracking</td>
</tr>
<tr>
<td>Project management</td>
<td></td>
<td>Internal control management</td>
<td>Data export</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KRI/KPI management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service delivery management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Audit</td>
<td>Issues management</td>
<td>Incident management</td>
</tr>
<tr>
<td>Regulatory content Management</td>
<td>Program management</td>
<td>Risk treatment</td>
<td>Event capture</td>
</tr>
<tr>
<td>Leading practice content</td>
<td>Scheduling</td>
<td>Risk acceptance</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Attestation</td>
<td>Policy exceptions</td>
<td></td>
</tr>
<tr>
<td>Compliance monitoring</td>
<td>Evidence capture</td>
<td>Risk transference</td>
<td></td>
</tr>
<tr>
<td>Compliance assessment</td>
<td>SAS 70/SOC 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2012 ISACA. All Rights Reserved

Follow us @ISACAANews
#NACACS
IT-GRC tool vendor geographic footprint

Leader: RSA Archer, Thompson Reuters
Presence: All others

Leader: Bwise
Presence: RSA Archer, Thompson Reuters

Leader: RSA Archer
Presence: Thompson Reuters

Leader: Modulo
Presence: RSA Archer, Thompson Reuters, Bwise

Leader: None
Presence: BWise

Leader: None
Presence: RSA Archer, Thompson Reuters

Leader: None
Presence: RSA Archer, Thompson Reuters

Leader: None
Presence: RSA Archer, Thompson Reuters
Risk process implementation
Core GRC solution components

• Populations / inventories / authority information
  – Determination of CMDB (Configuration Management Database) and asset management tool integration for applications and supporting infrastructure, databases, operating systems and data centers
  – Identification of relevant industry regulations and best practices to align with

• Business hierarchy
  – Considerations around functional, line of business (LOB) or entity hierarchy embedded within the GRC tool
  – Determination of depth and breadth of hierarchy

• SSO integration
  – Integration with LDAP (Lightweight Directory Access Protocol) to simplify user authentication and user access administration

• Access control strategy
  – Groups, roles and privileges assigned to users
## Potential technology enablement coverage

<table>
<thead>
<tr>
<th></th>
<th>IT Risk</th>
<th>Op Risk</th>
<th>ERM</th>
<th>Internal Audit</th>
<th>Regulatory Risk</th>
<th>Legal &amp; Compliance</th>
<th>Info Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRC Framework</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Assessments</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Program Mgmt</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Issues Mgmt</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Case Mgmt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>KRI’s</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Content Mgmt</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UI / Metrics / Dashboards</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Other</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
GRC technology implementation considerations
Key GRC functional requirements

- Policy, Standards and Procedures Mgmt.
  - Content Management
- Risk Mgmt Processes (Assessments, KRI’s, Event Capture, Risk Profiling, etc...)
  - Vendor Management
  - Risk Assessment and Risk Analysis Capabilities
  - Risk Identification and Profiling
  - Issues, Mitigation, Risk Acceptance Lifecycle Management
  - Training and Awareness
  - Risk Identification Methodology
- Frameworks & Hierarchy Structure (Org, Process, Risk, Control)
  - Asset Management Capabilities
  - Hierarchy Structure – Organizational, Process, Risk, Control, Metrics and Reporting
  - Best Practice Content
  - Technology Controls/Information Security
- Regulatory Mapping
  - Regulatory Mappings
  - Regulatory Compliance Capabilities and Leading Practices - Standards
    - SOX, Basel II, GLBA & Data Protection Laws, PCI, FFIEC, BITS, COSO, ISO27002, CobiT, ITIL, etc.
  - Compliance Monitoring
- Business Process Management
- Business Workflow Management
- Audit Processes
  - Audit Processes and Workflow
  - Attestation Capabilities
  - Archival
- Control Automation & Monitoring
  - Automated Control Testing
  - Real Time Monitoring
  - Notification Services
- Metrics, Measurements, and Reporting
  - Quantity & quality of template reports
  - Ad-hoc Reporting
  - Risk Simulation Capability
  - Risk Weighting & Calculations
  - Statistical Analysis
  - Dashboards
- Financial Risk Management
  - Financial Risk Modeling
  - Financial Risk Impact Analysis
  - Quantification Engine
  - Event Loss/Capture - Incident Management
  - Financial Risk Content (i.e. ratings)
- Configuration Flexibility
  - Interoperability/Application Interface/Open Standards
  - Configuration Capabilities
  - Customization Capabilities
Key GRC functional requirements (cont.)

- Available Modules and descriptions
- Additional Functionality
  - Management Assurance
  - Ease of Use
  - Auditing and Logging
- Vendor Qualifications
  - Financials
  - Client Base
  - Market ratings and rankings
- Release Cycle
- Implementation Requirements
- Product Training
- Risk Based Services
- Maintenance & Support
- Enterprise Scalability
- End User Experience/Interface
- Teaming and Support from Vendor
- Industry Saturation/Customer loyalty
- System Administration
  - Backup & Recovery
  - System Performance
  - User Administration
  - Documentation & Guidance
  - Security Configuration
- Technical Architecture
  - Infrastructure Requirements
  - Application Requirements
  - Integration Capabilities
  - Data Ownership & Management
  - Performance and Scalability
  - Single Sign-On Integration
  - Data Integrity and Audit
  - Future Product Roadmap
  - Deployment & Migration
- Fees, Contracts and Software Arrangements

Note: The provided GRC Function Requirements are a sample only, a full requirements gathering and weighting exercise must be done to ensure proper tool selection.
Design considerations

- Convergence of risks, controls, processes, issues and themes
- Roadmap and strategic approach
- Solution ownership and governance
- Reporting requirements and data considerations
- Process and workflow requirements
- Source of record vs. data feeds
- Implementation management
- Functional and technical requirement validation
- Support personnel
## GRC technology enablement approach

<table>
<thead>
<tr>
<th>Suggested key milestones</th>
<th>Suggested program deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Evaluation and approval of a GRC solution</td>
<td>► Foundational components technical specifications</td>
</tr>
<tr>
<td>► Development of technical specifications from business and functional requirements</td>
<td>► Technical specifications for risk assessments, issues management, and reporting</td>
</tr>
<tr>
<td>► Detailed design of core foundational components</td>
<td>► Core framework solution implementation</td>
</tr>
<tr>
<td>► Organizational hierarchy</td>
<td>► Risk process solution implementation</td>
</tr>
<tr>
<td>► Process hierarchy</td>
<td>► Reporting and dashboarding implementation</td>
</tr>
<tr>
<td>► Risk Hierarchy</td>
<td>► UAT completion and a run book/design binder</td>
</tr>
<tr>
<td>► Control Hierarchy</td>
<td>► Training material and procedural guides</td>
</tr>
<tr>
<td>► Hierarchy relationships and interdependencies</td>
<td></td>
</tr>
<tr>
<td>► Design and implementation of risk assessment methodology and assessments</td>
<td></td>
</tr>
<tr>
<td>► Design and implementation of Issues Management</td>
<td></td>
</tr>
<tr>
<td>► Design and implementation of additional risk management processes</td>
<td></td>
</tr>
<tr>
<td>► Design and implement reporting and dashboarding requirements</td>
<td></td>
</tr>
</tbody>
</table>
Value considerations
Value proposition

- Measurable and documented enterprise commitment to transparency and compliance
- Decreased exposure to fraud, catastrophic losses and the full compliment of operational risks
- Prepared to anticipate and respond to new and changing regulatory matters
- Greater insight and more effective decision support
- Better equipped to lower cost and improve performance
- More effective management and use of enterprise information
Questions?

Thank you!