IT Risk Management Life Cycle and enabling it with GRC Technology

21 March 2013

Ernst & Young
Quality In Everything We Do

Overview

- IT Risk management lifecycle
- What does technology enablement mean?
- Industry perspective
- Business drivers
- Trends and challenges
- Risk process implementation
- GRC technology implementation methodology
- Integration with complementary solutions
- Budgetary considerations
- Case Studies

IT Risk Management Lifecycle

What does 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, compliance and audit, streamline reporting, better manage risk, and deliver insight for better decision making. Technology can provide the foundation for efficiency, consistency and repeatability by enabling:
  - 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.

Business drivers

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

Business drivers

- Increasingly complex and updated risk management, regulatory and compliance requirements
  - 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 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

Trends and challenges

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

Market issues are driving product trends

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

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 under estimated –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

Foundational GRC components

Foundational GRC components

- Populations / inventories / authority information
  - Determination of CMDB and asset management tool integration for applications and supporting infrastructure, databases, operating systems and data centers
- Business hierarchy
  - Considerations around functional, LOB or entity hierarchy embedded within the GRC tool
  - Determination of depth and breadth of hierarchy
- Authentication integration
  - Integration with LDAP to simplify user authentication and user access administration
- Access control strategy
  - Groups, roles and privileges assigned to users

GRC technology implementation considerations

GRC tool capabilities

- 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.
- 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)

GRC tool selection considerations

- 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

- Process convergence needs
- **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

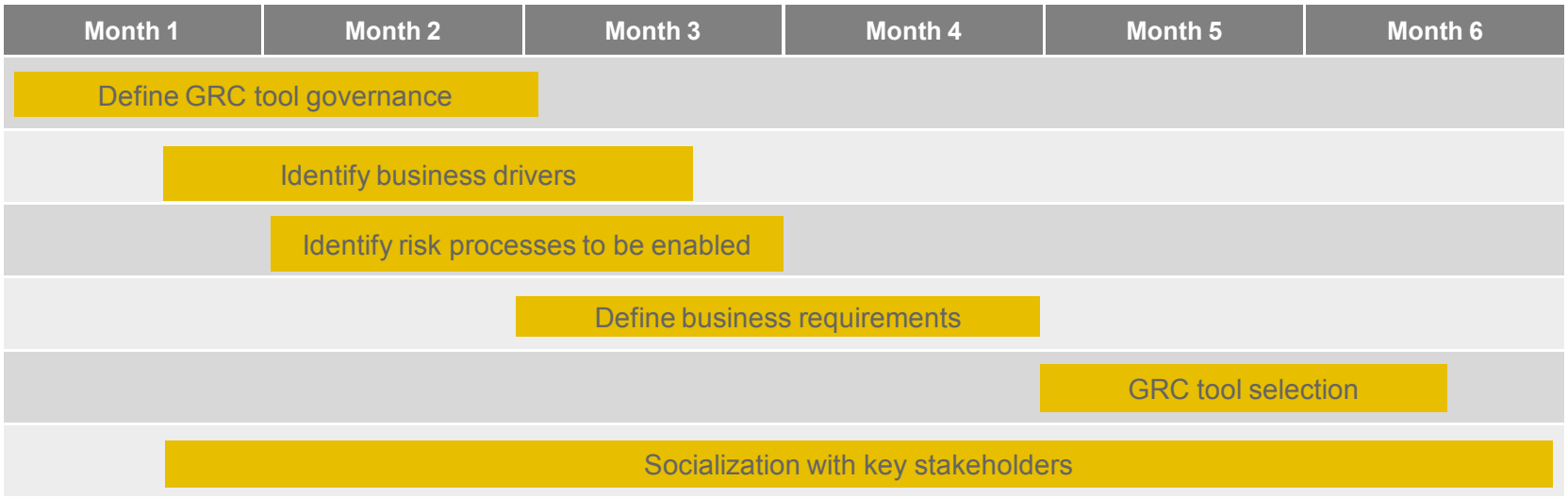
Suggested key milestones

- Evaluation and approval of a GRC solution
- Development of technical specifications from business and functional requirements
- Detailed design of core foundational components
  - Organizational hierarchy
  - Process hierarchy
  - Risk Hierarchy
  - Control Hierarchy
  - Hierarchy relationships and interdependencies
- Design and implementation of risk assessment methodology and assessments
- **Design and implementation of Issues Management**
- Design and implementation of additional risk management processes
- Design and implement reporting and dashboarding requirements

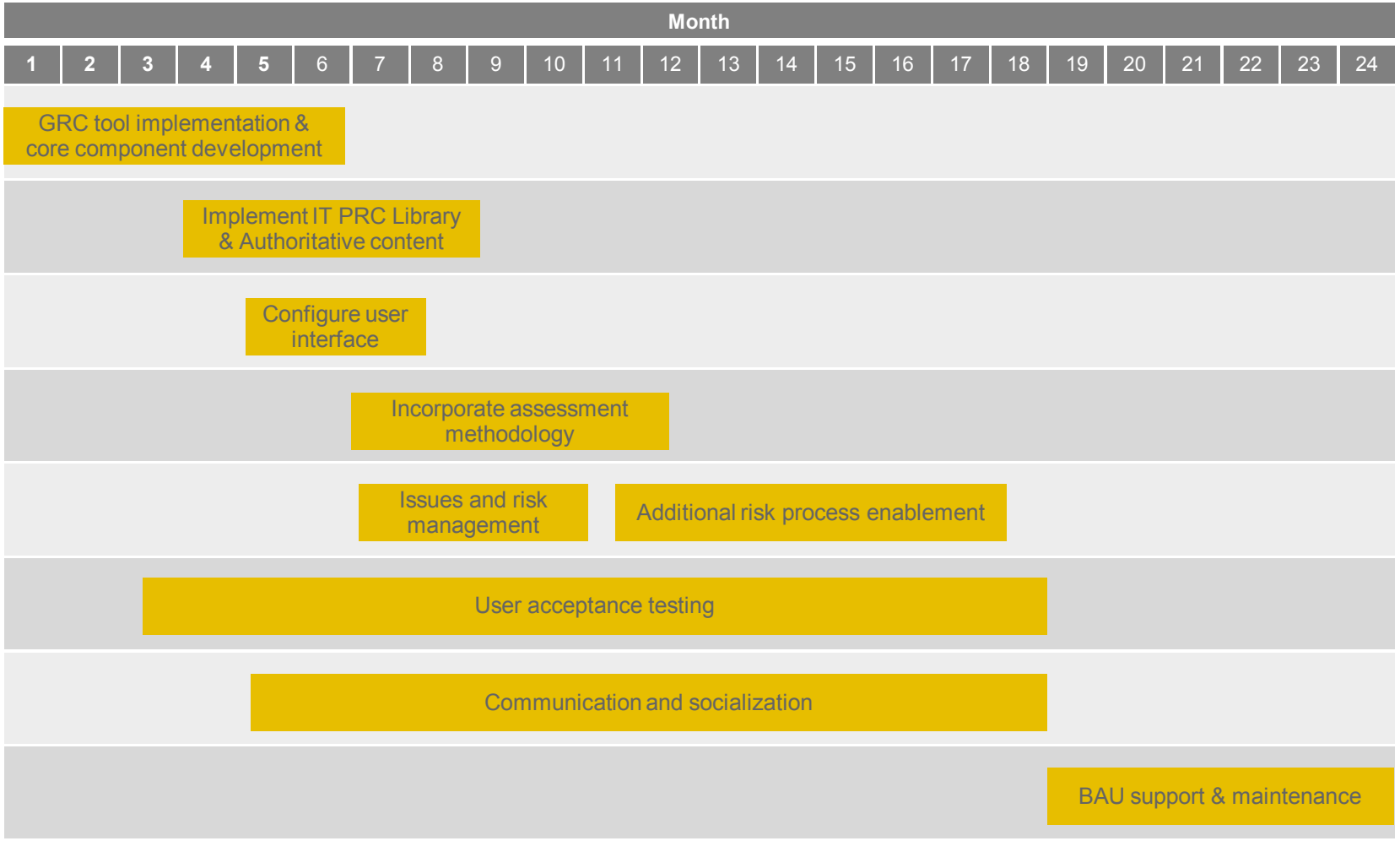
Suggested program deliverables

- Foundational components technical specifications
- Technical specifications for risk assessments, issues management, and reporting
- Core framework solution implementation
- Risk process solution implementation
- Reporting and dashboarding implementation
- UAT completion and a run book/design binder
- Training material and procedural guides

High level phase I timeline



High level phase II timeline



Budgetary considerations

Estimated budget

- GRC technology implementations can range from $250,000 to $1.5m in initial investment
- GRC technology support and maintenance can vary based on the complexity of the solution and the level of customization
- Sample cost breakdown:
  - 20% software licensing and hardware
  - 30% internal resources
  - 40% external support for tool design, configuration, testing and implementation
  - 10% ongoing costs