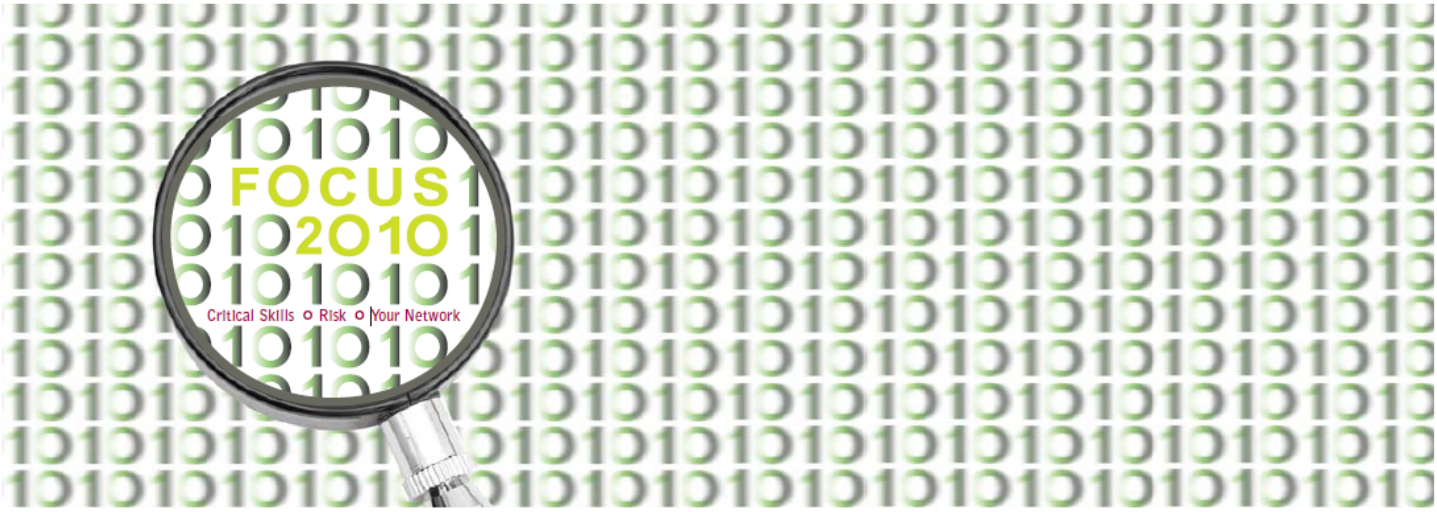
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010




# C32: GRC (Pro)(Con)Fusion – Tools, Processes, and Pitfalls

Jason Kobus, SVB Financial Group

ISACA®

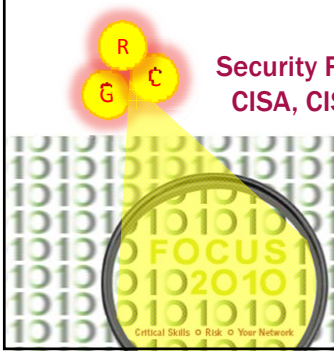
Trust in, and value from, information systems

San Francisco Chapter

# GRC (Pro)(Con)Fusion – Tools, Processes, and Pitfalls

ISACA
Trust in, and value from, information systems
San Francisco Chapter

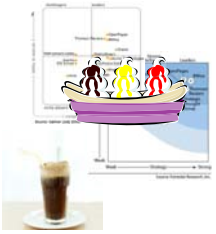
Jason Kobus,
Security Project / Privacy Program Manager
CISA, CISM, PMP, CIA, CISSP-ISSMP, CIPP




## Session Objectives

1. Provide guidance on how to navigate the GRC marketplace
2. Provide practical approaches to execute GRC as a project and operationalize into a sustainable program and product
3. Share tips on how to align GRC processes and technology
4. Learn to avoid pitfalls

## 1. Many Flavors of GRC Tools



- Enterprise/IT or "integrated" GRC suites
  - Check Gartner and Forrester
- Apps with GRC functionality added on
  - ERP, IAM,
  - Inventory and documentation apps
- Niche compliance products
  - Use limited to single function
- Patchworks
  - Sometimes more is not better
  - consider integration effort and product lifespan
- Homegrown: CMDBs+analytical tools



## GRC≠Tool: Process and People Factors

- Seek Out Vendor-neutral luminaries to understand the larger GRC problem space
- Remember that a tool does not equate to compliance
  - The tool will need people to use it and processes to bring it to life
- Empathize: Put yourself in their shoes to understand their pain points and objectives
- Ally with other GRC groups to
  - Define scope of the joint GRC effort
  - Establish communication protocols
  - Discuss cost sharing
  - Look for "champions"
- Begin with the end in mind …

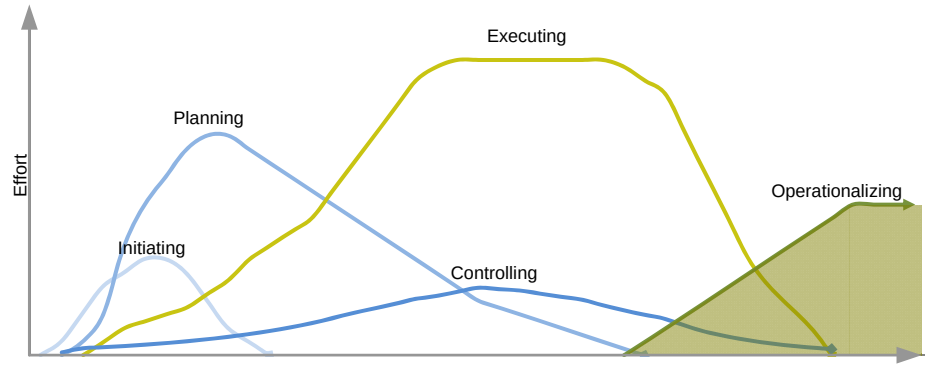
## GRC Tool Critical Success Factors

- Will people use it?
  - Adoption: more active users is better
  - Utilization: users can perform their work in the tool
- Efficiency gains via better information and resource management
  - Communication and analytical features result in less time searching for the right person and the data
  - Risk assessment and management data consolidated into a central repository, reduced audit planning and auditee burden
  - Compliance Coverage: What portion of company's compliance frameworks are included and can they be easily cross-referenced
  - GRC holy grail "test once, comply many"
- Refer to GRC Tool Balanced Scorecard



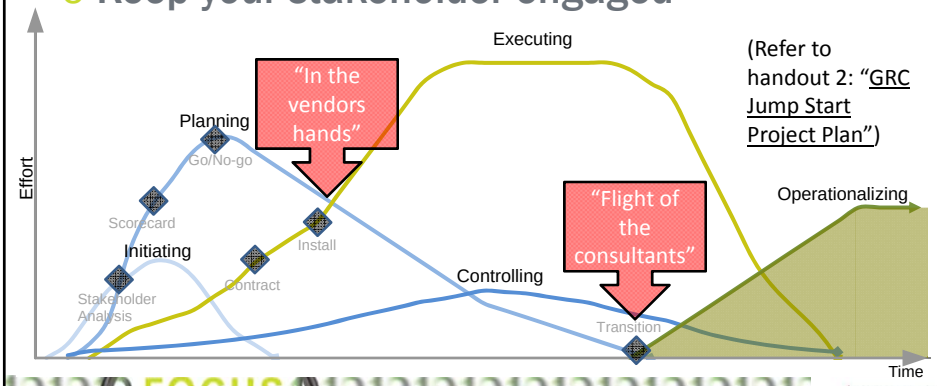
## 2. GRC Project-Program Life Cycle

- Starts as a project and evolves into a program (with our without a tool)



## GRC Project-Program Life Cycle

- Set specific milestones
- Keep your stakeholder engaged






## Initiate: GRC Stakeholder Roadshow

- Who's got skin the game? Internal Audit, Information Security, ERM, Compliance, Legal, IT (esp. governance/risk), Privacy, Incident Response, Business Continuity, Vendor Management, Quality, Finance, etc.
  - How much resource time can they commit to the GRC project (short term) and program (long term)
  - What criteria are most important for selecting a product
  - Who has budget? If not when could they obtain funding?

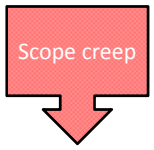
## Initiate: Cost-Benefit Considerations

- People
  - Soft costs of internal resources
  - Consulting fees
- Process
  - Reduce testing hours, consulting fees
- Technology
  - TCO over useful life: Upfront + Maintenance
  - Savings via de-commissioning of old tools and reduced licensing and support costs
  - Systems integration and customization fees
  - Consulting fees



## Plan: Scope

- What is in scope for assessment: what will be the subject of the risk assessment activity:
  - IT assets, systems and applications
  - Business processes (BIA)
  - Physical locations (data centers, branches)
  - Financial accounts (SOX)
  - Client accounts (fraud, customer retention)
  - Etc.



## Plan: Resources

- Develop or leverage RACI approach to clarify "who does what" and understand interactions between groups and common needs
- Critical: Estimate resources required for the project and for sustaining activities
- Critical: The project manager should be also be a subject matter in a GRC-related field. This provides a vital first person perspective and is essential to find common ground across teams.

Unsustainable Effort



## Control: Project Management

Project Support Disappears

- How to avoid some common Project Manager pitfalls:
  - Ensure that changes in scope approved by sponsor(s) only to avoid early bailouts and keep your charter current
  - Scheduling and resource contention: understand competing high priority projects which will can constrain critical resources and sap project momentum
  - Cost: Keep tabs on soft resource allocation as well as managers may become concerned and withdraw support
  - Quality: validate functionality with the most directly affected stakeholder(s)
  - Performance: get people using the tool via pilots and poll them for feedback
  - Risks: project team is loaded with risk specialists – leverage this to keep team engaged and to avoid major risks early

## Execute: Tool Acquisition

- Solicitation
  - Request information from your vendors using a structured questionnaire so you can populate your scorecard
- Source selection
  - Understand the relationship between the software provider, their professional services staff, consultants, and partner firms
  - Ensure you have solid and objective basis for your selection
- Contract administration
  - Leverage your vendor management experts and check that the proof-of-concept meets critical requirements



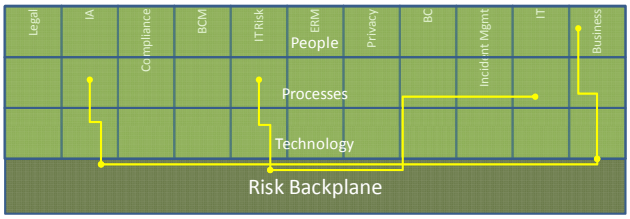
## Program Operationalization

- *"Operationalization is the process of defining a fuzzy concept so as to make the concept measurable in form of variables consisting of specific observations. In a wider sense it refers to the process of specifying the extension of a concept."*
- Translation: you need metrics (KPI/KRI) to sustain your GRC program

## Embrace A Risk Backplane

- Multicast risks quickly between GRC groups
- Standardize risk classification and nomenclature
- Higher bandwidth risk analysis and reporting
- Create a culture of clarity and accountability

Risk produced and reported by one group

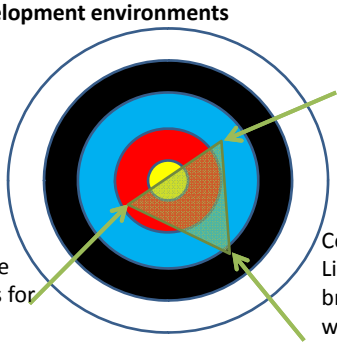





## Correlate to identify systemic risks

- Seemingly unrelated risks can be identified
- Threats can be identified prior to a loss event

**Control Objective: Limit data leakage in offshore development environments**



Internal Audit: Of 25 computers samples, 6 had USB ports enabled. Also, of 12 engagement team members added this year 2 did not complete all steps of the background screening prior to systems access.

A policy exception is granted to give offshore app support DBA rights for a large data migration effort.

Compliance Risk Assessment: Limited ability to respond to a data breach within required time period which has been a focus of regulator exams this year.

## Correlate to identify systemic risks

- More timely and complete information gives you a different viewpoint

**Control Objective: Limit data leakage in offshore development environments**

Data leakage via people who should never have been hired

Regulators have a rationale for concentrating on specific risks and have visibility into operational loss and criminal investigations

Bad actor: Rogue DBA



## Maximize GRC Program Value

- Apply Six Sigma continuous improvement practices (DMAIC) as GRC tools require tuning as with any automated control mechanism
- Market your GRC platform internally to attract new users and cost justify new functionality
- Use post mortems to see if the GRC program/tool had indicators of a risk prior to its occurrence and aim for predictive capability
- Don't forget the risks which are NOT in scope for your GRC tools analytics

## 4. GRC program pitfalls

- Avoid "Glue, Rot, and Corruption"
  - Glue: policies and controls which are too constraining which have a negative impact on the company
  - Rot: risks which are vague and in-actionable and likely to languish or have poor or only partial remediation
  - Corruption: When culture sours, people circumvent the controls and there is increased auditor antagonism



## Questions?