GRC Lessons Learned: Suggestions for Deployments

Roland Kelly, Archer Account Manager, RSA

Steve Kruse, Solutions Success Manager, RSA

Governance, Risk & Compliance – G11

AGENDA AND INTRODUCTIONS

Agenda

- Discuss common pitfalls
- Provide suggestions for avoiding the pitfalls
- Solicit attendees stories, good and bad
- Session attendees interaction on proposed solutions
- Wrap up

COMMON PITFALLS

Common Pitfalls – Top 10 List

Price, Effort, Value, Desired End State

1. Initial cost exceeds demonstrable value
2. Not recognizing work investment is still required after initial product investment
3. Vague goals and moving without a clear understanding of the end state

Micro vs. Macro Perspective

4. Focus on point solution and project instead of shared solution
5. Focus on Compliance instead of Risk or Governance
6. No political capital to effect substantive change
7. Turf wars between departments
8. Insistence on a single way – "I don't care how the product is designed, I want X"

Language and Technology

9. Terminology and taxonomy used differently
10. Hamstrung due to technical constraints

Initial costs exceeds demonstrable value

May be reworded to: Investment cost does not deliver the ROI based on the perceived value of the initial solution.

“GRC is significant investment, a lot of preliminary work makes showing my management progress challenging”

- Initial configuration requires work (pre-requisites), this preliminary work doesn't’t always provide the hoped for dramatic results

Technology Investment is not enough, significant work is still required

"I spent a lot on this stuff, where's the payoff?"

- Product alone is insufficient, work must be done to configure solutions and use cases
- The business case either did or does not include the labor investment required to operationalize programs
- Effective GRC drives valuable reporting- which requires ongoing support – this is often not properly budgeted

Vague Goals

“We want our GRC program up and running”

- Configurations are required. Your business units are different from other companies, as are your goals, servers, processes, workflows, etc.
- If GRC is treated as a strategic initiative, this lack of precise definitions and goals should not occur
- Dissect the use cases – are we talking compliance, risk, what?

Point Solutions Focus

"Product was purchased for SOX compliance. There is no need to modify product to accommodate Business Continuity requirements"

- Not properly positioned as a strategic solution - instead focused on a point solution
- Product is built to collect findings and infractions. These can be tracked and addressed or accepted.
- Findings and exceptions can be aggregated. Determinations and actions based on the number of outliers and offenders.
- Trend analysis can be performed based on various programs, this effort is crippled if used for a single or few purposes.
- If the product is designed solely for a single use case, then we may have to revisit to accommodate additional use cases
  - Otherwise the output can be redundant repositories of like business objects

Focus on Compliance instead of Risk or Governance

"Product handles my annual PCI audits"

- Products can do significantly more than compliance efforts
- If someone wants to buy GRC for compliance, they are unlikely to get their business case approved. They should be buying it to develop a risk intelligence platform, that will also provide their compliance posture, and drive compliance sustainment.

One GRC Consultant position is that compliance management should be a by-product of an effective risk management program. GRC helps deliver that.

No Political Capital to effect Change

“My vulnerability management program is working OK, the risk people aren’t interested ”

- Customer has some success with his domain, but not enough or not sufficient to warrant adoption by other programs in the GRC space

Another GRC Consultant position is that “He/she did not tie the value to something that was fundamental for the business. Initial view (GRC effort) was improperly scoped and deployed.

Turf Wars

“My program takes precedence over yours, my changes must be implemented prior to your team’s involvement.”

or “You can “share” some space (a VM) on that server.”

- Program roll out is done in an ad hoc fashion. No validity to prioritization.
- Shared resources initially appear to be cost effective, Difficulties arise when upgrades are required to either the back end databases or front end web servers in shared environments.
- Lack of organizational alignment drives turf wars between departments. A good GRC program helps foster that organizational alignment.
  - This is an example of a cultural problem that is being used to explain the lack of success of GRC

Insistence on a Single Way

"We must use the product while leveraging the web services bus our architects created"

- Products are malleable, but at what cost? Significant configurations can impact ongoing support and upgrade efforts
- GRC is process re-engineering. If treated that way, the Current Mode of Operation/Future Mode of Operation (CMO/FMO) workshop will call out use cases where GRC cannot fit, and others that can add automation that is very valuable for the firm.

Terminology used Differently

“What does a risk score of 4 mean? If everyone does not agree, then how can the risk data be trusted?”

- Taxonomy, frameworks, etc. cannot be left in silos if the goal is to achieve a vision of aggregated risk information that helps the executives make more confident business decisions.
  - Language and risk inconsistencies between business units

“You call it findings, I call it incidents. You call it incidents, I call it events”

- Products can be configured and relabeled. Compromises should be reviewed to understand WHY the vendor configured and labeled things the way they did.
- Vendor language and product needs to be well understood and either accepted or modified
  - In the case of RSA Archer, the Findings application is often misused by customers, who then re-work the information and application to align with the vendor.

Hamstrung due to technical constraints

“My security team wont let me expose a portion for Vendor and Contractor access.” or “My company only wants to adopt technologies supporting X platform (cloud, mobile)” or “We are a bunch of smart people, we’ll just build our own.”

- Focus is on platform, the “how” and not the “why”
- GRC is pervasive, these issues are being worked by all companies
- Your core competence may not include GRC product building, are there benefits to leveraging a vendor?

SUGGESTIONS TO AVOID THE PITFALLS

Common Remedies – Top 5 List

1. Board or Committee to govern Governance
2. Sr. Management "champion" willing to take the leap
3. Business cases justify investment – multiple cases are required
4. Keep it simple
5. Expectations are managed, initial wins are recognized and celebrated

Board or Committee to "Govern" Governance

- GRC is a strategic solution, not a product
  - Investment pitfalls can be avoided if GRC is treated as a strategic step to providing trusted, aggregated and transparent risk data to the Senior Executives - then the solution is not just a product, and proper service estimating and executing occurs.
- Board or Committee may be too high level:
  - Does not address the implementation issues
  - Subordinate board, committee and/or workshops may be appropriate as well
  - Subordinate group may meet more frequently, be more involved in the ongoing implementation work occurring.
- May be too low level
  - Does not have the authority to make enterprise-wide decisions
  - Cannot enforce terminology decisions, support a holistic approach across business units
  - Risk Management may be the "hammer" needed to ensure harmonization occurs.

Governance extends past the Board

- Focus on Governance and/or Risk – Compliance as a by product
- Risk needs to be an enterprise, strategic initiative that requires management workshops to get alignment, and drive success. A broad view of risk
- Workshops are expensive in terms of pulling management away from day-to-day tasks
  - But they foster and promote buy-in
  - They solicit and capture additional use cases, issues and nuances the board may not have considered
- Governance in this case taking the broad view of Governance
  - COBIT, ISACA view that Governance includes risk management, also value management
  - Reporting taking a larger role
    - Balanced Scorecard
    - Cascading scorecards

Sr. Management "Champion" willing to "Take the Leap"

- An executive sponsor may be required to stave off naysayers, demand patience, and ensure project and program stay on course.
- He/she must have sufficient authority, and recognize this is a large scale undertaking
  - Risks of potential delays and cost overruns are common, this should be anticipated and accounted for.
  - Cadence can be suggested for periodic meetings with champion, biweekly or monthly.
  - Can set expectations with his peers and Sr. Management to ensure potentials are not overhyped and realistic milestones can be provided and achieved

Business Cases justify Investments

Non recurring costs

- Market research / purchasing
- Solution assessment
- Solution configuration

Tangible benefits

- Cost avoidance
- Reduced taxes (credits and depreciation)

Recurring costs

- Maintenance
- Updated configuration work
- Technology refresh

Intangible benefits

- Vendor maintains the product
- Package mature (better quality, more robust)
- Leverage the marketplace
- Market drives the features

Business Cases justify Investments 2

Categories of Breach Impact Exposures	Cost Estimate
Lost business	$$
Productivity loss	$-$$
Loss of data	$-$$$
Restoration costs	$$
Litigation costs	$$
Detection and containment costs	$
Service disruption	$
Legal and regulatory compliance	$-$$
Reputation	$-$$$
Total	

Categories can be generated based on historical evidence, company artifacts, or other sources. Estimates can be reviewed to ensure they pass the tests and are not double counting impacts from various categories.

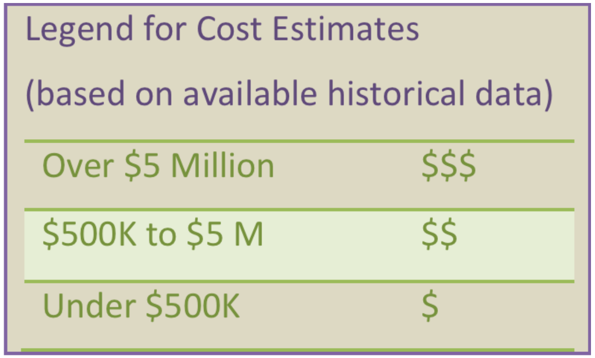
Impacts can be based on high, medium, low or other estimates

Legend for Cost Estimates (based on available historical data)	
Over $5 Million	$$$
$500K to $5 M	$$
Under $500K	$

Business Cases justify Investments 3

- Multiple business cases can identify GRC use cases and map expected value from each
  - Compliance – estimated value of “Medium” (between $500K and $5M)
  - Risk – Operational Risk - estimated value of “Medium” (between $500K and $5M)
  - IT and Security Risk - estimated value of “High” (above $5M)
  - Business Resiliency (BC/DR) - estimated value of “Medium” (between $500K and $5M)
  - Third Party (Vendor) Management - estimated value of “Low” (under $500K)
  - Audit - estimated value of “Low” (under $500K)

  - Potential enterprise specific business/use cases



Legend for Cost Estimates

(based on available historical data)

Over $5 Million	$$$
$500K to $5 M	$$
Under $500K	$

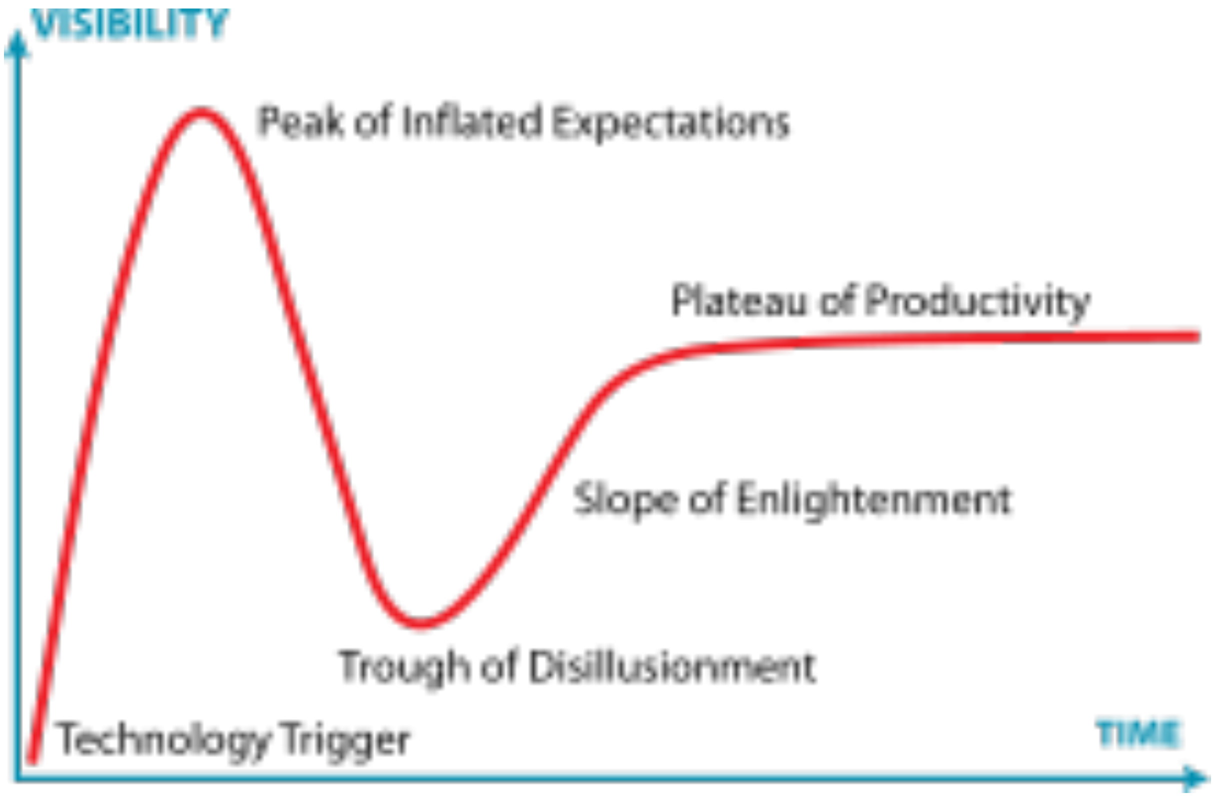
Keep it Simple

- Top down (strategic) reviews can identify initial candidate programs and projects that deliver early and tangible value to the enterprise
- Small projects with straightforward use cases can be implemented fairly quickly and demonstrate progress
- Overly complex workflow to accommodate rare use cases can be implementation expensive

- Start small, start simple – look for those paper intensive projects which consume significant audit, compliance, consultant costs for early wins

Expectations are Managed

- Many GRC technologies are in the early stages of a hype cycle



Graphic courtesy Jeremy Kemp, wikipedia

Initial Wins are Recognized and Celebrated

- Champions, project leaders can drive these promotions
- Improve morale for workers
- Keeps future stakeholders intrigued
- Cannot be artificial, some progress and demonstration of value is required

AUDIENCE STORIES – GOOD? BAD?

AUDIENCE INTERACTIONS ON PROPOSED SOLUTIONS

WRAP UP AND THANK YOU