It's Time to Break Out of the GRC Mold

May 15, 2018

2018 Secure360 Twin Cities
@drinfosec presents

Agenda

• A brief history of (GRC/ERM) time...
• Limitations of current GRC approaches
• How is GRC evolving
• Strategy
  • Why tying it all back to the business is a winning activity
  • The value of what you do (to create/preserve value)
• How do we communicate about security projects and thinking beyond GRC... but how?
Guiding Questions

1. What's the purpose of your GRC/ERM tool?

2. How well is your GRC/ERM tool working for your organization?
91% of directors say they’ll need to modify their company’s strategy in the next 3 years because of the threat of the speed of technological change. Change has come fast and furiously in recent years and will continue.
Short Bio

• Has written lots (80+ articles for IBM-SI, 3xWP, 2xBooks) since 2015.
• Has worked with and for CIOs. Has shadowed CISOs. Has performed many cybersecurity gap analyses.
• Has written lots (80+ articles for IBM-SI, 3xWP, 2xBooks) since 2015.
• Good communication is key to good management of cyber risks.

BIO

Beyond academia, also consulting with CISOs looking to improve their risk communications

Security vendors looking to improve their tools

Boards & executives looking to make sense of it all.
Deep dive into GRC fog

Just give me 10 minutes!
GRC is an invention?

GRC is primarily a software vendor driven invention that has had little practical success or value. ERM, if done right, can be a major source of success for any organization...

Src: IIARF Report: Contrasting GRC and ERM 2013

@secure360
@drinfosec presents

GRC is an invention?
The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

IIA on Governance –

IIA Research Foundation Report on GRC vs ERM:

GRC vs ERM
GRC is the manner in which a board of directors (trustees) ensures an organization attempts to meet its objectives by identifying and managing risks and obtaining assurance that controls (including compliance) are in place and efficiently and effectively mitigating risk.

Src: IIAF Report: Contrasting GRC and ERM 2013

@secure360
@drinfosec presents
ERM is an integrated systematic process of identifying major risks to achieving the specific goals and objectives of the organization. These risks should be analyzed by likelihood and impact and mitigated to an acceptable level of residual risk.

Src: IIA Report: Contrasting GRC and ERM 2013

ERM is an integrated systematic process of identifying major risk to achieving the specific goals and objectives of the organization.
GRC vs ERM

- IIA on GRC
  - GRC is the manner in which a board of directors (trustees) ensures an organization attempts to meet its objectives by identifying and managing risks and obtaining assurance that controls (including compliance) are in place and effectively mitigating risk.

- IIA on ERM
  - ERM is an integrated systematic process of identifying major risks to achieving specific goals and objectives of the organization. These risks should be analyzed by likelihood and impact and mitigated to an acceptable level of residual risk.

IIA on ERM – GRC vs ERM

- GRC vs ERM
  - GRC is the manner in which a board of directors (trustees) ensures an organization attempts to meet its objectives by identifying and managing risks and obtaining assurance that controls (including compliance) are in place and effectively mitigating risk.
Does one include the other?

GRC vs ERM
GRC vs ERM

- Michael Rasmussen, VP of Ent. Risk & Compliance at Forrester Research:
  - GRC is really a philosophy, and a framework for communicating around governance and compliance issues.
  - In effect, GRC encompasses ERM.
  - ERM, on the other hand, is the measurement and quantification of risk, and the establishment of individual risk ownership.

Forrester Research:

Michael Rasmussen, VP of Ent. Risk & Compliance at GRC vs ERM
Russ Banham, contributor to Treasury & Risk Magazine

ERM = methodology for managing the entire spectrum of risk

GRC = technology platform for illuminating governance and compliance risk

James Lam, ERM Consultant:

GRC = methodology platform for illuminating governance and compliance risk

ERM = methodology for managing the entire spectrum of risk

It's useful to think about GRC in terms of an IT platform...
Christina Kite (Cisco VP of Finance & ERM):

We see GRC really as a tool, a technology module, and not ERM per se...

ERM is not about being compliance-driven or regulatory-driven.

...but risk-takers in the business model area.

We’re very conservative in governance and compliance,

GRC vs ERM
We see GRC really as a tool, a technology module, and not ERM per se. ERM is not about being compliance-driven or regulatory-driven, but risk-takers in the business model area. We’re very conservative in governance and compliance, and not. Christina Kite (Cisco VP of Finance & ERM):
<table>
<thead>
<tr>
<th>Activity</th>
<th>GRC</th>
<th>ERM</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>8%</td>
<td>27%</td>
<td>65%</td>
</tr>
<tr>
<td>Internal controls</td>
<td>64%</td>
<td>10%</td>
<td>45%</td>
</tr>
<tr>
<td>Organization-wide assurance</td>
<td>59%</td>
<td>11%</td>
<td>70%</td>
</tr>
<tr>
<td>Independent internal audit function</td>
<td>9%</td>
<td>34%</td>
<td>52%</td>
</tr>
<tr>
<td>Alignment of company actions with shareholder value</td>
<td>15%</td>
<td>28%</td>
<td>43%</td>
</tr>
</tbody>
</table>

Table created by Chris Vellos based on the data in the IIARF report, sorted by “Both” column.
Software Tools for GRC/ERM?

Src: IIARF Report: Contrasting GRC and ERM 2013

Exhibit 14.4. Does your organization use software to manage processes and activities related to GRC or ERM? (Question 7)
Okay, we get it...
Considering the pace of change, companies and boards need to be agile in addressing threats to executing their current strategy, as well as disruptions to their entire business model.

PwC on Spotting Strategic Threats

SRC: PwC’s 2017 Annual Corporate Directors Survey Report
Only 22% of board directors rated the information they get about “emerging/disruptive technologies that could impact the company” as EXCELLENT.

32% of directors said their organization has adequately tested cyber IR plans.

37% of directors said they get adequate reporting on cybersecurity metrics.

PwC on Spotting Strategic Threats

Src: PwC’s 2017 Annual Corporate Directors Survey Report
1. Understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Understand the legal implications of cyber risk and ensure that discussions about cyber risk management should be given regular and adequate time on board agendas.

3. ... discussions about cyber risk management should be.

4. Management will establish an ERM with staffing and budget.

5. Board-management discussions about cyber risk should identify risks to avoid, accept, mitigate, transfer.

Source: @secure360 @drinfosec presents 23
Src: Cybersecurity Risk Management Oversight | Harvard Law Forum
What’s the point of GRC?

- Risks
- Setting & monitoring org-wide risk tolerances
- Governance
- Oversight that risks are managed within established levels
- Effectiveness of controls - Are controls having the intended effect?
- Evaluate controls “to ensure proper risk management”
- Controls/compliance
- Setting & monitoring org-wide risk tolerances
Who should care about GRC/ERM?

- Board directors
- General counsels
- CEOs
  - Rest of C-Suite
- CISOs
- Internal Audit
- CROs
Has GRC/ERM worked so far?
Gartner has replaced GRC w/ IRM

Integrated Risk Management consists of

• IT Risk Management (ITRM)
• Vendor Risk Management (VRM)
• Business Continuity Management (BCM)
• Audit Management (AM)
• Corporate Compliance & Oversight (CCO)
• Enterprise Legal Management (ELM)

@secure360
@drinfosec presents

27
Characteristics of Gartner’s IRM

• Strategy
• Assessment of risks
• Risk Response
• Communication and reporting of risks
• Monitoring of risks
• Using technology
Limitations of current GRC/ERM

Does it bring... the right value?

- Right approach?
- Right frequency?
- Right granularity (across lines of business)?
- Right scope/visibility (organization-wide)?
- Right support/tone from the top?
- Does it have...

Is it used in the right manner?
How is the world of GRC/ERM changing?

- Improved frameworks — clarity, integration, mappings

  - Embedded consideration of risk in all decisions
  - Continuous monitoring — boards are increasingly asking for more frequent reporting, and shorter, real-time snapshots
  - Continuous auditing (CA) — internal audit functions are increasingly talking about CA. CA happening at 16% of orgs > $5B. Tools help.

- Improved frequency — towards continuous consideration/exporting

- Improved tools — usability, dashboards,
Communications are key.
Management (across the org), and good
integration (from top) over right (at
appropriate levels).

Both emphasize that tone (from top), and
appropriate levels.

The COSO ERM framework -
ERM Framework

1. Managing risk is part of governance and leadership, and is
2. Both “governance” 9 times
3. Mentions “governance” 9 times
4. Mentions “governance” 9 times
5. Mentions “governance” 9 times
6. Mentions “governance” 9 times
7. Mentions “governance” 9 times
8. Mentions “governance” 9 times
9. Mentions “governance” 9 times
How well does your GRC/ERM approach work for your organization?

1. Is risk management integrated within the governance of the organization?

2. Does your GRC/ERM enable quality risk decisions?
A good tool would...

- Support continuous auditing & monitoring & (review of)
- Have multi-level views
- Show current snapshot, target state, trend-lines
- Can automatically pull the latest figures
- Risk decisions
- Facilitate tracking and communication of risks and
- Support multiple templates/frameworks (map to each)

...
Does security bring value?

How do you make the case for the value that the security function brings to your organization?

Does security bring value?
Framing your message & value

• Tying it all back to the business is a winning strategy

• Risks don’t exist in a vacuum.
• Risks matter because of their potential impact on the organization’s ability to create value or preserve value.

• Make it personal! Well, at least granular
• Report risks for each Line of Business (LoB)
• Make each LoB accountable for their cyber risks
In their own words

Cybersecurity & Privacy at PwC

— Aaron Weller, Managing Director

Everything that gets presented to the board has to have a clear link back to business strategy. And business value and business strategy. Everything that gets presented to the board has to have a clear link back to business strategy. And business value and business strategy.
Do you provide what they need?

Understand what decisions your target audience makes every day.

What do you have for them that will influence their decisions?

Src: Gartner - To the Point: Reporting Cybersecurity and IT Risk to the Business
It’s time to take a trip to Framework-land

A worthwhile journey
Here’s my recommended itinerary:

1 day – add NIST CSF (20 pages)

2 days – add ISO 31000:2018 Executive Summary (16 pages)

3 days – add Center for Audit Quality’s “Tool” (16 pages)

4 days – add COSO ERM - Executive Summary (16 pages)

5 days – add WEF Cyber Resilience for Boards (28 pages)

6 days – add NACD Cyber Risk Handbook (20 pages)

Framework—A Trip Planner
GRC without ERM is like...

Lunch without dessert...
Resources
Resources

• Co-authored a book with Paul Ferrillo, a data-breach lawyer from NYC.

• Available in PDF for free

• Available on Amazon in Kindle & paperback formats

• Cybersecurity for executives
Books on boards & governance (or management and leadership)

- Presenting To The Board ($)
- The CISO’s Handbook
- Rhetoric, Logic, & Argumentation
- The Trusted Advisor
- World Class Risk Management (N. Marks)
- HBR’s 10 Must Reads on Communication

And all the links found throughout the presentation.
Let’s talk. Over coffee?

- Email: chris@drinfosec.com
- Twitter: @DrInfosec
- LinkedIn