Performance GRC: A Well Positioned GRC Program Protects and Enables Business Performance

Steve Zawoyski
National Performance GRC - Risk Management Leader
PwC

Christopher Chung
San Francisco Performance GRC Solution Leader
PwC

Governance, Risk & Compliance – G12

Your Speakers Today

Steve Zawoyski, PwC
National Performance GRC Leader – Risk Management

Direct: (612) 596-4931
Mobile: (847) 323-4946
stephen.v.zawoyski@us.pwc.com

Chris Chung, PwC
SF Performance GRC Solution Leader

Direct: (415) 498-7449
Mobile: (408) 505-0646
christopher.s.chung@us.pwc.com

What we'll accomplish today

- Gain insight and perspectives into a better integrated, performance-oriented GRC program
- Discuss how to tie business trends to their related strategic consequences
- Learn how to grow your perspective on the business to create more relevance
- Gain ideas on moving from value protection to value creation
- Compare traditional vs. performance based models of GRC
- Take away GRC optimization and integration strategies

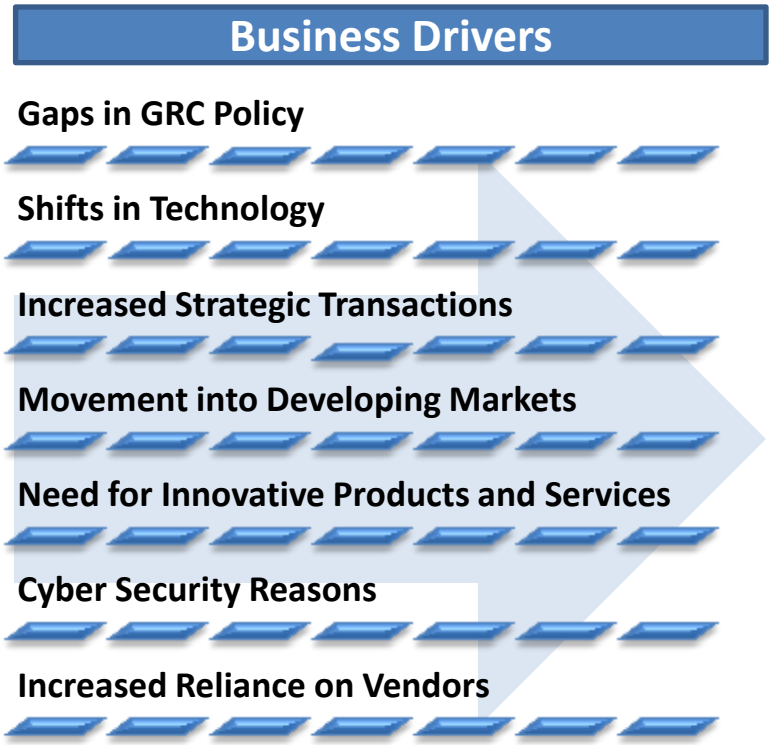
A well positioned Performance GRC program protects and enables business performance

In today's complex business environment, ***companies typically build Governance, Risk and Compliance (GRC) functions on an ad hoc basis – addressing specific risks and compliance responsibilities as they arise.***

This approach reduces the potential for cross-functional alliances and business strategy coordination, while increasing costs. But by ***linking integrated GRC activities to key business performance drivers and strategic priorities, companies can operate in a more efficient and focused manner,*** *leading to more informed decision making, lower costs and improved ROI.*

Trends in today's GRC Landscape

The inability to keep pace with multidirectional changes has put many organizations on a defensive footing



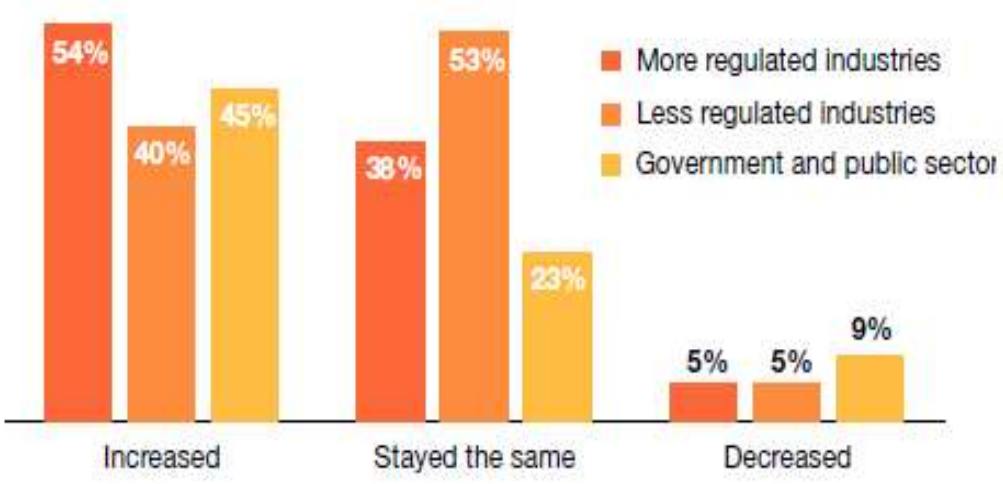
Potential Strategic Consequences

- Depressed market value and share price
- Inability to meet customer demands related to quality and innovation
- Regulatory/Legal actions leading to damaged reputation
- Operational Issues impairing business objectives
- Loss of confidence by internal and external stakeholders

The growth of GRC within organizations

Over the past 12 months, 45% of all surveyed companies have increased their compliance budgets

Growth in Compliance Staffing Across Industries



Compliance budgets have increased for “less regulated” industries such as retail and consumer or automotive.

This could reflect the fact that, across industries, business is becoming more global and more complex, driving increased regulatory requirements for many companies.

Source: PwC State of Compliance Survey 2014

The growth of GRC within organizations

Indicators and Metrics Used when Evaluating the Effectiveness of the Organizations Compliance Program

71% of all Surveyed Companies Regularly Assess the Effectiveness of their Compliance System

Many organizations are measuring compliance **activity** rather than the impact of their compliance programs on the business

Source: PwC State of Compliance Survey 2014

	2014 (Base:751)	2013 (Base: 781)
Compliance audit results	66%	71%
Risk assessment results	61%	65%
Training completion rates	53%	**
Hotline/helpline metrics	50%	56%
Results from a regulatory visit	48%	46%
Customer & other third party feedback/complaints (not reported through hotline/helpline)	39%	41%
Employee questionnaires or culture surveys	35%	52%
Employee disclosures (e.g. conflicts of interest and gift reporting)	35%	56%
External benchmarking**	33%	**
Internal benchmarking**	28%	**
Training competency tests**	24%	**
Cost of non-compliance (penalties, litigation and other consequences of non-compliance incidents)	22%	44%
Exit interview responses**	20%	**
Cost of compliance program activities	19%	17%
Training trend analysis**	17%	**
Monitoring of press and public statements	16%	24%
Aging and disposition of litigation and enforcement	14%	20%
Training data (completion rates, competency tests etc)	**	65%

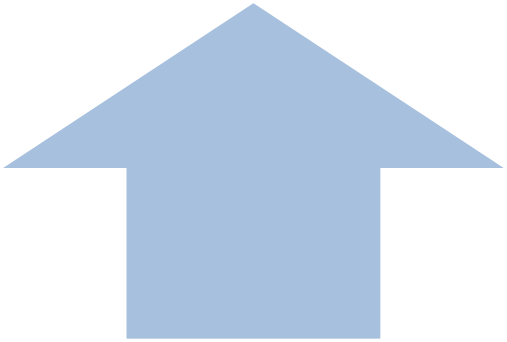
The growth of GRC within organizations

Driven by the need to comply with business and regulatory requirements and protect the organization and stakeholders from loss, many organizations have built their GRC activities on a practically ad hoc basis, each focused solely on protecting the business from a specific risk or addressing a specific risk/regulatory responsibility.

Is GRC a necessary evil or a positive, proactive force that pushes companies forward?

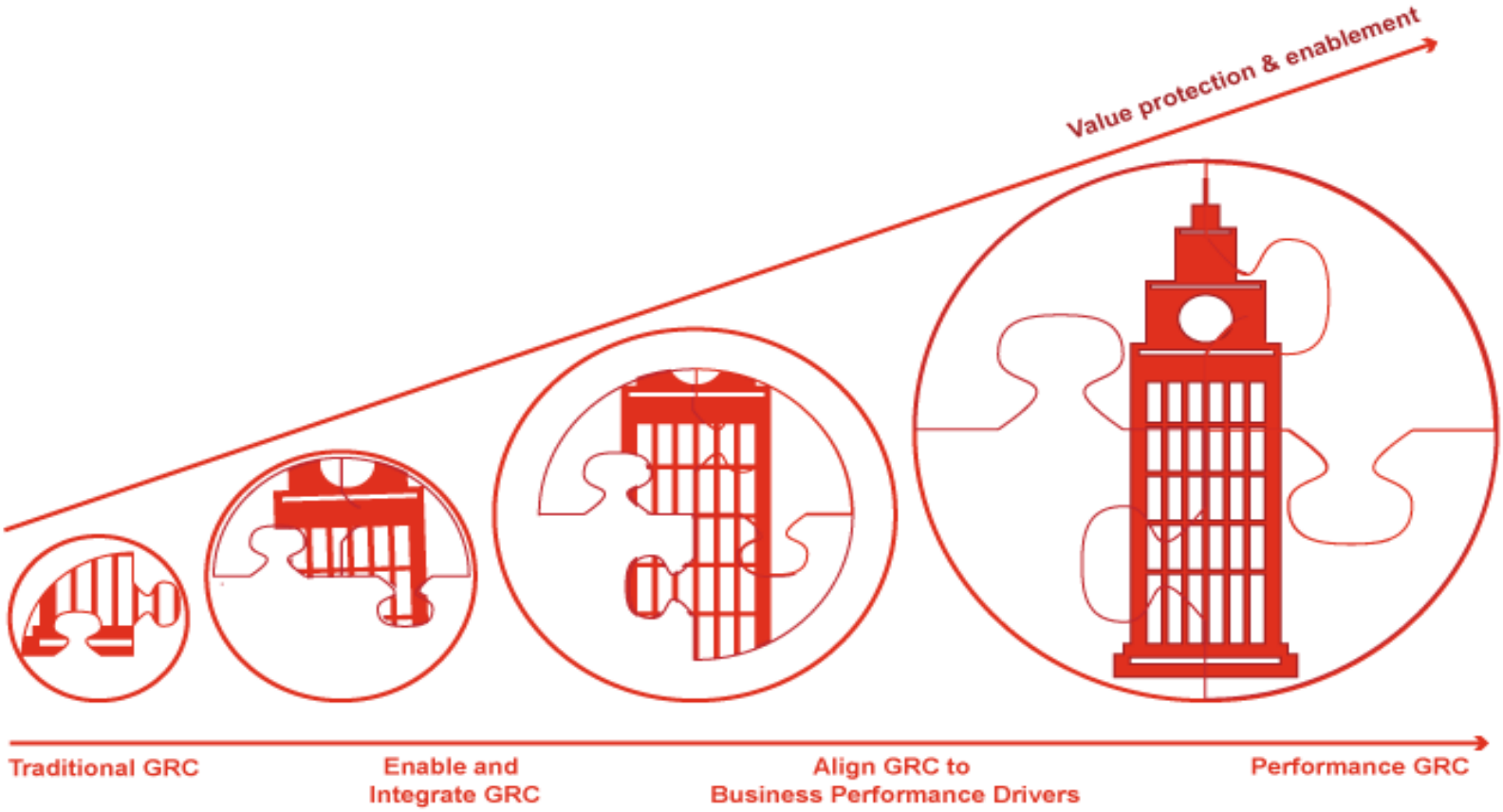
Many business leaders continue to view GRC as a necessary evil, a set of expensive corks that act as stoppers against value loss and keep the company in compliance, but do little to create value and move the enterprise forward.

Instead of functioning in silos, the disparate strands of GRC must be brought together into a coordinated, collaborative system. GRC must become a positive, proactive force that pushes companies forward by providing a holistic view of risks, responsibilities, and opportunities.



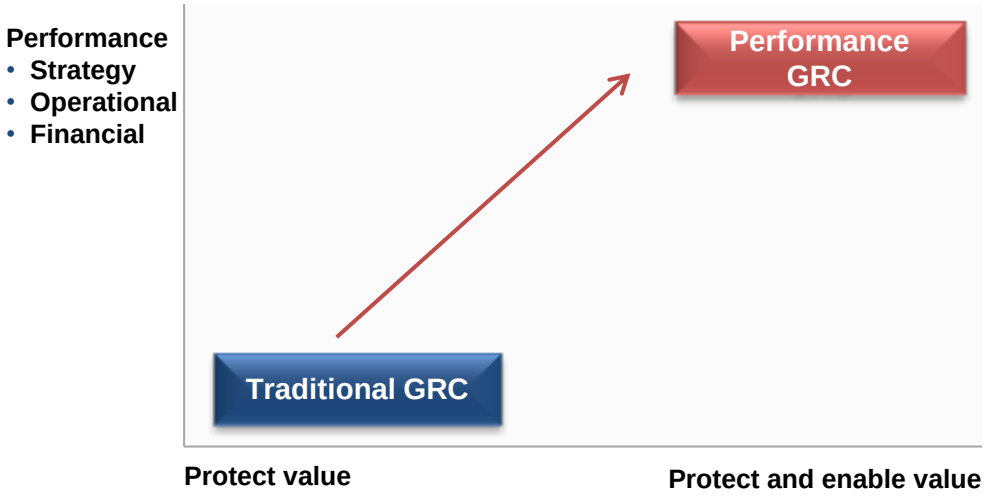
Traditional vs. performance based GRC

*Getting to **Performance GRC** is a journey, a process of breaking down walls and opening up lines of communication, coordination, and collaboration between the organizations various risk and compliance groups and activities*



Traditional vs. performance based GRC

The complexity of today's business environment demands that GRC assumes a new role, upping its value protection and compliance game and also becoming a direct enabler of business performance



Traditional GRC	Performance GRC
Risk functions operate in silos	Risk functions collaborate
High cost/difficult to measure ROI	Efficiency gains/measurable ROI
Gaps/redundancies in risk coverage	Coordinated risk coverage
Minimal focus on emerging risks	Heavy focus on emerging risks
Focus on value protection	Focus on value protection and creation
Indirect linkage to performance drivers	Direct linkage to performance drivers
Not leveraged for management decision making	Supports management decision making

Key benefits of performance GRC

*For business leaders, **Performance GRC** provides a proactive, unified risk management framework to enable better decisions.*

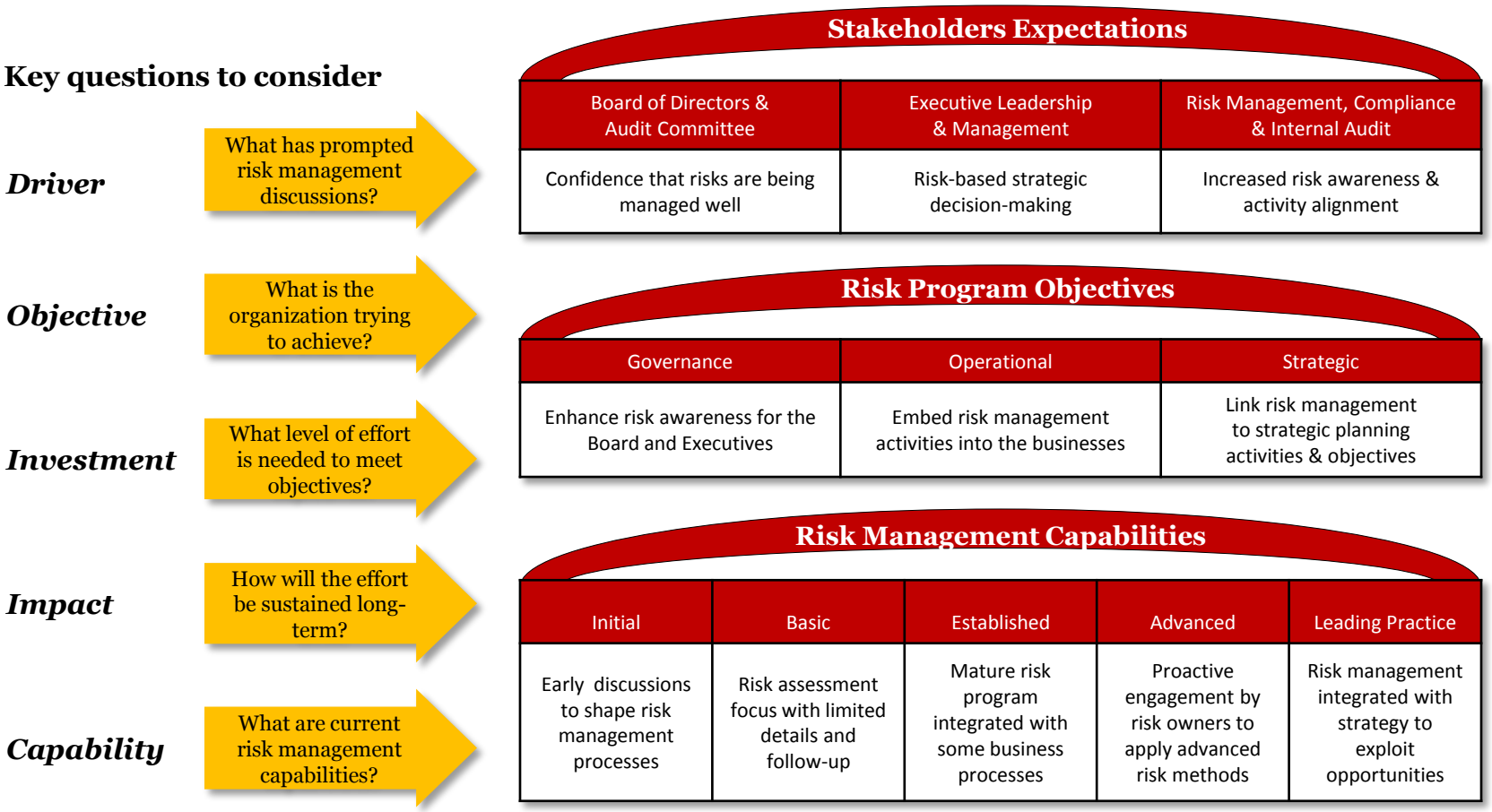
- Support for strategic priorities
- A more effective early-warning systems for emerging risk issues
- Enhanced ability to spot gaps and optimize coverage
- Enhanced visibility to interconnected risks across the enterprise and reduced audit fatigue on the business
- Metrics to support management decision making
- Increased stakeholder confidence and support for the board in discharging its oversight responsibilities

Support for strategic priorities

*A **Performance GRC** based Risk Management Program allows Managers to better link the organization's risk appetite and their overall strategic objectives*

Support for strategic priorities

Is there alignment between Stakeholder Expectations, Risk Program Objectives, and Risk Management Capabilities?



Support for strategic priorities

- A large retailer plans to open 190 new stores in FY15 including emerging markets to provide significant exposure to more diversified customer base and strengthen its brand image

- A large technology company plans to expand its innovative product offerings to cater to the changing consumer demands toward mobile computing and serve diverse markets more efficiently

- A large online retailer continues to focus on the growing e-commerce market, and views acquisitions as a key part of its growth strategy to expand its business, including new technologies, additional products, and geographic reach

A more effective early-warning systems for emerging risk issues

How is the organization managing emerging risks associated with third parties, with which the company does business or shares data?

The hackers who stole **40 million credit- and debit-card numbers** from large discount retailer appear to have breached the discounter's systems by using credentials stolen from a vendor.
– *Wall Street Journal*, January 2014

FTC Data Security Settlement Highlights Need for Third-Party Vendor Management and Oversight

Federal Trade Commission (FTC) announced a settlement with Transcription Services following the public exposure of thousands of medical transcript files containing personal medical information

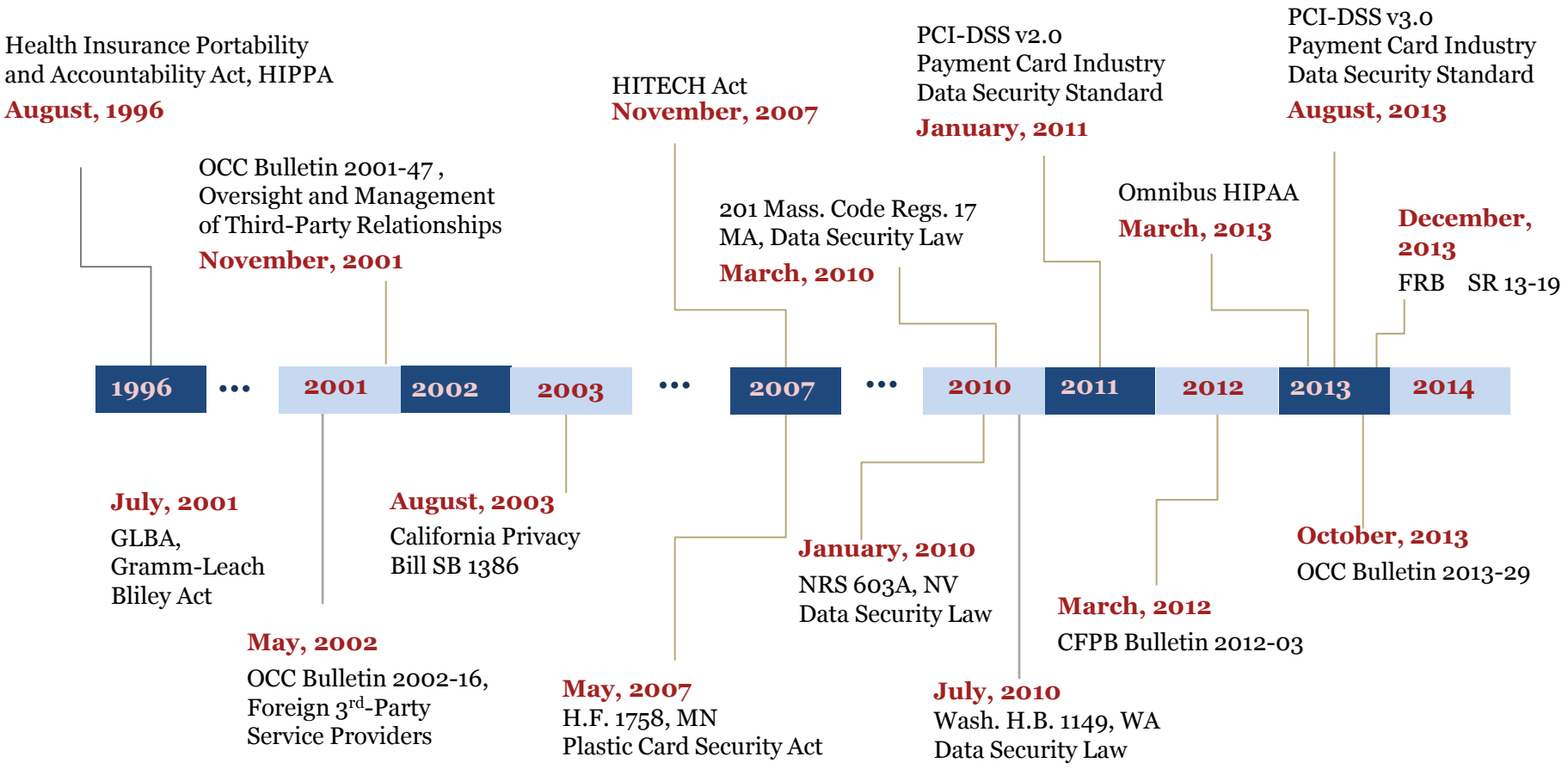
– *HL Chronicle of Data Protection*, January 2014

3.6 million personal income tax returns and 657,000 business filings exposed due to third party data breach.

– *Washington Post*, October 2012

Foreclosure defense lawyer is missing; his law partner says at least $6M in firm money is gone
A foreclosure defense lawyer in Florida has been reported missing as authorities investigate the reported disappearance of at least $6 million in funds held by his law firm in trust accounts.
– *Criminal Justice Apr. 15, 2013*

A more effective early-warning systems for emerging risk issues



A more effective early-warning systems for emerging risk issues

Third parties

- Vendors
- Suppliers
- Joint Ventures
- Business Channels
- Marketing Partners
- Operators

Risk Considerations

- Reputational
- Service Delivery
- Financial
- Business Continuity and Resiliency
- Geographic Location
- Information Security and Privacy
- Regulatory
- Exit Strategy

A more effective early-warning systems for emerging risk issues

Let's add another layer, how is the organization managing emerging risks associated with business continuity from a vendor resiliency perspective?

A more effective early-warning systems for emerging risk issues

Regulators get tough on recoverability

Regulators in at least one major industry recently raised the bar for resiliency and recoverability capabilities. In October 2013, the US Office of the Comptroller of the Currency (OCC) issued Bulletin 2013-29, "Third-Party Relationships," which addresses the growing volume and complexity of operational interconnectedness with third parties in the national banking industry and among federal savings associations.

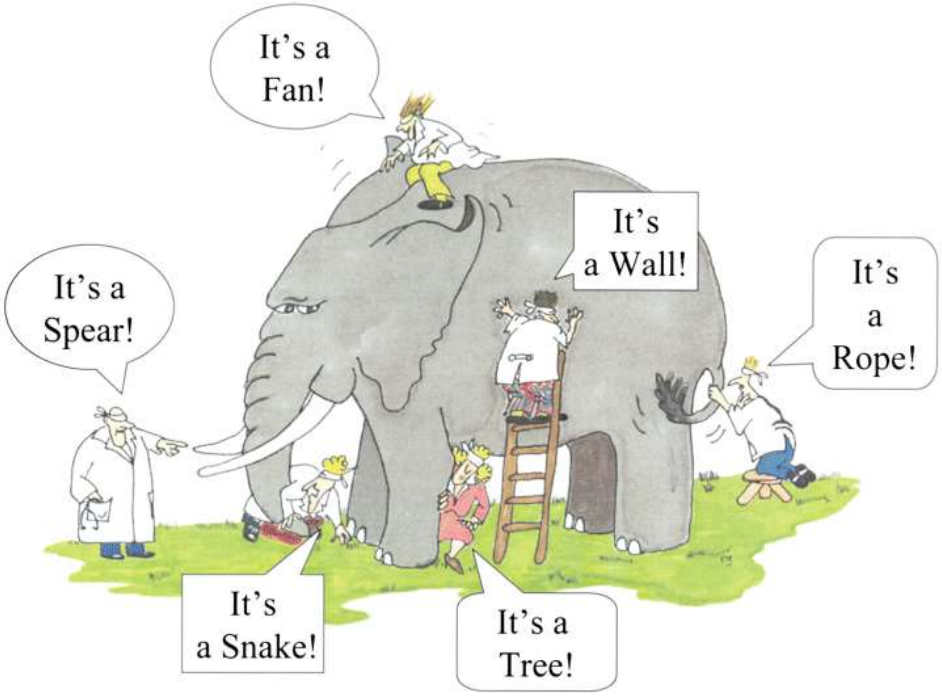
Three major points stand out in regard to vendor risk management:

1. The bulletin specifies that consideration of a third party's resilience would henceforth be considered a required part of due diligence.
2. It introduces the concept of third-party relationships that involve "critical activities" and sets an expectation that banks will exercise more comprehensive and rigorous due diligence, management, and oversight of such relationships.
3. It establishes an overarching standard that institutions under the OCC's regulatory umbrella should adopt risk-management processes commensurate with the level of risk and complexity in its third-party relationships.

These three elements signal that, at least in these sectors of the banking industry, companies need to get serious about mapping their vendor risk landscape, determining the criticality of each vendor relationship, and adopting robust analytical processes to identify, measure, monitor, and control recoverability risks and other risks associated with third-party relationships, particularly for their most critical vendors.

Enhanced ability to spot gaps and optimize coverage

With multiple functions following their own agendas, there's great potential for unfounded assumptions regarding who's covering which risk area, leading to gaps in risk coverage.

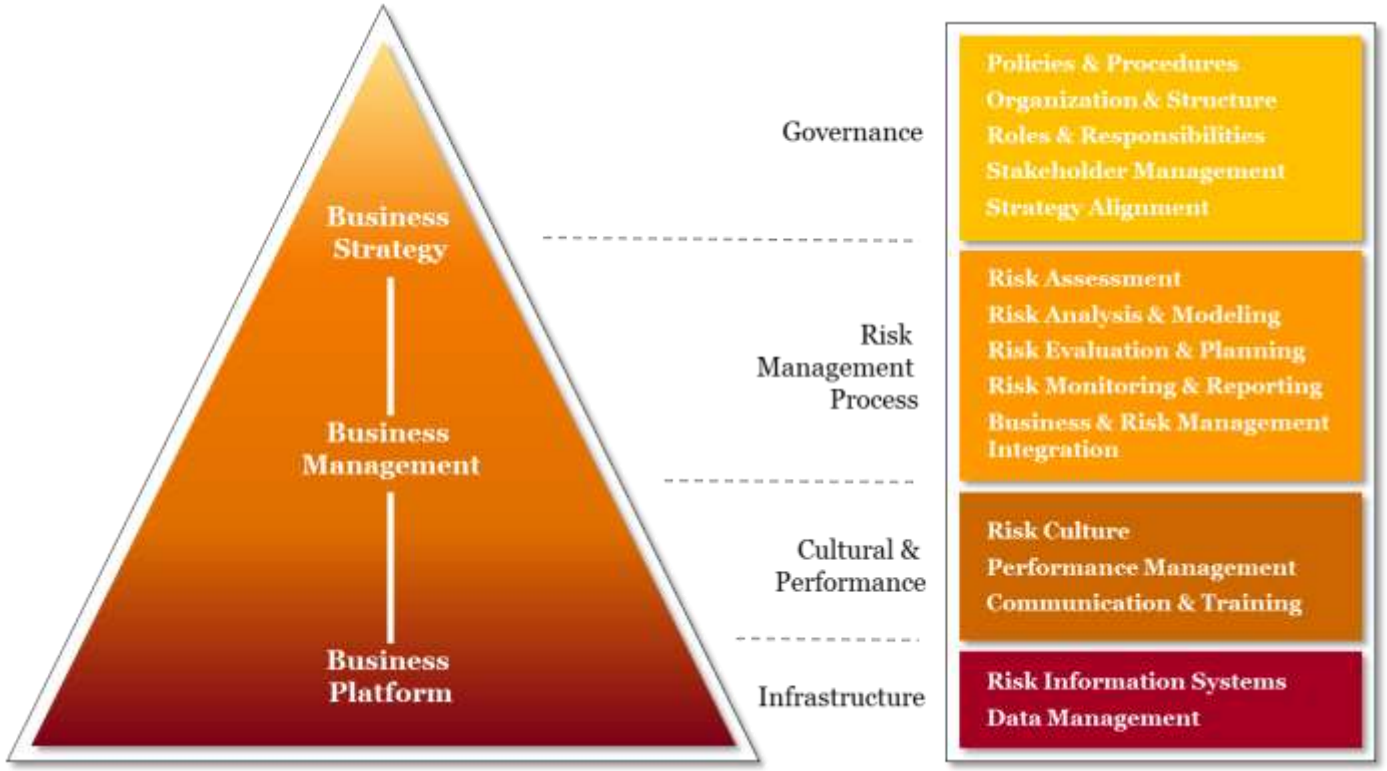


Enhanced ability to spot gaps and optimize coverage

By duplicating efforts around these low-lying risks, the company may be in danger of under-reviewing other, more important risk areas.

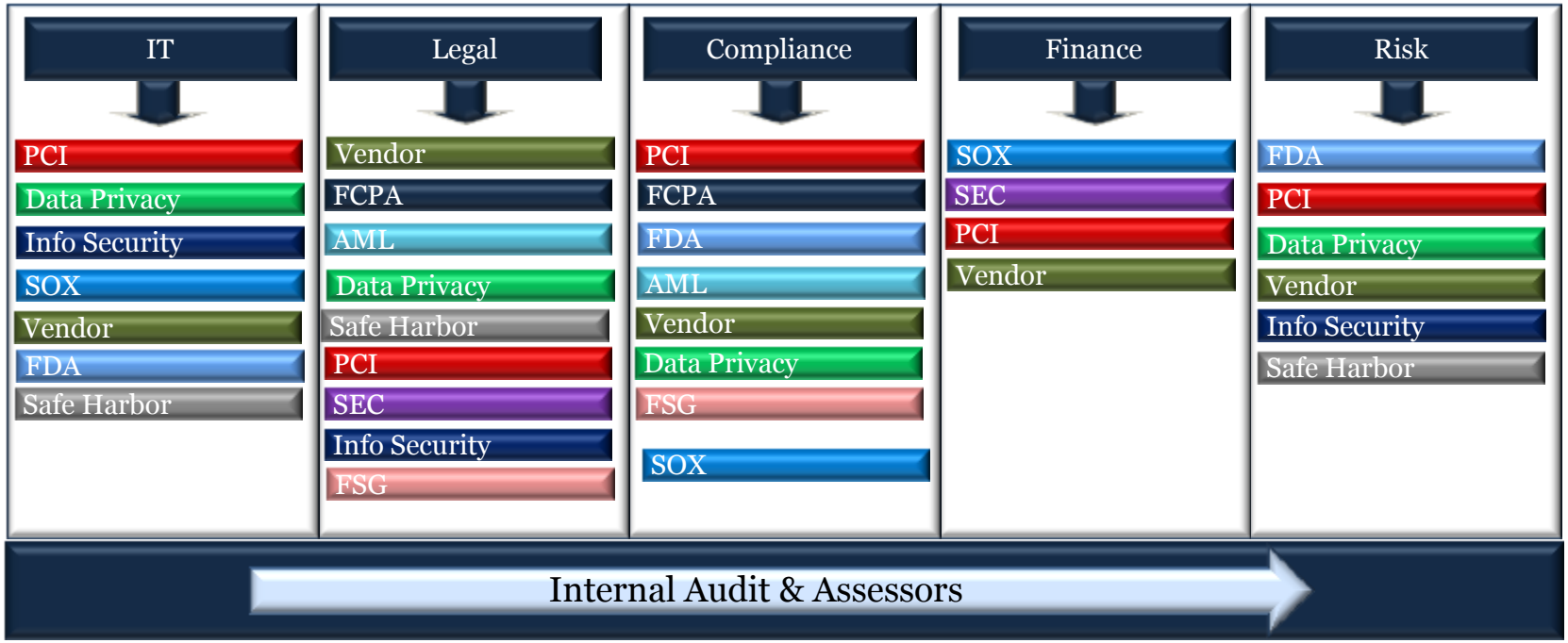
Enhanced ability to spot gaps and optimize coverage

What framework is the organization using to enhance the ability to spot gaps and optimize coverage, and is it tied to the strategic objectives and priorities?



Enhanced visibility to interconnected risks across the enterprise and reduced audit fatigue on the business

Integration across a company's GRC activities can lead to enhanced abilities to map risk connections, allocate appropriate monitoring, and generate results.



Enhanced visibility to interconnected risks across the enterprise and reduced audit fatigue on the business

Sample Control: Review of Access Control Policy

Developed Rationalized Control Framework

- Included six standards: NIST 800-53v3 (FISMA), HIPAA, ISO 27001, SSAE16 SOC1, PCI, EUMC
- Developed common monitoring procedures and evidence requirements
- Developed procedure templates/guidance to drive consistent creation of SOPs across 20 product groups

Control Activity ID	Control Activity Name	Control Description
Access Control-01.02	Review of Access Control Policy	The organization reviews/updates at [Assignment: organization-defined frequency] the formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

One control for the organization

NIST ID	ISO ID	HIPAA ID	PCI ID	SOC1	EU Model Clause
AC-01	A.05.01.02	45 CFR 164.316(b)(2)(iii) Updates (Required)	PCI-DSS 12.01.03	None	None

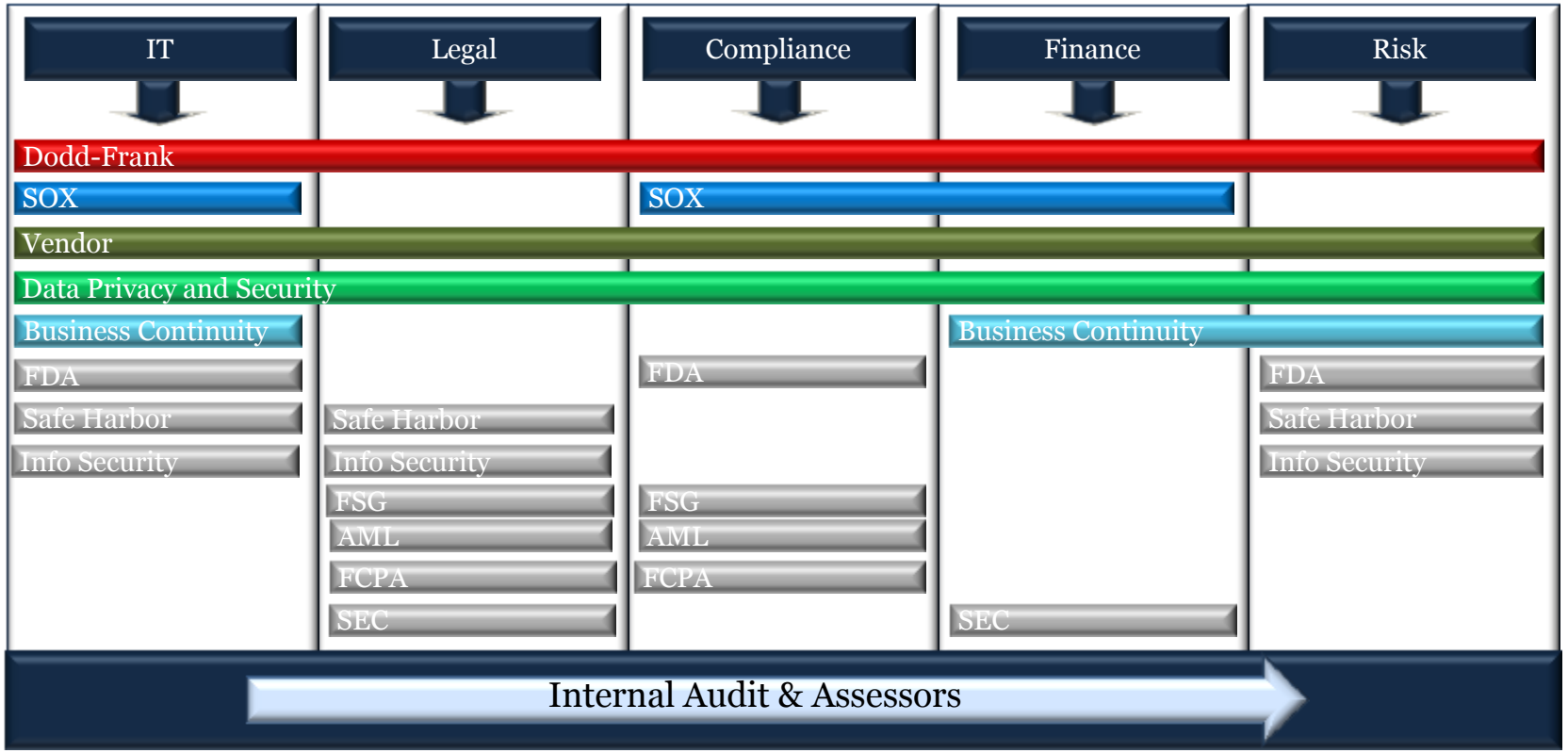
Four standards/regulatory control requirements

Recommended Monitoring Procedures	Recommended Monitoring Evidence	Ownership
1) Obtain the Access Control policy. 2) Look in the change log within the policy to see if a review and/or updates were logged within the [ODV frequency]. If neither were logged, obtain evidence (e.g. email communication) that a review and/or updates took place within [ODV frequency]. 3) Attach the Access Control policy and any evidence gathered.	1) Access Control policy including the change log. 2) Evidence (e.g. email communication) that a review and/or update took place within [ODV frequency] (if necessary).	Program Level

One set of testing guidance to evidence effectiveness

Enhanced visibility to interconnected risks across the enterprise and reduced audit fatigue on the business

An integrated risk and compliance effort provides alignment of risk and compliance stakeholders with improved communication and structure, time and cost savings, and improved transparency and accountability through common reporting.

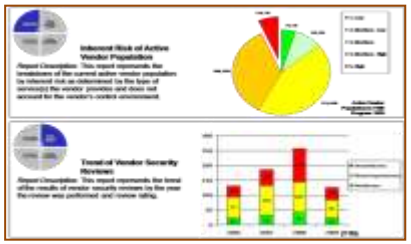


Metrics to support decision making

Crisp and focused reporting by management/governance level will enable the appropriate stakeholders to make key decisions on the functional operations and health of the program's effectiveness.

Board Level Reporting

- Management level metrics are aggregated to provide an overall metric for program performance
- Historical trends for each risk metric are provided



Management Level Reporting

- Operational metrics are aggregated by classifications to provide a holistic metric by region. Examples of these classifications include the following:
  - Category
  - Region
  - Segment

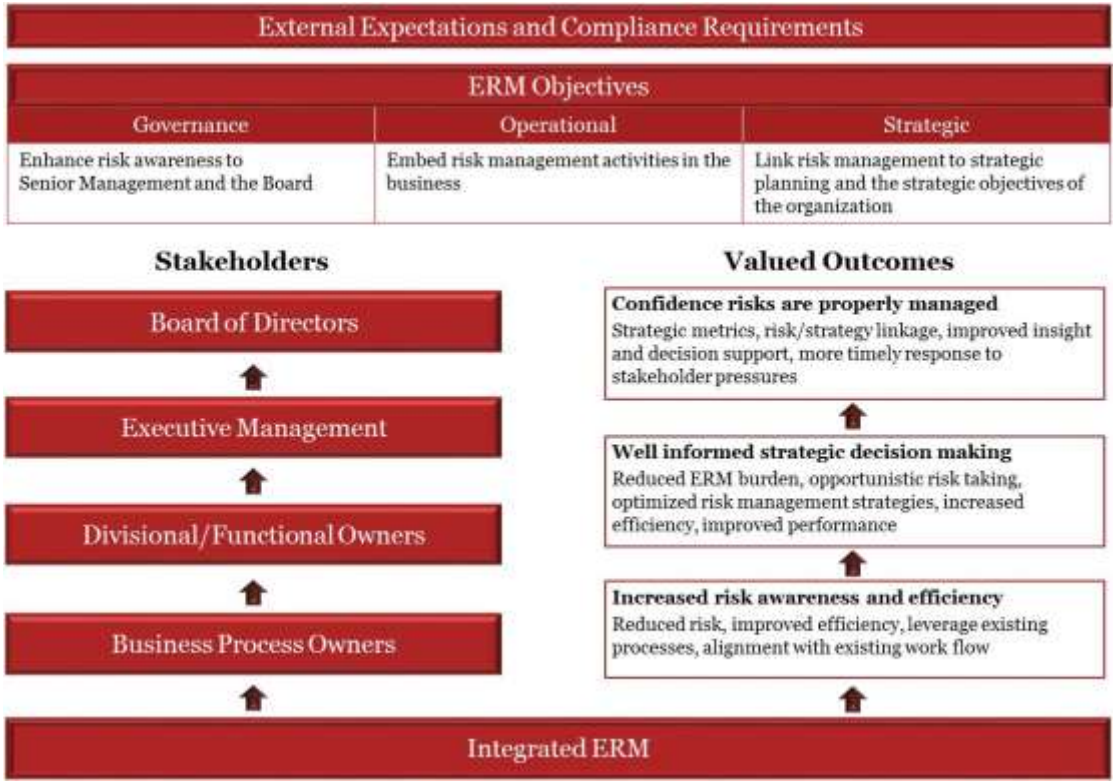
Business Unit Level Reporting

- Metrics are measured at the business unit with an individual score-card
- Each process is associated to a category, region, business unit, vendor segment and other relevant classifications

Increased stakeholder confidence and support for the board in discharging its oversight responsibilities

An integrated view over GRC is critical to understanding of key business risks and necessary for the board to fully discharge their oversight responsibility.

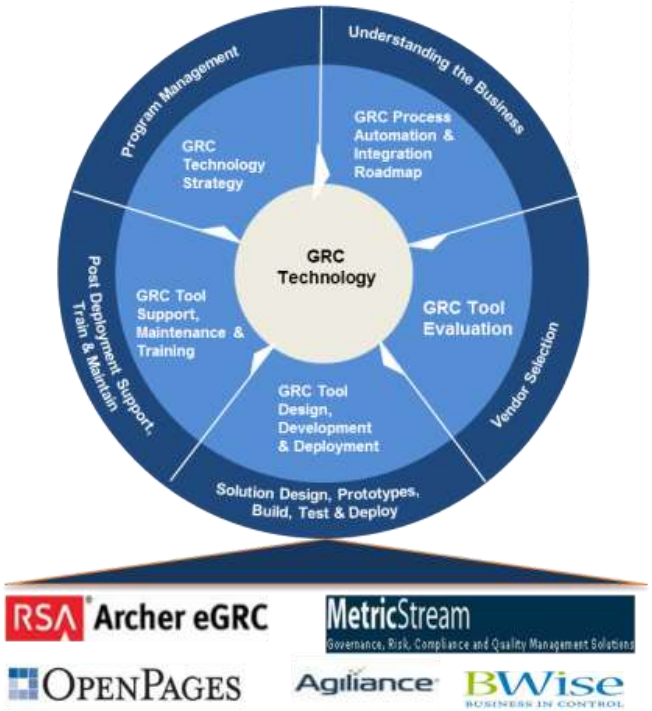
Board members, executives, operational leaders, and third parties all rely on the intelligence produced by GRC activities, and the more fully those activities are integrated and optimized, the more confidence they can provide stakeholders vis-à-vis their respective enterprise risk oversight responsibilities.



Use of technology – GRC as a platform and for analytics

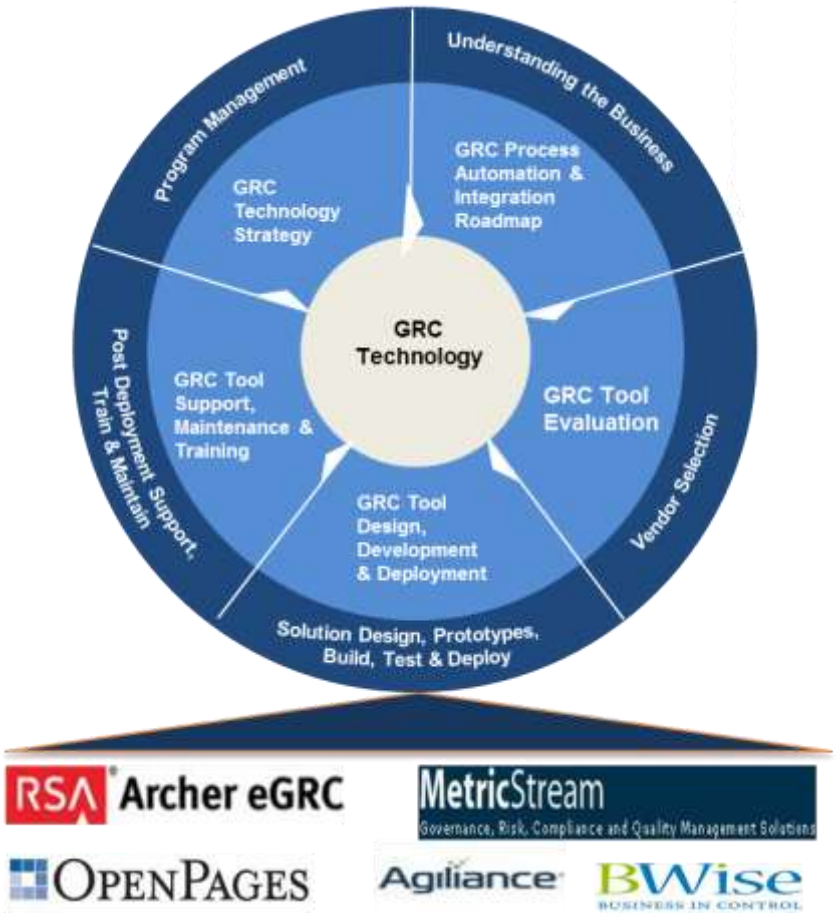
GRC technology as "platform" *supports the organization's compliance and risk management programs stakeholders a single source for managing compliance/risk*

Using technology for analytics and executing GRC efforts *supports the organization communicate and monitor GRC program initiatives*



GRC technology

Enabled with technology, an integrated GRC program supports compliance and risk management programs across the organization. Some of the benefits are listed below:



- Manage multiple compliance/risk frameworks
- Link controls, risks and processes to eliminate redundant efforts
- Automate manual processes and controls
- Integrate results of security and controls point solutions and link them to risks and controls
- Provide stakeholders a single source for managing compliance/risk testing, issues and corrective action plans (CAPs)
- Provide real-time trends analysis and performance management and support informed decision-making with automated reports and role-based dashboards

Use of technology – Social Media

How is Social Media and GRC linked? What risks do they pose to the organization from a compliance and ethics standpoint?

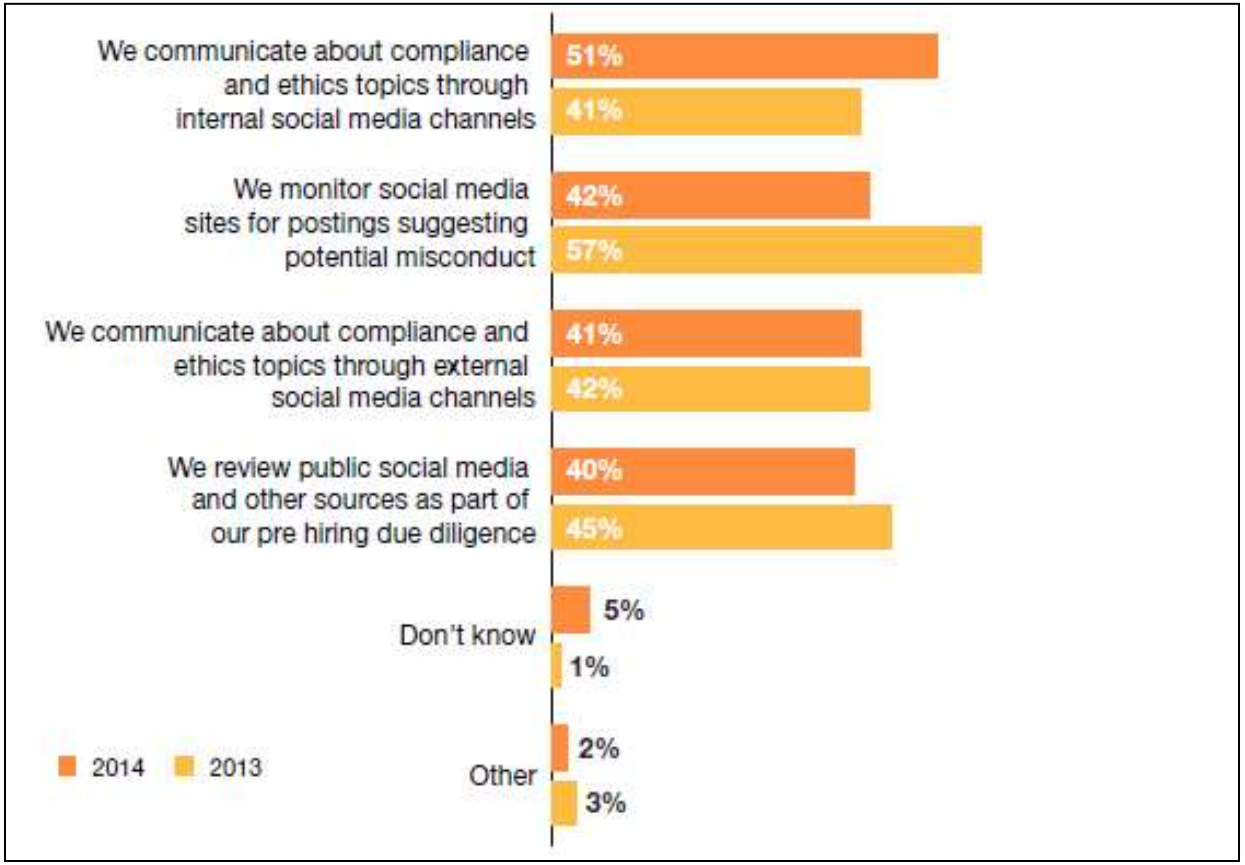
Use of technology – Social Media

Many companies leverage social media to communicate GRC program messages to their employees and organizations.

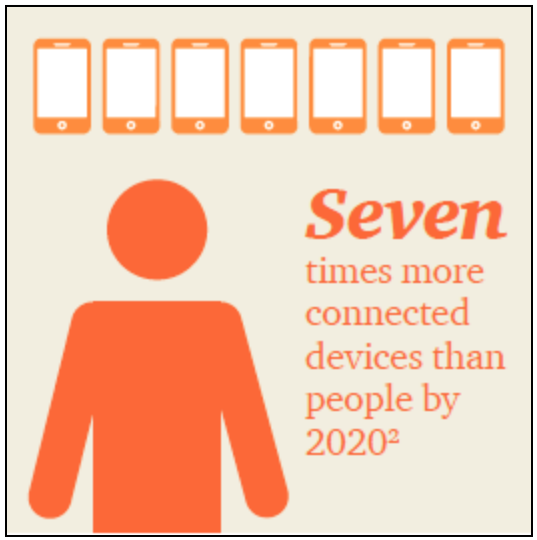
Furthermore, some companies are seeking ways to more effectively monitor the use of social media to support their regulatory and compliance requirements

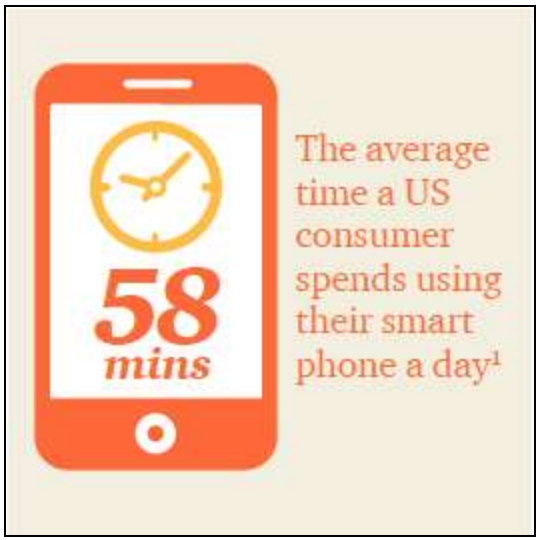
Source: PwC State of Compliance Survey 2014

Ways companies use Social media in their Compliance and Ethics Program



Use of technology





The exponential pace of technology growth requires a system that can take full advantage of the opportunity that a GRC technology can provide

Performance GRC – Putting it all together

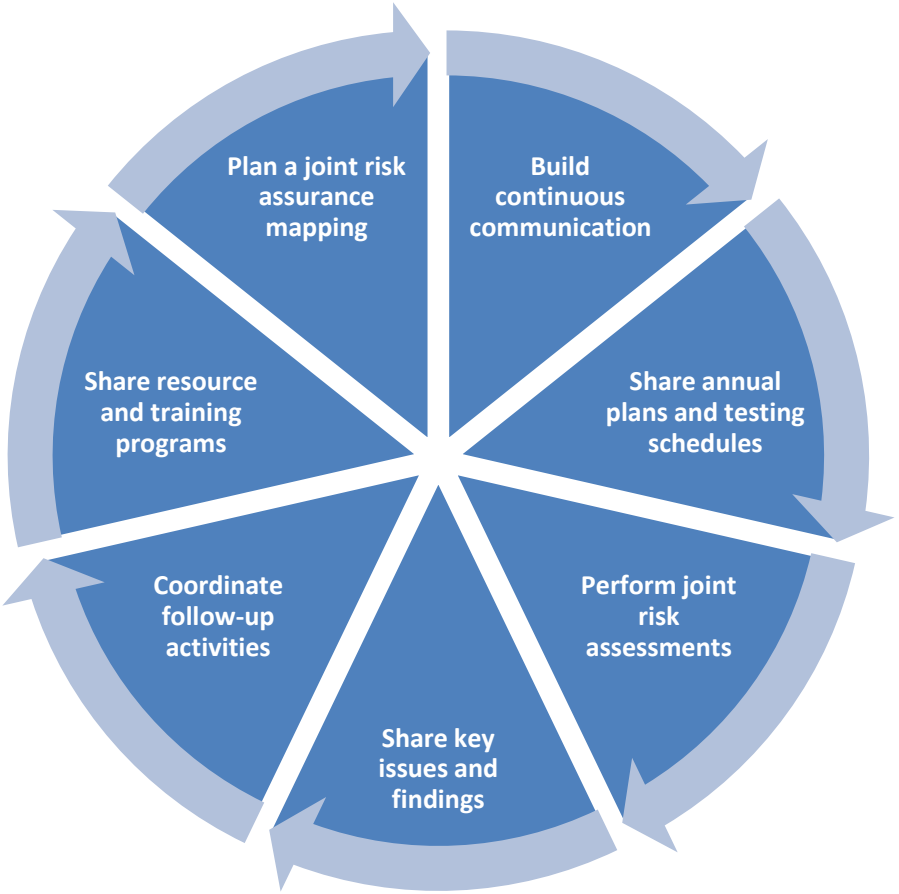
Performance GRC - Putting it all together

The process of moving a company's GRC activities from a strict value protection stance to one that also enables business performance must begin with an assessment of the business' current GRC abilities and alignment.

Stakeholders must ask themselves:

Performance GRC - Putting it all together

Strategies to help put you on the path to GRC integration and optimization:



Performance GRC - Putting it all together

When governance, risk, and compliance matters are complex, it is important that organizations today have the appropriate framework and governance in place, to diagnose and address "risks" to ensure the business and its partners can make better business decisions.

Today's Business Challenges

- Increasingly complex regulatory environment resulting in need to regularly review and update rules, requirements, and business processes
- Limited/ad hoc policy governance structures, oversight and ownership of Corporate processes and polices
- Decentralized, hard to access and inconsistent corporate policies and procedures
- Limited processes for updating policies and communicating policy changes
- Differences in cultural norms and local standards as companies become more global
- Uncoordinated and duplicative compliance efforts

Bringing it to a point: Performance GRC is…

- An enabler of a Company's **business performance**
  - Do things right the first time (at lower costs!)
  - Take-on complex risks and manage them up-front
  - Align compliance to performance drivers

- A **competitive advantage**
  - Protect/enhance your brand and other key assets
  - Become the less "risky", preferred business partner
  - Spend more time looking forward; less time reacting

- An organizational capability that **builds trust** of
  - Customers, investors and other stakeholders
  - Senior Management / Board
  - Regulators

- A program to help **navigate complex and changing rules**

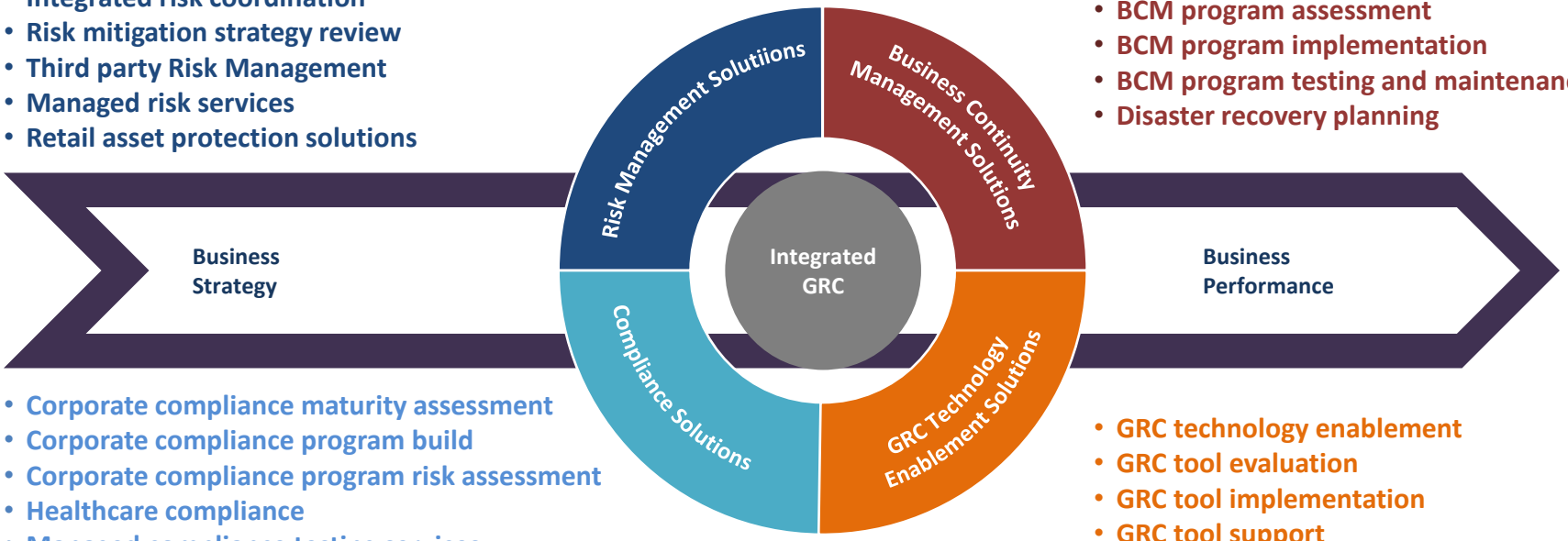
- An integrated component of an organization's **risk management** program

- **Not…**
  - Limited to laws and regulations
  - The sole responsibility of the Compliance Department

PwC's Perspective on Performance GRC

Our perspectives on Performance GRC spans risk management activities, corporate compliance efforts, business continuity management, and GRC tools. We would appreciate the opportunity to discuss any of these solution areas:

- PGRC maturity assessment
- PGRC framework build
- Risk assessment (enterprise, business unit, emerging)
- Integrated risk coordination
- Risk mitigation strategy review
- Third party Risk Management
- Managed risk services
- Retail asset protection solutions



- BCM program assessment
- BCM program implementation
- BCM program testing and maintenance
- Disaster recovery planning

- Corporate compliance maturity assessment
- Corporate compliance program build
- Corporate compliance program risk assessment
- Healthcare compliance
- Managed compliance testing services
- Conflict minerals compliance

- GRC technology enablement
- GRC tool evaluation
- GRC tool implementation
- GRC tool support

About the Presenters

Steve Zawoyski, PwC
National Performance GRC Leader – Risk Management
Direct: (612) 596-4931
Mobile: (847) 323-4946
stephen.v.zawoyski@us.pwc.com

Steve Zawoyski has been with PwC since 1989 serving primarily as a Risk Assurance partner. He began his career in Chicago and has worked in PwC's Minneapolis and San Francisco offices. He has extensive knowledge and experience in providing risk assurance, enterprise risk management and internal audit services to clients across the multiple industries, including retail, services, consumer and industrial product industries. Steve is the National Leader of PwC's Performance GRC – Risk Management practice which is dedicated to developing, implementing and managing leading risk management programs across a variety of risk areas, including: Enterprise Risk Management, Performance/Strategic Risk Management, Integrated Risk and Compliance Management, and Vendor Risk Management.

As a partner Steve supports his clients in a variety of services, including the design, building and implementation of risk management programs, conducting comprehensive and/or highly focused risks assessments, leading the integration of risk and compliance programs and performing strategic benchmarking and regulatory assessments of risk management programs.

Chris Chung, PwC
SF Performance GRC Solution Leader
Direct: (415) 498-7449
Mobile: (408) 505-0646
christopher.s.chung@us.pwc.com

Chris Chung is a Director in the Risk Assurance practice and the Performance Governance, Risk and Compliance (PGRC) solution leader for the San Francisco market. Chris' experience includes assessing, designing and implementing coordinated risk and controls compliance programs across a variety of industries, including over 13 years of serving clients in the energy, industrial products, technology, entertainment and media, higher education, academic medical center, and not-for-profit sectors.

He specializes in enhancing governance, risk and compliance activities, bringing the knowledge and experience of PGRC professionals across Risk Management, Compliance, Business Continuity Management, and GRC Technology capabilities to support client issues and priorities.

Questions?


ISACA
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA