Evolutionary Convergence(Merging) of Enterprise Risk and Compliance Programs into Corporate GRC Program

2015 - Case Study

Kashif Latif

Global GRC Officer | FIS

MetricStream

GRC
SUMMIT **2015**
May 11-13, 2015
ARLINGTON, VA
WASHINGTON, DC AREA

Maximize Business Performance Through GRC Journey

FIS Overview

Founded as Systematics™ in 1968, FIS boasts a 45-year history focused on the financial services industry

- Serves more than **14,000 institutions** in over **110 countries**
- Processes more than **27 billion transactions every year**, touching more than **750 million end consumers**
- Employs more than **40,000 people** worldwide
- Ranked **426 on the Fortune 500** and a member of Standard & Poor's 500® Index
- Experienced **6% revenue growth in 2014** for a total of **$6.4 billion** in revenue
- Named the No. 1 overall financial technology provider in the annual FinTech 100 rankings four times running (2011, 2012, 2013 and 2014)

FIS is focused on the success of our clients through a set of core values and a focus on risk, information security and compliance – with a goal to be best in class among technology service providers

GRC Program – OCEG Reference

OCEG: Your Path to Principled Performance™

Principled Performance™ is a management discipline that enables an organization to clearly define its principles and goals, determine how it will address risks and uncertainties, and grow and protect value. Achieving Principled Performance™ demands the clear articulation of objectives and the methods by which you will establish and stay within mandatory and voluntary boundaries of conduct while driving toward those objectives.

OCEG is ready to help you address the challenges that you face today. Join the thousands of individuals in the OCEG community and stay on the path to Principled Performance™

OCEG®
LEARN MORE AT
www.oceg.org

OPTIMIZE YOUR:

Governance
Ensure that sound governance structures are in place "below the board" so that the right information about the right issues is available at the right time.

Risk
Integrate risk management with strategic planning and maintain a 360-degree view of organizational risks and effectively allocate resources to address them.

Ethics & Compliance
Establish practices and a culture to prevent misconduct, inspire desired conduct, detect problems and improve outcomes.

Finance
Reduce costs and optimize how you allocate capital to governance, risk and compliance processes so that GRC is better aligned with the business.

Technology
Address IT compliance issues and the alignment of information technology to general GRC needs in the rest of the business.

Audit
Go beyond financial processes and assess the design and operation of controls for governance, risk management, compliance and ethics efforts throughout the enterprise.

Legal
Identify and establish sound practices to address your legal risks and improve your ability to detect and correct issues; while improving your ability to defend the organization.

Core Processes
Embed sound GRC practices in all lines of business and core processes so that business owners and operators are accountable for GRC success.

RESOURCES AND TOOLS

Thousands of resources developed, collected and organized by OCEG and shared within the OCEG Community:

- Guides and handbooks
- GRC Surveys, research and benchmarking reports
- GRC 360°- OCEG's magazine presenting critical perspectives on governance, risk, compliance and culture
- The GRC Illustrated Series – pictorial explanations of key GRC processes
- Topical whitepapers and articles
- Links to key government and organizational guidance documents

EXECUTIVE SUPPORT AND SOLUTIONS

- Bring your management team together in the OCEG Strategy Lab, with OCEG experts who can help you integrate GRC with business strategy
- Learn how to implement the OCEG Framework in your organization by working with OCEG staff and partners

EVENTS AND NETWORKING

- Opportunities to work together with peers to address GRC challenges from every angle
- Live and archived webinars
- Exchange viewpoints and ideas

FRAMEWORKS & GUIDANCE

- Comprehensive GRC Capability Model developed and vetted by hundreds of experts and reviewed by thousands
- Searchable database of laws, regulations, standards and guidance from many sources
- Searchable library of sound practices you can apply to address governance, risk and compliance requirements at your organization
- Select the information you need and use it the way that works best for you through OCEG's custom report feature

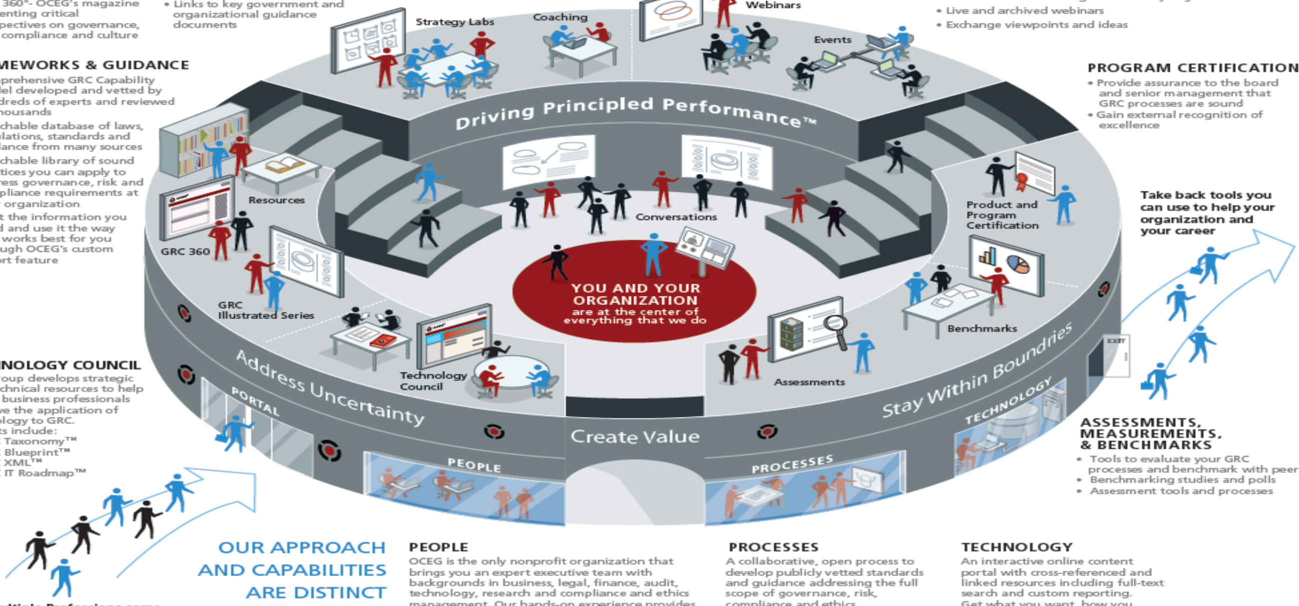
PROGRAM CERTIFICATION

- Provide assurance to the board and senior management that GRC processes are sound
- Gain external recognition of excellence

TECHNOLOGY COUNCIL

This group develops strategic and technical resources to help IT and business professionals improve the application of technology to GRC.
Projects include:

- GRC Taxonomy™
- GRC Blueprint™
- GRC XML™
- GRC IT Roadmap™



Multiple Professions come together in ONE PLACE

Take back tools you can use to help your organization and your career

ASSESSMENTS, MEASUREMENTS, & BENCHMARKS

- Tools to evaluate your GRC processes and benchmark with peers
- Benchmarking studies and polls
- Assessment tools and processes

OUTCOMES

OCEG can assist you on the path to Principled Perfomance™ with tools and resources you can use to:

- Establish an integrated, organization-wide approach to GRC ensuring the flow of consistent information.
- Design and measure your GRC efforts against a business process model developed by hundreds of business, financial, legal and technology experts and publicly vetted by thousands.
- Benchmark your organization's performance against peers and participate in targeted industry research and resource development.
- Join forces with peers who are managing governance, risk and compliance challenges from every angle
- Do your job better, faster, and more economically with the right tools.

OUR APPROACH AND CAPABILITIES ARE DISTINCT

PEOPLE
OCEG is the only nonprofit organization that brings you an expert executive team with backgrounds in business, legal, finance, audit, technology, research and compliance and ethics management. Our hands-on experience provides the background and understanding to help you put principles into practice in your organization.

PROCESSES
A collaborative, open process to develop publicly vetted standards and guidance addressing the full scope of governance, risk, compliance and ethics management and measurement.

TECHNOLOGY
An interactive online content portal with cross-referenced and linked resources including full-text search and custom reporting. Get what you want, how you want, and when you want it.

XPLANATIONS™ by XPLANE®

FIS GRC Program – Objectives

- **Governance Objectives**
  - Provide **Risk Centric** Corporate **Governance** structure for Compliance toward
    - Corporate **Strategic Objectives** and Initiatives
    - Corporate **Policies and Standards**
    - **Statutory and Regulatory** Requirements
- **Business Objectives**
  - Provide and support scalable **Service Delivery and Service Support** in alignment with strategic business objectives and service offering.
  - Enable and facilitate business in **delivering Services and Products securely and effectively.**
  - Provide 3rd party assurance about internal controls and capabilities to facilitate **negotiation, sales and closing of deals.**
- **Compliance and Risk Objectives**
  - To put **Security and Compliance controls** in place to **limit** the **Legal, Financial and Reputational liabilities**.
  - To meet **Contractual, Regulatory** and **Industry Standard** (FFIEC, FDIC, SSAE 16, ISO 27001, ISO 20000 etc..) related requirements.
  - Ensuring the **security and protection** of all Computing Resources, Confidential Data and Intellectual property of **FIS and of its Clients to reduce** noncompliance and risk exposure.

FIS GRC Program – Benefits

- For People:
  - **Greater insight for better oversight** of Enterprise Governance
  - Enterprise-wide **visibility and control**
  - Engaged **Governance** and Operational Processes
  - **Strong Stakeholder Relationships** (Business, Finance, Legal, Audit etc.)
- For Processes:
  - **Policies mapped** to Regulatory and Business Requirements
  - **Controls mapped** to Policies and continuous monitoring of controls
  - **Maturity , Capability, and Best Practice** Assessments against Peers
  - Commitment to **Automation, Streamlining** and **Synthesizing GRC processes**
- For Technology:
  - **Integration of IT and Security** Operation, Monitoring and Management Systems
  - **Continuous**, automated, **consolidated assessments** for IT and Security Operations
  - GRC Management Platforms to align **IT GRC , Security and Risk GRC with Corporate GRC**

GRC Program – Objectives and Benefits

GRC Illustrated

How do I know if my program is performing?

Measuring performance is a difficult task; there are no laws or regulations that demand your program (whether it be a compliance program or program of internal control over financial reporting) is efficient or delivers business value. Here's a look at going beyond effectiveness to deliver total program performance.

EFFECTIVENESS

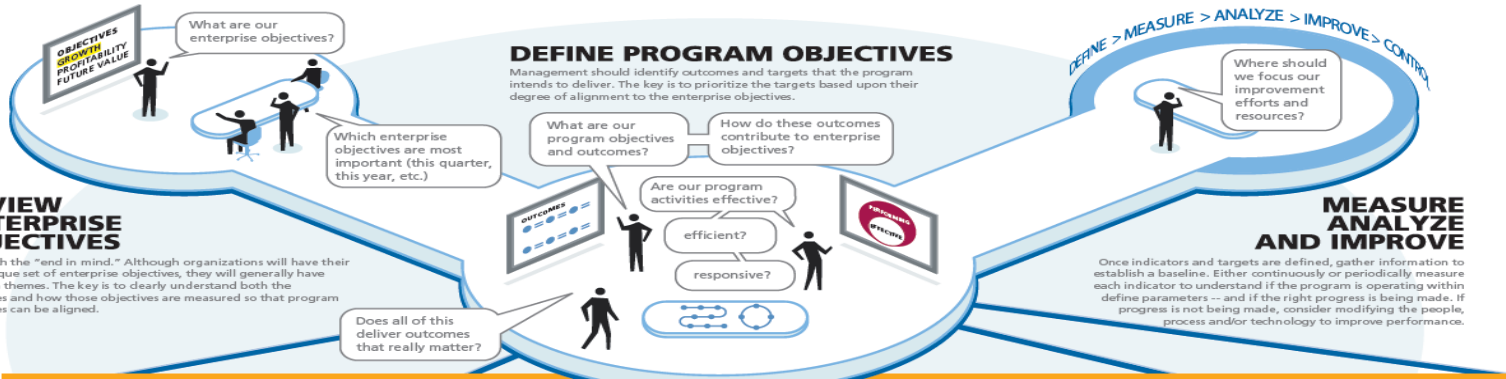
The basis of all evaluation, "effectiveness" looks at whether the program is logically designed to address all key risks and requirements, and whether it is actually operating as designed.

PERFORMANCE

"Performance" looks at effectivness, efficiency, responsiveness and overall value beyond simply meeting legal and regulatory requirements.

DEVELOPED BY OCEG®

SPONSORED BY ERNST & YOUNG *Quality In Everything We Do*


OBJECTIVES
GROWTH
PROFITABILITY
FUTURE VALUE
What are our enterprise objectives?
Which enterprise objectives are most important (this quarter, this year, etc.)
What are our program objectives and outcomes?
How do these outcomes contribute to enterprise objectives?
OUTCOMES
Are our program activities effective?
efficient?
responsive?
PERFORMING
EFFECTIVE
Does all of this deliver outcomes that really matter?
DEFINE > MEASURE > ANALYZE > IMPROVE > CONTROL
Where should we focus our improvement efforts and resources?

REVIEW ENTERPRISE OBJECTIVES

Start with the "end in mind." Although organizations will have their own unique set of enterprise objectives, they will generally have common themes. The key is to clearly understand both the objectives and how those objectives are measured so that program objectives can be aligned.

DEFINE PROGRAM OBJECTIVES

Management should identify outcomes and targets that the program intends to deliver. The key is to prioritize the targets based upon their degree of alignment to the enterprise objectives.

MEASURE ANALYZE AND IMPROVE

Once indicators and targets are defined, gather information to establish a baseline. Either continuously or periodically measure each indicator to understand if the program is operating within define parameters -- and if the right progress is being made. If progress is not being made, consider modifying the people, process and/or technology to improve performance.

GOOD INDICATORS ARE S.M.A.R.T.

SPECIFIC / SIMPLE
- Is it clear exactly what is being measured?
- Would two different people measure it in the same way?
- Does the indicator isolate the true event?
- Does the indicator avoid "mixed messages?"

MEASURABLE
- Can it be quantified? Is it accessible and worth the cost to obtain the data?

ACTIONABLE
- Once we understand the value of the indicator and any trends, will it be possible for us to take meaningful action?
- Are the underlying processes that can affect this indicator under our control?

RELEVANT
- Will tracking this indicator drive the appropriate behavior – or generate unintended consequences?
- Does the indicator capture the essence of the desired outcome?

TIMELY
- Can it be frequently updated?
- Will the indicator reveal itself in time to take appropriate action?

PROGRAM OUTCOMES*

CULTURE
Does the program inspire a principled culture of performance, accountability, trust, and open communication?

PREVENT
Does the program actually prevent weaknesses, noncompliance and unethical conduct?

PREPARE
Does the program actually prepare the organization to address key risks, noncompliance and unethical conduct?

PROTECT
Does the program adequately protect the organization from negative consequences if/when noncompliance and unethical conduct materialize?

DETECT
Does the program actually detect weaknesses, noncompliance and unethical behavior when it occurs?

RESPOND
Does the program appropriately and quickly respond to adverse events once they are detected?

IMPROVE
Once the organization detects and responds to a weakness, is the weakness actually fixed so that similar events do not materialize in the future?

REDUCE LOSS
Does the program reduce the tangible and intangible damage caused by noncompliance and unethical behavior?

OPTIMIZE COSTS
Does the organization continuously optimize costs to deliver similar or even improved outcomes?

ENHANCE STAKEHOLDER VALUE
Does the program improve stakeholder perceptions of the organization?

*NOTE: GRC Program refers to the full suite of enterprise processes that help an organization stay within boundaries, protect value and address uncertainty as it drives toward objectives and creates value. These processes include (among others) the governance, risk management, compliance, ethics and internal audit functions and key programs such as the compliance program and the program of internal control over financial reporting (ICFR)

contact info@oceg.org for comments, reprints or licensing requests

FIS's GRC Program : An Evolutionary OR A Journey

Is a GRC program a journey or evolution. For FIS, we realize it is a combination of both of them. This acknowledgment and awareness is important as it helped in deciding what strategies and approaches to adopt as part our evolutionary journey.

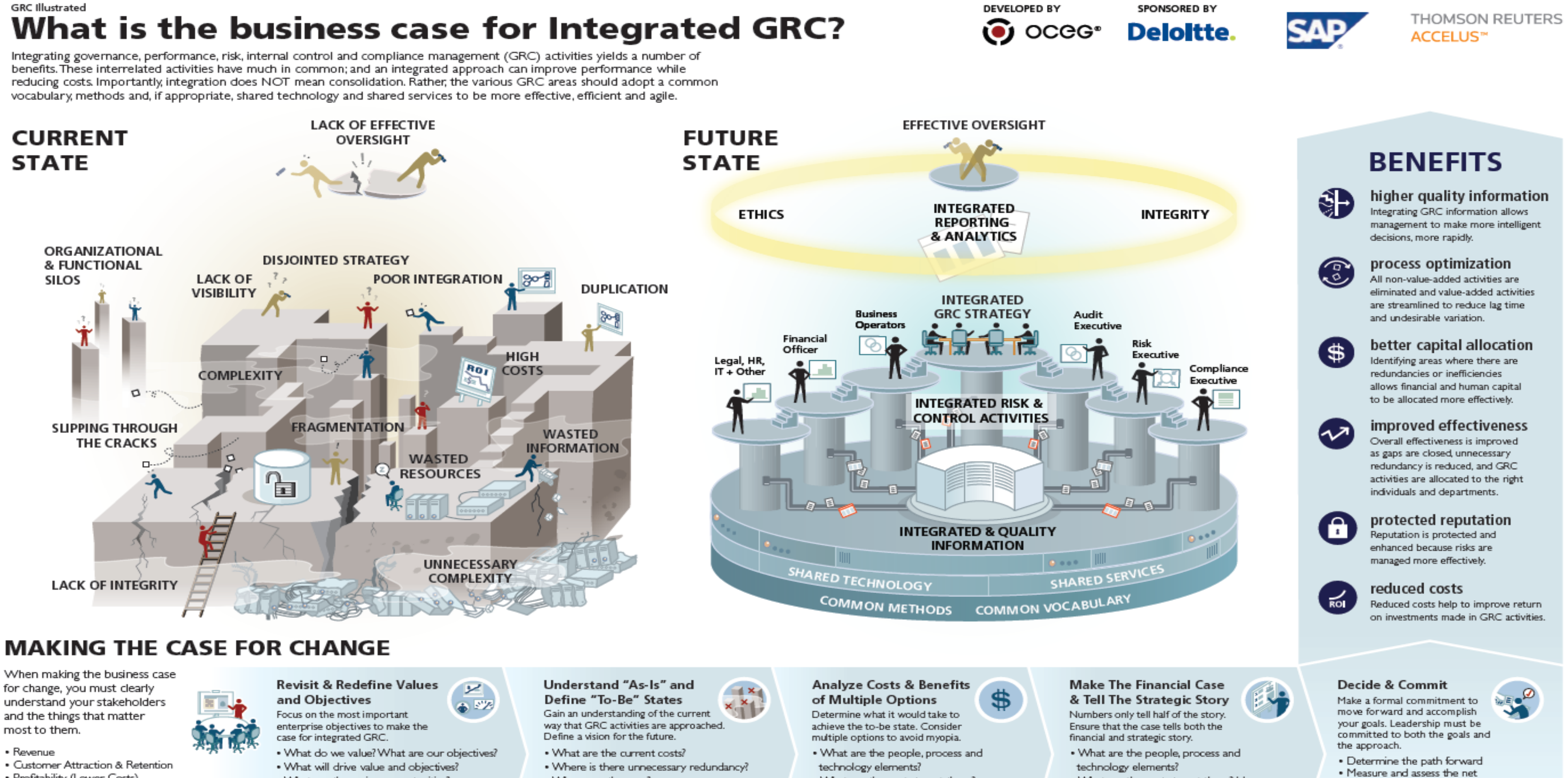
Journey

- □ Structured Program
- □ Defined Business Objectives
- □ Use of GRC Industry Standard
- □ Dedicated GRC Team

Evolution

- □ Natural Adaption for Business Need
- □ Agile Approach for Program and Architecture
- □ Business Needs vs. Wants
- □ Unmanageable Forces of Disruption or Change

GRC Program – Making a Case of GRC Journey



GRC Illustrated

What is the business case for Integrated GRC?

DEVELOPED BY OCEG® SPONSORED BY Deloitte. SAP THOMSON REUTERS ACCELUS™

Integrating governance, performance, risk, internal control and compliance management (GRC) activities yields a number of benefits. These interrelated activities have much in common; and an integrated approach can improve performance while reducing costs. Importantly, integration does NOT mean consolidation. Rather, the various GRC areas should adopt a common vocabulary, methods and, if appropriate, shared technology and shared services to be more effective, efficient and agile.

CURRENT STATE

FUTURE STATE

BENEFITS

higher quality information
Integrating GRC information allows management to make more intelligent decisions, more rapidly.

process optimization
All non-value-added activities are eliminated and value-added activities are streamlined to reduce lag time and undesirable variation.

better capital allocation
Identifying areas where there are redundancies or inefficiencies allows financial and human capital to be allocated more effectively.

improved effectiveness
Overall effectiveness is improved as gaps are closed, unnecessary redundancy is reduced, and GRC activities are allocated to the right individuals and departments.

protected reputation
Reputation is protected and enhanced because risks are managed more effectively.

reduced costs
Reduced costs help to improve return on investments made in GRC activities.

MAKING THE CASE FOR CHANGE

When making the business case for change, you must clearly understand your stakeholders and the things that matter most to them.

- Revenue
- Customer Attraction & Retention
- Profitability (Lower Costs)

Revisit & Redefine Values and Objectives
Focus on the most important enterprise objectives to make the case for integrated GRC.

- What do we value? What are our objectives?
- What will drive value and objectives?

Understand "As-Is" and Define "To-Be" States
Gain an understanding of the current way that GRC activities are approached. Define a vision for the future.

- What are the current costs?
- Where is there unnecessary redundancy?

Analyze Costs & Benefits of Multiple Options
Determine what it would take to achieve the to-be state. Consider multiple options to avoid myopia.

- What are the people, process and technology elements?

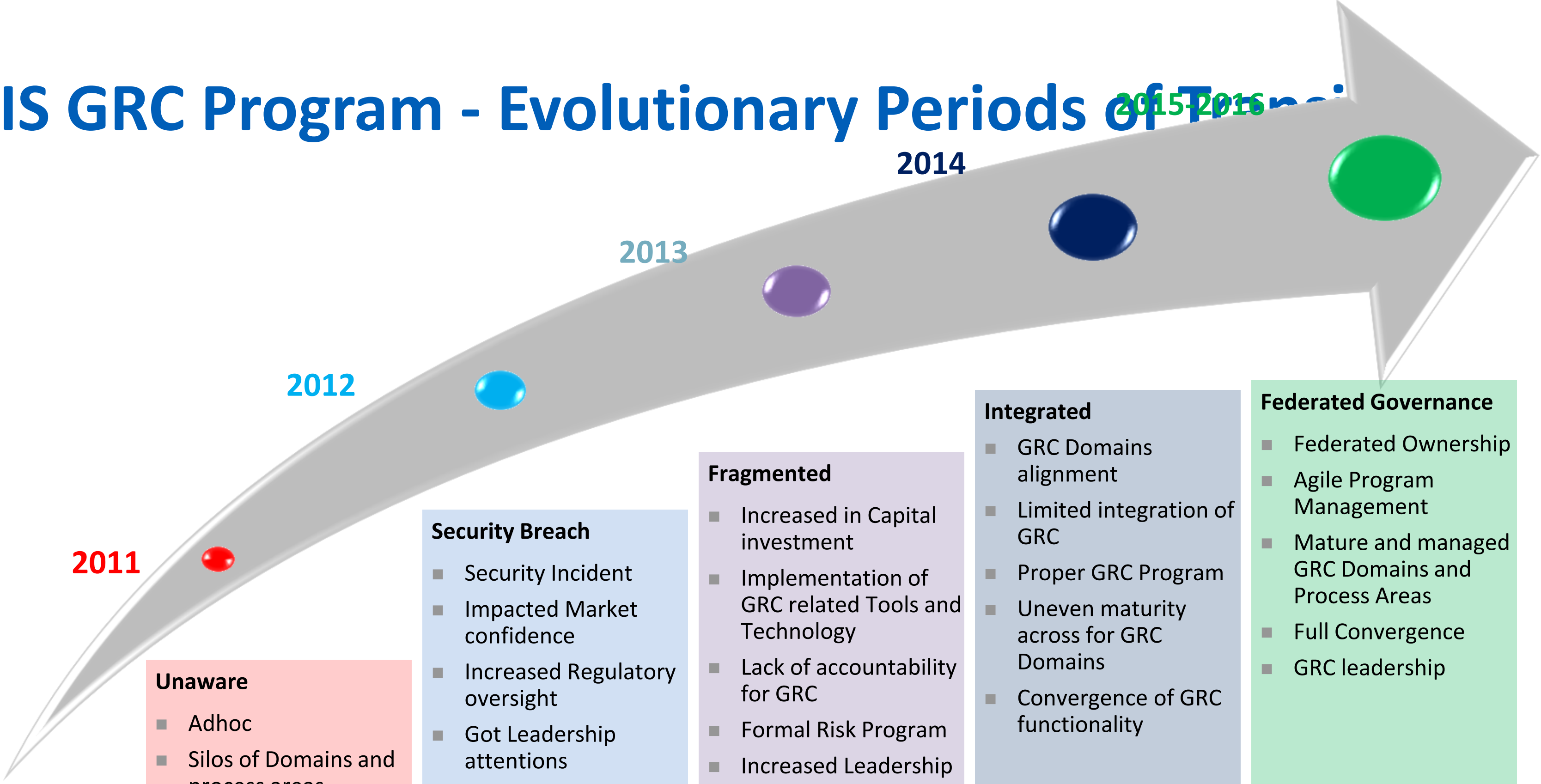
Make The Financial Case & Tell The Strategic Story
Numbers only tell half of the story. Ensure that the case tells both the financial and strategic story.

- What are the people, process and technology elements?

Decide & Commit
Make a formal commitment to move forward and accomplish your goals. Leadership must be committed to both the goals and the approach.

- Determine the path forward
- Measure and assess the net

FIS GRC Program - Evolutionary Periods of Transi



Unaware

- Adhoc
- Silos of Domains and process areas
- Lack of accountability
- Lack of ownership

Security Breach

- Security Incident
- Impacted Market confidence
- Increased Regulatory oversight
- Got Leadership attentions
- Lack of maturity

Fragmented

- Increased in Capital investment
- Implementation of GRC related Tools and Technology
- Lack of accountability for GRC
- Formal Risk Program
- Increased Leadership awareness

Integrated

- GRC Domains alignment
- Limited integration of GRC
- Proper GRC Program
- Uneven maturity across for GRC Domains
- Convergence of GRC functionality

Federated Governance

- Federated Ownership
- Agile Program Management
- Mature and managed GRC Domains and Process Areas
- Full Convergence
- GRC leadership

GRC Program – Journey and Roadmap

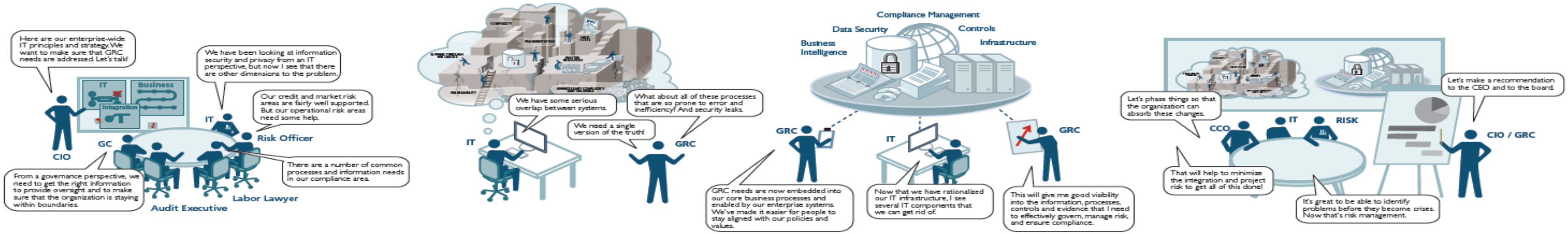
GRC Illustrated

IT Roadmap for GRC

DEVELOPED BY oceg

SPONSORED BY Deloitte. SAP cisco

Information technology projects, priorities, and processes are being increasingly driven by governance, risk management, and compliance (GRC) considerations. But there is a great deal of confusion and uncertainty about how to proceed. The reason: IT strategies, architecture decisions and applications have not approached GRC considerations in a comprehensive and integrated manner. Companies have typically dealt with GRC needs in a fragmented fashion. Moreover, there has been limited attention to automating controls and enabling the information requirements necessary to improve the efficiency and effectiveness of GRC processes and programs. Whether you are considering the GRC impacts on how you manage IT, or wondering how IT can make GRC better, it is necessary to begin with a well established framework. Follow this roadmap to start the journey to align your IT assets with your GRC.


Here are our enterprise-wide IT principles and strategy. We want to make sure that GRC needs are addressed. Let's talk!
IT
Business
Integration
CIO
GC
IT
We have been looking at information security and privacy from an IT perspective, but now I see that there are other dimensions to the problem.
Our credit and market risk areas are fairly well supported. But our operational risk areas need some help.
Risk Officer
There are a number of common processes and information needs in our compliance area.
From a governance perspective, we need to get the right information to provide oversight and to make sure that the organization is staying within boundaries.
Audit Executive
Labor Lawyer
We have some serious overlap between systems.
What about all of these processes that are so prone to error and inefficiency? And security leaks.
We need a single version of the truth!
IT
GRC
Compliance Management
Data Security
Controls
Business Intelligence
Infrastructure
GRC
IT
GRC
GRC needs are now embedded into our core business processes and enabled by our enterprise systems. We've made it easier for people to stay aligned with our policies and values.
Now that we have rationalized our IT infrastructure, I see several IT components that we can get rid of.
This will give me good visibility into the information, processes, controls and evidence that I need to effectively govern, manage risk, and ensure compliance.
Let's phase things so that the organization can absorb these changes.
Let's make a recommendation to the CEO and to the board.
CCO
IT
RISK
CIO / GRC
That will help to minimize the integration and project risk to get all of this done!
It's great to be able to identify problems before they become crises. Now that's risk management.

IT Principles & Strategy

Get GRC practitioners at the table with IT professionals to discuss how IT can support GRC needs:

- **Information needs**
- **Process / transaction needs**
- **Control / monitoring needs**
- **Documentation / system of record needs**

"As-Is" Situation

inventory all of the existing processes and the technology that supports these processes:

- **What do we already have in place?**
- **Who owns and maintains these systems?**
- **Who operates them?**
- **What do they really do?**

"To-Be" Vision

Define, enhance, evolve an enterprise architecture that supports GRC needs. Leverage existing technology investments where possible and look for ways to consolidate technology to serve multiple GRC areas. Integrate technology into core business processes to serve GRC needs.

Priorities, Projects, Budgets & Ownership

GRC and IT professionals work together to define priorities and specific projects to phase into the ultimate vision.

- **Try to start in a specific area and expand**
- **Try to avoid "big bang" solutions**
- **Consider parallel operation of "high stakes" systems**
- **Involve business leaders in prioritization**
- **Assign ownership and accountability**

GRC / IT Maturity Model

1 Unaware

Businesses at this stage do not understand the interdependencies of governance, risk, and compliance and few if any IT resources are allocated to GRC.

- **Ad hoc approach to technology**
- **Little if any technology in place**
- **Information is not available let alone shared**
- **New requirements are not easily addressed**
- **Success is not measured**

2 Fragmented

Businesses at this stage see some of the interdependencies between governance, risk, and compliance, but do not provide a common platform for GRC.

- **Tactical, siloed approach to technology**
- **Silos have systems in place w/o integration**
- **Information is not shared between silos**
- **New requirements within a silo are addressed without considering other areas**
- **Measurement is difficult**

3 Integrated

Businesses at this stage see the need to integrate GRC systems to provide better information and results. A common GRC platform and approach is in place.

- **Unified approach to GRC**
- **Silos are broken down**
- **Information is shared across the enterprise**
- **New requirements are rapidly addressed by a common platform**
- **GRC benefits are measured**

4 Aligned

Businesses at this level align and leverage the GRC platform to realize not only GRC benefits, but also general business benefits such as growth, profitability, and asset utilization.

- **Strategic approach to aligning GRC with the overall business**
- **Silos are nonexistent**
- **Technology is consolidated wherever possible**
- **Business benefits are measured**

5 Optimized Platform

Businesses at this level use a common language and set of metrics to continuously improve the platform year over year.

- **Strategic approach to optimize the GRC platform**
- **GRC technology and non-GRC technology are almost indistinguishable**
- **GRC is "baked into" all business systems**
- **Business benefits are measured and improved year over year**

contact info@oceg.org for comments, reprints or licensing requests

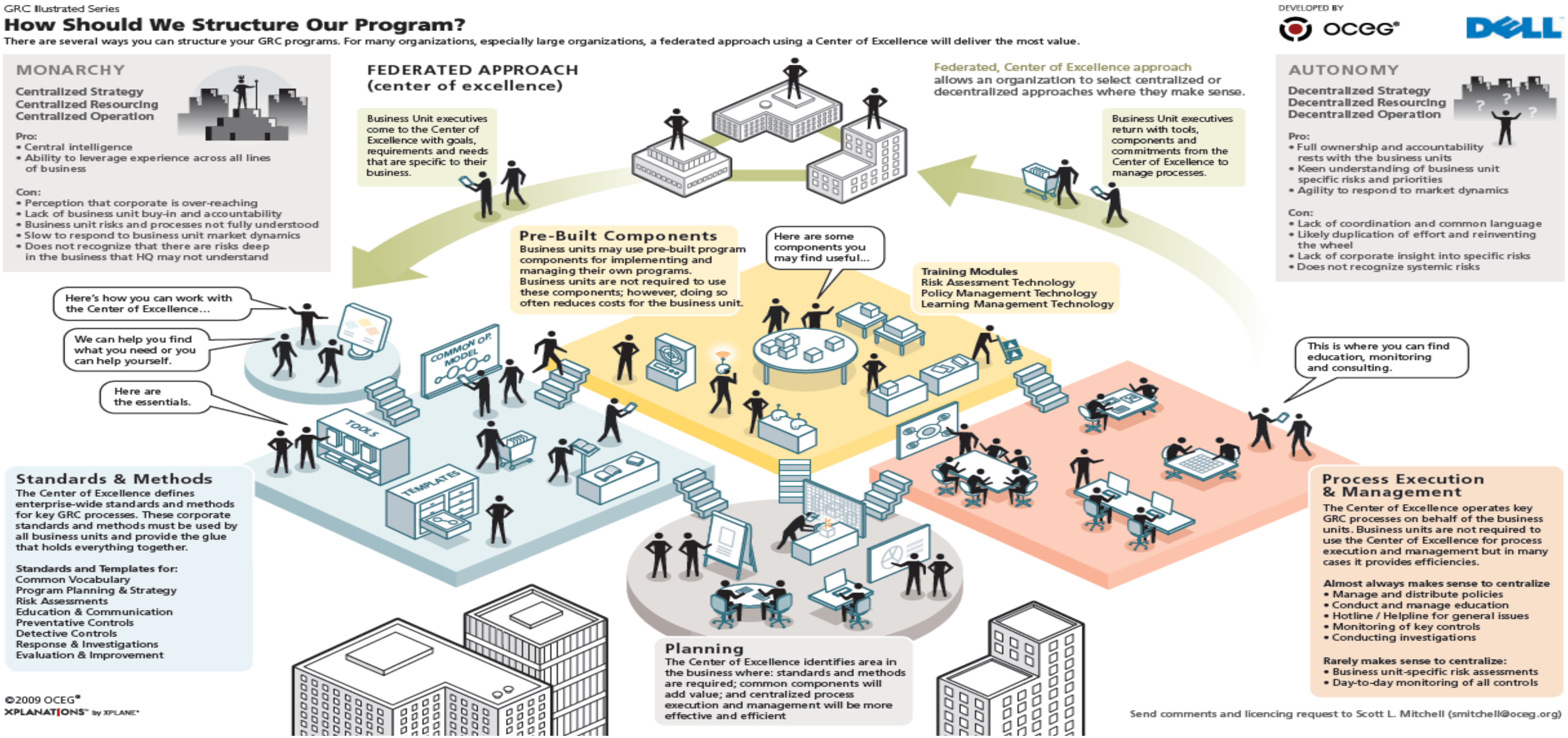
XPLANATIONS™ by XPLANE®

Lesson Learned and Recommendations

- Understand the **Organization** , its **Ecosystem** and **Force of Disruptive Changes.**
- Building internal awareness about emerging **GRC industry best practices like OCEG, UCF, COSO etc.**
- Treat GRC program as an **strategic Initiative** but also be mindful of your immediate business need **IT GRC , Security and Risk GRC** and **Corporate GRC**.
- **GRC Domain Journey** is different from implementation of **tools and technology facilitating GRC.**
  - Use of **Agile Architecture** for GRC tools and technology and **Agile Program Management** for GRC Program
- Ensure to firewall between those responsible for **GRC strategic roadmap** versus **GRC technology roadmap**.
- Think of GRC Technology and Architecture in a **3 Tier approach**:
- Build a **Center of Excellence** or **Federated GRC Steering** committee. A federated Center of Excellence at an operational level managing upward reduce change resistance .

MetricStream
GRC
SUMMIT 2015

GRC Program – Federated Approach



GRC Illustrated Series

How Should We Structure Our Program?

There are several ways you can structure your GRC programs. For many organizations, especially large organizations, a federated approach using a Center of Excellence will deliver the most value.

DEVELOPED BY
oceg® DELL

MONARCHY

Centralized Strategy
Centralized Resourcing
Centralized Operation

Pro:
- Central intelligence
- Ability to leverage experience across all lines of business

Con:
- Perception that corporate is over-reaching
- Lack of business unit buy-in and accountability
- Business unit risks and processes not fully understood
- Slow to respond to business unit market dynamics
- Does not recognize that there are risks deep in the business that HQ may not understand

FEDERATED APPROACH (center of excellence)

Business Unit executives come to the Center of Excellence with goals, requirements and needs that are specific to their business.

Federated, Center of Excellence approach allows an organization to select centralized or decentralized approaches where they make sense.

Business Unit executives return with tools, components and commitments from the Center of Excellence to manage processes.

AUTONOMY

Decentralized Strategy
Decentralized Resourcing
Decentralized Operation

Pro:
- Full ownership and accountability rests with the business units
- Keen understanding of business unit specific risks and priorities
- Agility to respond to market dynamics

Con:
- Lack of coordination and common language
- Likely duplication of effort and reinventing the wheel
- Lack of corporate insight into specific risks
- Does not recognize systemic risks

Pre-Built Components

Business units may use pre-built program components for implementing and managing their own programs. Business units are not required to use these components; however, doing so often reduces costs for the business unit.

Training Modules
Risk Assessment Technology
Policy Management Technology
Learning Management Technology

Here are some components you may find useful...
Here's how you can work with the Center of Excellence...
We can help you find what you need or you can help yourself.
Here are the essentials.
COMMON OP. MODEL
TOOLS
TEMPLATES
This is where you can find education, monitoring and consulting.

Standards & Methods

The Center of Excellence defines enterprise-wide standards and methods for key GRC processes. These corporate standards and methods must be used by all business units and provide the glue that holds everything together.

Standards and Templates for:
Common Vocabulary
Program Planning & Strategy
Risk Assessments
Education & Communication
Preventative Controls
Detective Controls
Response & Investigations
Evaluation & Improvement

Planning

The Center of Excellence identifies area in the business where: standards and methods are required; common components will add value; and centralized process execution and management will be more effective and efficient

Process Execution & Management

The Center of Excellence operates key GRC processes on behalf of the business units. Business units are not required to use the Center of Excellence for process execution and management but in many cases it provides efficiencies.

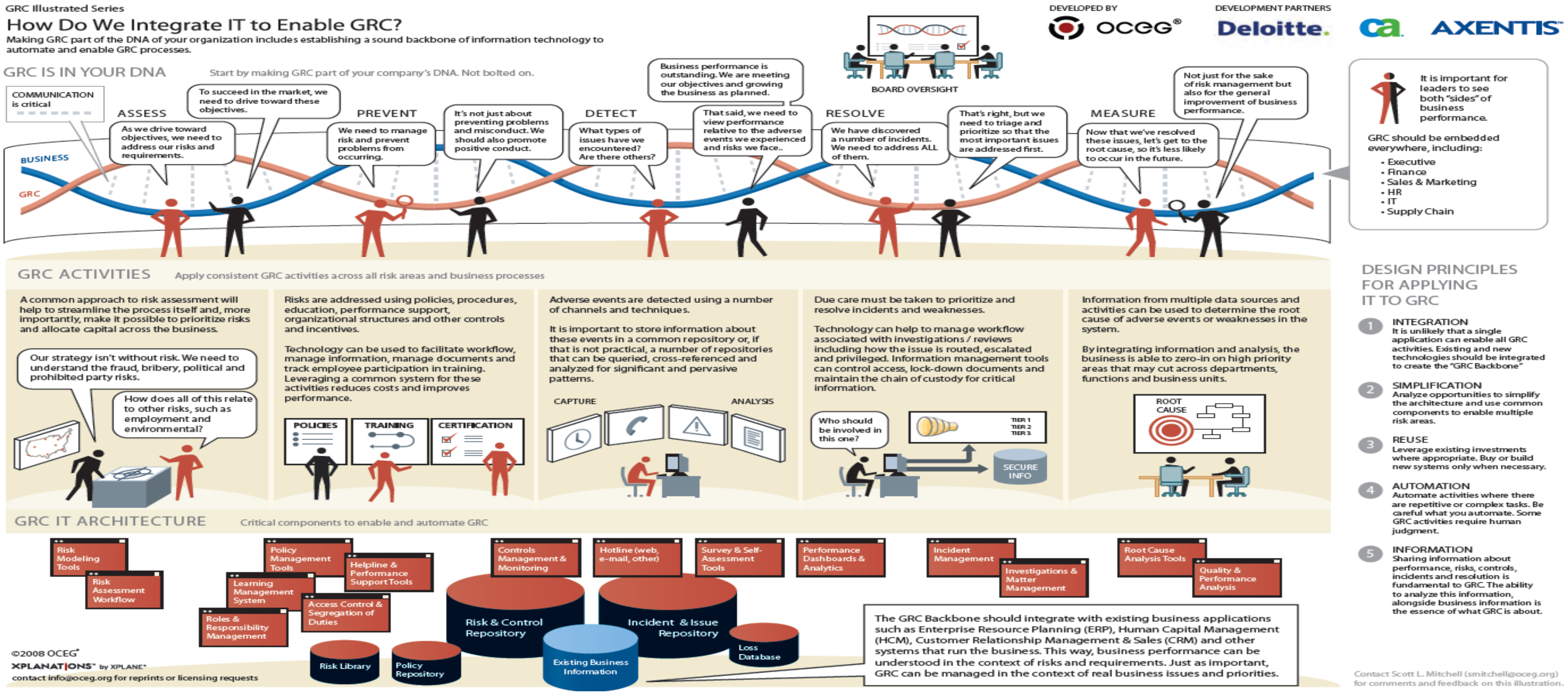
Almost always makes sense to centralize
- Manage and distribute policies
- Conduct and manage education
- Hotline / Helpline for general issues
- Monitoring of key controls
- Conducting investigations

Rarely makes sense to centralize:
- Business unit-specific risk assessments
- Day-to-day monitoring of all controls

Send comments and licencing request to Scott L. Mitchell (smitchell@oceg.org)

GRC Program – IT and Technology

MetricStream
GRC
SUMMIT 2015
May 11-13, 2015



GRC Illustrated Series

How Do We Integrate IT to Enable GRC?

Making GRC part of the DNA of your organization includes establishing a sound backbone of information technology to automate and enable GRC processes.

DEVELOPED BY OCEG®
DEVELOPMENT PARTNERS Deloitte. ca AXENTIS

GRC IS IN YOUR DNA

Start by making GRC part of your company's DNA. Not bolted on.

COMMUNICATION is critical
BUSINESS
GRC
ASSESS
As we drive toward objectives, we need to address our risks and requirements.
To succeed in the market, we need to drive toward these objectives.
PREVENT
We need to manage risk and prevent problems from occurring.
It's not just about preventing problems and misconduct. We should also promote positive conduct.
Business performance is outstanding. We are meeting our objectives and growing the business as planned.
BOARD OVERSIGHT
DETECT
What types of issues have we encountered? Are there others?
That said, we need to view performance relative to the adverse events we experienced and risks we face..
RESOLVE
We have discovered a number of incidents. We need to address ALL of them.
That's right, but we need to triage and prioritize so that the most important issues are addressed first.
MEASURE
Now that we've resolved these issues, let's get to the root cause, so it's less likely to occur in the future.
Not just for the sake of risk management but also for the general improvement of business performance.
It is important for leaders to see both "sides" of business performance.

GRC should be embedded everywhere, including:

- Executive
- Finance
- Sales & Marketing
- HR
- IT
- Supply Chain

GRC ACTIVITIES

Apply consistent GRC activities across all risk areas and business processes

A common approach to risk assessment will help to streamline the process itself and, more importantly, make it possible to prioritize risks and allocate capital across the business.

Our strategy isn't without risk. We need to understand the fraud, bribery, political and prohibited party risks.
How does all of this relate to other risks, such as employment and environmental?

Risks are addressed using policies, procedures, education, performance support, organizational structures and other controls and incentives.

Technology can be used to facilitate workflow, manage information, manage documents and track employee participation in training. Leveraging a common system for these activities reduces costs and improves performance.

Adverse events are detected using a number of channels and techniques.

It is important to store information about these events in a common repository or, if that is not practical, a number of repositories that can be queried, cross-referenced and analyzed for significant and pervasive patterns.

Due care must be taken to prioritize and resolve incidents and weaknesses.

Technology can help to manage workflow associated with investigations / reviews including how the issue is routed, escalated and privileged. Information management tools can control access, lock-down documents and maintain the chain of custody for critical information.

Information from multiple data sources and activities can be used to determine the root cause of adverse events or weaknesses in the system.

By integrating information and analysis, the business is able to zero-in on high priority areas that may cut across departments, functions and business units.

GRC IT ARCHITECTURE

Critical components to enable and automate GRC

Risk Modeling Tools
Risk Assessment Workflow
Policy Management Tools
Helpline & Performance Support Tools
Learning Management System
Access Control & Segregation of Duties
Roles & Responsibility Management
Controls Management & Monitoring
Hotline (web, e-mail, other)
Survey & Self-Assessment Tools
Performance Dashboards & Analytics
Incident Management
Investigations & Matter Management
Root Cause Analysis Tools
Quality & Performance Analysis
Risk & Control Repository
Incident & Issue Repository
Existing Business Information
Loss Database
Risk Library
Policy Repository

The GRC Backbone should integrate with existing business applications such as Enterprise Resource Planning (ERP), Human Capital Management (HCM), Customer Relationship Management & Sales (CRM) and other systems that run the business. This way, business performance can be understood in the context of risks and requirements. Just as important, GRC can be managed in the context of real business issues and priorities.

DESIGN PRINCIPLES FOR APPLYING IT TO GRC

1. **INTEGRATION** It is unlikely that a single application can enable all GRC activities. Existing and new technologies should be integrated to create the "GRC Backbone"
2. **SIMPLIFICATION** Analyze opportunities to simplify the architecture and use common components to enable multiple risk areas.
3. **REUSE** Leverage existing investments where appropriate. Buy or build new systems only when necessary.
4. **AUTOMATION** Automate activities where there are repetitive or complex tasks. Be careful what you automate. Some GRC activities require human judgment.
5. **INFORMATION** Sharing information about performance, risks, controls, incidents and resolution is fundamental to GRC. The ability to analyze this information, alongside business information is the essence of what GRC is about.

XPLANATIONS™ by XPLANE®
contact info@oceg.org for reprints or licensing requests

Contact Scott L. Mitchell (smitchell@oceg.org) for comments and feedback on this illustration.

MetricStream
GRC
SUMMIT 2015
May 11-13, 2015
ARLINGTON, VA
WASHINGTON, DC AREA

QUESTIONS AND DISCUSSIONS

2015 - Case Study