# Agenda

<table>
<thead>
<tr>
<th>Session</th>
<th>Speaker</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Mark Gibbons</td>
<td>12:00 – 12:05</td>
</tr>
<tr>
<td>Governance, Risk and Compliance Overview</td>
<td>Mark Gibbons</td>
<td>12:05 – 12:10</td>
</tr>
<tr>
<td>Enterprise Risk Management</td>
<td>Jason Plummer</td>
<td>12:10 – 12:40</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>Ron Brown</td>
<td>12:40 – 01:10</td>
</tr>
<tr>
<td>Integrated Compliance</td>
<td>Mark Gibbons</td>
<td>01:10 – 01:20</td>
</tr>
<tr>
<td>Conflict Minerals</td>
<td>Molly Tarin</td>
<td>01:20 – 01:35</td>
</tr>
<tr>
<td>GRC Technologies</td>
<td>Brian Behan</td>
<td>01:35 – 01:50</td>
</tr>
<tr>
<td>Questions &amp; Answers</td>
<td>Team</td>
<td>01:50 – 02:00</td>
</tr>
</tbody>
</table>
Governance, Risk & Compliance overview

Learning Objectives

• Provide high level overview of several key areas of Governance, Risk and Compliance
• Provide an update on trends and hot topics
• Discuss the role of Internal Audit related to these areas
• Suggest ideas on how to audit
• Share examples
Governance, Risk & Compliance (GRC) Overview – Definition

GRC is the term covering an organization's approach across these three areas:

**Risk Management**
Ability to identify, measure, prioritize, and mitigate areas of risk (financial, operational, IT, brand or reputation related risk) in the business through proactive risk management process

**Functionalities:** Risk Analysis, Risk Assessments, ERM Dashboards

**Compliance**
Ability to manage compliance at a lower cost through a streamlined process to make it repeatable and sustainable

**Functionalities:** Process and Risk Documentation, Control Management, Effectiveness of Control Analysis, Disclosure and Certification, Loss & Incident Database

**Corporate Governance**
Ability to define and communicate corporate control, key policies, enterprise risk management, regulatory and compliance management, and oversight, and evaluate business performance through balanced scorecards, risk scorecards and operational dashboards

**Functionalities:** Internal Audit, Policy & Procedure Management, Board & Entity Management, Reporting
Governance, Risk & Compliance Overview

Role of Internal Audit in Governance, Risk and Compliance

Definition of Internal Auditing

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
Governance, Risk & Compliance Overview

Role of Internal Audit in Governance, Risk and Compliance

• Expectation that Internal Audit understands respective areas and are competent to evaluate them

• Provide insight to leading trends and practices and provide value added advice and comments

Observation:

• IIA Standards expect that Audit Groups either develop competencies or use external resources (1210 - Proficiency, also 1210.A1 and 1210.C1)

• Many organizations don’t have or can’t afford to develop internal competencies/resources in some diverse areas of risk

• Look to Subject Matter Specialist to assist in the evaluation

• Many companies continue to engage third parties such as accounting firms to assist with their internal audit functions in specialty areas
Governance, Risk & Compliance

How We Look at GRC

- Governance
- Risk
- Compliance
- ERM
- BCM
- Ethics and Compliance
- Dealing with Regulation
- Integrated Compliance
- Pre-IPO Compliance
- Other Compliance Services (ie Sustainability, Conflict Minerals)
- GRC Technology
**Discussion items**

- Typical Challenges to Overcome with ERM
- Three Lines of Defense
- Internal Audit’s Role
- Assessing Risk Management Capabilities
**Typical challenges to overcome with ERM**

- The Board’s role in ERM becomes increasingly challenging as expectations for their engagement increase.
- Leadership doesn’t buy in to a formal ERM process because “enterprise risk is handled by management as part of their day-to-day responsibilities.”
- When implemented, ERM tends to be bureaucratic and an annual event that is not well integrated with existing strategic planning and other business processes.
- Enterprise risk assessments are often superficial and don’t highlight the real risks and their interconnections.
- Risks are identified and managed inconsistently within silos – organizational interdependencies are not fully understood.

**To overcome these challenges:**
- **Align ERM with existing business activities**
- **Provide periodic reporting that is tailored and brings value to the audience**
3 Lines of defense

An example organizations implement three distinct lines of defense into their Combined Assurance programs.....
Internal audit’s role

Roles internal audit may not be in the best position to undertake

- Assuming responsibility for risk management
- Making decisions on risk responses
- Setting the risk appetite

Potential internal audit roles

- Championing establishment of ERM
- Facilitating the identification & evaluation of risks
- Coordinating ERM activities

Core internal audit roles in regard to ERM

- Evaluating risk management processes
- Reviewing the management of key risks
- Providing a point of view on key risks and risk management
Assessing risk management capabilities
An approach on how IA can effectively assess ERM

One way IA can effectively assess the Organization’s ERM capabilities is by utilizing a five stage maturity model framework – “Initial, Repeatable, Defined, Managed, and Optimized” and provide a current state assessment of its ERM foundation and attributes.

**ERM Foundational Elements**

- Governance and Culture
- Process and People
- Tools and Technology

**ERM Attributes**

- Organization and Governance Structure
- Value and Incentives
- Risk Management Process
- Risk Analytics, Infrastructure and Resources
**ERM Objectives**
Start by ensuring that key stakeholders are aligned to objectives

- **Governance**
  - Enhance communication to Senior Management and the BOD
    - *Existing threats require assessment and attention*

- **Reputation**
  - Protect the brand & shareholder value
    - *Integrated assessment activities*
    - *Emerging risk discussion*
    - *Sustainability and risk culture considered*

- **Strategic**
  - Improve the balance between growth, risk & return
    - *Optimize risk management, return on investments and business growth*
    - *Intelligent strategic decisions account for risk*

- **Operational**
  - Align the company’s risk appetite with business activities
    - *Opportunistic and seeking measurable benefit*
    - *Risk monitoring may provide an early warning system on real time basis*

---

**Technology**

*Technology* – Supports objectives, creating process efficiency and more effective data management and reporting.
Is ERM considered during strategic planning

- Perform Analysis
- Formulate Strategies
- Develop Strategic Plan
- Execute Initiatives
- Monitor
- Report

- Assess enterprise risk
- Evaluate risk appetite
- Assign risk ownership
- Continuously assess & refine risks
- Deliver valued risk reporting
Consider whether reporting provides value to the business AND addresses risk management needs

Department

Organizational Unit

Executive
Questions

Contact:
Jason D Plummer

PwC | Director, Enterprise Risk Management
Office: 410-659-3406
Email: Jason.D.Plummer@us.pwc.com
Business interruption risks are increasing

Threats have accelerated and are trending to increase:

- Natural disasters (Sandy, Japan Tsunami, Mid-West Tornadoes,
- Man-made disruptions (Cyber, Crime, Poor Economies, Technology Dependence, Environmental damages)
- Biological / geo-political events (Food/Water Contamination, Civil unrest, poverty)
Vulnerabilities are more exposed due to change

Business continuity management functions should consider:

• Increased business process automation
• Financial distress
• Workforce reductions
• Business combinations and divestitures,
• Level of reliance on outsourcing
• Highly efficient and vulnerable supply chains
• Increased regulation
• General risk management awareness that links continuity planning to operational resiliency
Definitions

Business Continuity Management (BCM) – A risk-based approach and process to identify, prepare for, plan, respond to, and recover from a major disruption where acceptable levels of risk have been exceeded.

Business Resilience (BR) – Managing enough risk to sustain operations at an acceptable level in the event of business interruptions.

Disaster Recovery (DR) – The processes and steps needed to recover from a major disruption (mainly technology services).
BCM is a core risk management capability

- BCM is one of the ways an organization can respond to risk
- Ratings and compliance agencies (e.g., S&P) consider a company’s business continuity program as part of the risk management culture
- BCM objectives focus on the protection of business critical products and services
Why Audit BCM

BCM has been moving up the corporate risk agenda, often cited as a top risk. Audits of BCM can help determine whether:

- **Public disclosures and contractual / regulatory compliance** related to the organization’s business continuity risk management are accurate
- The company has identified their **business interruption risks** and quantified the potential impact
- The company has developed **resiliency and recovery strategies** to address business interruptions
- **Business continuity plans** have been developed for critical business functions to reduce the impact of business disruptions
- **IT’s disaster recovery** efforts are aligned with the business need for recovery and resiliency
- **Sourcing interruption risk** has been reduced
- Crisis management, business continuity and IT disaster recovery **programs are tested and adjusted as the organization changes**
Audit BCM assessment value

Providing insight to leadership about whether:

- The organization effectively addresses relevant business interruption risks
- The organization uses business continuity planning effectively as part of its overall enterprise risk management approach
- Opportunities exist to become more competitive using business continuity and service resilience
BCM regulatory drivers and standards

- Sarbanes-Oxley
- FFIEC
- SEC, NASD
- British Standards
- FDA, OSHA
- Graham Leach Bliley
- FERC, NERC
- Private Sector Preparedness Act (PS-Prep)
- HIPAA / HITECH
- NIST
- ASIS Standard
- ISO Standards
- G30
- BASEL Accord
- State Insurance Dept., NAIC
- Dodd-Frank
Providing Audit with Insight into the Characteristics of a leading BCM Program

- Oversight and Ownership
- Planning and Deployment
- Exercise / Testing
- Training and Awareness

PwC Business Continuity Management
There are no specific detailed ‘audit’ standards for business continuity outside of the financial services industry. However, there are a variety of business continuity standards and guidance that can be incorporated into an Internal Audit business continuity management assessment. These include:

- PS-Prep standards (NFPA 1600, ASIS SPC.1-2009, BS 25999:2-2007)
- IIA’s Global Technology Guidance on Business Continuity Management (GTAG 10)
- ISO 22301

PwC utilizes an assessment approach that tailors this guidance into a tailored audit program. We perform the assessment using business continuity consultants who are part of our larger Governance, Risk and Compliance practice.
Questions

Contact:
Ron Brown

PwC | Director Business Continuity Management
Office: 703-918-3249 | Mobile: 703-930-4634
Email: ron.brown@us.pwc.com
Integrated compliance overview
# Complex and evolving compliance landscape

<table>
<thead>
<tr>
<th>Regulatory Agencies</th>
<th>SEC</th>
<th>OSHA</th>
<th>FERC</th>
<th>FDA</th>
<th>NERC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Requirements</td>
<td>PCI</td>
<td>HIPAA</td>
<td>FISMA</td>
<td>FCPA</td>
<td>GLBA</td>
</tr>
<tr>
<td>Leading Practices and Frameworks</td>
<td>ISO</td>
<td>COBIT</td>
<td>COSO</td>
<td>NIST</td>
<td></td>
</tr>
<tr>
<td>Organizational Requirements</td>
<td>Customer</td>
<td>Operational Objectives</td>
<td>Vendor</td>
<td>SSAE 16</td>
<td></td>
</tr>
</tbody>
</table>
**Integrated compliance**

**Integrated Compliance** helps companies consolidate divergent compliance requirements, eliminate duplicative controls and reduce compliance effort and risk by combining similar controls from disparate requirements into one consolidated view.

This approach increases the efficiency and effectiveness of compliance functions by creating a centrally managed, consolidated controls framework which can be sustainably monitored, measured, and adapted to the changing control environment.
Integrated compliance

Example Approach:

- **Assess** the company’s existing compliance landscape (e.g., SOX, PCI, HIPAA, HISNA, ISO, etc; and sector specific regulations).

- **Rationalize** compliance controls across all the compliance requirements.

- **Develop/Implement** a streamlined and consolidated controls framework.

- **Establish** a monitoring program to test controls and an assessment mechanism to ensure framework is up to date.
Integrated compliance

Potential Benefits:

- Reduction of duplicative controls
- Reduced management monitoring effort as a result of compliance integration
- Reduced management time devoted to assisting the auditors and more time for value adding activities
- Improved awareness of the control environment and expectations with regard to compliance
- Accelerated audit preparation and design evaluation phases
- Reduced audit effort to monitor/test compliance in turn freeing up time for operational audits
Integrated compliance

Potential Triggers:

- New highly regulated or complex compliance environment
- Repetitive compliance failures
- Sense of being over audited
- Decentralized compliance function and roles
- Mergers, acquisitions and divestitures
- Service provider organizations with multiple clients
Questions

Contact:
Mark Gibbons

PwC | Director
Office: 412-355-7719 | Mobile: 724-612-6198
Email: mark.d.gibbons@us.pwc.com
Conflict Minerals
(Dodd-Frank Section 1502)
Understanding the final rules
**Dodd-Frank Section 1502 requires companies to determine whether their minerals are conflict free**

**What are “conflict minerals”?**
- Conflict minerals, as determined by the U.S. Secretary of State, may finance conflict in the Democratic Republic of the Congo (DRC) or adjoining countries. The “3TG” metals are:
  - Tantalum
  - Tin
  - Tungsten
  - Gold

**Who is in scope of Section 1502?**
- Any company that files periodic reports under Sections 13(a) or 15(d) of the Exchange Act who:
  - Manufactures or contracts to manufacture products, and
  - Conflict minerals are necessary* to the functionality or production of those products

*No de minimis exception associated with “necessary”

**What is required of companies?**
- Examine products to determine whether and to what extent Section 1502 applies
- Develop and conduct reasonable country of origin inquiry (RCOI) and due diligence
- Acquire independent audit (if needed)
- Comply with disclosure requirements

**When does compliance begin?**
- First filings are due May 31, 2014 for calendar year 2013.
## Who is impacted

The SEC estimates approximately 6,000 issuers and 275,000 suppliers will be impacted

<table>
<thead>
<tr>
<th>Examples</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEC issuers directly subject to Section 1502</strong></td>
<td>• Any company that either manufactures or has influence on the specifications of products that include these metals, e.g.:</td>
</tr>
<tr>
<td></td>
<td>- High-tech</td>
</tr>
<tr>
<td></td>
<td>- Autos and auto components</td>
</tr>
<tr>
<td></td>
<td>- Aerospace and defense</td>
</tr>
<tr>
<td></td>
<td>- Industrials</td>
</tr>
<tr>
<td></td>
<td>- Medical devices (electronic components)</td>
</tr>
<tr>
<td></td>
<td>- Pharmaceuticals (packaging)</td>
</tr>
<tr>
<td></td>
<td>- Jewelry</td>
</tr>
<tr>
<td></td>
<td>- Food products (packaging)</td>
</tr>
<tr>
<td></td>
<td>- Consumer products</td>
</tr>
<tr>
<td><strong>May experience indirect exposure to final rules</strong></td>
<td>• Suppliers responding to customer requests</td>
</tr>
<tr>
<td></td>
<td>• Mining companies to support implementation of on-the-ground certification mechanisms</td>
</tr>
<tr>
<td><strong>Scoped out of final rules</strong></td>
<td>• Retailers who have no significant level of influence over product specification</td>
</tr>
<tr>
<td></td>
<td>• Mining companies who have only extraction activities and no manufacturing activities</td>
</tr>
<tr>
<td></td>
<td>• Scrap or recycled materials</td>
</tr>
<tr>
<td></td>
<td>• Metals used (e.g., catalyst, tools) that are not contained in the final product</td>
</tr>
</tbody>
</table>
Managing compliance requires thoughtful preparation to create a sustainable process

Example of what companies should consider doing:

<table>
<thead>
<tr>
<th>Step</th>
<th>Establish strong management systems</th>
<th>Assess risk in the supply chain</th>
<th>Implement response to identified risks</th>
<th>Report</th>
</tr>
</thead>
</table>
| Key tasks | • Adopt a company policy  
• Establish project governance  
• Identify impacted products and components  
• Develop RCOI and due diligence strategy  
• Implement tools to assist in information gathering | • Identify suppliers  
• Map the supply chain  
• Conduct RCOI  
• Review responses to identify and assess risks in the supply chain  
• Conduct additional due diligence if needed | • Design and implement controls around vendor management and procurement procedures  
• Test and monitor effectiveness of controls  
• Address new risks or changing circumstances as needed | • Engage independent third-party audit if needed  
• Meet reporting requirements per the final rules  
• Respond to information requests from customers |

• Program/project/change management  
• Technology and data management
What are some of the key challenges to compliance

- Determine how Section 1502 applies to the company
- Understand and manage the complexity of the supply chain
- Develop and conduct an RCOI and, if needed, due diligence process that will meet industry standards and audit requirements
- Understand how to leverage the OECD guidance to implement an effective control framework to prevent and detect conflict minerals
- Manage responding to customer information requests
## How can PwC help

<table>
<thead>
<tr>
<th>Offering</th>
<th>Companies that might benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Conflict Minerals Assessment to assess the readiness of a company to conduct the RCOI/due diligence process and meet compliance requirements</td>
<td>• Those companies who have done little to prepare</td>
</tr>
<tr>
<td>Assessment of a company’s current conflict minerals program against the OECD framework and audit requirements</td>
<td>• Those companies who have already begun to implement the OECD framework and/or begun to conduct due diligence on their supply chain</td>
</tr>
<tr>
<td>Assistance with design, implementation or operation of the conflict minerals program</td>
<td>• Immature or mature companies</td>
</tr>
<tr>
<td>• Those who may have insufficient resources to manage the RCOI and due diligence process</td>
<td></td>
</tr>
<tr>
<td>“Supplier Audit”/Vendor Assessment - third party audits for suppliers /other supply chain players to provide to their customers, including readiness reviews</td>
<td>• Non-OEMs</td>
</tr>
<tr>
<td>• Those with a significant customer base</td>
<td></td>
</tr>
<tr>
<td>Third Party Audit of Conflict Minerals Report, including readiness reviews</td>
<td>• Those companies who believe they will require an audit to be conducted in accordance with the standards.</td>
</tr>
<tr>
<td>• A “readiness assessment” can be conducted to prepare for the audit requirements for the 2013 reporting year</td>
<td></td>
</tr>
</tbody>
</table>
Questions

PwC resources and contacts:

- Visit our website (external): [www.pwc.com/us/conflictminerals](http://www.pwc.com/us/conflictminerals)
- Contacts:
  - conflict.minerals@us.pwc.com
  - Molly Tarin – molly.tarin@us.pwc.com (Risk Assurance, Lake Erie Market Conflict Minerals Champion)
  - Daniel Webster – [daniel.webster@us.pwc.com](mailto:daniel.webster@us.pwc.com) (Industrial Products, Conflict Minerals Champion)
GRC Technologies - Building a business case
Companies have responded to increasing stakeholder and regulatory pressures by forming multiple governance, risk & compliance (GRC) oversight functions, processes and information systems across the organization.
Use of a technology to define, manage and monitor, on a continuous basis, the company’s overall Internal Control Framework.

Use of a technology to define, manage and monitor, on a continuous basis, the company’s overall Compliance & Business processes.

Use of a technology to identify, assess and monitor, on a continuous basis, the company’s overall Enterprise Risk Management processes.

Use of a technology to document, consolidate and centralize the company’s overall Internal Control Framework.

Use of a technology to define, manage and monitor, on a continuous basis, the company’s overall Security Environment.
GRC Technology magic quadrant by Gartner

[Diagram showing the GRC Technology magic quadrant with companies placed in different quadrants based on their ability to execute and completeness of vision.]

Source: Gartner (October 2012)
The Forrester wave: Enterprise governance, risk, and compliance platforms
## GRC Business case – common foundations

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Internal Audit</th>
<th>Internal Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation</td>
<td>Reporting</td>
<td>Control Effectiveness</td>
</tr>
<tr>
<td>Centralization &amp; Shared services</td>
<td>Protect investment</td>
<td>Visibility</td>
</tr>
</tbody>
</table>
Questions

Contact:
Brian Behan

PwC | Manager - Risk Assurance
Office: 412-355-7581 | Mobile: 814-440-8209
Email: brian.behan@us.pwc.com