Coordination between Ethics & Compliance, Internal Audit, and Enterprise Risk Management

David J. Heller
Edison International
Vice President Enterprise Risk Management and General Auditor

Heinz Wustmann
Deloitte
Partner, Risk Advisory

Frankfurt, 27th March 2018, 6th Annual European Compliance & Ethics Institute

Definition and Basics
What does GRC stand for?

Governance
The company’s structures, policies, processes and controls that focus on long-term value through the ethical, equitable, efficient and effective operation of the business.

Risk
The company’s systematic process to identify, assess, manage and monitor both upside and downside risks to the business.

Compliance
The company’s process to demonstrate that its employees and agents adhere to policies and procedures, laws and regulations.

Governance, risk, and compliance should be viewed as related functions, with common activities, best approached in a comprehensive, integrated manner.
Conceptual Approaches
Three Lines of Defense

- **1st Line of Defense**
  - Operational Management
  - Internal Control Measures

- **2nd Line of Defense**
  - Risk Management
  - Internal Controls System
  - Ethics and Compliance
  - Security
  - Safety and Environmental Affairs
  - Quality

- **3rd Line of Defense**
  - Internal Audit

Regulators

1. **Eliminate** | e.g., by exiting relevant market
2. **Minimize** | by reducing the probability of occurrence or the impact
3. **Transfer** | e.g., by signing an insurance contract
4. **Contingency** | by setting up comprehensive contingency plans
5. **Bear** | by accepting the risk

Residual Risk
**Integrated GRC**

*Avoid inconsistencies, redundancies and insufficient communication*

---

**Executive Management**

- Assess, monitor and report enterprise risks to support management decisions
- Assess, monitor and document internal controls over financial reporting
- Re-assess process controls to further optimize ICS

**RMS**

- Assess compliance risks and derive programs to prevent, detect and respond to risks
- Company-wide promotion of compliance principles (e.g. Code of Conduct)

**ICS**

- Assess risks threatening the continuity of business and safety of people
- Develop contingency plans and measures
- Raise awareness for security-critical incidents

**Ethics and Compliance**

- Performance of risk-based process and control audits
- Review of ICS, control and governance systems and processes
- Independent assurance provider

**Safety and Security**

- Audit of financial statements and corporate governance
- Review of the early warning and monitoring system (incl. internal audit)
- Assess financial controls

---

**Option**

**Integrated GRC**

*Structural GRC elements to consider*

---

**Governance & Reporting**

- Policies
- Evaluation of Effectiveness
- Training
- Documentation

**Organization & Infrastructure**

**Taxonomy**

---

2018 Deloitte
Integrated GRC
GRC Ecosystem

|---------------------|-------|----------------|-------------------|------|-----------|------------|-----------------|-----|-----------------------|

Risk Management Applications

- Risk Management
- Compliance
- Auditing
- Information Security
- Service Delivery
- Compliance Management

Lines of Business
- Corporate
- IT

Trends in GRC – Example: Internal Audit
Internal Audit 3.0: Broader Perspective on Internal Audit
Strategic objectives are long-term organizational goals that help to convert a strategy from a broad vision into more specific plans and are supported by identifiable data sources.

Internal and external risks challenge the organization's ability to achieve its strategic goals and objectives.

Observable indicators are qualitative and quantitative parameters to detect changes, track performance, and predict emerging changes related to strategic objectives that are based upon data modules or existing analytic tools.

Thresholds are event triggers that require a further review or action. The action will depend on the type of event, probability and severity of the expected impact.

Monitoring of the indicators to raise alerts and signal to management for further decision making.

Focuses on automation through program identification, process mapping and integration.

Vulnerability Management
Integration with vulnerability scanners can automatically pull vulnerabilities and correlate them to tangible enterprise risks

Policy Management
Automated policy management ensures all updates to policies are easily propagated to all stakeholders, and tied into the enterprise risk register

Risk and Compliance Assessments
Automate risk assessment activities using a homogenized platform that increases efficiency and reduces subjectivity
Definition and Basics
GRC as defined by Analysts

Forrester
“Well-developed GRC programs do more than mitigate risk; they help maximize company performance, providing a holistic view of corporate risk with further insight into areas of under- and overexposure.”
Maximize Business Performance With A World-Class GRC Program, 2014

Gartner
“GRC should be approached as an enterprise-wide initiative that aims at improving governance through better understanding of the impact of risk on business performance and through more-effective compliance.”
Governance, Risk and Compliance, May 2015

OCEG
“A capability and a culture that enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity.”
OCEG GRC Fundamentals

Case Study
Interactive discussion

Cases
1 “Scrap”
2 “Country Risk”
3 “Safety”
Many thanks for your attention!