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.

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

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

Conceptual Approaches
Three Lines of Defense

Governance / Risk / Audit Committee

Senior Management

Operational Management

Internal Control

Risk Management

Internal Controls

Ethics and Compliance

Sustainability

Environmental Affairs

Quality

Internal Audit

First Line of Defense

Second Line of Defense

Third Line of Defense

External Audit

Regulators
Conceptual Approaches
Standard Risk Mitigation Strategies

- **Inherent Risk Exposure**
- **Residual Risk**

### Eliminate**
- e.g., by exiting relevant market

**Minimize**
- e.g., by reducing the probability of occurrence or the impact

**Transfer**
- e.g., by signing an insurance contract

**Contingency**
- by setting up comprehensive contingency plans

**Bear**
- by accepting the 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
  - Assess compliance risks and derive programs to prevent, detect and respond to risks
  - Company-wide promotion of compliance principles (e.g. Code of Conduct)
  - Assess risks threatening the continuity of business and safety of people
  - Develop contingency plans and measures
  - Raise awareness for security-critical incidents
  - Performance of risk-based process and control audits
  - Review of risk, control and governance systems and processes
  - Independent assurance provider
  - Audit of financial statements and corporate governance
  - Review of the early warning and monitoring system (incl. internal audit)
  - Assess financial controls

### Structural GRC elements to consider

- **Governance & Reporting**
  - Policies and procedures
  - Evaluation of effectiveness
  - Training
  - Documentation

- **Organization & Infrastructure**
  - Policies
  - Evaluation of effectiveness

- **Taxonomy**
Integrated GRC
GRC Ecosystem

Trends in GRC – Example: Internal Audit
Internal Audit 3.0: Broader Perspective on Internal Audit

Trends in GRC
Risk Sensing and Strategic Risk Management
Trends in GRC
Focused program automation

1. Identify key programs mature enough in their manual processes to facilitate automation
2. Map manual processes and procedures to the automation tool
3. Establish integrations with all the software across the enterprise

Use Cases

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 ties into the enterprise risk register

Risk and Compliance Assessments
Scanned risk assessment and mapping tools to ensure programs that maximize efficiency and optimize expenditure

Definition and Basics
GRC as defined by Analysts

Forrester
“Well-developed GRC programs do more than mitigate risk; they help companies change our performance, providing a holistic view of corporate risk that further reduces costs across all stakeholders.”
Forrester Business Performance Brief: A World-Class GRC Program, 2018

Gartner
“GRC should be approached as an enterprise-wide initiative that views IT changes in the process through better understanding of the impact of risk on critical performance and through more effective compliance.”
Governance, Risk and Compliance, May 2018

OCEG
“A capability and a culture that enables an organisation 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!