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
Compliance
Risk

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.

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

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

Governing Body / Board / Audit Committee
Senior Management

Regulators
External Audit

Conceptual Approaches
Standard Risk Mitigation Strategies

| “Eliminate” | e.g., by exiting relevant market |
| “Minimize” | 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 |

Residual Risk
Integrated GRC
Avoid inconsistencies, redundancies and insufficient communication
Integrated GRC
GRC Ecosystem

Risk Integration

Risk Management Applications


Functional Leads | Compliance Managers | Legal | Audit | Information Security | Service Leads | Compliance Managers

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.

Strategic drivers / disruptors

1. Define strategic objectives
2. Identify internal and external risks
3. Establish observable indicators
4. Define thresholds
5. Conduct monitoring

Focused program automation

Approach

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 other 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 tied into the enterprise risk register

Risk and Compliance Assessments
Automate risk assessment activities using a homogenized platform that increases efficiency and removes subjectivity

2018 Deloitte
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

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