Definition and Basics
What does GRC stand for?

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

External Audit
Regulators

1st Line of Defense
Senior Management
Risk Management
Internal Controls
Ethics and Compliance
Security
Human Resources
Environmental Affairs
Quality

2nd Line of Defense
Internal Audit

3rd Line of Defense
Governance / Board / Audit Committee
Operational Management
Internal Control Measures

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
**Conceptual Approaches**

**Standard Risk Mitigation Strategies**

- **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**
- **Governance & Reporting**
- **Organization & Infrastructure**
- **Evaluation of Effectiveness**
- **Risk & Compliance**
- **Internal Audit**
- **External Audits**

**Integrated GRC**

Structural GRC elements to consider

- Policies
- Evaluation of Effectiveness
- Training
- Documentation

**Options**

- Governance & Reporting
- Organization & Infrastructure
- Processes
- Evaluation of Effectiveness
- Training
- Documentation

**ABC Ltd.**

 BU B
BU A
BU C

- Policies
- Evaluation of Effectiveness
- Training
- Documentation
Trends in GRC – Example: Internal Audit

Internal Audit 3.0: Broader Perspective on Internal Audit

- Agile IA
  - Execution
    - Sprint Execution
    - Daily Scrum Retrospectives
    - Sprint Review

- High Impact Reporting
  - Interactive reporting
  - Video and audio reporting
  - Dashboard reporting

- Communication channels
  - Robotics process automation
  - Automated quality assurance
  - Management dashboards

- IA tooling
  - Polymath
  - Purple
  - Person

- SMEs

- Resourcing
  - Rotational secondments
  - Guest Auditors

- Points of Insight
  - Real-time Remediation
  - Thematic Root cause
  - Culture Monitor/influencer

- Intelligent risk governance
  - Risk Sensing
  - Cognitive risk anticipation

- Anticipate
  - Advise
  - Design
  - Effectiveness
  - Enhance 3LoD
  - Design in Assurance
  - Assist during change

- Assist
  - Change catalyst
  - SWAT task force

- Assure
  - New technologies
  - Automate
  - Core Assurance
  - Assure 3LoD
  - Assure decision governance
  - Assure behaviours

- Brand
  - Delivery mind-set
  - Discovery

- Brand and stakeholder management

Trends in GRC – Example: Internal Audit

Risk Sensing and Strategic Risk Management

- Strategic objectives
  - Long-term organizational goals
  - Data-driven approach to identify trends and patterns
  - Forecast future risks and opportunities

- Internal and external risks
  - Identify emerging risks
  - Analyze potential impacts

- Observable indicators
  - Qualitative and quantitative data
  - Real-time monitoring
  - Early warning signals

- Thresholds
  - Event triggers requiring action
  - Impact assessment

- Monitoring and alerting
  - Continuous feedback loop
  - Decision support system
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 other solutions 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

Definition and Basics
GRC as defined by Analysts

- "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.”
  - Forrester, "World-Class GRC: A Business Imperative," 2014
- "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.”
- "A capability and a culture that enables an organization to reliably achieve objectives while addressing challenges and acting with integrity.”
  - OCEG, "GRC Fundamentals"

Case Study
Interactive discussion

Cases
1. "Scrap"
2. "Country Risk"
3. "Safety"
Many thanks for your attention!