


**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.

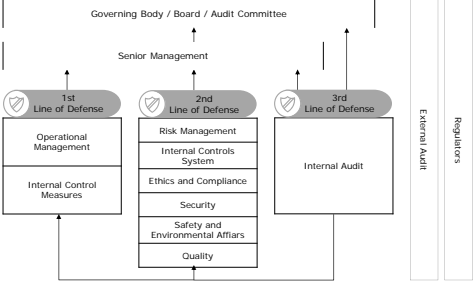
Risk
The company's systematic process to identify, assess, manage and monitor both upside and downside risks to the business.

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.

2018 Deloitte 2

Conceptual Approaches
Three Lines of Defense



Governing Body / Board / Audit Committee

Senior Management

1st Line of Defense
Operational Management
Internal Control Measures

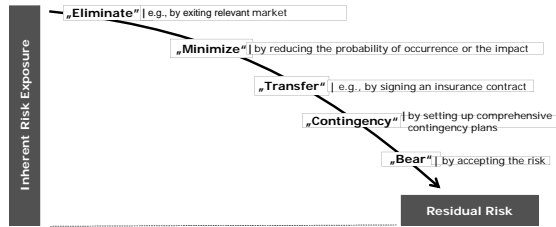
2nd Line of Defense
Risk Management
Internal Controls System
Ethics and Compliance
Security
Safety and Environmental Affairs
Quality

3rd Line of Defense
Internal Audit

External Audit
Regulators

2018 Deloitte 3

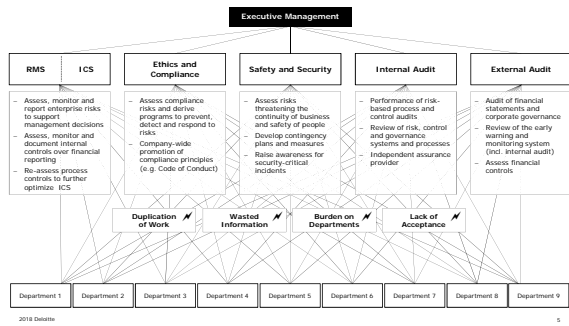
Conceptual Approaches Standard Risk Mitigation Strategies



2018 Deloitte

4

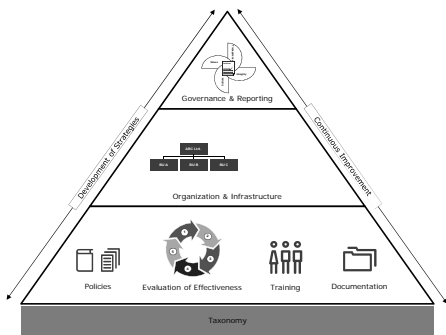
Integrated GRC Avoid inconsistencies, redundancies and insufficient communication



2018 Deloitte

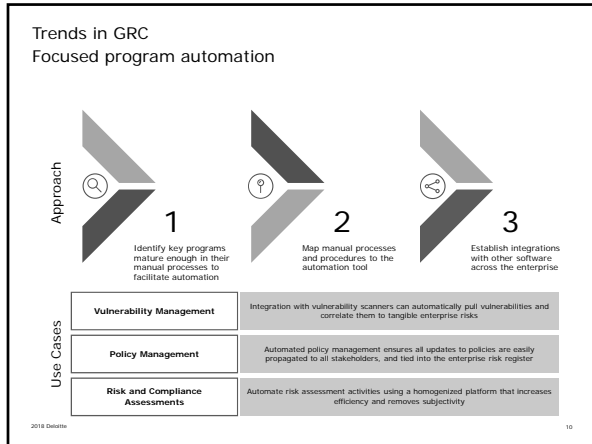
5

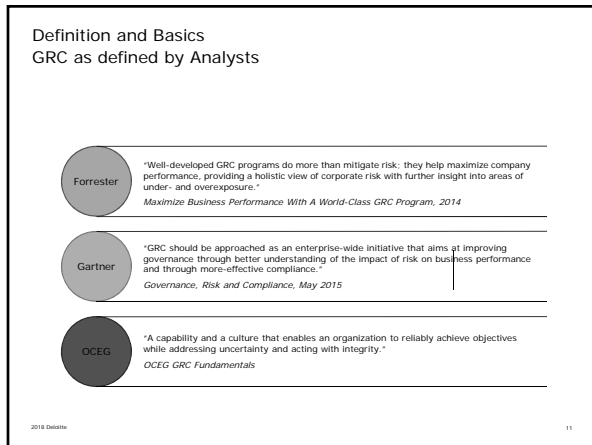
Integrated GRC Structural GRC elements to consider

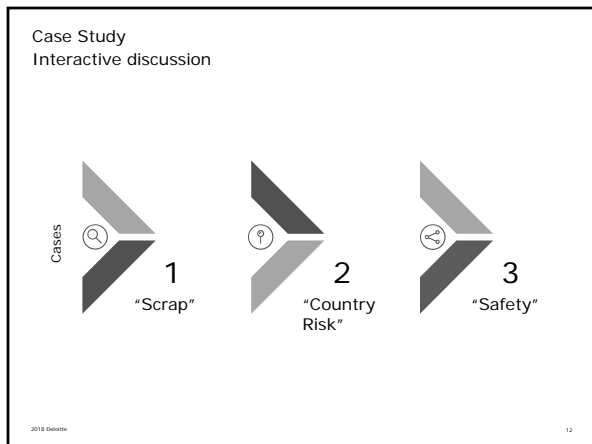


2018 Deloitte

6







Many thanks for your attention!

2018 Deltatix

13
