Deloitte.

Digital:
Governance Risk and Compliance

Vladimir Remyga, CISA, CISSP, CGEIT, CRISC, PRINCE 2

November, 2019

Agenda

- Introduction
- GRC benefits
- GRC scope covered
- Main GRC vendors
- GRC challenges

© 2019 Deloitte Touche Tohmatsu Limited.

Introduction

© 2019 Deloitte Touche Tohmatsu Limited.

GRC : What is it?

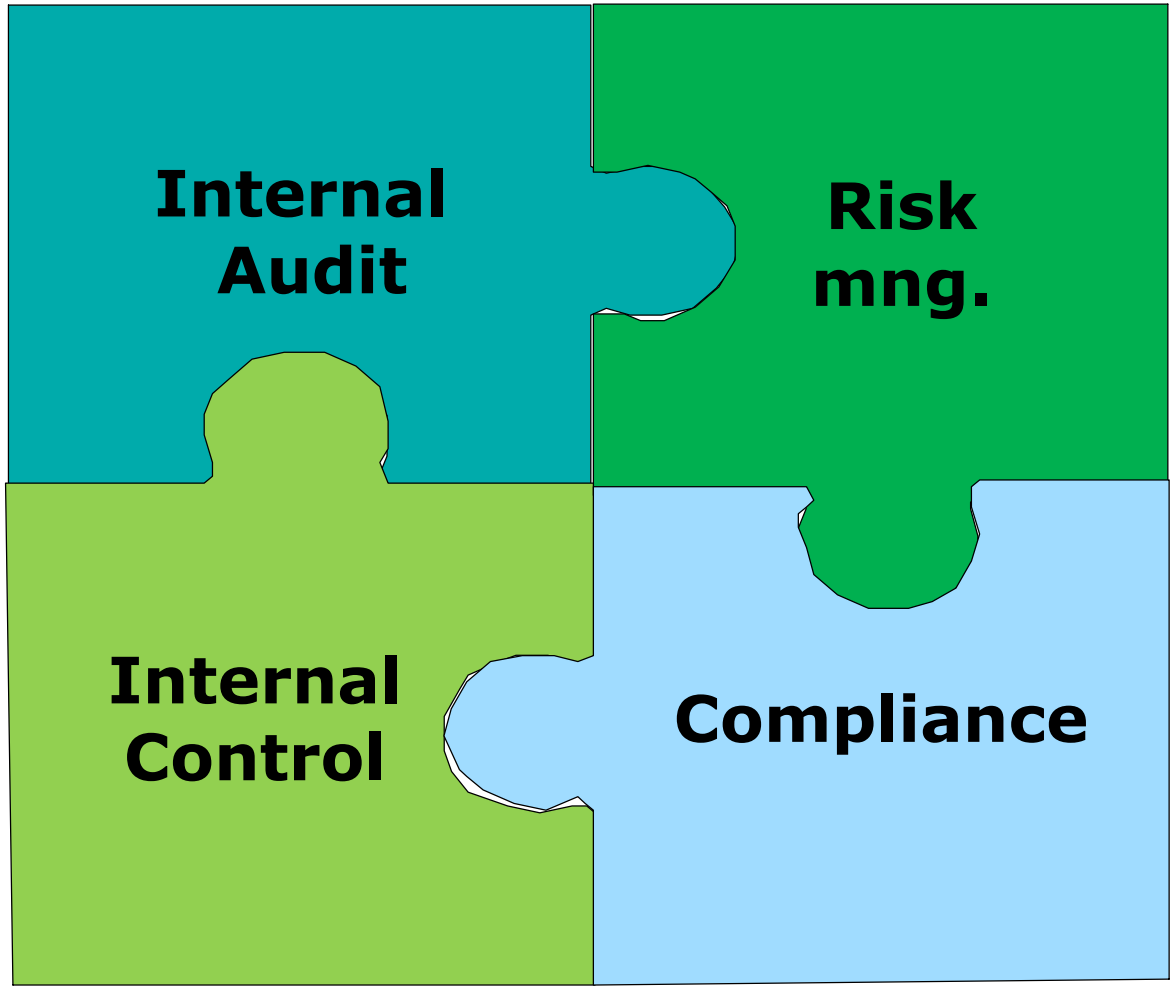
Integrated software solution for three key areas:
Corporate Governance, Enterprise Risk Management and Compliance

▸Internal control:
management repositories, questionnaires, testing, monitoring of action plans, reporting

▸ Risk Management:
risk repository, risk assessment, risk maps, action plans, data collection and incident tracking, reporting

▸Compliance:
stated requirements repository, assess the state of compliance, non-compliance risk assessment, corrective actions planning, monitoring, reporting

▸Internal audit:
management of work programs, planning, monitoring missions, monitoring recommendations



© 2019 Deloitte Touche Tohmatsu Limited.

GRC benefits

© 2019 Deloitte Touche Tohmatsu Limited.

Governance Risk and Compliance

Main stakes and benefits

Formalize, homogenize and sustain the knowledge database in a unique solution

Support the alignment of audit and internal control functions by sharing the frameworks and providing transversal analysis

Consolidate the data in real time

Senior Management Expectations

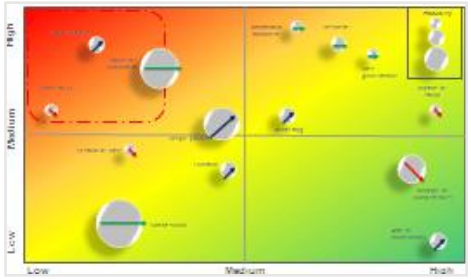
Secure and trace the data in a reliable and centralized manner

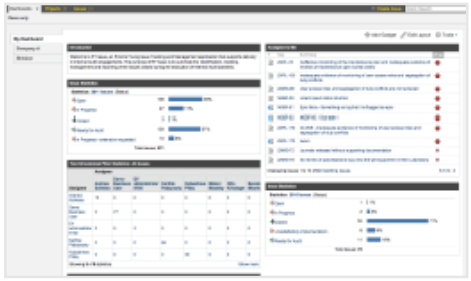
Spend less time consolidating data and more time analyzing

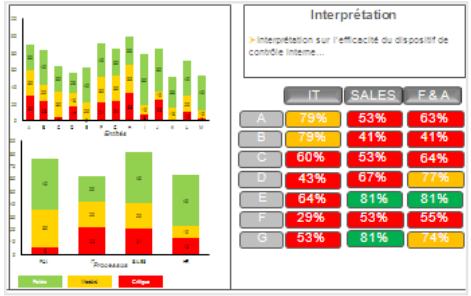
Facilitate the recommendations and action plan follow-up

Facilitate the comparisons multiannual of control management and risk exposure

Optimize the sharing of good practices, risk management & controls







© 2019 Deloitte Touche Tohmatsu Limited.

GRC scope covered

© 2019 Deloitte Touche Tohmatsu Limited.

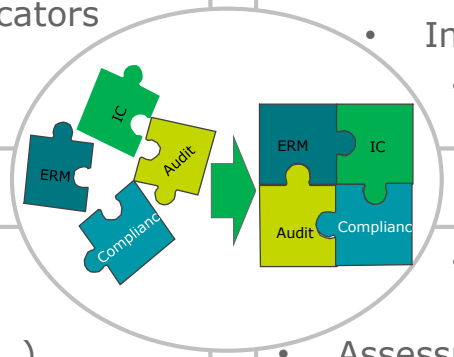
GRC : Scope covered by such solutions

Internal control

- Formalization / management of framework
- Questionnaire of self-assessment, documentation, testing, indicators
- Action plan follow-up
- Analysis and reporting

Risk management
(quantitative or qualitative)

- Risk identification (central / local)
- Risk assessment (risk cartography)
- Risk treatment (action plan)
  - Incident collect and follow-up
    - Analysis and reporting



- Audit program and planning management
- Audit missions (workpaper, …)
- Recommendations and action plan follow-up
- Analysis and reporting

Internal Audit

- Formalization and sharing of regulations framework
- Assessment of regulation compliance
- Alert management and market information
- Analysis and reporting

Compliance

BCP | **Quality** | **HSE / sustainability**

Imagine this as a real-time scenario:

Your phone just received an alert. You click into the corporate app, use an iris scan and code authentication to gain secure mobile access, and immediately receive a recommendation to "update a specific section of the company's T&E policy with a new rule and release it to employees in the whole country's divisions before Friday."

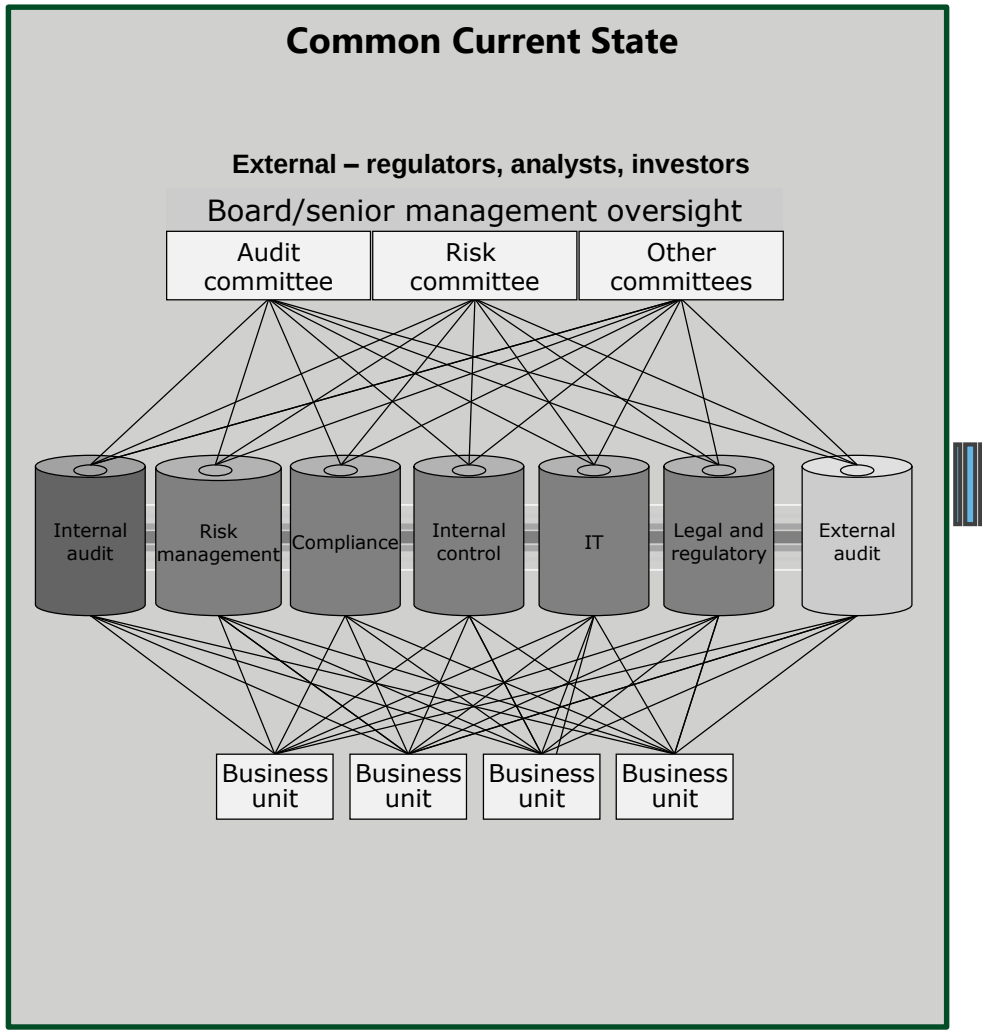
There's a dashboard on your screen, and a flashing node indicates a new series of anti-bribery rules were released, effective six months from now. The red color indicates that control weaknesses noted in that region for areas designed to mitigate risk of Foreign Corrupt Practices Act (FCPA) violations. Your behavioral science analysis tool homes in on conduct pattern anomalies on a particular sales team. Swiping left shows related news stories-examples of other companies that have been fined for similar infractions dealing with like counterparties.
From the time you got the alert, you haven't moved from your chair. But moments later, now that you're informed, you have a plan to act.

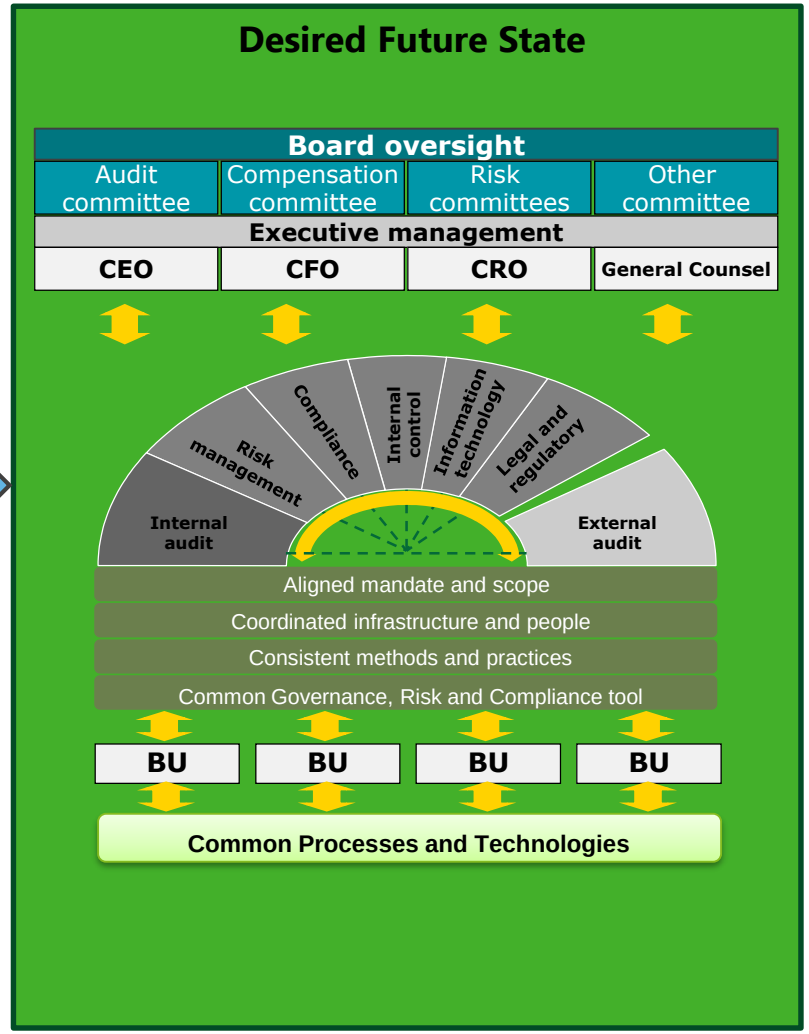
© 2019 Deloitte Touche Tohmatsu Limited.

GRC : Convergence of Risk Functions

Transformation from siloed into integrated approach

- Most companies have take a very siloed approach to risk management which creates multiple redundancies and extensive inconsistency in how risks are assessed and managed.
- An effective GRC program will aggregate the evaluation of risks and controls to create a convergence of Risk Management activities which results in greater consistency and efficiency across the GRC program and the company as a whole.





© 2019 Deloitte Touche Tohmatsu Limited.

Main GRC vendors

© 2019 Deloitte Touche Tohmatsu Limited.

Main GRC solutions offering

…and the list is not complete

© 2019 Deloitte Touche Tohmatsu Limited.

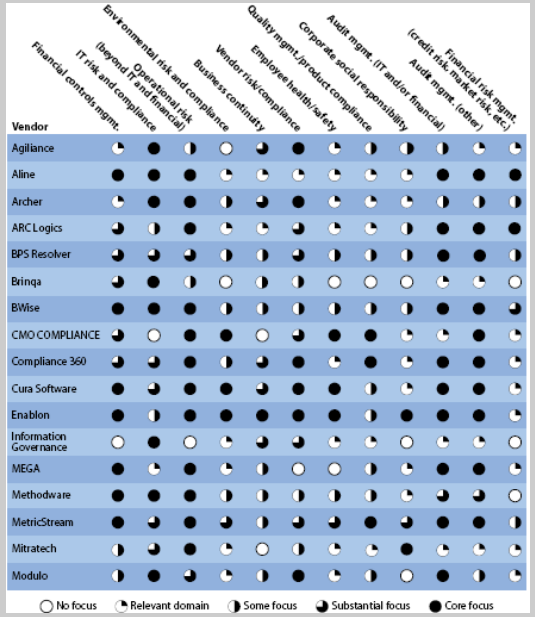
Some benchmarks (Gartner, Forrester, AMRAE)

…

Gartner

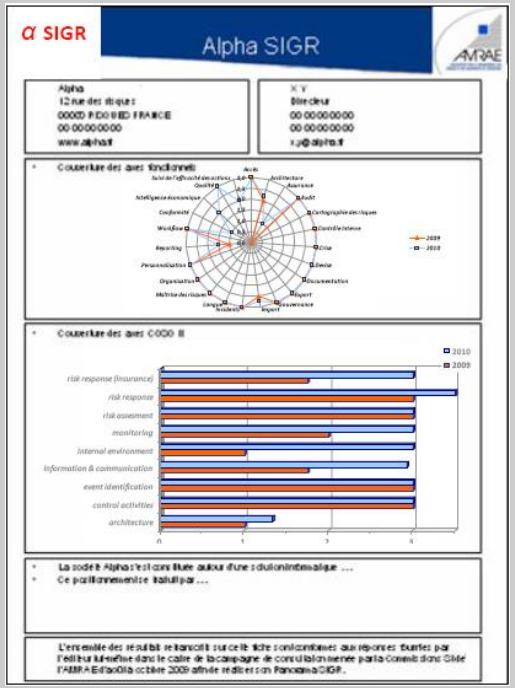
Source: Gartner (2019)

Forrester



Source: Forrester Research Inc.

AMRAE



Source: Panorama SIGR

OpenPages:
Approximately 50% of its customers are in the financial services sector.

Refinitiv: Customer base is widely distributed in all major geographical regions, with concentration in the financial services sector (44% in 2018)

BWise: Approximately 40% of its customer base is in the financial services sector.

© 2019 Deloitte Touche Tohmatsu Limited.

GRC challenges

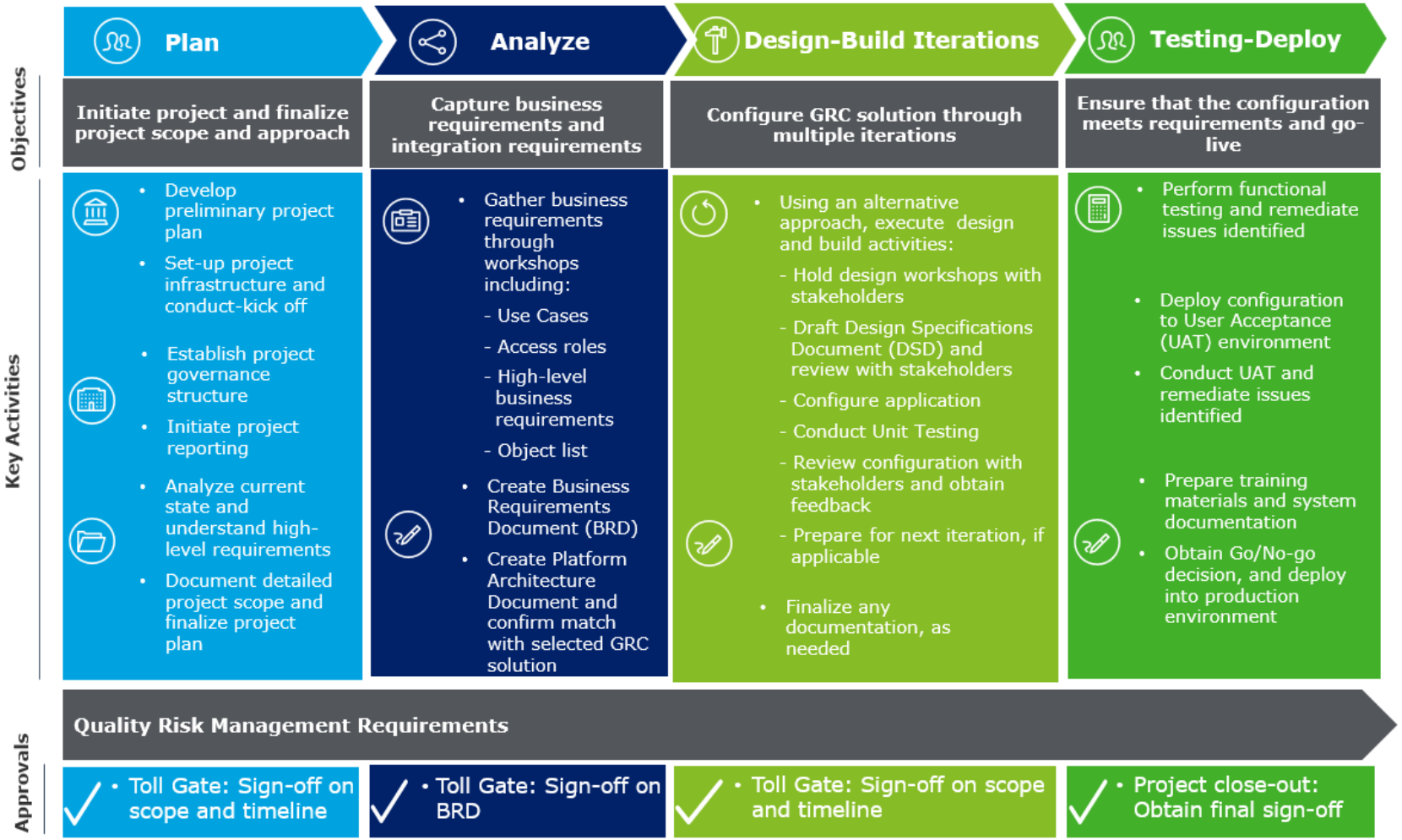
© 2019 Deloitte Touche Tohmatsu Limited.

GRC Implementation: holistic approach

Such a project requires an adapted methodology adapted to the selection, the successful integration and deployment of the solution

Selection of the solution

- Justification for the approach
- methodological framework
- Needs analysis and drafting specifications
- Identification of key market players
- Preparing an analysis grid offers
- Preparation of demonstration scenarios
- Critical revision of the contract with the vendors



However, if you think of GRC as a technology implementation, you've limited its power from the start

© 2019 Deloitte Touche Tohmatsu Limited.

Q&A

Vladimir Remyga
Director
Risk Advisory

telephone: +994 12404 1210

mobile: +994 51206 0123

+7 700 714 5505

e-mail: vremyga@deloitte.com