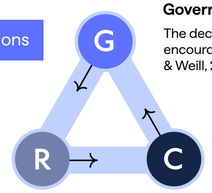
● Organizational Excellence & Transformation

The basics

1. The dilemma of GRC and agility

Some definitions



Governance
The decision rights and accountability framework for encouraging desirable behaviors in the use of IT (Ross & Weill, 2014).

Risk
Identifying, assessing and managing risks that could hinder reliable achievement of objectives.

Compliance
Adhering with the laws and regulations and company policies, procedures, etc.

How to solve the Risk vs Agile dilemma?
Agile focussing on fast and flexible delivery, with gradual improvements.
Risk focusses on control of a process, situation or change; this requires knowing in advance what will be changed.

2. 3L(OD) model is a key first step: Agile/DevOps teams are responsible for risk

1st line of defence
The Product Owner is responsible. Team members support the PO by performing risk analyses, design and implement security measures, implement controls and provide evidence.

2nd line of defence
Sets the standards such as policies, guidelines and methodologies. Challenges the 1st line. Skilled and competent "craftspeople" who also support the business. There are several ways to organise the 2nd line of defence (e.g. through Professional Groups or Competence Centers). Adaptation to Agile/DevOps WoW is necessary.

3rd line of defence
Nothing much changes for the 3rd line. Internal audit which directly reports to the board and to the audit committee.

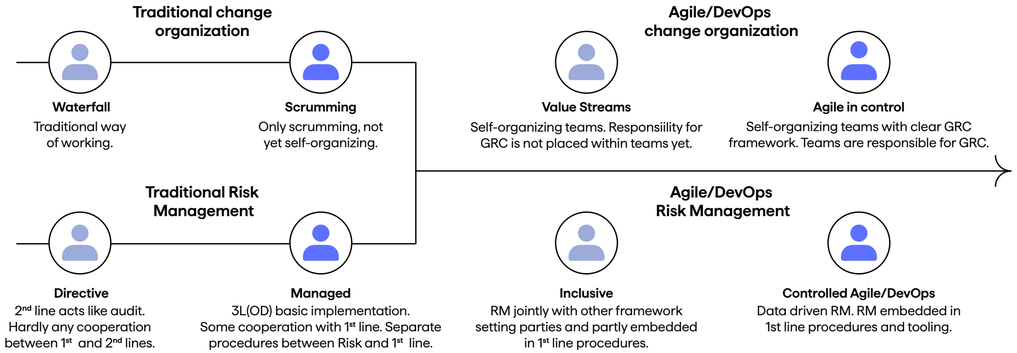
3. Risk Management culture: The role of Risk and Compliance needs to change

From Gatekeeper: stopping at the end

To Traffic Monitor: helping in advance

Growth in maturity

4. A mature Agile/ Devops organization needs a mature and Agile Risk Management approach



eraneos

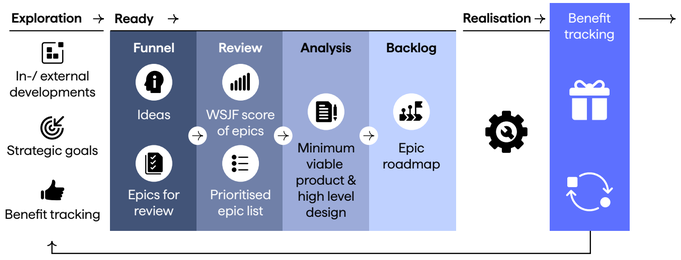
Agile Risk & Compliance Governance: A growth model

5. Growth in maturity is needed on the following topics

From:	To:
• Requirements at a late moment • A separate tooling/committe per risk area and 1st line area • Risk = Directive • Generic requirements on paper in policies • Demonstrating control after changes is mostly manual	• Well in advance • Integrated approach for all framework setting parties (1st and 2nd line) • Risk = Supportive • Specific searchable requirements in tool • Continuously demonstrable in control

Embed in processes

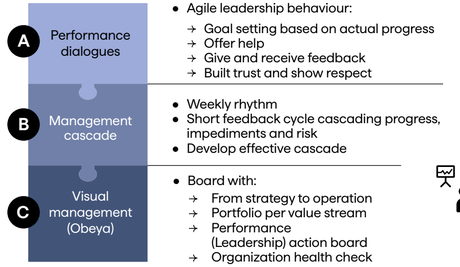
6. Involvement of Risk and Compliance early in the ready phase prevents rework later



7. Volg de voortgang via Obeya: Visualiseer, inspecteer en pas aan

Alignment between teams and on portfolio or enterprise level.

Insight and overview of performance, identified risk and compliance items.



- Agile leadership behaviour:
  - → Goal setting based on actual progress
  - → Offer help
  - → Give and receive feedback
  - → Built trust and show respect
- Weekly rhythm
- Short feedback cycle cascading progress, impediments and risk
- Develop effective cascade
- Board with:
  - → From strategy to operation
  - → Portfolio per value stream
  - → Performance (Leadership) action board
  - → Organization health check

8. Use the Agile/ Devops delivery process to be in control

Early involvement of Risk and other parties	Clear defined and searchable Risk requirements (setup)	Risk verification embedded in automated Testing to prove existence	Meta-controls to verify operational working of controls

Business participation
"Agile backlog management", programma portfolio

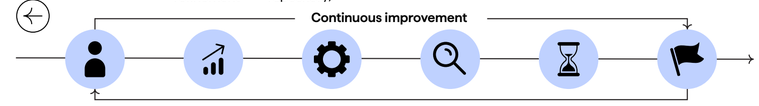
Plan
Analysis, capacity planning, sprint planning, refinement

Development
= code (source code management, code analysis)
= build (continuous integration, centralized repository)

Test
Automated testing (static, unit & integration), validation, user acceptance

Release
Automated deployment & provisioning

Operate
Monitoring, Support, Maintenance, Access



eraneos