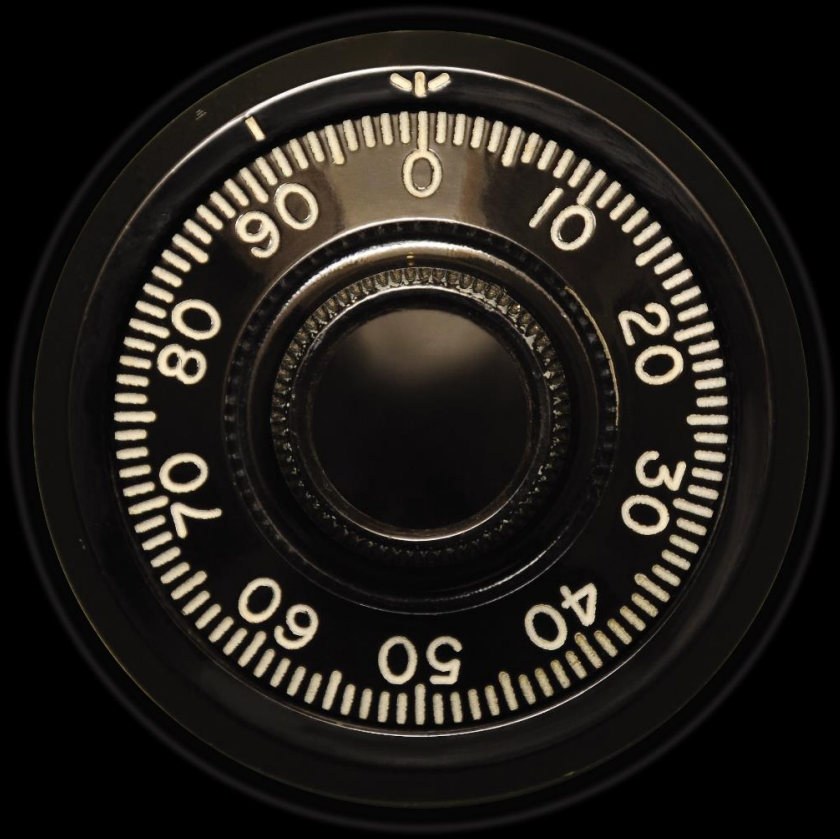
Bridging Development & Compliance

Point of View

Unlock the value of aligning development and GRC functions



Deloitte.

Agile governance, risk and compliance

"Regulators today are no longer satisfied with frameworks, documentation, and audit validation alone; they want tangible evidence, including end-to-end testing, as well as compliance program management that is baked into day-to-day operating processes."

Source: 2020, Banking regulatory Outlook, Deloitte

Introduction

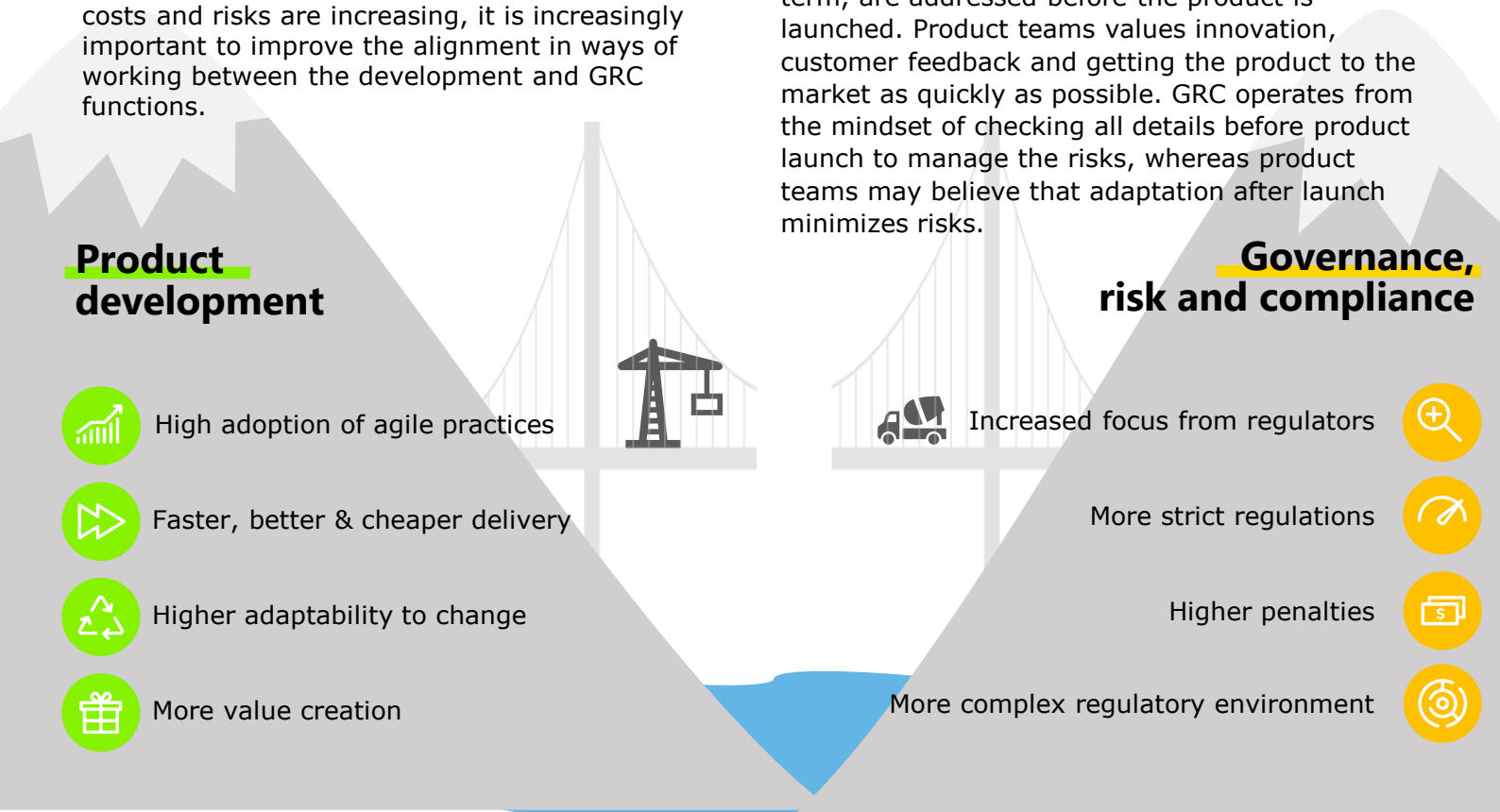
A gap is growing in many organizations. Many modern organizations have implemented agile ways of working to increase the speed and value of their product development. However it can be difficult to align these agile ways of working with the increasing amounts of regulatory requirements of the governance, risk and compliance functions. For instance, agile teams work in many short iterations, whereas the interaction between GRC functions and development often only happened at a few key touchpoints to review new products and ensure compliance with regulations. The ability to collaborate may suffer as a result, leading to risks of non-compliant products being launched unintentionally or costly delays and rework if compliance issues are discovered late in the product development process. The lack of alignment between ways of working is therefore increasing risk and cost.

Risks of brand damage is increasing because of customers empowered with social media, risks of regulatory fines and need to remediate regulatory findings is increasing due to regulatory and legislative efforts to safeguard consumers. Costs increases because time-to-market is a growing success factor in many markets. Since costs and risks are increasing, it is increasingly important to improve the alignment in ways of working between the development and GRC functions.

Problem: misalignment

The problem itself can be viewed from different perspectives within the organization. A CEO might see two sides that communicate poorly causing delayed innovation and instances of non-compliance that need costly remediation. A person from the product development side might see the GRC as unnecessary slow and rule-based. A GRC officer might see the product developers as careless and out of control. A CFO might be worried about unnecessary low return-on-investments, and the marketing department might see lost opportunities for gaining market share. Customers might have the anti-experience of losing out because of product-delays. The consequences are felt throughout the organization and its ecosystem. So, what is the cause of the problem?

The problem may arise because GRC functions operate with a different set of objectives than product development teams and these equally relevant success objectives are not aligned successfully. For instance, GRC teams are required to ensure compliance with regulations and that all potential risks, both short and long term, are addressed before the product is launched. Product teams values innovation, customer feedback and getting the product to the market as quickly as possible. GRC operates from the mindset of checking all details before product launch to manage the risks, whereas product teams may believe that adaptation after launch minimizes risks.



Aligning the way GRC and development functions interact

The differences in mindset manifests itself in different operating practices. For instance, GRC acts as a safeguard between the organization and the environment by approving or rejecting products, and they typically evaluate the entire solution at the end of the delivery. In contrast, agile teams are dependent on user feedback to adapt products, so they work to blur the boundary between the organization and its environment, and they therefore release products frequently to gain many, small insights. Therefore operating from these different practices makes collaboration difficult when there is not defined a framework for how these practices should co-exist.

The consequences of the problem are many. Risk is allowed to build up because the product is developed iteratively with only few GRC touchpoints. Products are delayed and require costly rework, because compliance issues are discovered too late. Non-compliant product features may be unintentionally launched because they were not raised in a GRC touchpoint. This slows down time to market, decreases the ability to innovate and increases risks of brand damage, penalties and lost customers. Those consequences can harm any organization badly.

The need for better collaboration and alignment is growing for external reasons, e.g. increasing globalizing with a growing reliance on doing business online requires proactive evaluation of requirements due to local legislation and regulation. Especially three effects are relevant. First, IT-systems are growing and multiplying, leading to higher exposure to cyber security risks. Second, the regulatory environment for organizations is increasingly uncertain with a raising complexity and accelerating rate of change. Thirdly, the general business environment is growing in complexity which increases risks and exposure. These effects raise the importance of GRC functions which means that potential tension and collaboration difficulties becomes an increasingly important problem for the organization to address.

The problem is also growing due to internal reasons. Traditionally, products were developed following a stage-gate process, where a new idea was first fully described as a set of requirements then fully developed and then launched.

Here, GRC could easily act as a safeguard at the few, big touchpoints between the phases. Now however, product teams develop in iterations, meaning that a product is described, developed and released frequently in small batches.

The change that has taken place in the product development process may not have been replicated in the GRC functions and consequently be difficult for them to handle. These difficulties will grow as long as product development and GRC are not synchronized.

GRC	Product development
• Traditional requirement and policy driven practices	• High adoption of agile practices
• More strict regulations,	• Faster, better & cheaper delivery
• More complex regulatory environment and less maneuverability	• Higher adaptability to change
• Risk of higher penalties	• More value creation

Table: Oppositional mindsets and practices

To solve the problem, GRC and product development should be better aligned. This should be done through designing a product development process that allows for more frequent and targeted GRC involvement, taking advantage of the considerable benefits that organizations have already gained from transforming product development teams to agile ways of working. Benefits typically include better user experiences, increased time-to-market and increased employee engagement. By adapting in a similar direction GRC can deliver additional benefits to the organization and additionally increase job satisfaction with less frustration for GRC and development employees, organizational synergies etc. An adaptation can also deliver GRC specific benefits like increasingly compliant products. Those working in product development would also benefit from adapting to this change, by ensuring a more pro-active and frequent engagement with the GRC functions they develop a common understanding of the company's objectives, enabling better collaboration and safer products.

It becomes clear that better collaboration requires efforts from both sides. However, the immediate transition will be more focused on ensuring that GRC functions efficiently can collaborate and engage with product development in the development process.

Creating a strong foundation for increased collaboration

The foundation for change is having the right mindset. Therefore, both GRC functions and development teams need to re-orient the mindset that have worked well in the past to a new mindset of cross company collaboration that will make them thrive in the future. When changed, the new mindset shows the direction for how work practices should change to fit the new mindset.

Current vs future mindset
Mindset changes are by nature abstract. The values, beliefs and principles we normally operate on are usually unsaid and only tacitly impacts our behavior. To make the change tangible, it is necessary to clearly articulate the current and future mindset, as shown in the table.

	Current	Aspired future
Value	• Comprehensive review of all details • Functional expertise • Compliant and secure solutions	• Cross-functional collaboration • Frequent review of new details • Safer solutions
Beliefs	• Clear set of requirements from the beginning, processes and gates decrease risk of non-compliance and insecure solutions	• Collaboration between development and GRC enables compliance and security by design and ongoing adaptation to regulator requirements
Principles	• Directives • Policies • Processes • Training (e-learning)	• Collaboration on Cadence • Shared view on backlog (list of work to be completed) of items to develop and prioritization • Compliance and Security described in developer friendly language • Acceptance criteria is established in collaboration • *Achieving business friendly Directives and policies*

Organizing for collaboration
New structures need to be shaped by the new mindset. Structures can for instance be how professions are grouped and mixed, how decisions are made, how to collaborate with other parts of the organization. An example is changing from functional silos to virtual cross-functional teams. The structures are supposed to guide behavior and action so that the mindset becomes part of the daily practices in GRC. Since behavior and action is very contextual, the specific structures need to be adapted to the specific organization.

Safety Teams as example
The concept of 'Safety Teams' is one general example on how the new mindset can be implemented. Safety teams is a small team, aligned to the product development work streams, operating in similar cadence and including the relevant and needed members from each of the GRC functional areas.

This team is empowered to and capable of making decisions on all GRC related questions that arises during product development. The team collaborates with product development teams frequently by formulating and prioritizing GRC-related work and reviewing new details of the product, through agile artefacts such as Solution intent, product breakdown, backlogs and feature/story descriptions replacing traditional Software Requirement Specifications.

Individual Safety team members are also organized in groups of professional peers to uphold high professional standards, share good practices and coordinate compliance across teams. Safety teams is thereby a structure that implement the new mindset and is capable of engaging in an efficient product development process, that does not compromise legal requirements.

Are you ready to increase your enterprise agility?

We can help you accelerate your journey

Terkel Tolstrup - Partner

Enterprise Agility Advisor

Terkel has worked with agility since 2002, and is leading Deloitte's agile community in the Nordics. Furthermore, Terkel is one of Deloitte's global experts in agile methods, and has extensive experience in transforming IT organisations, projects and programs. To him, agile transformations are first and foremost about the people, and how to motivate them in changing their agile behaviours.

Morten Ankjær – Senior Manager

Enterprise Agility Advisor

Morten has more than 15 years in the financial sector and unique experience in delivering large scale (EUR 1b+) technology solutions, driving IT/technology and analytics strategy, building agile capabilities and executing change efforts in an agile manner.

Furthermore Morten is leading Deloitte Denmark Agility Advisory towards Financial Service Industry and Lean Portfolio Management.

Nicola O'Regan – Senior Manager

Risk Management Advisor

Nicola is a UK qualified actuary with over 20 years experience across the financial sector, leading cross-jurisdictional projects to implement regulatory-compliant governance, designing and implementing risk management frameworks across different risk areas, as well as creating high-quality risk reporting to Board and senior management.