

# Agile on the Rise: Controlled, compliant adoption of Agile and DevSecOps

The key risks an enterprise needs to  
manage when IT adopts Agile and  
DevSecOps

With the exception of digitally native startup companies that were “born Agile”, most organizations are complex with well entrenched silos, centralized hierarchies, and reliance on antiquated technology architecture that was established decades ago. The adoption of Agile and DevSecOps can should be considered a major technology transformation. As with all transformations, there are many risks that must be carefully mitigated.

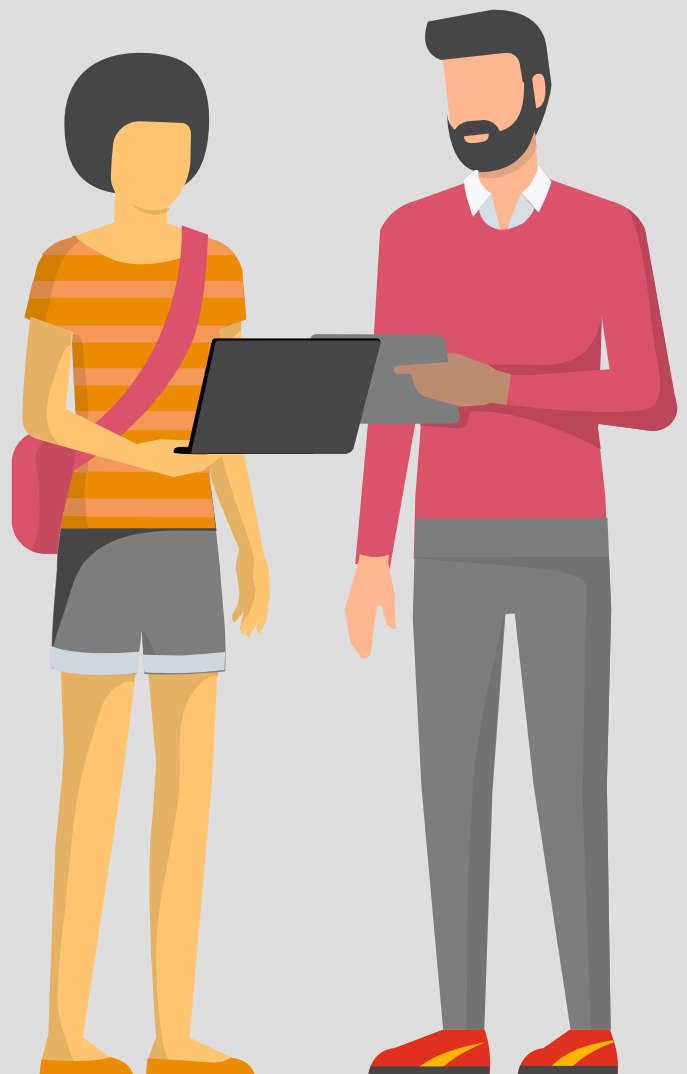
### In general, we see two major areas of risk:

1. **Adoption risk:** Can the enterprise adopt Agile and DevSecOps successfully?
2. **Governance and controls risk:** How can we keep governance, risk, and compliance in alignment with Agile and DevSecOps so that management, regulators, and auditors are comfortable that:
  - a. Financial, planning, and oversight processes remain valid;
  - b. Effective internal controls are maintained over the System Development Lifecycle (SDLC); and
  - c. Products deployed by the SDLC are compliant and adequately controlled.

### In this paper we address one common pattern:

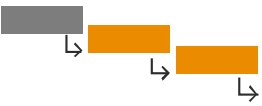




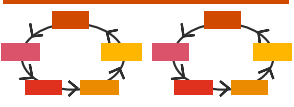
IT is enthusiastically adopting Agile and DevSecOps, while enterprise stakeholders are interested in its risks and impacts. Readers that are interested in a more holistic enterprise adoption of Agile (i.e., all business functions) are encouraged to visit:

<https://www.pwc.com/us/en/services/consulting/technology/taking-a-holistic-approach-to-enterprise-agility.html>



# Stages of Evolution

Those areas of risk align to the different evolutionary stages organizations often follow in adopting Agile and DevSecOps. There is no single path to maturity, and every organization's context is unique. Common interim stages are depicted below.

Stage	Features	
<b>Waterfall</b>	Sequential development process where all required activities in the preceding phases are complete before progressing (i.e., all design is completed before any development commences).	
<b>Hybrid</b>	Hybrid blends waterfall and Agile structures. The overall project follows defined, sequential phases (e.g., package selection and fit-gap assessment), with some iterative development within those phases (e.g., customizations).	
<b>Agile pilot</b>	Organizations often start their Agile journey with an individual pilot project. They have a defined scope, then deliver that scope using Agile, after which the project stops. Requires initial training in team-level Agile and an introduction of new roles (e.g., Scrum Master and Product Owner).	
<b>Agile 'projects'</b>	Agile is established as an enterprise endorsed delivery option for individual effort. Requires a defined Agile 'playbook' with formalized training to establish repeatability and consistency across teams.	
<b>Continuous delivery team(s)</b>	A team that continues to work on a specific area, taking the next highest priority request as their 'scope', with no defined conclusion. Teams should be organizationally structured around the customer value they create. Appropriate DevSecOps/Agile tools should also be leveraged for planning, collaboration and automation.	
<b>Agile at scale</b>	As more teams embrace agile, the surrounding organization needs to evolve (i.e., portfolio, IT operations, finance, etc.). Requires an agreed upon common framework for operating, synchronizing and managing cross team coordination and dependencies across large initiatives.	

# Friction points:

## Can the enterprise successfully adopt Agile and DevSecOps?

When converting to Agile and DevSecOps, through an individual effort or scaling across the enterprise, the impact stretches beyond technology and their business partners. There are many parts of the organization that should be included during the early stages of the adoption.



### Leadership

- Large scale transformations require strong executive sponsorship, promoting organization-wide inclusion and responsibility to ensure successful adoption.
- Adoption of new leadership techniques (e.g., servant leadership) will allow leadership to embrace the Agile mindset and protocols of their teams.



### HR

- The Agile and DevSecOps workforce of the future requires different skills (e.g. Design Thinking, Test Driven Development), roles (e.g. fewer Project Managers, more Scrum Masters), and ways of working (e.g. from “command and control” to “servant leadership”). In some cases, the location of workers and reliance on outsourcing, offshoring, and automation may be re-examined. This workforce transition requires careful calibration, planning, and execution.
- Performance Management Frameworks typically focus on individual performance, however, mature Agile organizations will move to employ a framework that promotes, encourages, and compensates team success.



### Portfolio & Project Governance

- In the interim, many organization will be utilizing waterfall and Agile methodologies in tandem, therefore portfolio management and governance process will need to be updated to enable prioritization, selection, funding, and monitoring across multiple methodologies.
- Typical annual budgeting processes only support project based funding. Processes should be enhanced to support dedicated funding for standing teams



### Procurement

- Traditional deliverables based contracts will typically not work for Agile vendors due to the natural level of uncertainty. Contracts for DevSecOps vendors and tools will need to reassess service level agreements and other success measures.
- Standard contracting templates traditionally incorporate milestone-based payment terms. Involve Procurement during contract negotiations to mitigate the inherent risk to the organization when adopting Agile and DevSecOps



### Risk & Compliance

- Gain commitments from risk, application control, compliance, and regulatory group specialists and their leadership so they are available, knowledgeable and ready to embrace new ways of working to foster real-time involvement throughout the lifecycle of the product.
- Include risk, application control, compliance and regulatory requirements prior to the “Design” phase for earlier socialization among teams through the iterative phases.



### IT General Controls

- Control obligations and objectives remain static, however the controls need to evolve. Involve internal and external audit as you modify the controls.
- An increase in automation increases risk on the automation tools. Therefore, audit partners need to know how to both audit and leverage automation.



### Audit functions

- Auditors will be faced with new controls, owners, and evidence due to the changing nature of the risk environment, and will need to adjust their approach accordingly.
- With an increase in the use of automation tool, the focus of audit will need to pivot with it (e.g., role based access, access reviews, and automated testing).



### Finance and Tax

- Existing CapEx vs OpEx decision and tracking models typically assume waterfall so these models may no longer work effectively.
- The Tax team should be consulted to understand the best use of R&D, and how other tax concessions can be leveraged (e.g., Can prototypes and wireframes be considered R&D?).



### Business partners

- Product owners and managers are critical as they need to be knowledgeable, available, and have authority. Individuals who understand the technical products, business processes, customer needs, and key stakeholders throughout the organization are rare, and typically in heavy demand. Making them available for daily interaction with Agile teams is a common challenge.
- True partnership is the goal where the product team is seen as one and IT and business silos no longer exist.

# Making it fit: Concurrent changes to enterprise governance, risk, and compliance as you rollout Agile and DevSecOps

Given the many impacts identified above, enterprises need to make changes to processes, controls, tools, mindset, and structures to keep governance, risk, and compliance functions in lockstep. Each organization will need to carefully consider their progress, and unique context (typically through a change impact analysis), but common work packages include:

- A new Product Lifecycle (PLC) or SDLC framework (with mandatory outputs and approvals) created to drive adherence to compliance and internal controls.
- Revised risk and control matrices, and controls narratives over the SDLC. In general, key IT general controls (i.e., change management) may remain the same, however operational and monitoring controls may require updates.
- Agile and DevSecOps playbooks created or augmented to set guardrails in order to enable consistency and repeatability in processes across teams.
- Review tools used in the development process and DevSecOps pipeline to ensure they are appropriately 'locked down' for reliability, and the extent to which controls may be impacted is well understood.
- Review tools to determine if SOC reporting is available, then understand which controls are covered, determine responsibility, and if there are any qualifications team members should be focused on obtaining.
- New audit procedures created to factor in the changing nature of the risks associated with Agile delivery.
- Ways of working/interaction models agreed for risk teams to provide their SME and requirements, without disrupting the Agile teams' flow.
- Updated CapEx/OpEx policy and procedures to ensure Agile projects are treated and distinguished correctly.

## Changing controls activities to enable the rise of Agile

As the use of Agile becomes pervasive, all risk, compliance, and assurance executives need to embrace how these highly effective methods can co-exist with effective controls. With a sufficient understanding of the Agile and DevSecOps environment and leading controls development practices, risk professionals can take the right steps to integrate controls that protect against risk and non-compliance without compromising much needed agility.

### Contact us

For a deeper conversation about integrating effective controls into Agile environments, please contact us.

## Contacts

Andrew Schuster  
(416) 687-8356  
[andrew.schuster@pwc.com](mailto:andrew.schuster@pwc.com)

Sarah Shafey  
(416) 687-8356  
[sarah.shafey@pwc.com](mailto:sarah.shafey@pwc.com)

Karsten Kuhrmeier  
(403) 509-7558  
[karsten.k.kuhrmeier@pwc.com](mailto:karsten.k.kuhrmeier@pwc.com)

Ravinder Bains  
(604) 806-7000  
[ravinder.bains@pwc.com](mailto:ravinder.bains@pwc.com)



# Thank you!