Azure Annual DevOps Report

Microsoft

sogeti
Part of Capgemini

Enterprise DevOps Report

Governance 2020-21

Governance

IT governance is part of the overall enterprise governance strategy and ensures IT decisions are aligned with the business strategy. Good governance is about not only 'doing the right things' but also 'doing things right'.

There is a wide breadth of IT governance frameworks; from more common ones like COBIT 2019, to international standards like ISO38500. Most frameworks describe the roles, responsibilities, organizational structure, and processes to guide the decision-making within IT.

Governance influences how goals are set and achieved by IT. At the same time, governance also conflicts with the independence desired by DevOps teams. These teams need to follow the organization's standards in terms of architecture, security, and procedures, but often see them as obstacles to rapid delivery. While they are guiderails to support them, the team often views them as innovation inhibitors. But these guiderails can also be the base of knowledge sharing to grow teams and individuals. This tension between the chaffing restrictions of traditional governance models and the broader benefits that good governance can bring is at the heart of the DevOps governance challenge.

Startups and small agile companies tend to lend themselves well to adopting and maturing DevOps practices. They often have lightweight governance processes that are easy to manage and even easier to automate. Larger enterprises with deeply rooted governance processes and strict rules often take longer but can benefit hugely from simplification and automation.

If IT governance often determines the speed of IT change, then it can either be a force for enabling rapid change, or slow down value delivery.

What are the Challenges?

IT as cost center rather than a strategic enabler

Many existing governance implementations are based on the IT-as-cost-center model and, as a result, their primary focus is on cost effectiveness. DevOps, on the other hand, is based on an "IT-as-strategic-business-enabler" model, with a dedication to accelerating innovation and time-to-market. The sluggish pace of existing non-DevOps governance processes cripples innovation, and often makes IT feel more of a hindrance than an asset.

One large financial services corporation we interviewed takes a minimum of two months and 23 handovers to get a purchase order approved. In another example, a global telecommunications provider takes a minimum of four weeks for a proposal to be approved for new software development, five weeks to obtain an environment, two to three weeks to make a firewall change, and four to six weeks for end-to-end testing. Each of these steps is required to pass governance approval processes via service desk tickets being raised. These processes are purportedly in place to "save money."

Overly prescriptive governance

Highly prescriptive rules-based governance frameworks break down at enterprise scale. Across an enterprise's technology landscape, with different operating systems, polyglot software implementations, and diverse attitudes to risk, the number of times an exception to the rules is required ends up resulting in *everything* becoming an exception, completely undermining the goals of good governance.

Legacy governance implementations largely struggle to adapt to the rapid evolution of technology. For example, if we look at the evolution of application hosting—from physical servers, to virtual servers, to cloud hosted VM, to containers, to serverless—each evolutionary step needs governance rules. The pace at which technology is evolving means that trying to prescribe governance at a level of detail tied to technology implementation, while ensuring it remains relevant, is virtually impossible.

Making it about more than just IT

A popular perception is that DevOps is an 'IT thing' or a 'developer's toolkit', like Agile was before it. In reality, while DevOps is a newer operating model for IT, it is intrinsically linked to the entire organization's digital transformation and the governance framework needs to encompass the whole company, not just IT. However, the DevOps model itself poses governance challenges. Too often DevOps ways of working, notably the freedom and autonomy granted to teams, has been misinterpreted by some teams as a freedom from process or any formal governance—a misconception that needs to be addressed during implementation.

The need for real-time intelligence

Finally, without effective feedback, ideally in real-time, it can be difficult to achieve appropriate levels of governance. Dynamic application environments, the rapid release of new features, and the faster adoption of new technologies mean that the need for real-time business intelligence that underpins the governance model is more important than ever.

Addressing the challenges

Make doing the *right* thing, the *easy* thing

Successful governance teams should aim to work towards an overarching governance principle that makes doing the *right* thing, the *easy* thing. In this way, complying with governance becomes the path of least resistance, rather than a hindrance or obstacle to overcome.

The governance function can support DevOps teams by publishing best practices that provide helpful, actionable, guidance. Building a knowledge sharing culture can also make the whole organization more efficient and help grow teams and individuals in terms of their experience and capabilities.

Principles, not rules

Tichaona Zororo, a director at ISACA, the organization that publishes the COBIT governance framework, points to a key tenet when he says: "Governance should be principles and outcome based not rule based".

Governance is *not* about adopting a command and control mindset that seeks to mandate rigid rules to control the delivery of IT services in a rapidly evolving IT world. Rather, it is about outlining a set of core principles or outcomes to which teams and products are meant to adhere. Governance teams should provide common patterns, frameworks and tools that assist teams in adhering to these standards, while clearly delineating expectations. This, in turn, gives teams the flexibility to develop their own implementations, so long as they align with the agreed upon principles and outcomes.

An excellent example of this approach is the UK Government Digital Service Standard designed to improve the delivery of digital services by UK public sector organizations. The standard outlines 14 high-level principles that govern the full lifecycle of a digital service—see The Service Standard helps teams to create and run great public services.

Before any given service goes live, teams need to demonstrate that their service aligns with the defined standards, even though the specifics of each team's implementation may vary. For example, Standard #7 states, "Use agile ways of working" but doesn't mandate Scrum, DSDM, Kanban, or any other particular agile method. Implementation methods are left to each team, although whatever the team chooses must align with the more detailed guidance.

ADOPT AN INNERSOURCE MODEL

According to GitHub's Core Tenets of InnerSource[11], successful governance implementation should be based on these five key principles:

Open
Democratizing access, creating a level playing field for the open sharing of work, ideas, and feedback, and ensuring cultural and strategic alignment.

Transparent
Ensuring the process as well as the product is visible, predominantly by decoupling communications from time and space.

Participative
Sharing work and making it easy for others to discover, use, and contribute.

Collaborative
Working together to incrementally increase quality, distribution of knowledge, and shipping velocity.

Governed
Directing, guiding, and supporting the software community, through standards, patterns, roles, and executive sponsorship.

Governance should be viewed less as an external process imposed on teams and more a collection of shared best practices that makes work better and more efficient.

At a very practical level, ensuring everything (from application source code and architectural patterns, to security standards and development methodologies) is both open and transparent makes it evident that anyone has the opportunity to challenge these standards and contribute to improving them.

Governance guidelines and artifacts maintained via an InnerSource model bring shared ownership to teams and an increased drive to use and follow the guiderails of governance.

[11] GitHub, InnerSource, 2019

Platforms & executable reference architectures

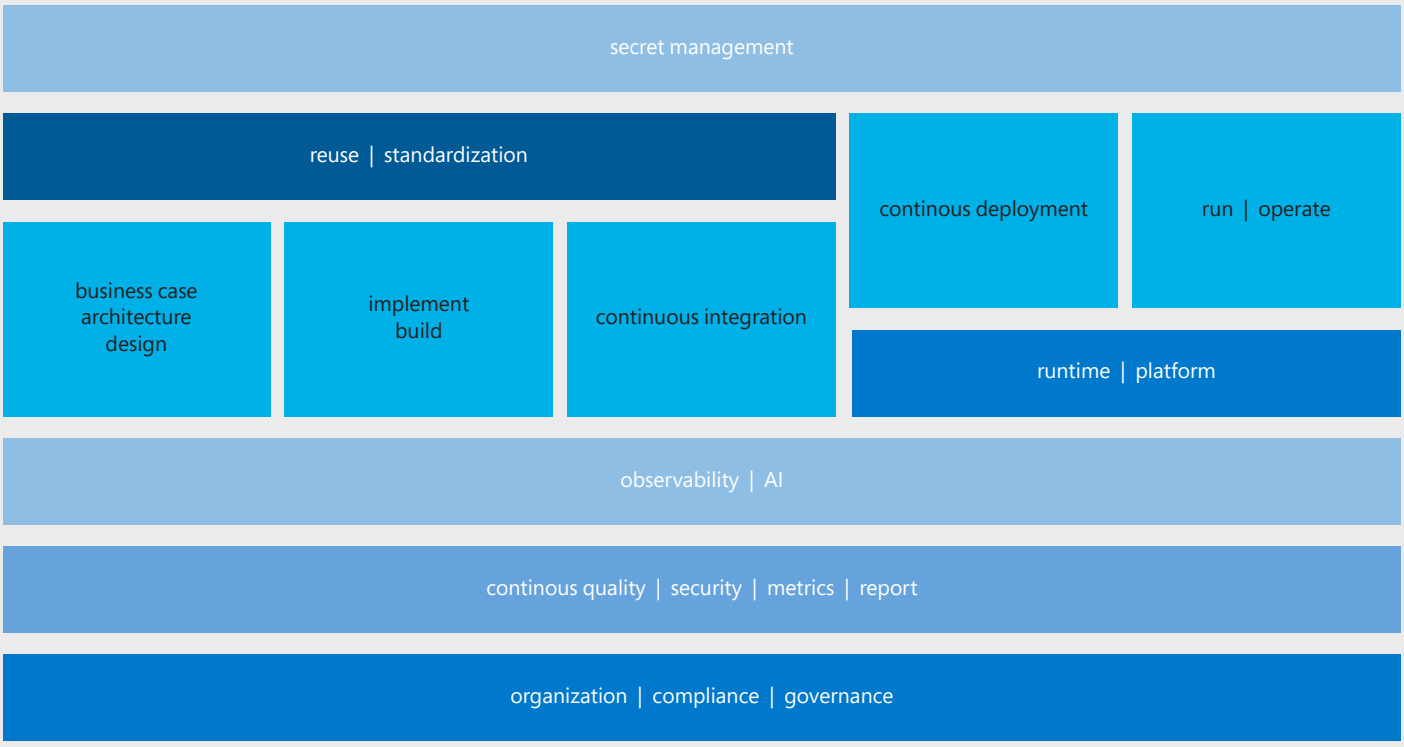
Top performing organizations are creating self-service technology platforms, supported by comprehensive documentation that helps users leverage these platforms to ultimately build better products. These shared platforms enable organizations to embed and facilitate governance, while making it easy for teams to do the right thing.

A company platform might include security, identity, consistency, cost management and deployment automation as key services provided. Each of these self-service platforms will have governance "built-in", so that teams who use the platform inherit the governance best practice at little or no effort to themselves. As an example, one way of ensuring that cost is accurately tracked and attributed to the correct products or departments is to utilize resource labels. The use of these cost management features can be mandated in the company platform.

Consistency at enterprise scale is often a governance challenge. Organizations can have hundreds of developers working in self-organizing teams, so it is important to have consistent implementation practices across the IT landscape. Almost all enterprises make use of reference architectures with best practice guidance for how to build and run applications, as well as how to incorporate governance and security. One of the more mature governance practices is to make this reference architecture executable via sets of templates, scripts and tools, and to move the reference architectures beyond Visio diagrams and Word documents into code when combined with DevOps tools like infrastructure-as-code, and configuration-as-code.

When combined with the InnerSourcing patterns mentioned previously, teams can contribute to the creation and constant iteration of these reference-architectures-as-code, helping to ensure a system of dynamic and effective governance.

INTERNAL SOGETI RESOURCE LABELING DIAGRAM *FIG. 5*



Continuous governance

Traditional approaches to governance have largely relied on an inspection process or quality gate prior to production/release, which isn't feasible at scale and pace. As a result, top performing companies are adopting continuous-delivery models for governance so that they can deliver value to customers sooner via the frequent release of new software features.

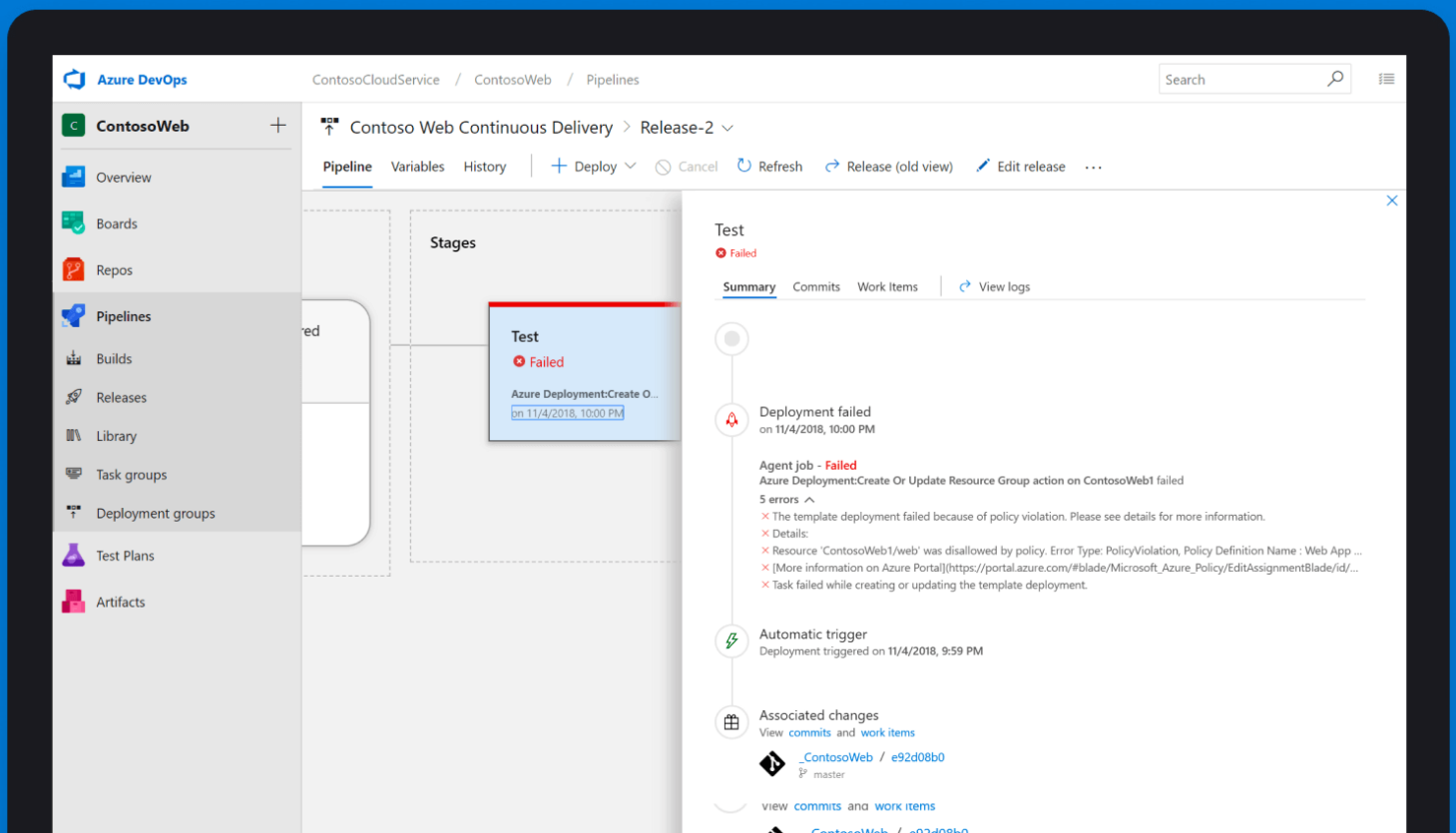
To combat cumbersome governance practices, enterprises are also moving towards automating their governance, reducing the burden on IT departments that no longer need to perform sluggish approval and validation workflows. At the heart of this continuous approach are CICD pipelines with governance steps built into each pipeline, which enable the frequent release of secure and high-quality products to customers. Continuous governance defines the principles that can be implemented via automated software controls that promote code from one stage of the pipeline to the next.

Seek feedback and insight

Traditionally, it has been difficult to gain visibility into the current state of an organization's adherence to its governance principles. It's also been hard to measure the organizational benefits of following that governance.

Adopting Enterprise DevOps solves this. One of the key tenets of DevOps is to create effective feedback loops—the faster the feedback cycle, the quicker an organization can learn what works and adapt accordingly.

Enterprises are increasingly turning to AI and machine learning platforms to solve this challenge. Governance teams use this technology to filter out and correlate data in order to turn the large volume of data generated by DevOps toolchains and cloud platforms into actionable intelligence that they can use to optimize their governance processes. By filtering out and correlating data, teams can focus on taking the corrective actions needed without being bogged down by the sheer amount of data that has been collected.



GOVERNANCE CASE STUDY

For one large European insurance company, good governance is critical in avoiding what it calls "chaos and security issues" across more than 20 different technology and development streams, each with their own domain architectures and DevOps teams. With over 700 active DevOps professionals, effective governance ensures that these teams work consistently, while complying with company and regulatory dictates—all without impeding speed of development.

To embed good governance, the insurer implemented a central team that monitors and supports adherence to the development toolchains. In turn, these toolchains have been rationalized with the help of enterprise architects and domain architects to bring more control and efficiency, and any disruptions, security issues, or illegal usages of tools can be quickly fixed.

As DevOps is as much about the people as it is about the enabling technologies, communication is vital in the firm's approach to governance. An IT service portal provides information on offerings and services for teams, together with a complete set of 'how to' and other relevant documentation. The communications team gives oversight into current happenings and future plans, while a communication forum is used for knowledge sharing between team members, which greatly reduces friction and work disruptions.

This governance team is highly active and keeps up its momentum via a notification and updates channel, as well as with regular mail distributions. For the insurer, this commitment to good practices through governance ensures that its DevOps teams work in tandem to support the business goals efficiently and compliantly.

GOVERNANCE NEXT STEP RESOURCES

Make doing the right thing the easy thing
Learn More about the Cloud Adoption Framework
Cloud Adoption Framework Governance Benchmark Tool

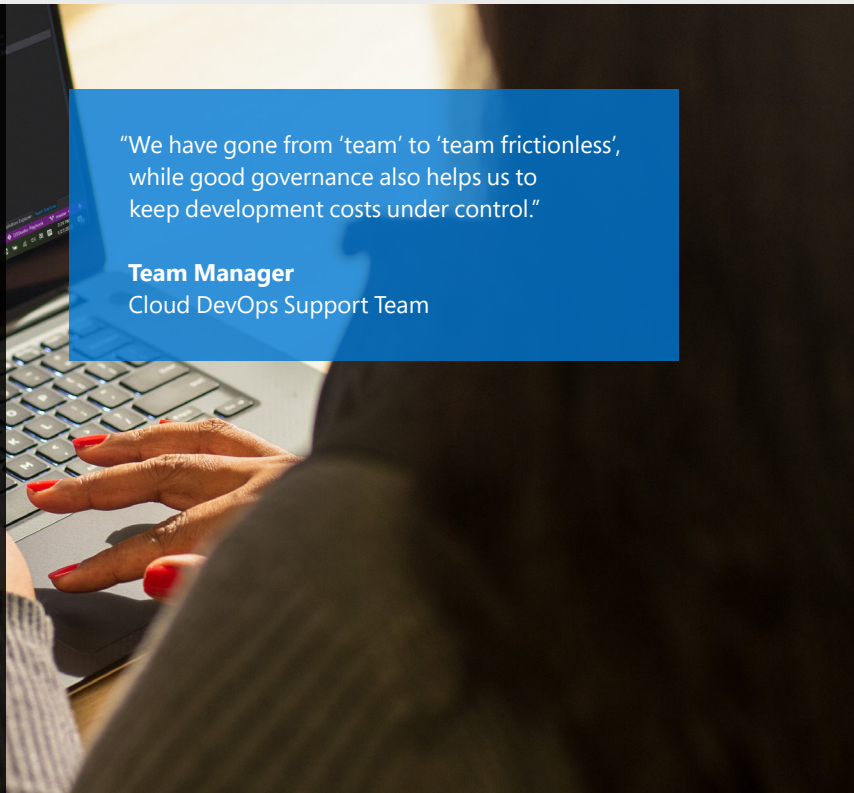
Principles, not rules
Learn more with Digital by Default Service Standard

Adopt an InnerSource Model
Read more on GitHub's Introduction to InnerSource

Platforms and executable reference architectures
Microsoft Azure Well-Architected Review

Continuous governance
How Azure tackles Governance Automation

Seek feedback and insight
Learn more about Cloud Monitoring Tools



> "We have gone from 'team' to 'team frictionless', while good governance also helps us to keep development costs under control."
>
> **Team Manager**
> Cloud DevOps Support Team