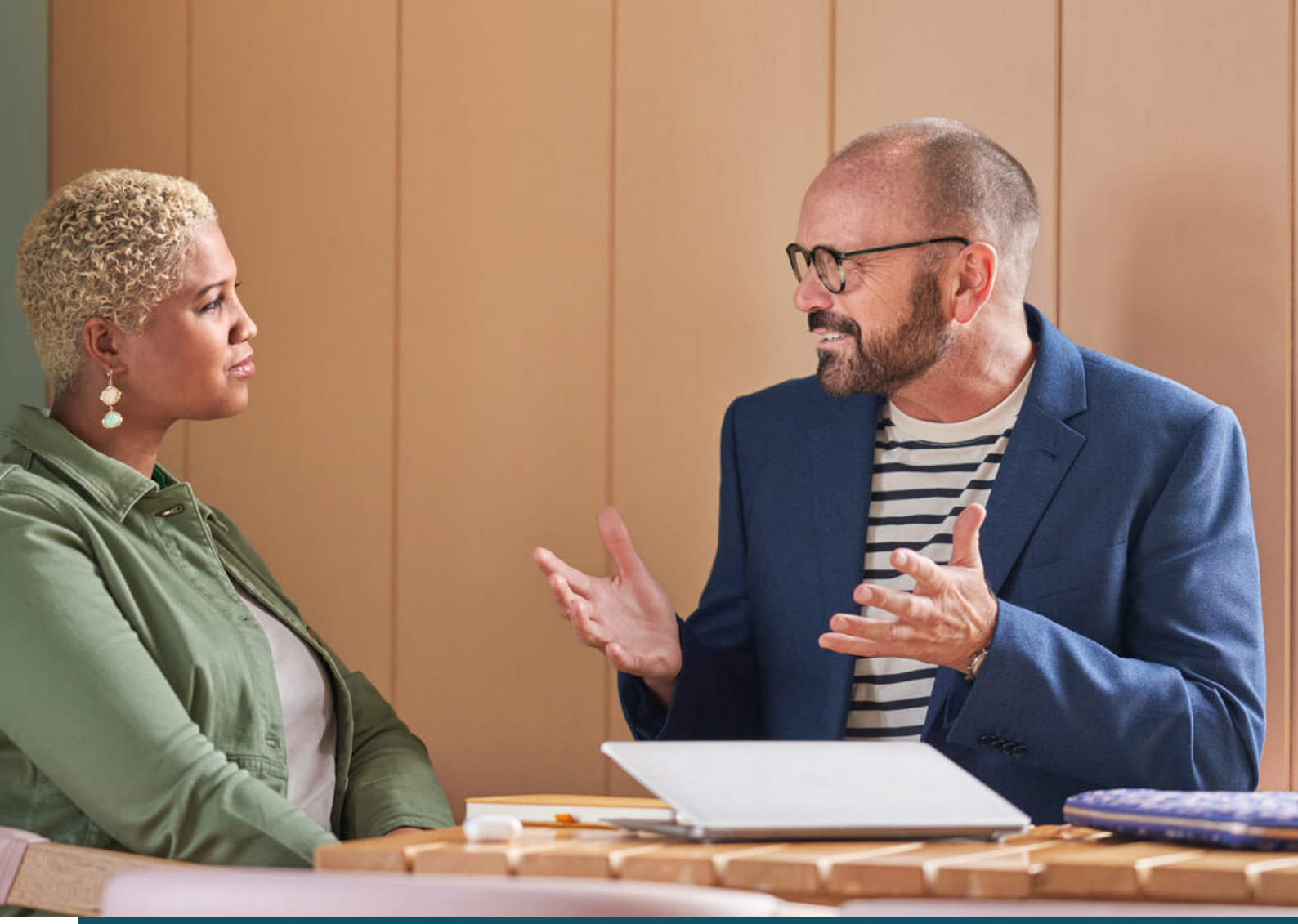
Cloud-first operations require a new approach to governance

Sound governance is the basis of all cloud operations. So, to bring the cloud experience to all your IT, you need to update your existing governance policies.



Without a solid set of governance practices, an IT organization is wandering around in the wilderness. It lacks a formal program to consider stakeholders' interests and ensure that IT is supporting the ongoing business strategy.

This is especially true for IT organizations transforming to any type of cloud-everywhere experience. The same rapid change that cloud brings to business can also create chaos in management and control. To take advantage of cloud everywhere, organizations need to create governance policies specifically suited to the cloud experience.

Embedding governance in systems

Governance plans need to focus not just on systems but also on people and processes. The technology is relatively straightforward, but people and process issues are not. When you take manual tasks out of the process, it is important to embed governance decisions in your systems. Organizations need that long list of well-documented operational management functions, including change management, configuration management, asset management, service desk, and logging and monitoring in order to determine how they will operate differently in a cloud-everywhere world.

Look for places you can streamline and automate tasks. Some areas, such as existing governance in security, can be adapted almost seamlessly. In other areas, you will need to create new policies and procedure that are cloud focused and retain visibility and control over the total economic picture as your IT mix adapts to the cloud business environment.

Foundational governance practices

As IT environments become more distributed and complex, visibility and control take on greater importance. We see areas for continued development of rigorous best practice given the unique challenges of hybrid, multicloud IT.

Understand your economics

A well-designed hybrid cloud strategy is underpinned by a concrete business case, with a defined economic strategy represented by a total cost of ownership and return on investment model. Initially, these models act as hypotheses that need to be tested and updated as the organization gains experience and knowledge with workloads running where they fit best across a hybrid cloud estate.

However, with the increased velocity, automation, and rapid scale of a cloud approach comes a risk of losing visibility and control over your IT economics. Automation and tooling can help enforce and enhance your economic strategy by providing guardrails on spending, enforcing right-sizing, and providing valuable insights into how your economic hypotheses need to evolve as real workloads are running.

Your approach to visibility and control over economics should focus on the following objectives:

- Accuracy and completeness of financial data across your IT estate
- Allocation of investments based on organizational and departmental priority
- Cost optimization based on objectives and analysis and informed by operational experience
- Insights into current and modeled future-state financials
- Reporting for faster, better quality decision-making

Change management

Change management is one of the easier functions to adapt, yet it is a common bottleneck as development and deployment processes become automated. While the workflows in the process remain the same, it must be streamlined wherever possible by finding decision points that can be standardized and automated. Since cloud models facilitate faster change, you are looking for ways to leverage automation and speed up the approval process while still balancing risk.

Most organizations have a robust process to govern change, which includes a change approval board that sets a commonly accepted throughput and frequency (establishing what is too slow, too infrequent). Rapid cycle time between the business needs and production deployment drive the most value out of the cloud. (This is your time to value.)

Common places to accelerate change management are anywhere you can adopt a preauthorized, lower risk, standard class of change within the process, which would flow through automatically. A starting point for this is a standard change process with automatic approvals for certain changes.

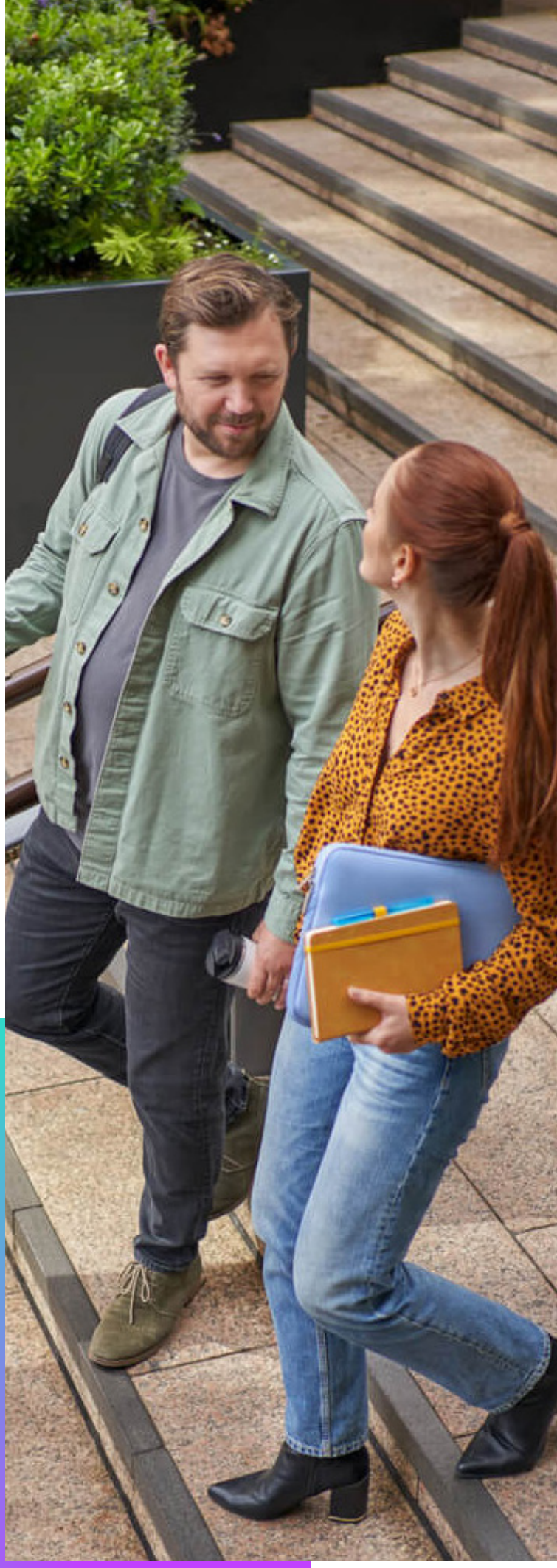
Once that new workflow is adopted, establish a regular optimization review of your change process. Minimize trips to the change review board by standardizing as much as possible over time. This approach is key to driving down your cycle time and increasing your velocity.

Configuration management

The biggest change for configuration governance in a cloud context is a singular focus on removing manual review and config steps. The goal is to develop gold images and gold configurations and move toward immutable infrastructure.

Configuration management is essential because the more you automate and shift left before implementation, the better. To extract the most value out of a cloud-everywhere approach, you need to streamline configuration management workflows and embed automation as early as you can. In cloud operations, humans do not touch environments, and you do not change configurations on the fly. If that initial system image is wrong, you replace it with a new image that has all the capabilities you need.

Getting to this plateau takes time, but make sure you understand, at the start, that the changes necessary for configuration and patch management are essential.



Asset management

Everyone claims to have a strategy for managing their IT assets, but most organizations do not implement their strategies well. With cloud everywhere, focus on having a structured program with a simple identification scheme to handle short-lived resources.

If you do not have those elements, the gap needs to be addressed as you move to a hybrid cloud environment. You cannot manage what you cannot see, and in an environment where resources reside on- and off-premises, you cannot validate your asset management accuracy by walking around and taking a manual inventory. So, it is important to understand early in the process what you have and to identify what is essential to track.

Compliance for a new paradigm

Applying automation to security and shifting left helps accelerate an enterprise's pipeline processes and accelerates time to value, but it does not remove the responsibility to manage compliance with security policies and regulatory obligations.

Ensuring compliance with regulatory and control obligations in a dynamic cloud-everywhere landscape requires a new approach to governing compliance. Regardless of where your workloads run, regulatory obligations still apply, and the increased velocity and rate of change in a hybrid cloud estate means compliance must be continuous.

Leverage automation tools to monitor, report, and manage the state of compliance across your edge-to-cloud IT as necessary. This new approach to compliance will evolve the overarching governance requirements, since a tighter relationship between the environment and expected controls is possible through automation.

These obligations can place a tremendous burden on organizations if they don't have the knowledge, skills, and tools to effectively evaluate compliance across their IT estate. Issues you need to address include:

- How to evaluate compliance across a distributed cloud environment with multiple providers
- How to remediate out-of-compliance resources
- How to manage compliance when users can constantly turn on and off resources
- How to provide visibility into compliance to users across the organization
- How to easily prepare for an audit

A side benefit of continuous compliance is an easing of the support burden technology teams incur during audits. Providing auditors with the ability to see not only the current state of compliance but the continued, ongoing, and constant governance of compliance will increase trust for this new operating model while, once again, decreasing the labor burden and increasing time to value.

Service desk

Organizations need to anticipate how to integrate alert data from across the IT estate, encompassing data centers, public clouds, and edge locations. While the processes stay the same, how are you going to resolve the issue changes? This will be an incremental change at first, but the increasing adoption of automation will allow you to have issues raised and closed automatically by adopting architecture and operational principles of autoscaling, self-healing, and immutable infrastructure.

While you can reuse a great deal of your existing service desk capabilities, you will need to plan for alert integration from the hybrid cloud estate and begin to think through the classes of issues that can be streamlined and addressed through automation.

Logging and monitoring

While existing logging and monitoring strategies can be modified to support hybrid cloud workloads, there are a few key differences to consider. First, you will need to make sure your team understands the differences in managing hybrid cloud architectures and services versus managing traditional IT. Training IT and security operations personnel on the appropriate architecture helps ensure they respond to real signals and not noise based on legacy assumptions.

Most critical, however, exponential data growth from increased multicloud infrastructure, application, and network traffic has outpaced the ability of most monitoring and event platforms to effectively leverage data to detect, alert, and prevent security events. According to one estimate, more than half of the security-related digital exhaust is not even being used in security analytics because the data cannot be accessed and processed in time. Effective cloud operations implement scalable data aggregation and analytics capability to maintain event management integrity.

a50004854ENW, Rev. 1