Best Practices: Cloud Governance

Processes: The Cloud Computing Playbook

by Andras Cser and Lauren E. Nelson

October 9, 2019 | Updated: October 28, 2019

Why Read This Report

Transitioning workloads and data to the cloud is unstoppable — but the most difficult question is how to govern the process so you have a predictable, accountable, and scalable transition that accounts for the diverse interests of the internal stakeholders and the regulators. This report gives infrastructure and operations (I&O) and security and risk (S&R) professionals a blueprint and best practices for cloud governance, accounting for stakeholders, workload targets, processes, and tools.

Key Takeaways

Lack Of Cloud Governance Jeopardizes Cloud Transitions And The Use Of Cloud

Cloud governance shouldn't be a retroactive, afterthought process. Unless enterprises properly plan and execute a cloud migration, they quickly face near-certain chaos. At a US-Canadian bank, Forrester has witnessed workload repatriations from the cloud to on-premises because the bank lacked a robust cloud governance regime.

Cloud Governance Is A Foundational Building Block Of Cloud Security

Only a formalized cloud governance process can guarantee that a firm will be able to ensure a cost-efficient security regime for data, apps, and other resources in the cloud. Avoiding data breaches and meeting regulatory compliance mandates isn't optional, given the fact that remediation costs, sanctions, and fines are rapidly increasing.

Best Practices: Cloud Governance

Processes: The Cloud Computing Playbook

by Andras Cser and Lauren E. Nelson
with Glenn O'Donnell, Jenny Thai, and Diane Lynch

October 9, 2019 | Updated: October 28, 2019

Table Of Contents

Related Research Documents

Adoption Profile: Public Cloud In North America, Q3 2019

The Forrester Wave™: Cloud Security Gateways, Q1 2019

Gauge Your Cloud Maturity

Hybrid Cloud Security Best Practices

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Establishing A Pervasive Cloud Governance Program Is Mandatory

Cloud is no single technology. It's software. It's developer tools and platforms. It's infrastructure delivery models. And in any given category, enterprises are adopting multiple versions. To keep up with this exploding landscape of vendors, I&O and S&R pros find they need a pervasive governance program to respond to the various technologies; vendors; and speed with which security, compliance, or cost issues occur. Forrester defines cloud governance as:

> *The ability to provide strategic direction, track performance, allocate resources, and modify services to ensure meeting organizational objectives without breaching the parameters of risk tolerance or compliance obligations.*[1]

This practice is inclusive of cloud security; we outline our top cloud security recommendations in the Forrester report "Hybrid Cloud Security Best Practices." Enterprises must build out full cloud governance practices because:

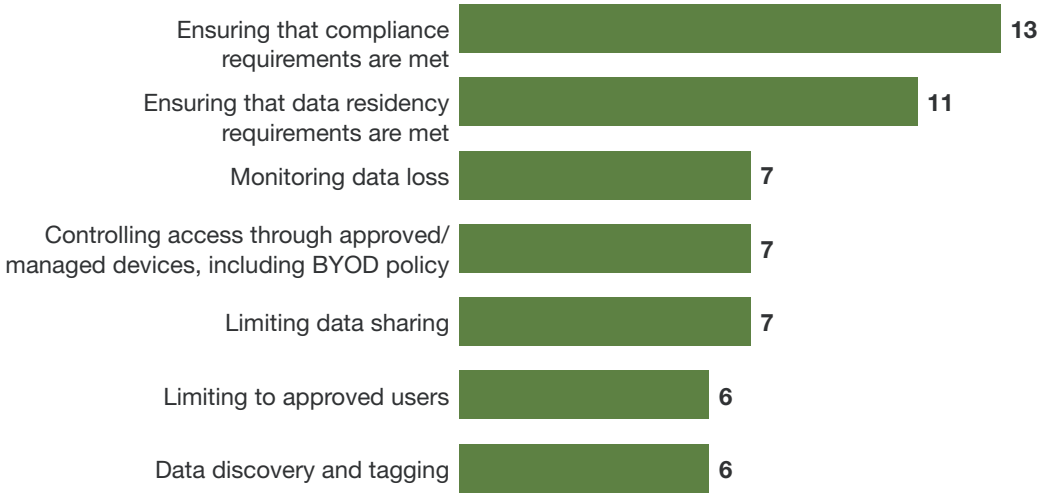
- **Cloud serves critical apps.** Over half of surveyed infrastructure technology decision makers at enterprises leverage public cloud (61%).[2] In the early days, this represented small new development environments, websites, and mobile apps, but since 2015, public cloud has grown to include legacy applications migrated from on-premises data centers. Mission-critical workloads can live on the public cloud and at scale. For example, a US bank aims to move 85% of its on-premises infrastructure to the cloud by 2022, and a large food manufacturer has moved all workloads to public cloud platforms outside its manufacturing-specific infrastructure. With usage exploding, enterprises struggle to control costs and unique configurations and reduce costly human error.
- **Cloud costs are rapidly increasing.** Cloud autoscales to adjust consumption and allows developers to procure new resources quickly. Although cloud provides organizations with the agility to support modern demands, leaving it ungoverned could lead to significant excess spending. Similarly, software-as-a-service (SaaS) technologies are easy to obtain, but failure to track licenses or manage your SaaS portfolios can lead to fines or overspending.
- **Data protection is mandatory — everywhere.** On average, surveyed infrastructure technology decision makers at enterprises report that 39% of their infrastructure is in an owned facility, 19% is in a colocated facility, 22% is in a public cloud, and 20% is hosted or outsourced in another environment.[3] This, paired with the reported hundreds of SaaS applications in use as well as increasing pressures for GDPR compliance, emphasizes that enterprise data is everywhere.[4] Forrester's interviewees tell us that protecting data in the cloud is mandatory (see Figure 1). Although the underlying capabilities are robust and auditor-approved, enterprises must seek complete data protection or deal with the kind of situations that Accenture, Capital One, and Verizon Wireless are facing.[5] With data everywhere, full cloud governance requires a different approach to data management and protection.

› **Cloud increases third-party risk.** With cloud workloads in the picture, the risk surface of the firm increases. To counter this increased risk of data breaches, a formalized set of controls and processes to understand and control risk from third parties, including cloud platform providers, managed security service providers, and even security vendors, is mandatory.

› **Cloud governance can't slow down productivity.** Traditional approaches to governance that restricted cloud use and forced slow procurement processes or approvals are no longer acceptable to business users. This inflexibility leads to circumvention, or with more agile leaders, to replacement. Without significant efforts to establish a governance program that first enables and then seamlessly weaves optimization and governance into business usage, cloud usage brings risk across performance, cost, access, compliance, and data protection.

FIGURE 1 Monitoring Compliance And Data Protection Are Top Enterprise Cloud Concerns

"Which of the following does your company utilize for cloud data governance?"
(Number of responses)



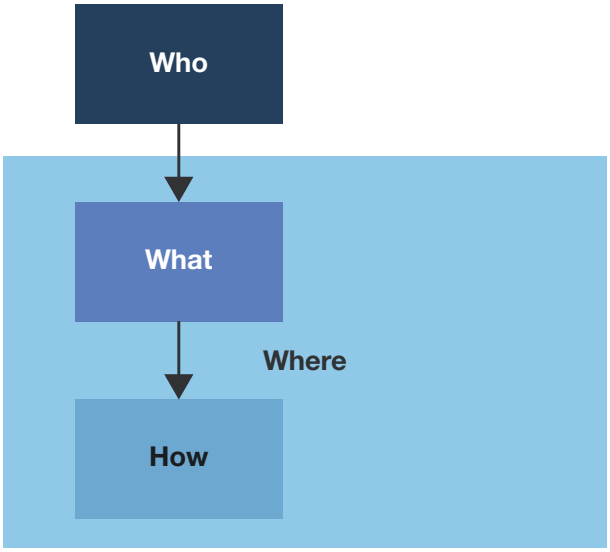
Base: 20 security professionals at end user and vendor companies
Note: Multiple responses were accepted.
Source: Forrester interviews

The Structure Of Cloud Governance

You can't have a solid cloud governance structure without fully understanding the scope of what exactly you're trying to govern in your cloud portfolio. An overall structure for cloud governance will ensure:

- **Repeatability.** The structure guarantees that cloud governance won't merely be an enthusiastic, one-off checkbox exercise. Documenting a process and structure will help make cloud governance become second nature across the entire organization. This also aids with meeting regulatory compliance requirements.
- **Executive support.** If you can show a formal structure for cloud governance, it's easier to gain and ensure the ongoing support of senior management. It's also a good idea to detail the benefits of a cloud governance process, including a shorter administration cycle time and less rework, in your organization's cloud governance framework and documentation.[6]
- **Coverage.** Your firm may have many different areas and infrastructure components that it wishes to cover in cloud governance, including, but not limited to, on-premises, private clouds, public clouds, and managed workloads. Having a planned cloud governance process allows S&R and I&O professionals to comprehensively view cloud workloads. You have to understand the stakeholders (the "who"), the activities (the "what"), the infrastructure components you're covering (the "where"), and the best practices of cloud governance (the "how") (see Figure 2).

FIGURE 2 Clearly Define The Who, What, Where, And How Of Cloud Governance



Best Practices: The Who, What, Where, And How Of Cloud Governance

Cloud computing allows business users to procure new services on demand, increasing their productivity and encouraging innovation across your company. The goal of a cloud governance framework is to provide guardrails for these innovators without impeding speed or other cloud benefits. For large organizations, having one central governing body that manages all cloud usage will quickly create a bottleneck. While standardizing policies is critical to success, a federated approach to management and continuous improvement is what you need today. To set standards across the entire organization, you need the who, the what, the where, and the how to work together.

Who: The Internal Stakeholders Of Cloud Governance

Cloud governance is impossible without involving key stakeholder groups and their dedicated representatives, who should be at least 10% to 15% dedicated to maintaining a cloud governance process. Forrester's clients have identified seven main types of cloud governance stakeholders and the reasons why they care about cloud governance:

- **Cloud architecture.** Cloud architects supervise the company's cloud systems, including strategy, application designs, approval plans, and platform decisions. Cloud architects help establish the cloud governance strategy and prepare a plan to successfully implement this strategy through templates and automated policy. Ungoverned environments lead to cost escalation, overlap, and failure to comply with security and regulations.
- **IT security.** Security administrators are responsible for protecting IT infrastructure, edge devices, networks, applications, and data against breaches and responding to any attacks. For cloud governance, security pros work with cloud teams to set policies while ensuring that they cover threat detection and protection, all without compromising the productivity and experience of cloud users. Security pros who drag their feet on cloud quickly find themselves out of the conversation — yet still responsible at time of breach.
- **Network operations.** Network administrators maintain enterprise networks while problem-solving for any issues or new technologies that the business or development wants to use. For cloud governance, network administrators help problem-solve for the shifting sourcing models and minimize the burden of data transit costs and latency. Doing so will aid the organization and justify networking investments.
- **Compliance.** Compliance officers ensure that the organization operates in a legal and ethical manner. In terms of cloud governance, this individual will be responsible for mapping cloud usage to the regulations that organization is beholden to. For some, this will mean rewriting internal policies to align to both the intent of the regulation and the technologies that the business and developer groups wish to leverage. Failure to update these practices for cloud will quickly lead to circumvention and expose the organization to greater risk.

- **IT operations.** Operations handles the day-to-day activities of IT to ensure that systems, services, and infrastructure run reliably and securely. IT operations responds to alerts and approves suggested optimization tasks while ensuring the health of cloud systems. Failure to govern means loss of this critical role within the organization.
- **Developers.** Developers design, install, test, and maintain software. Eventually, cloud governance will be invisible; however, in the interim, developers must work with their cloud experts to abide by policies prior to retroactive or proactive policy enforcement. By actively complying, they more efficiently use their cloud budgets while protecting their organization against breach and brand damage.
- **DevOps.** DevOps pros hold a unique position in some organizations as more technical developers that enjoy power user status, often creating some of the organization's most technically challenging applications or devising a repository of templates for developers to consume. DevOps users help ensure that their usage incorporates governance as they receive custom access or apply policies to the templates they create for distribution.

What: Areas And Categories Of Cloud Governance

The firm should clearly define the scope of cloud governance, i.e., define the cloud areas and processes that cloud governance covers. Forrester recommends that your firm include the following areas and processes:

- **Cost optimization, budgets, and billing integration.** Cloud presents a new subscription-based cost model. Public cloud platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform charge per individual service. A cloud bill can be thousands of pages long. Billing departments need a way to interpret bills, sync to existing systems, and charge back to individual departments. Similarly, the chaos of cloud bills makes it difficult to decipher whether the correct configurations are in use, unused resources have been turned off, or the right usage commitment has been selected, e.g., reserved instances or on-demand.
- **Regulatory compliance.** Forrester sees firms most often ask for SOC 2 Type 2 and ISO 27017 and 27018 certifications, not only for the underlying infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS) platforms but also for SaaS business apps; they need their own certification — the platform's certification isn't enough. GDPR and other regulations or requirements often dictate that sensitive data, especially personally identifiable information (PII) can't be stored outside of jurisdiction (data sovereignty) or be transmitted via networks outside of jurisdiction (route sovereignty).[7]
- **Cloud migrations and enablement.** "Cloud washing" and dumb lift-and-shift of data and workloads to the cloud without a proper governance structure and oversight usually lead to data sprawl, inadequate data protection, high costs, and audit findings. The configurations and protection appropriate for a workload on-premises are rarely the correct answer in a public cloud. Forrester's interviewees indicate that cloud migrations are a great opportunity to replatform,

reconfigure, or refactor applications to use cloud-native storage, databases, containerization, and logging. Cloud governance should proactively extend to the choices and ongoing use of cloud-native tools while implementing the appropriate protection and resource allotment to each relocated workload.[8]

- **Onboarding, permissions, and access.** Your firm must have a regimen of how it onboards, manages, and offboards IaaS, PaaS, and SaaS cloud workloads. A North American insurer told Forrester it uses three categories of SaaS applications: sanctioned/supported apps (Box, Office365, or Salesforce), tolerated apps (personal social media, including Facebook, LinkedIn, and Twitter), and prohibited (confirmed cloud malware). Sanction access to your cloud applications and platforms based on the sensitivity of data you've stored in them.
- **Threat detection.** It's critical to be able to automate the detection of changes and cloud threats that exist: 1) in access to the administrative consoles of cloud platforms (Amazon Web Services, Google Cloud Platform, or Microsoft Azure); 2) in configuration of cloud workloads (compute, storage, and network); 3) in cloud workload instances (hypervisor, guest/host OS, containers, and functions, including Lambda; 4) in data movement between the corporate network and cloud workloads; and 5) in data movement between cloud workloads.
- **Threat prevention.** Detecting threats but not responding them is like crying loudly when you see a drowning person but not throwing them a lifesaver. Threat detection and prevention solutions and methods should integrate. When you detect a threat, the solution should have an automated or semiautomated way to remediate. It should also quarantine malicious files and disallow transfer of documents with sensitive data in them.

Where: Governance Models For Different Cloud Technologies And Deployment Models

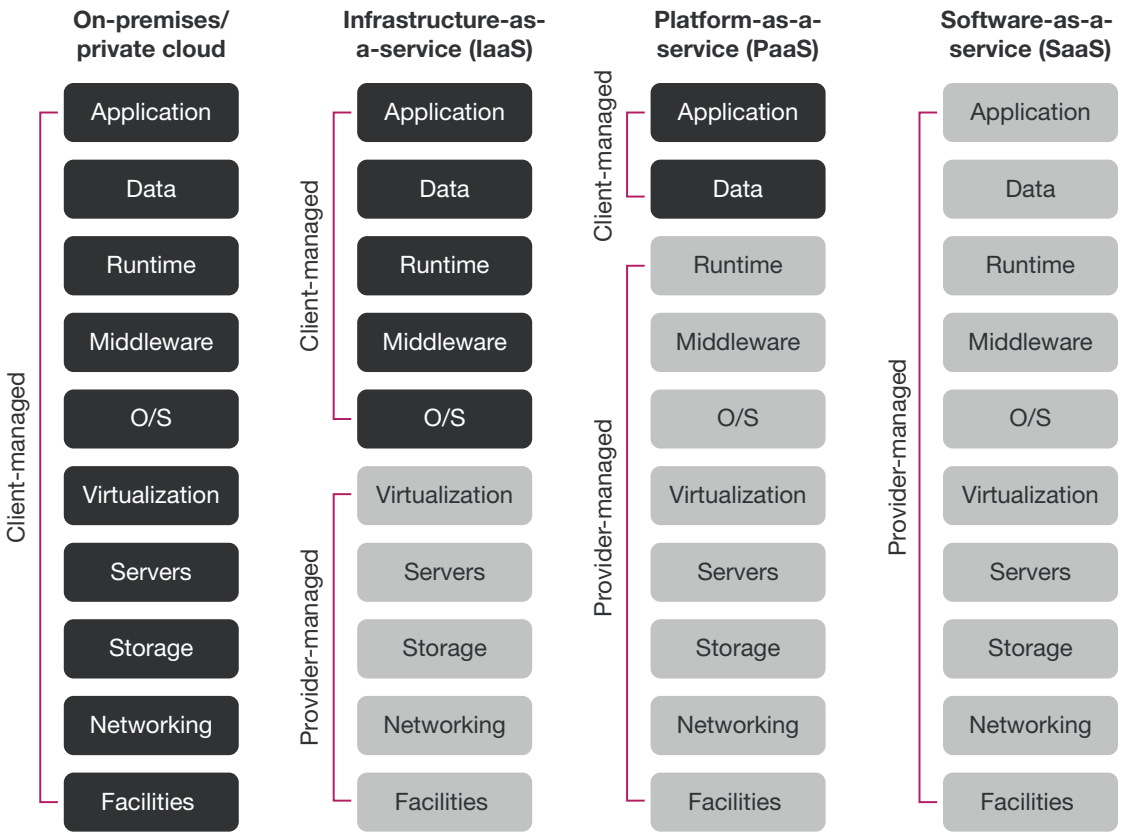
Cloud governance has to extend to all aspects of cloud use at the enterprise. The best way to kick off a governance practice is to map cloud usage to the four classic variations of cloud technologies and deployment models and build out the added complexity of your usage from there. For example, some companies that leverage private cloud platforms choose to enhance the experience with remotely managed services, which adds additional complexity to your private cloud governance map. Other companies leverage serverless on their public cloud platform of choice, which shifts some responsibilities to the public cloud vendor. Forrester recommends that S&R and I&O professionals start with the following classic cloud target areas and customize from there — often presenting the simplistic model in strategy materials but having more complex mappings that match their usage (see Figure 3):

- **Private cloud (on-premises).** While using on-premises or private cloud services is deceptively simple ("we need to do everything"), governance practices for on-premises private cloud deployments are notably missing.[9] Many got unofficial permission to bypass traditional governance process in response to digital transformation pressures; however, this is notably changing. Enterprises are using governance to help control costs to reinvest in the second wave of their initiatives while preparing for larger investment outside their own data center with modern security

frameworks and automation. Clients are responsible for all aspects of cloud governance across the stack. Although many IT pros like this control, it also places the weight of investment, updates, and management solely on their shoulders.

- **IaaS.** IaaS platforms deliver infrastructure services hosted in an external cloud environment. This includes dedicated hosted private cloud (e.g., Rackspace OpenStack Private Cloud and Virtustream Enterprise Cloud), and multitenant public cloud platforms (e.g., Amazon Web Services, Google Cloud Platform, and Microsoft Azure).[10] For IaaS, providers manage the data center and up to the hypervisor, with some shared hypervisor responsibilities. Clients are responsible for auditing the provider, data protection (in use, in transit, and at rest), patching, access and usage management, business continuity, and compliance above the provider offering.
- **PaaS.** PaaS is a terribly complex space, with many variations of management layers. Some carve out 16 unique categories; we highlight the many variations in the Forrester report "An I&O Pro's Guide To Platform-As-A-Service." At its core, PaaS includes application or developer services, usually hosted and with management of OS, middleware, and runtime.[11] Each segment of PaaS targets productivity for a certain segmentation of developers. Customers no longer do patching or technology selection for underlying components; however, they're still responsible for data protection, compliance for unmanaged layers, and managing access and usage.
- **SaaS.** SaaS is a hosted software solution that resides in a cloud environment, but the client is responsible for auditing the provider and securing data in transit.[12] The software provider takes on the responsibility of the full stack outside data in transit, backup, access, and usage. However, many software providers increasingly don't own the data centers where their software runs. Many leverage IaaS vendors to host their software, splitting up the responsibility model even further. Companies leverage hundreds of SaaS applications, making a custom governance model for each application impossible. Most enterprises may make custom models for their largest SaaS suites while standardizing the remainder.

FIGURE 3 Each Cloud Model Shares Governance Responsibility Differently Across Providers And Customers



How: Models, Tools, And Best Practices For Cloud Governance

So far, we've defined the dots of cloud governance (who, what, and where). Now it's time to connect them — that's the how. You should approach the connective tissue, or the how, as:

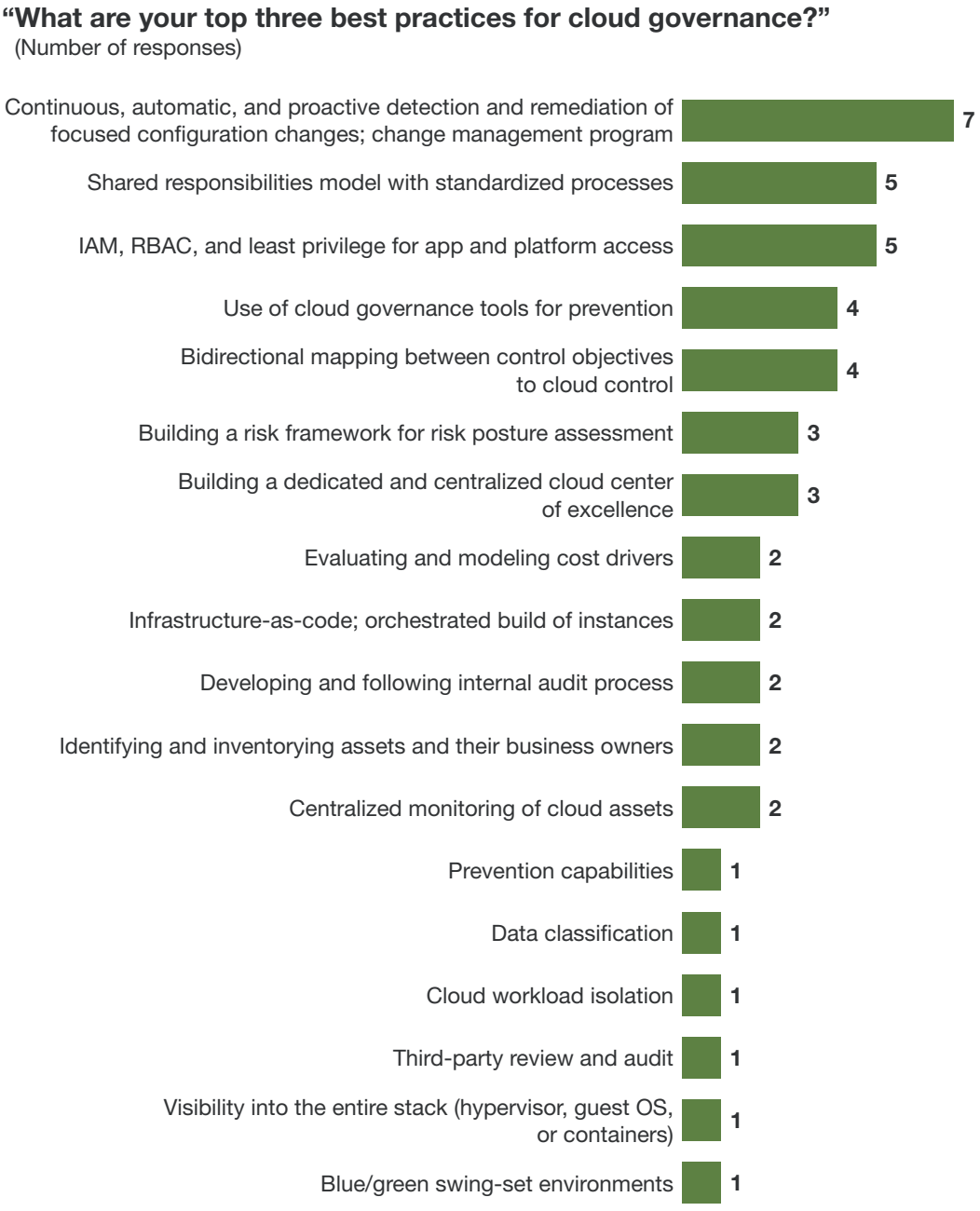
› **Creating a RASCI chart.** Enterprises must map out their cloud practice to the stakeholders, using a responsible, accountable, supportive, consulted, and informed (RASCI) model, as outlined in Forrester's report "Set Risk And Compliance Accountability With Forrester's RASCI Tool." This ensures a repeatable process, reduces the number of assumptions and misunderstandings, and leads to a higher-efficiency cloud governance regime.

› **Automating everything.** Manual tasks create delays at scale, inability to sort through massive lists of alerts, organization vulnerabilities tied to specific individuals, and room for human mistake. You can't track the build-out, configuration, and ongoing inventory of your cloud infrastructure on an Excel spreadsheet or Visio diagram. You can't maintain a cloud-cost optimization spreadsheet manually. You can't provision for developers through email requests or tickets. You

need automation. Continuous integration/continuous delivery (CI/CD) solutions, such as Chef, Jenkins, or Puppet, assist with building out your cloud infrastructure-as-code (IaC) to help with initial provisioning and more secure configuration and reduce administration overhead, reworking, and cost of operations. Cloud monitoring, optimization, and security tools all heavily leverage automation to identify areas for attention and recommendations for remediation.

- **Delivering education.** Part of governance is outreach. Your organization needs to see how it can work smarter and incorporate best practices. These efforts not only close the gap between provisioning and optimization or provisioning and compliance but also act as an outreach that helps build the relationship between your center of excellence (CoE) or operations teams and your business or developer customers. Visibility tools go a long way toward educating, as do pizza, T-shirts, and humor.[13]
- **Proactive and reactive approaches.** Business users and developers are in charge of their technical decisions, making any governance program contingent on their support and I&O's ability to appear invisible. However, this isn't an overnight transition. Rather than serving up a compromised experience, many companies opt to take a reactive approach to cloud governance while they build out the necessary artifacts and automation to deliver it proactively. They do this to preserve the relationship with the business at the most critical moment. When they're ready, they switch to proactive models to eliminate temporary noncompliance and avoid rework for their users.
- **Leverage advice from your peers.** In a Forrester survey of 20 security and risk stakeholders, respondents identified best practices of cloud governance (see Figure 4). They include 1) continuous, automatic, and proactive detection and remediation of focused configuration changes and creating a robust change management program; 2) setting up and adhering to a shared responsibilities model with standardized processes; 3) deploying identity and access management (IAM), role-based access controls (RBAC), and least privilege for app and platform access; 4) using cloud governance tools for prevention; and 5) establishing bidirectional mapping between control objectives to control cloud.

FIGURE 4 The Best Organizations Govern Cloud With The Right Balance Of Change Management



Base: 20 security professionals at end user and vendor companies
Note: Multiple responses were accepted.
Source: Forrester interviews

Endnotes

[1] See the Forrester report "Adapt Your Governance Framework For Cloud."

[2] In 2018, 61% percent of North American and European infrastructure technology decision makers working at enterprises (1,000 employees or more) reported that their firms were in the process of implementing, had already implemented, or were expanding/upgrading their implementation of public cloud. Source: Forrester Analytics Global Business Technographics® Infrastructure Survey, 2018.

[3] Surveyed North American and European infrastructure technology decision makers working at enterprise firms (1,000 employees or more) that prioritize servers stated that 39% of their infrastructure were located in owned facilities, 19% in colocation facility, 22% in public cloud, and 20% in hosted private cloud or outsourced. Source: Forrester Analytics Global Business Technographics Infrastructure Survey, 2018.

[4] GDPR is the European Union General Data Protection Regulation.

[5] Source: Steve Andriole, "The Capital One Data Breach is No Exception & Why We Can Expect Many, Many More," Forbes, July 30, 2019 (https://www.forbes.com/sites/steveandriole/2019/07/30/the-capital-one-data-breach-is-no-exception-why-we-can-expect-many-many-more/#355be61efc48).

[6] For more information on Zero Trust, see the Forrester report "The Zero Trust Extended (ZTX) Ecosystem."

[7] Forrester's interactive data privacy heat map provides detailed, current information about global privacy and data regulations. Source: "Privacy And Data Protection By Country," Forrester Global Heat Map (http://heatmap.forrestertools.com/).

[8] For more information on cloud migration, see the Forrester report "Top 10 Facts Tech Leaders Should Know About Cloud Migration" and see the Forrester report "Best Practices: Cloud Database Migrations."

[9] Private cloud comes in many flavors. At its most basic level, there's enhancement of existing owned software with automation tooling, e.g., VMware vSphere with Ansible, Chef, Puppet, or Terraform. Companies taking this approach tend to investment in software-defined infrastructure (SDI) and IaC as they modernize their data centers. Some companies take a more developer-centric view, first leveraging a development platform, e.g., Pivotal Application Services or Red Hat OpenShift, atop their platform of choice. Most recently companies look to Kubernetes (K8s) distributions. For more information on the evaluation of this space, see the Forrester report "The Forrester New Wave™: Enterprise Container Platform Software Suites, Q4 2018."

[10] Although both fit in this category, it's not a perfect map to infrastructure responsibilities. The hosted private cloud market is equally split between vendors that manage the OS layer by default and those that don't. Public clouds contain more than infrastructure services. In fact, much of what they differentiate on are application and developer services that more classically fall into the PaaS categorization.

[11] Forrester outlines a more advanced version of PaaS. See the Forrester report "An I&O Pro's Guide To Platform-As-A-Service."

[12] Forrester outlines a more advanced version of SaaS. See the Forrester report "Buy Then Build: The New World Of SaaS Development." Similarly, there are ASP providers that pose as private SaaS but that lack many of the benefits. See the Forrester report "Beware Of The 'SaaS' Trap."

[13] For more information on cloud strategy, see the Forrester report "Build A Pragmatic Cloud Strategy That Delivers Real Value To Your Organization."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
- Infrastructure & Operations

Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

158301