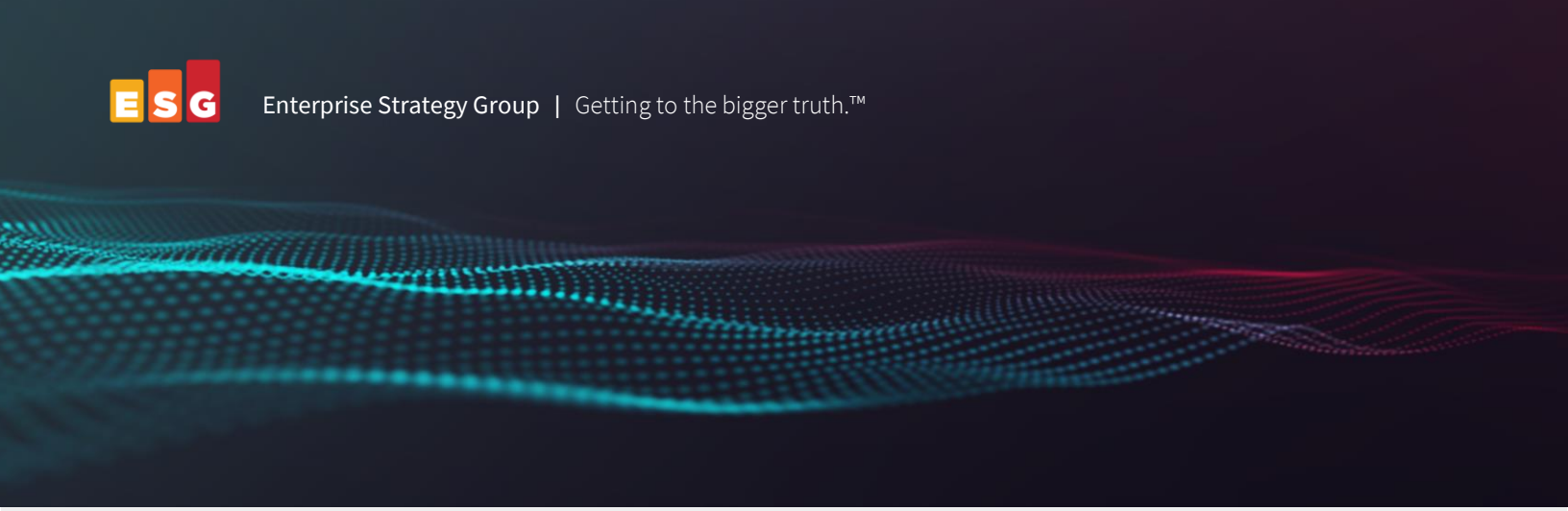


ESG WHITE PAPER

Improve Configuration, Compliance, and Auditing with AWS

Resource Inventory Monitoring and Management in the Cloud Using AWS Config and AWS CloudTrail

By Mark Bowker, Senior Analyst

September 2020

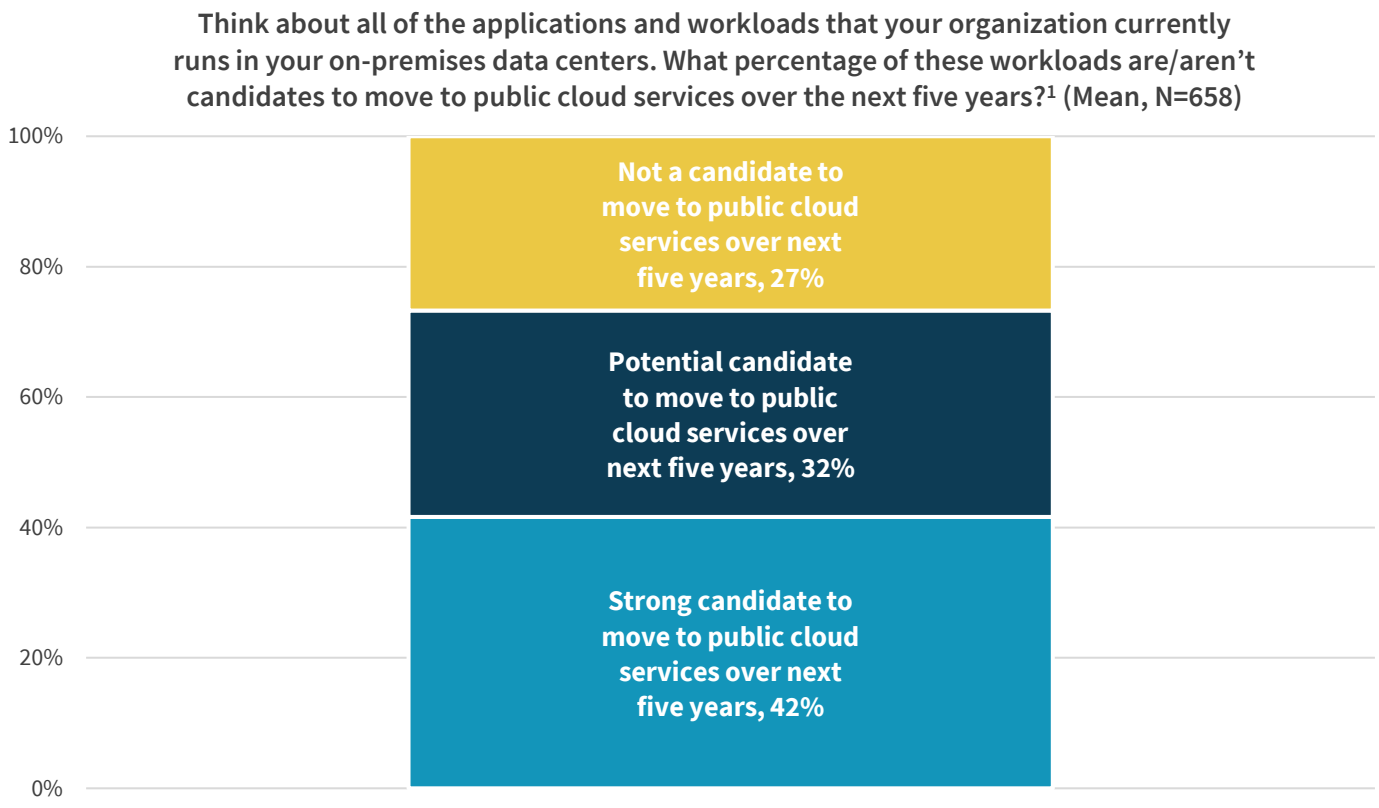
This ESG White Paper was commissioned by Amazon Web Services and is distributed under license from ESG.

Contents

How Important Are Configuration Audits and Compliance in Cloud Environments?

As cloud and hybrid resources grow in an organization, it is more difficult to know whether resource configurations are efficient and compliant with best practices, internal policies, and applicable internal and external regulatory requirements . On average, nearly three-quarters of remaining on-premises workloads could move to public cloud providers in next five years (see Figure 1),[1] but the traditional mechanisms of inventory management, compliance verification, and configuration are no longer effective. Information technology organizations now require tools that match the dynamic nature of cloud and align with the configuration, compliance auditing, and policies that are active in the cloud. Small and mid-size businesses with limited IT resources may be especially hard-pressed to match those compliance requirements and so may businesses that have accelerated public cloud usage due to the COVID-19 pandemic.[2]

Figure 1. The Data Center of the Future: More Cloud, Remote Mirroring, and Automation



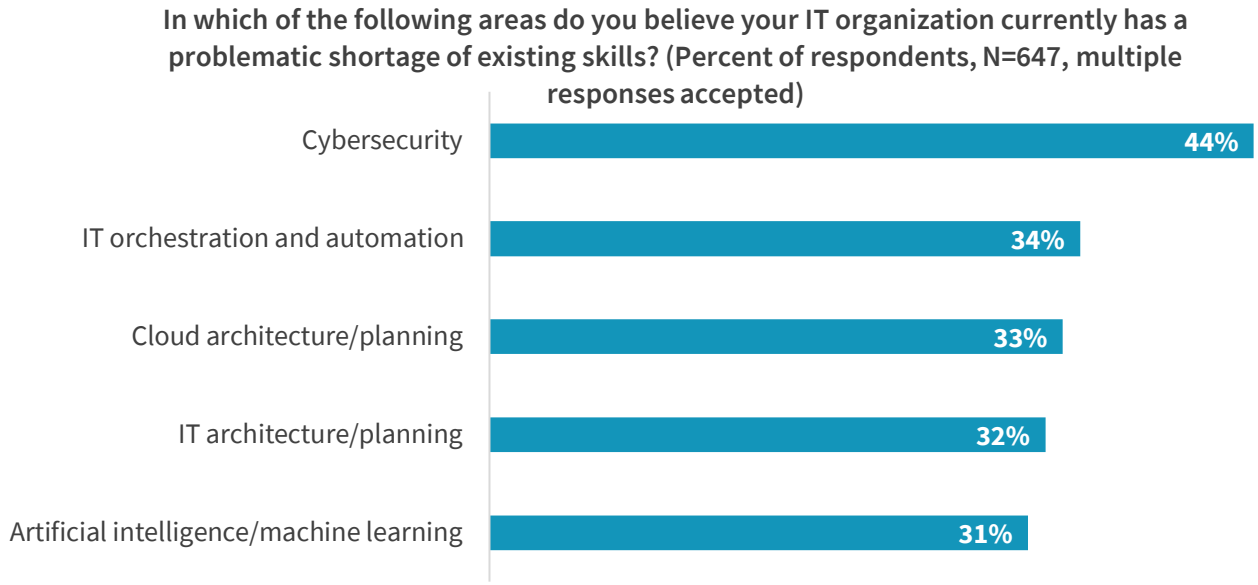
Source: Enterprise Strategy Group

As organizations move to the public cloud, a lack of talent/skills can lead to greater risk. As shown in Figure 2, cybersecurity skills, IT orchestration and automation, and cloud architecture/planning are the most cited areas of problematic skills shortages reported by ESG research respondents.[3] The lack of talent/skills can lead to greater risk of inadequate process, non-standard processes and configurations, and poor oversight. For organizations that lack the right people and tools, resource misconfiguration is often pointed to as the leading cause of breaches, security issues, and compliance defects.

[1] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Research Report, *The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies*, June 2020.
[3] Source: ESG Research Report, *2020 Technology Spending Intentions Survey*, January 2020.

Misconfigurations that aren't caught and remediated immediately can create lingering vulnerabilities, increasing the risk of breach, resource deletion or change, and service disruption.

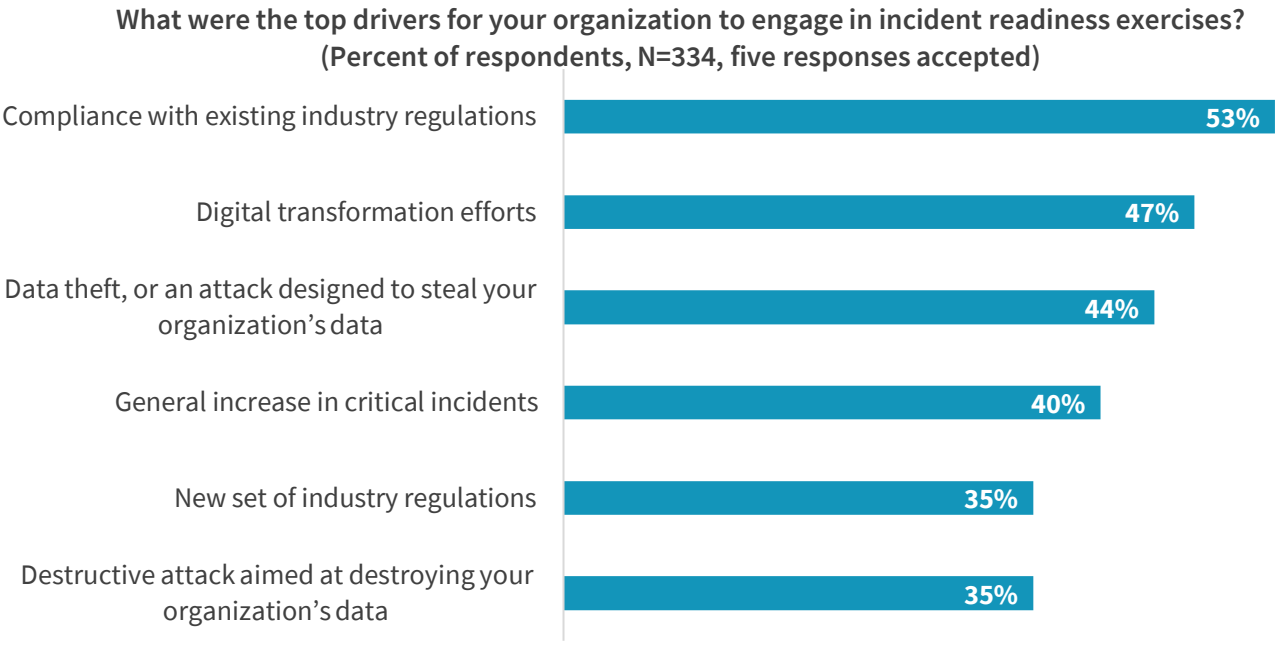
Figure 2. Top Five Areas of Skills Shortage



Source: Enterprise Strategy Group

Additionally, according to a separate ESG research study, compliance is one of the top drivers for incident readiness (see Figure 3).[4] Audit and compliance are key aspects of cybersecurity that require the skills and tools for organizations to proactively respond to threats, misconfigurations, and regulations.

Figure 3. Top 6 Drivers of Incident Readiness



Source: Enterprise Strategy Group

[4] Source: ESG Master Survey Results, *Incident Readiness Trends*, August 2020.

The pace of cloud adoption opens the door to less than adequate IT practices and exposes potential areas for which the lack of best practices and tools could slow and even stall the pace of cloud adoption. It is far better to implement configuration best practices upfront to be sure a resource, regardless of how long it is up and running, doesn't violate any policy.

Creating Business Value from Configuration, Compliance, and Auditing

Instead of building tools, setting up new processes, or using manual processes, organizations can automate, manage, and audit both existing AWS and third-party resources with existing tools and services that are designed for the dynamic nature of cloud. These tools and services simplify configuration and compliance while accelerating benefits such as reducing operational downtime, meeting service-level agreement (SLA) objectives, and enhancing security.

Be Proactive About Configuration Best Practices

- Create a resource inventory.
- Apply appropriate policies.
- Track resource changes and audit resources.
- Gather and share insights.
- Remediate non-compliant resources safely.

The AWS Config and AWS CloudTrail services can be enabled in a few clicks to provide powerful tooling that helps automate the process of collecting the information required to assess compliance. They help organizations extend the value of investments they have already made in cloud resources and other assets. IT teams can perform compliance and risk audits, analyze security status, manage changes, and troubleshoot issues—all without sifting through logs. Working at cloud speed, IT teams can act on concerns or issues immediately and accomplish these outcomes:

- Speed fulfillment of audit requests for regulations such as the Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard, and National Institute of Standards and Technology Probabilistic Signature Scheme.
- Enable security analysis by monitoring the log of user and system actions affecting AWS resources and the history of changes within an account.
- Remediate non-compliant resources automatically, saving IT time and promoting standardization.
- Expand compliance management with AWS Managed Services and third-party products on the AWS Marketplace, to improve flexibility and resource utilization. This extensibility also helps lower resource management costs and increase IT efficiency.

The challenge of operating in the cloud is how dynamic it is. AWS Config gives us a great view of the environment, what exists where, and in which account and region. We use AWS CloudTrail for debugging and for developing advanced protections. From a security and auditing perspective, I don't think companies could operate successfully without AWS CloudTrail.

--Director, Cloud Security

Recording and Evaluating Resource Configurations with AWS Config

For on-premises workloads, organizations have traditionally used configuration management database (CMDB) solutions. Autoscaling and ephemeral workloads, however, make the cloud far more dynamic. Supporting central cloud IT calls for resource inventory management, configuration, and auditing that provides:

- Comprehensive visibility.
- Real-time asset discovery.
- Continuous tracking of configuration changes.
- Real-time compliance evaluation and notifications.
- Automatic remediation of non-compliant resources.

AWS Config Integration with CMDBs

- Evaluation of non-AWS resources such as third-party and custom resources like Active Directory and GitHub repositories.
- The ability for CMDB users to provision, manage, and operate AWS resources natively.
- Integration with AWS Systems Manager to extend configuration recording to Amazon EC2 instances and on-premises systems.
- AWS Service Management connector, which enables integration with external systems such as ServiceNow or Jira Service Desk.

AWS Config records the configuration of the infrastructure resources as well as non-AWS infrastructure resources. It tracks changes accurately and automatically at cloud scale through continuous monitoring and recording. With real-time views of resource inventory, configuration history, and configuration change notifications, users can quickly evaluate recorded configurations against desired configurations. IT teams are more efficient as they:

- Discover existing resources.
- Export inventory resources with configuration details.
- Determine how a resource was configured (the default is seven years of history).
- Review changes in configurations and relationships between AWS resources.

- Aggregate multi-account and multi-region views of configurations and compliance status for configuration consistency throughout accounts, regardless of location.
- Evaluate compliance on an event-triggered basis. Standardize evaluations in multi-account environments using Conformance Packs, which provide a common framework throughout an organization.
- Remediate non-compliant resources automatically based on rules.
- Rely on immutability, which prevents tampering after standardization.

Simplifying IT Operations and Governance

Compliance control mappings are a great first step in preparing to migrate compliance to the cloud. The maps make it easier to identify, standardize, and automate configuration compliance using AWS Config. Standardizing governance as much as possible saves time across many IT activities:

- Remediate non-compliant resources across AWS and non-AWS resources; use AWS Systems Manager OpsCenter for deferred remediation of non-compliant resources.
- View resources, check compliance status, and pinpoint non-compliant resources quickly using a visual console.
- Reduce the impact of changes by understanding how a change to one resource affects other resources.
- Use configuration change histories to help identify root causes of operational issues by correlating changes to events in an account (via integration with AWS CloudTrail).
- Enforce enterprise-wide compliance from a single point without having to retrieve information individually from each account or region.

Streamline Governance at Scale with AWS Config Conformance Packs

A common framework helps IT manage policy definitions, auditing, reporting, and more across multiple accounts and regions.

- Package a collection of AWS Config rules and remediation actions.
- Deploy the package across organizational accounts.
- Establish a baseline of policies and best practices.

Monitor Software on Amazon EC2 and On-premises Systems

AWS Config enables views of Amazon EC2 instances, virtual machines, and servers.

- Assess security risks.
- Troubleshoot performance issues.
- Track license usage.
- Evaluate compliance with guidelines and policies.

Tracking and Auditing User and Account Activity with AWS CloudTrail

AWS CloudTrail captures a log of all API calls for AWS account activity and tracks console log-ins useful for identifying problems such as potential brute force attacks. This helps IT teams to increase visibility of user and resource activity and API calls across the control plane, allowing them to accomplish other tasks rapidly:

- Apply search filters to find desired information.
- Define and invoke workflows upon detection of events that may pose a security risk.
- Ingest AWS CloudTrail events into a log management and analytics solution for further analysis.
- Use the API call history to investigate incidents and troubleshoot issues by reviewing activity (creation, modification, deletion) of AWS resources.

Bolster Security in AWS Accounts

AWS CloudTrail can improve security in the cloud with robust functionality:

- Provides continuous monitoring.
- Enables forensic investigation.
- Generates data useful for detecting unsecure or inappropriate changes.
- Captures and stores logs automatically to help IT teams find out-of-compliance events.

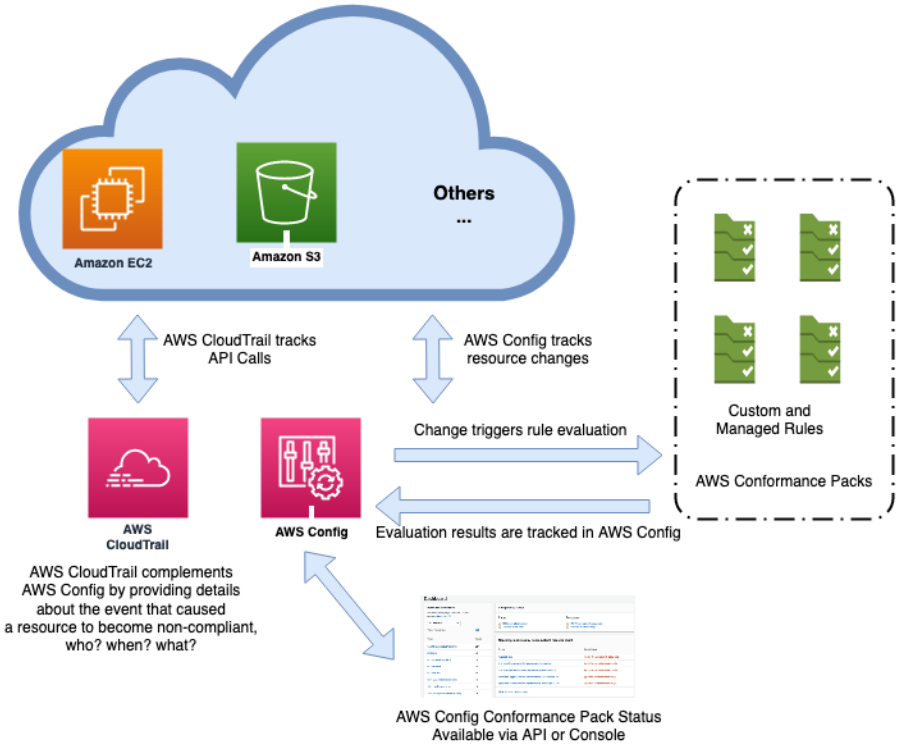
CloudTrail sends event information to the AWS CloudTrail console, Amazon S3 buckets, or Amazon CloudWatch Logs, allowing IT teams to act on events using Amazon CloudWatch Alarms and Amazon CloudWatch Events. CloudTrail provides AWS Config with the details of control plane (management) events and data plane events—covering the who, when, and from which IP address—that trigger a change.

AWS CloudTrail Insights monitors API calls and uses machine learning to generate events when volume is outside normal patterns. When CloudTrail Insights detects changes in API usage, it flags unusual activity such as:

- Jumps in resource provisioning.
- AWS Identity and Access Management actions.
- Gaps in periodic maintenance.

By monitoring, recording, and storing event activity, CloudTrail simplifies compliance auditing, operational troubleshooting, and security analysis. Whenever account activity threatens the security of AWS resources, CloudTrail helps organizations respond to events and threats that are based on defined workflows.

Figure 4. AWS Config and CloudTrail



Source: Enterprise Strategy Group

The Bigger Truth

Organizations race to the cloud for competitive and economic reasons, sometimes ahead of controls that enable resource inventory management and governance. Fortunately, AWS services already exist for configuration, compliance, and auditing purposes. Organizations don't have to slow their cloud journeys, reinvent wheels, rely on manual processes, or pursue an expensive DIY approach to build services. For these reasons, decision makers should strongly consider AWS Config and AWS CloudTrail, which have no prerequisites and do not require steep user learning curves.

When organizational leaders think about the cost of non-compliance and breaches, they realize it is never too early to implement good governance in the cloud, for which regulatory control mappings are an excellent first step.

The automated, integrated solution delivered by AWS Config and AWS CloudTrail enables businesses to focus on their core competencies while simultaneously enforcing best practices, internal guidelines, and regulations with native services that save time and effort. Additionally, the services simplify IT operations and strengthen security throughout organizations with built-in multi-account and multi-region management capabilities.

To learn more, IT leaders and internal audit teams can discuss their configuration, auditing, and compliance requirements with AWS.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188