

CISO's Guide to Cloud Security Transformation



Table of contents

| | |
|--|-----------|
| Table of contents | 1 |
| Introduction | 2 |
| Disclaimer | 2 |
| Prepare your company culture for cloud security | 3 |
| Think differently about security | 4 |
| Adopt a zero-trust philosophy | 4 |
| Take a risk-informed approach | 4 |
| Scale your security model | 5 |
| Evolve how your company works | 6 |
| Accelerate development timelines | 6 |
| Deploy and manage infrastructure as code | 6 |
| Evolve key security roles and responsibilities | 7 |
| Collaborate with your cloud service provider | 7 |
| Change how security roles are performed | 8 |
| Design your security operating model | 10 |
| Centralized security operating model | 10 |
| Federated security operating model | 11 |
| Hybrid security operating model | 11 |
| Identify cloud security best practices | 13 |
| Conclusion | 14 |

Introduction

This whitepaper is aimed at Chief Information Security Officers (CISOs) who are looking to the cloud to improve their security and at CISOs who find themselves moving to the cloud with the rest of their company.

Whether you are a CISO who is actively pursuing a cloud security transformation or a CISO who is being pushed towards the cloud, you are responsible for securing information for your company, your partners, and your customers. As information ecosystems grow more complex and new security threats emerge daily, your job of keeping that information secure—and maintaining trust in your company—is increasingly difficult.

In the face of these challenges, many companies and many CISOs are looking to the cloud for security. Cloud service providers can invest more in people and processes to deliver secure infrastructure and applications, can help you streamline and modernize your security approaches, and can help keep your information more secure.

Streamlining and modernizing your security in the cloud is about more than just changing technology and security implementations. It's about changing how your company thinks and works.

Those changes can feel daunting when you are new to the cloud. However, Google has been a leader and innovator in cloud security for years. We know how to prepare for a digital transformation, how to build an effective and sustainable cloud security operation, and how to collaborate with cloud security providers. This whitepaper explains how Google thinks about cloud security and gives you concrete steps to address the cultural, organizational, and operational changes that are required for a smooth and successful transition to cloud security.

As you prepare to move your security to the cloud, remember that the cloud is not just a bunch of servers. The cloud is a new way to think about your business and a new way to work. The cloud is a new—and better—way to approach security.

Disclaimer

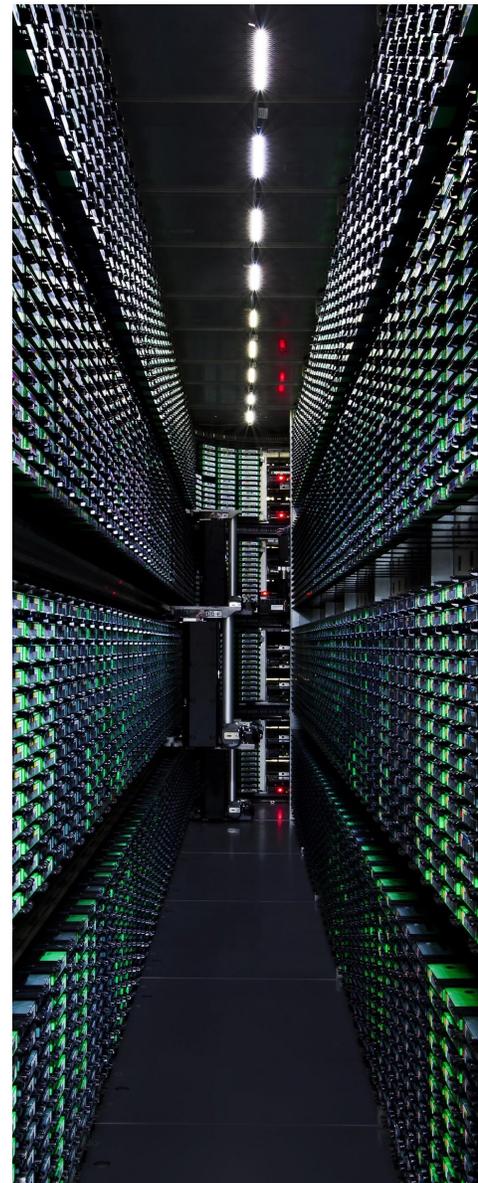
The content contained herein is correct as of February 2021, and represents the status quo as of the time it was written. Google Cloud's security policies and systems may change going forward, as we continually improve protection for our customers.

Prepare your company culture for cloud security

Organizations that succeed through any type of major change have strong underlying cultures and values that help to guide their transformation. For your business and your security operations to thrive through a digital transformation, you must ensure that you have instilled a strong security culture throughout the company.

What does a strong security culture look like? Each company is different, but companies with strong security culture typically share the following values:

- **Culture of security by default:** Security is not an afterthought, a “nice to have,” or a feature that’s added at the end of the development cycle. Instead, security is an expected part of all IT work from the earliest stages. For example, Google requires a security review for all development stages, from initial design documents to launch.
- **Culture of responsibility:** Security is not “someone else’s problem” or extra work that the security team makes the development team do. Instead, everyone shares responsibility for developing secure products and features.
- **Culture of awareness:** Education, documentation, and information sharing about security are pervasive throughout your company. Team members regularly share best practices for security. For example, Google security teams lead company-wide and team-specific security training sessions.
- **Culture of inevitability:** You are prepared for worst-case scenarios and ready to act if they occur. Failure scenarios are expected and response plans are widely discussed and understood. Google has a long tradition of simulating disaster scenarios to prepare for exactly these types of inevitable events.
- **Culture of review:** Open, transparent, and constructive code and design reviews are the norm across the company. Security is valued and included in these reviews.
- **Culture of sustainability:** IT work is well balanced between day-to-day operations and improvements for the future.



Think differently about security

As information ecosystems grow more complex, new threats and vulnerabilities emerge daily. As CISO, your thinking about security cannot be stuck in the past. You need to understand modern threats and modern security solutions to keep your information secure. Data-driven cloud security methods support these modern solutions, allowing you to efficiently secure your information, effectively mitigate risk, and quickly scale your company's services and user base.

Adopt a zero-trust philosophy

Traditional security approaches focus on hardening a secure perimeter and keeping threats outside of that perimeter. This perimeter model can lead to a significant underinvestment in configuring and securing internal applications and infrastructure and does not reflect the realities of modern security threats. Cloud security—really all modern security—means thinking differently because perimeters in modern information ecosystems are not well defined and not easily secured through traditional means.

To succeed with cloud security, you should reject the perimeter model and embrace a philosophy of *zero trust*. Zero trust means that, instead of trusting data and transactions after they have cleared your security perimeter, you verify every piece of data and every operation outside and inside your system. Constant verification, driven by automation, makes your information more secure against modern threats and lets you design information systems without the constraints of an inflexible perimeter.

Take a risk-informed approach

Cloud security also lets you think differently about risk. Traditional security approaches often take a risk-averse approach, cautiously avoiding threats, especially threats that existing security infrastructure cannot mitigate. However, in the current security environment, new threats are continuously emerging, your surface area is constantly increasing, and many threats are unavoidable.

Cloud security recognizes that these unavoidable threats exist and takes a *risk-informed* approach to securing your information. Risk-informed security is based on analyzing and assessing risks and then managing those risks in an informed way. For example, you can develop a risk taxonomy that details the risks that most concern you and your company, and then map the risks in your taxonomy to the controls for mitigating those risks. A risk-informed approach can help you address the most important security risks instead of addressing the risks that you already know how to mitigate.

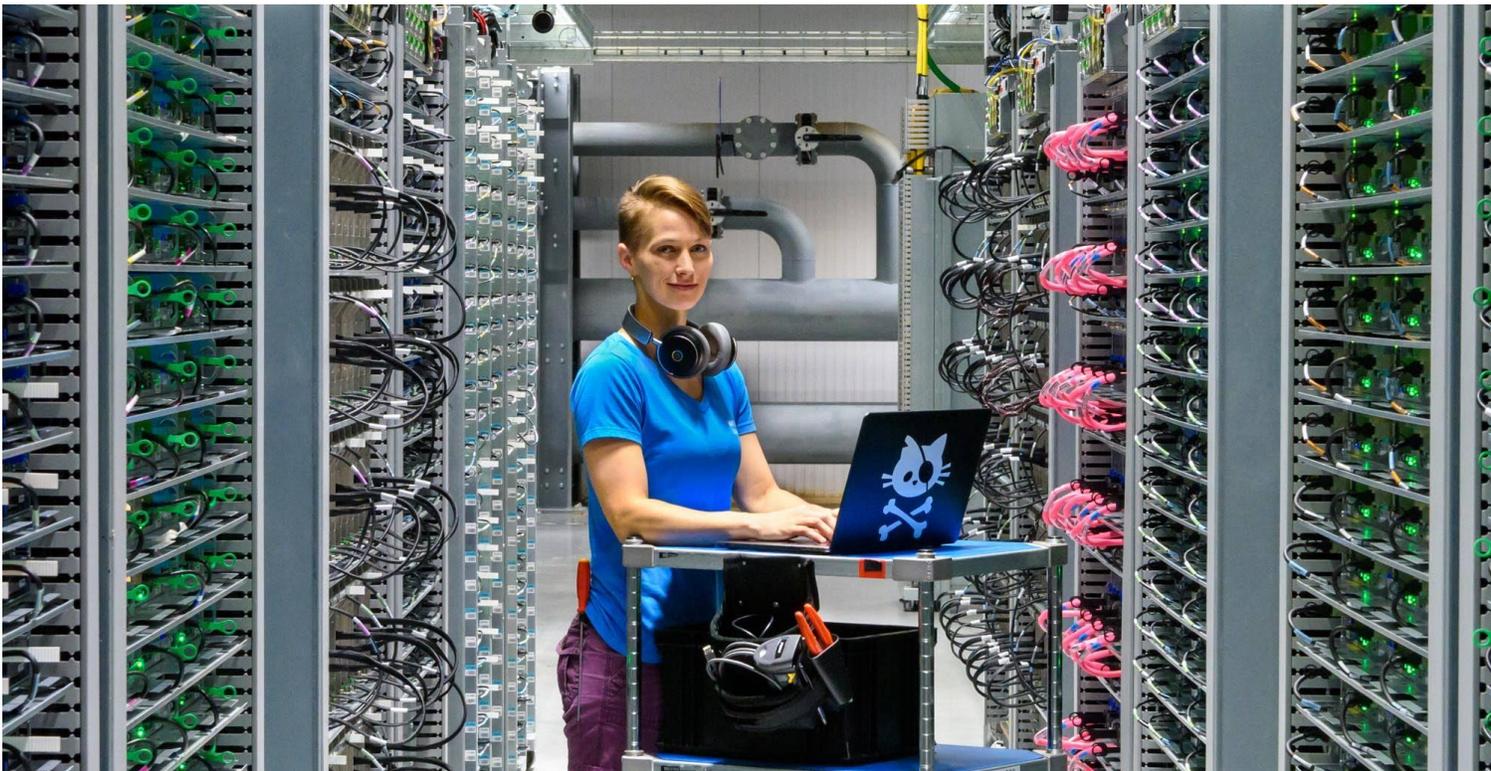
Cloud service providers make this risk-informed approach easier and more efficient for you by developing and maintaining many of the controls and tools that you need to mitigate modern security threats. For example, cloud service providers support key security telemetry, such as access logs and firewall logs, that can be difficult and expensive to develop in an on-premises environment. Cloud service providers also continuously update robust security processes around authentication and authorization keys.

Finally, remember that there are properties associated with the cloud that provide you with opportunities to manage security, and other risks associated with cloud, in different and enhanced ways. And as such, a well-executed migration to cloud can result in a net reduction of security, technology and other operational risks¹.

Scale your security model

Traditional security approaches can limit the scale of the systems that they aim to protect. After all, smaller and simpler systems are exposed to fewer threats and risks, right? Cloud security, which is scalable and data driven, lets you rethink these assumptions and scale your systems to millions of users and petabytes of secure data. For example, you can manage identity and access management (IAM) at massive scale by using secure services that have been developed by cloud service providers.

Traditional security approaches can also limit or distort the scope of the security controls that you develop. For example, traditional security infrastructure might be based on incomplete or inaccurate IT asset databases, rely heavily on manual review (leading to sample-based assurance models instead of complete security coverage), or assume a small and relatively static IT footprint. Cloud security can offer significantly greater breadth of security coverage and greater flexibility by using data-driven approaches to secure all relevant assets.



¹ [Strengthening Operational Resilience in Financial Services by Migrating to Google Cloud](#)

Evolve how your company works

When your business moves to the cloud, the way that your whole company works—not just how the security team works—evolves. As CISO, you need to understand and prepare for these new ways of working, so that you can integrate and collaborate with your partners and the rest of your company, and so that information security can thrive in the new, evolved business environment.

Accelerate development timelines

Developing and deploying in the cloud can significantly reduce the time between releases, often creating a continuous, iterative release cycle. The shift to this development process, whether it's called Agile, DevOps, or something else, also represents an opportunity for you to accelerate the development and release of new security features.

To take this opportunity and thrive in an accelerated development environment, security teams must understand—or even drive—the new release process and timeline, must collaborate closely or integrate with development teams, and must adopt an iterative approach to security development. These imperatives represent a major change from the role of security teams in the traditional software development cycle. However, implementing these changes can have huge benefits to security development and the speed with which you can deploy new security features and fixes.

Deploy and manage infrastructure as code

Transforming to the cloud means transforming how your company thinks about, deploys, and manages infrastructure. When servers, racks, and data centers are managed for you in the cloud, your code becomes your infrastructure. Deploying and managing infrastructure as code represents a clear opportunity for your security organization to improve its processes and to integrate more effectively with the software development process.

When you deploy infrastructure as code, you can integrate your security policies directly in the code, making security central to both your company's development process and to any software that your company develops, and also minimize security risks. For example, your company likely manages hundreds or thousands of security configuration policies. Many of these policies might require adherence to playbooks or human manipulation of security infrastructure and consoles. Managing and updating security policies using traditional security approaches can be labor intensive and error prone.

In contrast, deploying and managing these security policies as code lets you minimize human error, reduce inconsistencies and policy violations, and ensure that updates are properly reviewed before deployment. For example, you can use managed scripts to deploy and update security policies in a predictable and testable manner instead of relying on possibly inconsistent human interventions. You can also use mature change-management processes for software development to ensure that sensitive aspects of your security infrastructure are thoroughly peer reviewed before deployment and that your security infrastructure stays in sync with your company's software.

Evolve key security roles and responsibilities

Transforming to the cloud also transforms how your security organization works. For example, manual security work will be automated, new roles and responsibilities will emerge, and security experts will partner more closely with development teams. Your organization will also have a new collaborator to work with: your cloud service providers. As with any organizational change, your role as leader is to communicate these changes clearly and to help your team members adapt smoothly to a new way of working.



Collaborate with your cloud service provider

One of the major advantages of transforming to the cloud is that your cloud service providers becomes a key collaborator. In addition to developing security and monitoring tools and documenting cloud best practices, your cloud service provider handles many key security responsibilities for your organization.

The cloud shared-responsibility model assigns responsibility as follows:

- Your cloud service provider is responsible for **Security of the Cloud**, or securing cloud infrastructure, including hardware and networks.
- You are responsible for **Security in the Cloud**, or securing your data and choosing your security model.

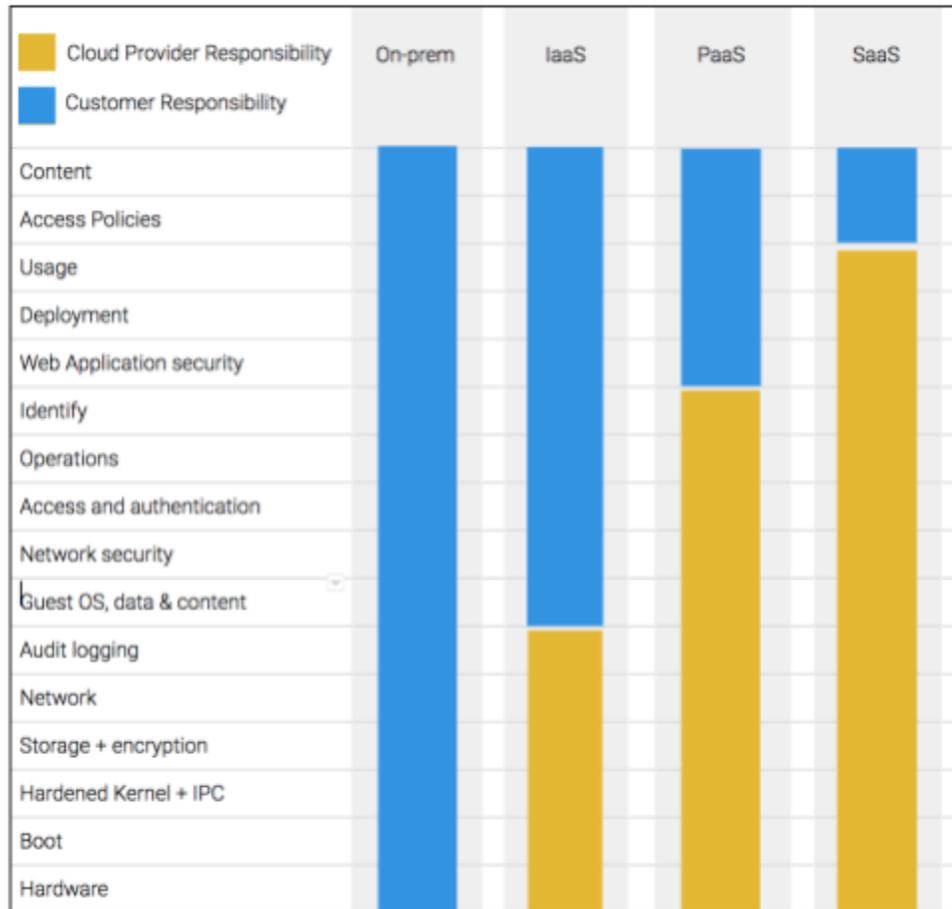


Figure 1. Your security responsibilities and your cloud service provider's security responsibilities under the cloud shared-responsibility model.

As shown in Figure 1, many responsibilities depend on whether you adopt an Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) architecture. For example, in a PaaS architecture, you are responsible for web application security, but in a SaaS architecture, your cloud service provider is responsible for web application security.

No matter which architecture you choose, collaborating with your cloud service provider is critical. Build a shared understanding of who is responsible for what, develop strong communication protocols to handle security issues, and institute oversight to ensure that your cloud service provider meets their security responsibilities.

Change how security roles are performed

In addition to working with a new collaborator in the cloud, your security organization will also change how it works from within. While every organization is different, Google has identified some typical changes to security roles and responsibilities that you can expect when your organization moves to the cloud. The following table details the type of work done in these roles during the transformation to the cloud and the new responsibilities in these roles moving forward.

| Role | Responsibilities in the cloud |
|--------------------------------|---|
| Policy & Risk Management | Identify policy and risk management objectives, independent of pre-existing frameworks and implementations. Refactor security policies and standards to focus on the right controls and to use cloud security models. |
| Security Architecture & Design | Define the organization's overall approach to security in the cloud. Enable nimble and effective implementation of cloud security by providing blueprints that incorporate guardrails. |
| Security Testing | Move closer to the development team and integrate tightly throughout the software development lifecycle. Perform security-focused testing for frequent iterative releases. |
| Security Operations | Extend monitoring to the cloud by using cloud-native telemetry to detect and respond to events, incidents, and threat intelligence. |
| Security Assurance | Implement continuous controls monitoring (CCM), which uses cloud configuration and takes a data-centric approach to verifying that architectures are adhered to and that controls are operational. |
| Security Engineering | Develop cloud-native security toolkits. Work with Infrastructure Engineering to define security policy directly in code. |
| Infrastructure Engineering | Engineer and operate cloud infrastructure and supporting services by using an infrastructure-as-code approach. This approach, which integrates policy directly in code and minimizes manual errors, is critical to success in the cloud. Your security organization might not have anyone with these specialized skills, so training and upskilling are particularly important for this role. |
| Application Development | Develop applications to be deployed on cloud infrastructure. Adopt accelerated development timelines and launches iteratively. Work more closely with security teams throughout the software development lifecycle. |

Each of these roles will change significantly in approach and in tools and technologies used, so training is especially important during your transformation to the cloud. As CISO, part of your role is ensuring that your security organization learns how to work in the cloud, knows how to fill new roles and responsibilities like Infrastructure Engineering, and understands how to integrate with the software development lifecycle. Plan to invest significant time in educating your organization. The upfront investment will pay dividends as you begin to implement your security policies in the cloud.

Design your security operating model

Your transformation to cloud security is an opportunity to rethink your security operating model. How should security teams work with development teams? Should security functions and operations be centralized or federated? As CISO, you should answer these questions and design your security operating model before you begin moving to the cloud. This section helps you choose a cloud-appropriate security operating model by describing the pros and cons of three models: centralized, federated, and hybrid.

Centralized security operating model

The centralized security operating model can be seen as a traditional or classic model. In this model, a central security team provides full security solutions, including security policies, security solutions, and incident management to other teams in the company. The security team interacts with these other teams, such as development teams, through well-defined processes that often use ticketing systems to manage workflow. Figure 2 shows how security roles and responsibilities are distributed in the centralized security operating model.

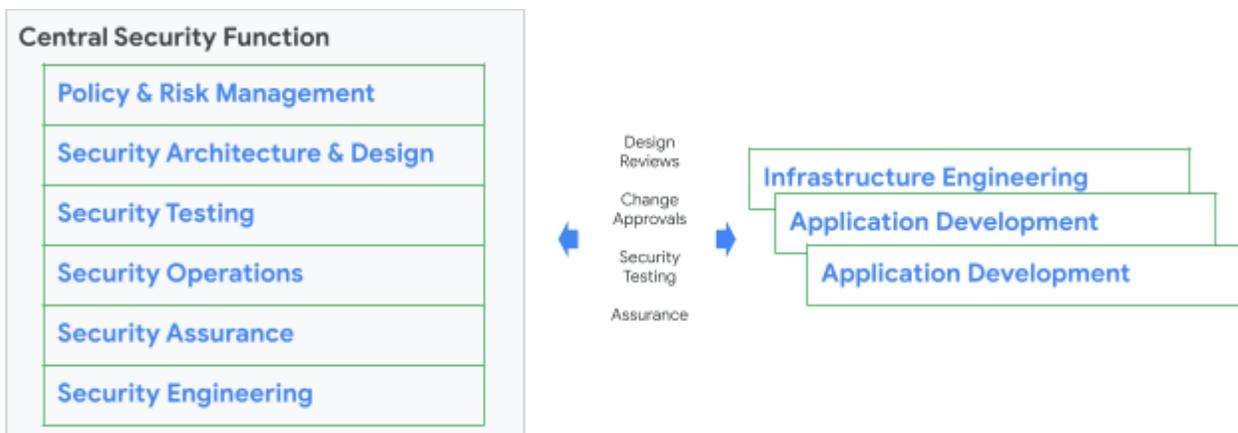


Figure 2. Distribution of roles and responsibilities in a centralized security operating model. In this model, most security work is done by a centralized security function that interacts with engineering and development teams across the company.

Pros: Employing the centralized model helps you maintain strong, consistent control of security across your company. You also enjoy some cost efficiencies from developing security policies and solutions centrally and deploying them across the company.

Cons: The centralized model fits best with slower IT delivery schedules associated with waterfall development, but typically is not fast or nimble enough for the accelerated development timelines that are common with cloud development. The centralized model can also lead to a culture of “Security is someone else’s responsibility” outside of the central security team.

Federated security operating model

The federated security operating model moves most security functions outside of a central security team and into individual engineering and development teams. This federated model is often employed in conglomerate organizations where a central team cannot adequately serve all teams in the organization. This model is also employed in small organizations that want to move quickly and integrate security expertise in engineering and development teams. Figure 3 shows how security roles and responsibilities are distributed in the federated security operating model.

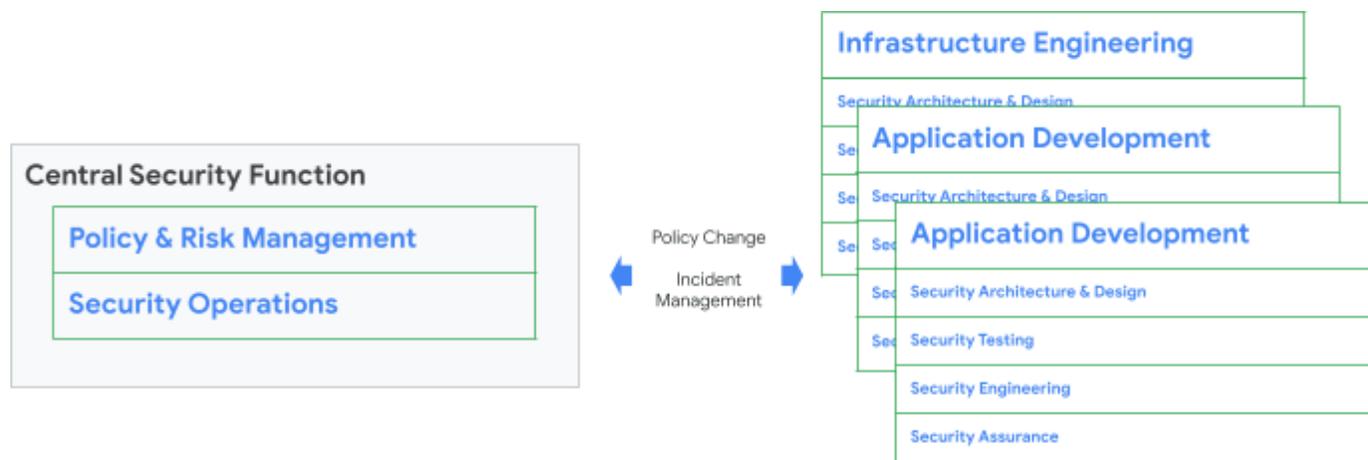


Figure 3. Distribution of roles and responsibilities in a federated security operating model. In this model, most security work is done within individual engineering and development teams.

Pros: Employing a federated model allows teams to move quickly and for security to be an integrated part of the accelerated development process. Security experts can understand the details of the teams that they are integrated with and provide “just enough” security for those teams’ needs.

Cons: The federated model increases risk because a central, independent security team does not provide security assurance and does not develop robust security solutions for broad security threats. Instead, teams develop customized security solutions that solve specific problems, but often miss other security threats.

Hybrid security operating model

The third security operating model, the hybrid model, presents a middle ground. In the hybrid model, the size, scale, and complexity of the relevant development teams determine the degree of centralization or federation of security functions. Figure 4 shows two types of hybrid models.

The infrastructure engineering team and the first application development team use a **light hybrid model**, which is the type used by most organizations that use a hybrid model. In a light hybrid model, the engineering or development team uses standardized tools, processes, and methods built by the central security team. A security coordinator in the engineering or development team acts as the interface with

the security team. The security coordinator might be a dedicated person or someone who also works on other aspects of development.

The second application development team uses a **heavy hybrid model**, which is more commonly used by large teams with complex security ecosystems. In a heavy hybrid model, the engineering or development team uses many standardized tools, processes, and methods from the central security team. However, the engineering or development team also designs and builds some of their own security solutions while communicating with the central security team. In the heavy hybrid model, the engineering or development team embeds some security team capabilities directly in their own team, both to keep pace and to develop expertise in the security ecosystem for that team's product.

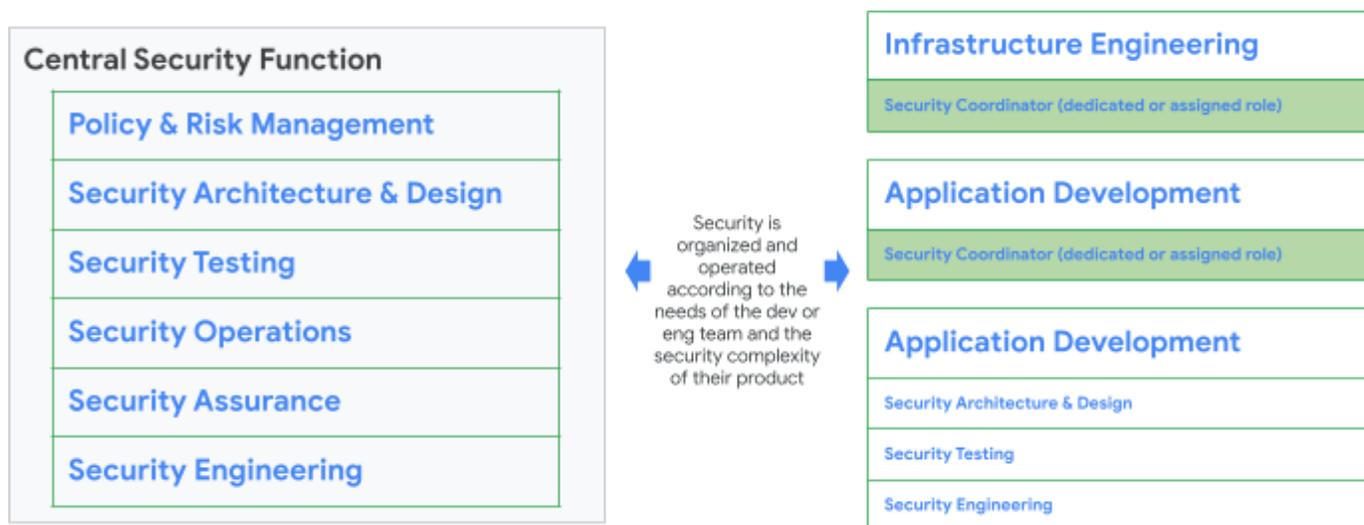


Figure 4. Distribution of roles and responsibilities in a hybrid security operating model. In this model, the centralization or federation of security functions depends on the needs of the development or engineering teams and the security complexity of their products.

Pros: The hybrid model is highly adaptable. Because this model employs a central security team, engineering and development teams can use standardized security solutions, but they also have the flexibility to build some customized solutions for their specific needs. The central security team in the hybrid model also provides independent assurance, but can rely on product-specific security expertise to improve security coverage and efficiency.

Cons: The hybrid model requires strong, ongoing communication and collaboration so that development and engineering teams and the central security team know who is responsible for what. The security coordinator role and the security specialists that are integrated in development and engineering teams are particularly important to this collaboration and must be strong communicators for the hybrid model to succeed.

Identify cloud security best practices

A common mistake when transforming to the cloud is to rely on existing security practices and policies in a cloud environment. But security approaches that work in on-premises and other traditional environments do not necessarily work well in the cloud.

As CISO, take your company's transformation to the cloud as an opportunity to transform your security approach. Set aside assumptions that you have made based on your existing security infrastructure and think through your security *goals*. What do you want to accomplish? And how can the scale and velocity of the cloud make that possible?

As you ask these questions about transforming your security infrastructure, avoid common anti-patterns based on traditional security implementations and identify best practices for cloud security, as described in the following table.

| ✗ Anti-patterns | ✓ Best practices |
|---|---|
| Assume that existing control implementations are effective. | Review control <i>objectives</i> first. Then implement to meet those objectives. |
| Assume that existing processes—especially centralized processes—will work in the cloud. | Enable teams to implement flexible cloud processes instead of finding workarounds to existing processes. |
| Use on-premises models, such as a virtual security appliance like an Intrusion Prevention System (IPS), for security controls in the cloud. | Use cloud-native approaches, such as log monitoring and access management. |
| Rely on historical approaches to assuring compliance with policies and standards. | Adopt data-driven approaches to achieve the scale and velocity needed for continuous controls monitoring. |

Conclusion

Moving to the cloud represents a huge opportunity to transform your company's approach to security. To lead your security organization and your company through this transformation, you need to think differently about how you work, how you manage risk, and how you deploy your security infrastructure. As CISO, you need to instill a culture of security throughout the company and manage changes in how your company thinks about security and how your company is organized.

To make your transformation successful, we at Google recommend that you remember these key points for security in the cloud:

- Engage in security planning early.
- Take a risk-informed, not a risk-avoidance approach.
- Embrace zero trust and forget the perimeter.
- Prioritize automation to reduce manual workload and improve velocity.
- Plan to re-train, re-skill, and reorganize your security workforce.
- Partner with cloud service providers, based on a shared understanding of risk and objectives.
- Challenge existing security assumptions and implement cloud-specific best practices.

These key points and the recommendations throughout this white paper come from Google's years of leading and innovating in cloud security. We are excited to answer your questions about cloud security and to collaborate with you on your cloud security transformation.

