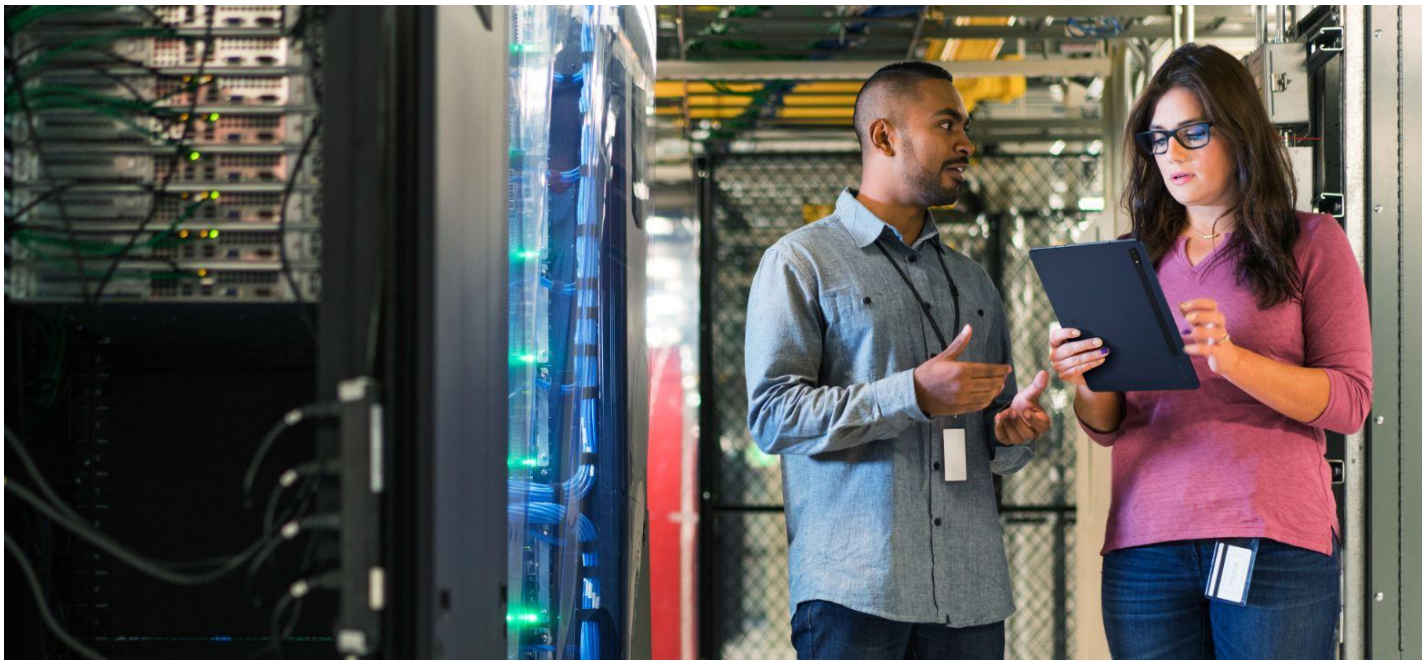
Google Cloud

Office of the CISO

Organizing Security for Digital Transformation



July 2024

Table of Contents

Reshaping cloud security begins with organizational transformation

01

Introduction

In the first guide for CISOs, Google Cloud Office of the CISO (OCISO) distilled insights gained from our experience working with hundreds of customers trying to transform their businesses by moving their enterprises to the cloud. Nearly two years later, we're here to provide an update on the journey and share additional lessons learned.

As we've helped more security teams make the move to the cloud, we've identified nuanced challenges that they face – namely those related to team structure, changing business operations, and establishing culture – that are critical to their success

In this guide, we've captured insights and recommended practices focused on the organizational and operational elements of digital transformation. As you read this guide, please refer to the appendix for deeper discussions on security teams before and after digital transformation and the relationship between organizational culture and transformation.

What we're seeing now

The journey through digital transformation and reinvention regularly involves challenges that many leaders and teams have not experienced or even thought of before. Determining which optimizations your organization's structure needs to match your expanding technical capabilities can be daunting, no matter how well you plan.

Organizations are surprised when embracing certain elements of transformation particularly around teams, skills, and the jobs to be done in cloud. Perhaps none more so than those who have to change their organization and its structure. These changes are often necessary to realign teams to new goals – many of which have become shared between teams that may not have worked closely together before. At the same time, the introduction of new technologies like cloud, and new ways of automating work, with infrastructure-as-code and continuous integration/continuous deployment (CI/CD), drive new levels of work velocity which challenge historical decision-making processes and related forms of governance. Teams shift from securing individual systems to securing services and products that are "built into" the cloud at speeds never seen before.

Digital transformation defined

Digital transformation uses modern digital technologies, including all types of public, private, and hybrid cloud platforms, to create or modify business processes, culture, and customer experiences to meet changing business and market dynamics.

Digital transformation spurs a new way of working and optimizing technology, processes, and organization toward accelerated business outcomes. Trying to predict what a transformed organization model will look like is challenging as there is no single "best practice." What's possible is to set goals on what business outcomes one seeks then model, orient, and adjust the organization model to achieve those outcomes at the highest velocity, balancing quality, cost, and risk along the way. What's our answer when we get the question, "How should I organize my cloud security team alongside my on-premise security team?" We say: it depends. It depends on what the business outcomes an organization wants and how much change its willing to endure to get there.

So where do we start when we talk about transforming the cybersecurity organization within a company that's historically delivered security to on-premise systems within a highly centralized function? Ideally, we think this conversation should start with defining security goals framed in business outcomes like capabilities, velocity, quality, cost, and risk. However, this type of goal framing rarely exists for the existing teams in the first place. We think goal setting is critical, but many organizations are faced with a different set of challenges that leaders should be aware of.

Pre-transformation realities

Working with the "day job": Many teams just getting started in transformation projects report struggling with managing legacy security processes, adopting new technologies like cloud, and all the while keeping up with emerging threats and servicing the existing needs of their organization. Adding more work to the already busy "day job" is a common, repeated term.

Reducing toil: What's also difficult to understand in the early stages of transformation is believing that adoption of the cloud will result in less work and a more secure system. Yet, many teams are structured to deliver services around tools that secure on-premise systems and follow processes that have remained unchanged for years. Many processes and controls have taken years to put into place. Teams may remember the pain of putting them in and may not want to change, or worse, these processes have become a dangerous source of pride. Moving away from the toil often associated with securing on-premise systems can be challenging for unexpected reasons. We think security in the cloud is a better future that can be difficult to imagine without inspiration and intentional culture development.

Building new skills: Moving away from these processes can feel expensive and require learning they may not have time, interest, or motivation to invest in. Moving on to new platforms like cloud can challenge a teams' existing skill sets, and, when paired without thoughtful or effective training, transformation initiatives can pause or stop as a result. Bringing in new team members with cloud skills is also challenge. Current estimates taken at the time of this paper indicate there being over 3.5 million unfilled job openings for cybersecurity professionals with 700,000 in the US alone.

Driving to new organization models: Many cybersecurity teams aren't designed to provide "product" security, which is a style of delivering security over the course of its entire life cycle (development, delivery, production use, retirement). With so many products existing within an enterprise, trying to deliver product-specific security controls in an on-premise network full of various operating systems, applications, network designs, operational technologies, and others is infeasible. In the place of an application or product-specific security approach, security teams build and deliver horizontal security services, like vulnerability scanning, that can detect vulnerabilities in all kinds of infrastructure and applications. Once detected, teams struggle to assign vulnerability correction (for example, patching) activities to application teams to take action on them.

Broadly, the activity of "find and assign" security problems to application teams creates slowness and if not well managed and governed, results in tremendous waste and worse security outcomes due to blurred accountabilities for who's doing the fix.

Product teams: High-performance product teams have all the skills they need to deliver a secure application through development, deployment, production use and retirement. Product teams increasingly place the burden of detecting and fixing security problems before they happen on themselves. Product teams can deliver platform capabilities (like Identity and Access Management) that other product teams (like teams that build inventory or manufacturing systems) consume.

In evolved organization models, cybersecurity teams might find themselves providing more coaching to product teams on how to increase their scope and improve their quality, governing (vs. driving) vulnerability mitigation, and providing consulting support around things like threat models.

A successful digital transformation requires a new approach and pushes teams to distribute responsibilities, not to centralized teams, but to more product-based teams. This way product teams own responsibility for the availability and security of the systems they build and operate.

Maintaining a "single organization" approach to how cybersecurity (or really any function) gets done can delay or even stop transformation initiatives from having the impact the organization's leadership seeks. Indeed, failure to transform the organization becomes the most substantial blocker to adopting faster, more efficient, and increasingly more secure ways of work.

It's important to note that every industry and company operates with its own dynamics and challenges. Keep in mind the insights provided here are intended to serve as a flexible guide meant to be adjusted, rather than as a prescriptive set of rules for a digital transformation journey.

About Office of the CISO

Office of the CISO (OCISO) brings together senior security leaders and advisors who enable Google Cloud customers to securely adopt cloud technologies and transform their organizations.

We have the singular mission of supporting the secure digital transformation of governments, critical infrastructure, enterprises, and small businesses. We work directly with regulators and deeply within industries, spanning sectors such as financial services, retail, public sector, telecommunications, media, healthcare and life sciences, and digital-first enterprises. We are security leaders, CISOs, researchers, engineers, and practitioners who care deeply about securing customers, securing the cloud, and securing the planet.

As with anything we do at Google Cloud, we want and appreciate your input and feedback. The exchange of best practices and information are essential in navigating the evolving landscape of cybersecurity, and we are committed to fostering collaboration and knowledge sharing. We invite you to send us your feedback.

About cloud transformation and DevOps

The key to creating faster, more efficient, and increasingly more secure organizations starts with the transformation of the organization itself. Many of the concepts covered in this paper are based on our collective experience working in cybersecurity engagements where we've supported organizations in their cloud transformation. Some of the research we use in this paper comes from our annual Accelerate State of DevOps Report.

Each year, these reports feature data gathered directly from tens of thousands of professionals working across every industry and in companies of varying sizes. Our Google Cloud DevOps Research and Assessment (DORA) engagements and expert teams work with survey respondents to review, compile, and publish insights that help teams understand the capabilities that drive software delivery and operations performance. The program started in 2014 and was acquired by Google in 2018. As part of Google Cloud, we continue our research and help customers on their journeys of continuous improvement.

We encourage readers of this paper to explore our most up-to-date DORA research at dora.dev.

02

Mindshift: Security goes cloud first

Here's something we know to be true: digital transformation isn't just about technology. It's more about transforming the organization, its operations and its technology. Done correctly, digital transformation can change who does the work and how it gets done using automation, machine learning, and other technology available on the cloud.

You'll find many opinions about how cybersecurity enables a successful digital transformation, but most observers are unaware of the complexity involved in effectively collaborating and sharing responsibilities, skills, tooling, and other capabilities with fast-moving product-based teams who own the full set of responsibilities – including cybersecurity – for the applications they build and run.

Unfortunately for many chief information security officers (CISOs) there's no one "perfect" operational model that an organization can implement coupled with clear recommendations on which responsibility, skills, tools, and capabilities become shared and with whom. These shifts depend greatly on factors outside of the CISO's control, including organizational risk appetite, budget, demand for the organization's services, and regulatory perspectives, among other factors.

03

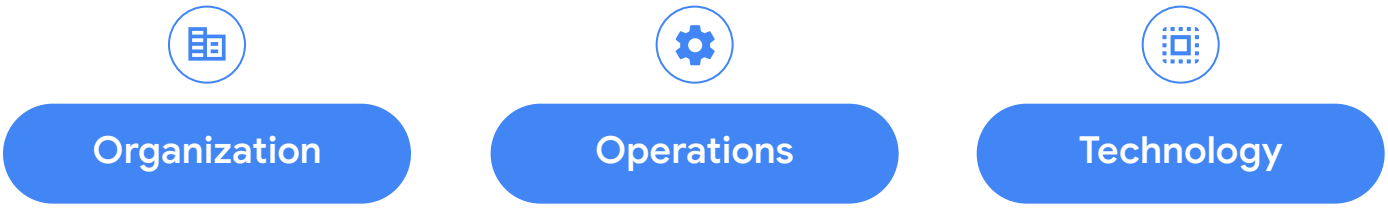
Why it's OOT, not TOO, in the cloud

Our first step in helping customers work through transition to the cloud and more modern ways to work starts with backing away from the belief that it's the technology that's transforming.

In the earliest days of cloud, organizations looking to transform did so by moving on-premises servers (or virtual machines) from their data centers "into the cloud." The concept of server movement was straightforward: create a connection between a data center and a cloud services provider, make a copy of the on-premises server, upload the copy to the cloud, initialize copy to a running server, do some networking magic, and you were done. Start saving money by shutting the server down when you aren't using it and voilà – Transformation!

Now, services could be acquired without complicated procurement or security processes to slow them down. Quickly, organizations deployed new mission-critical services, but without awareness into the longer term needs the organization would have for product support or who was now responsible for change control and ensuring uptime requirements were met. The speed was great, but questions about who was responsible for approving new systems or moving data to the cloud were sometimes answered following processes that had been stood up outside of establishing governance channels meant to stop proliferation of technical decisions that would result in future pain. In some cases, the rapid acquisition of cloud by early adopters led to challenges for security and other support teams who needed to support them.

We've studied the stories of success and caution and seen them play out time and again in the Fortune 500 and beyond. We believe organizations who rapidly transform using cloud – and do so securely – succeed by focusing on their initial priorities in this order:



We call this O-O-T or "OOT." As we'll explain, to avoid suboptimal outcomes, organizations must start with understanding their teams, their resources, locations, and constraining factors or conflicts, such as goals, incentive structures, and resource limitations, before approaching finalizing technology decisions.

04

Choreographing change

Successful transformation starts with an understanding of the goals the organization has for velocity, quality, security, risk and capability of its operations. Strong leadership direction, with clear goals and measurements, is critical.

To put the transformation efforts into context, we suggest a four-stage framework. In Appendix C, we offer a deeper explanation of what these stages mean when applied organizing cybersecurity teams. We use these stages to pinpoint what their challenges are and what progress looks like. This can help everyone working in cybersecurity better anticipate and prepare for organization transformation.

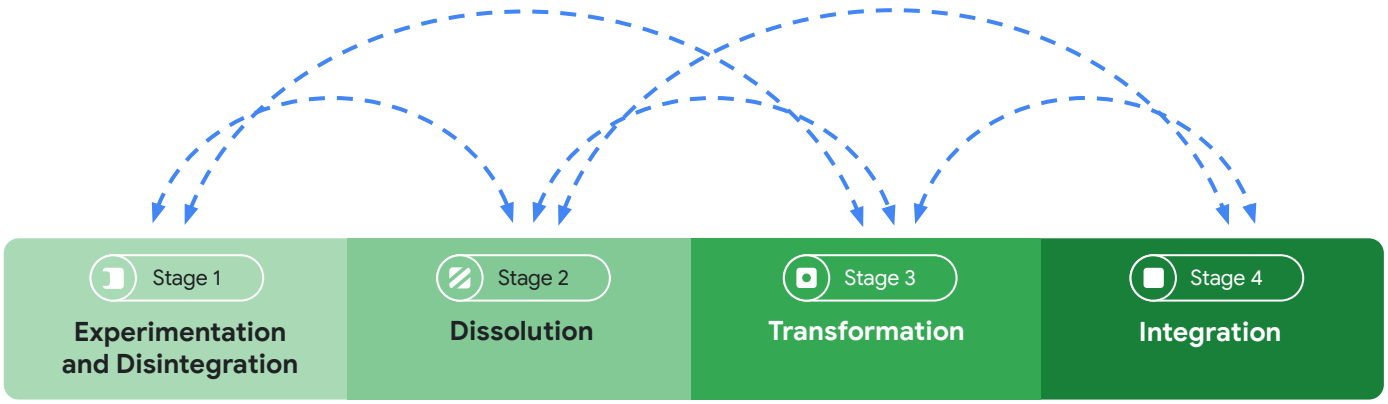
Organization transformation defined

Expectations

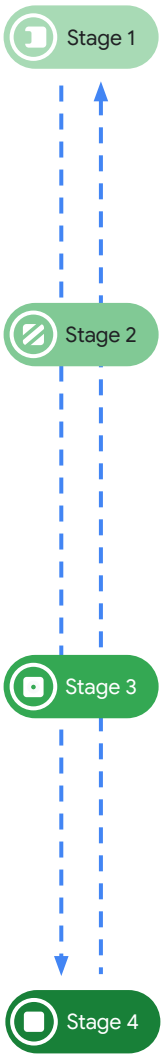
How organizations think digital transformation goes
The expectation is for a smooth progression through the stages of transformation.

Reality

How organization transformation actually goes
Progress isn't always smooth, as you'll often go back and forth between stages throughout the transformation as you experiment and optimize the work.



The four stages of organization transformation



Experimentation and Disintegration

Teams are encouraged and enabled to experiment with new technology and will be able to find and demonstrate its value. Teams given autonomy to build without rules find ways to reinvent their work. The value and benefit of cloud is teased through these simple examples. Excitement about what's now possible and what could be done on larger scales creates the need to disintegrate.

Dissolution

Teams begin to sense that disintegration of the "old way" of doing work (without automation, following manual processes, according to traditional ways of organizing processes to do work) seem to inhibit the speed that's possible using cloud. Team norms and structures begin to be challenged as organizations start to establish new ways of working, new shared goals and outcomes.

Transformation

Now begins the stage of implementing new capabilities that change and eliminate steps or entire ways that work was done previously. This move entails significant investment in new technologies and systems. This stage can be a long and complex one, as organizations need to carefully plan and execute the transformation across entire functions, business units, divisions, and the company itself.

Integration

Next comes the stage of integrating the new digital business model fully into how the organization's day-to-day operations run. Volumes of work go down as the use of automation and technologies like artificial intelligence (AI) become more rapidly deployed and improved. Organizations shift from building, to maintaining, and finally optimizing continuously.

05

How security is organized during transformation

How can we apply this framework to cybersecurity teams? This guide was designed to help teams do exactly that. To be as inclusive as possible, we put forward a reasonably comprehensive list of cybersecurity teams and functions. No two organizations are the same, and we did not intentionally leave any groups out. If you have a question about how a specific role or function transforms, send us your feedback.

You might be surprised to see functions in this list that aren't typically assigned explicit responsibilities for cybersecurity. We've included them to show you how functions and their related responsibilities change as the security transformation kicks in.

How to use this guide

In Appendix A, we share explanations and outline how the cybersecurity responsibilities and functions transition over the four stages of transformation.

To use this cybersecurity transformation framework, security leaders should:

01 Select a cross-functional group of individuals who are involved in planning or executing security responsibilities within your organization.

02 Review the stage descriptions and list of key functions, noting which ones exist within your security organization today and which do not. Find out where responsibility for certain functions exists for each function listed.

Note: We expect this to be a difficult activity, as no organization will perfectly match our list of functions and responsibilities. Truly understanding who is responsible and accountable for what and which responsibilities are unclear or not assigned is an important first.

03 Read the descriptions provided for each function in Appendix A. Determine what stage of transformation each individual function is in. (Note: Gather evidence, data, or other facts to find the markers and support your determinations.)

04 Share your stage selections with your team and each owner of a critical function that is currently outside of your team (or in early stages of forming). Ask:

- Do they think the list of functional security responsibilities is complete and accurate?
- Do they think the selections of each stage for each function makes sense?
- What would they change, add, remove, or modify to make this specific to your organization?

05 Review the stage-to-stage descriptions in the appendix and reflect on how these functions are performed today in light of the organization's current cloud and non-cloud usage.

06 Identify a target state and select one for each function. Use the appendix to determine how to achieve that state. Ask yourself:

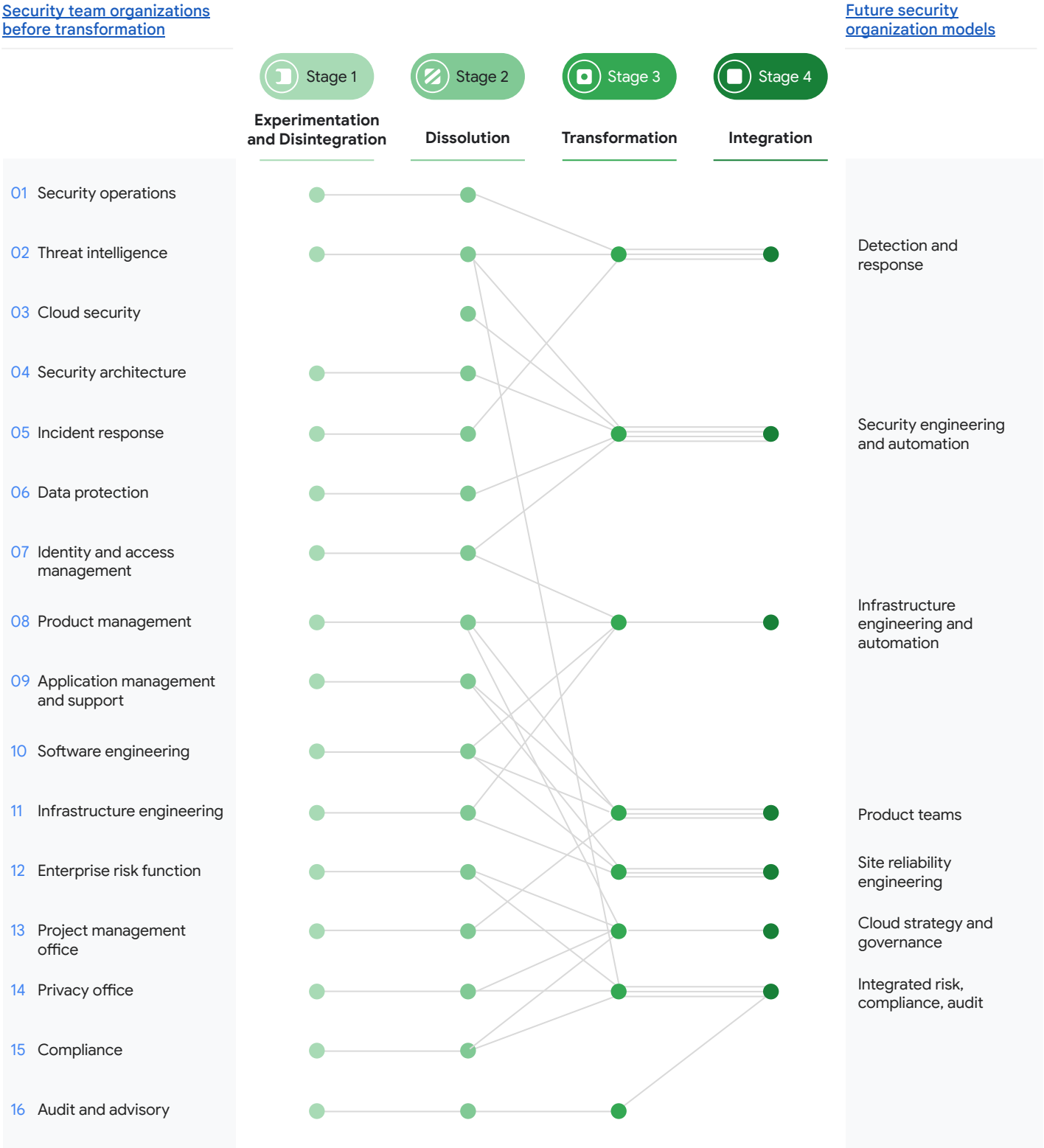
- Working backwards from the desired end state, what needs to change now to take my organization there?
- What's our desired state look like?
- What organizational, operational, or cultural issues might get in my way?
- What processes, including ownership of those processes, must change to achieve the desired state?
- What technical barriers exist that we must overcome to achieve that desired end state?
- What decisions must get made, and by whom, to initiate and sustain the organization and operational changes needed?
- Which of these decisions are directly within your control or outside of your control (or even, outside of your company?)

07 Take the results, socialize with your team, and select end states and target efforts (preferably, shared goals with functions that will be changing) to achieve desired results.

06

Modern security organization models

You can follow the path through the four stages of organization transformation and see how cybersecurity team organizations evolve, integrate, and streamline into future post-transformation models for teams.



Post-transformation security team models

The end goal is a more streamlined organization when transformation is achieved. Here are profiles of newly integrated teams and the roles they take on.

Detection and response

The detection and response (D&R) team includes security professionals responsible for detecting and responding to security incidents. The D&R team typically reports to the chief information security officer (CISO) or another senior security executive.

Threat intelligence is a critical function that is close to and drives D&R activities. Threat intelligence (TI) functions can be separate from D&R teams or highly integrated. TI is not used only by D&R teams but across the full spectrum of security, risk, governance, and other increasingly data-driven functions.

Security engineering and automation

The security engineering and automation team plays a vital role in helping organizations improve their security posture and reduce the risk of security incidents. The team works to implement increasingly more secure designs into cloud using code. They also help automate security tasks, freeing up security professionals to focus on more strategic work, and improve the overall efficiency and effectiveness of the organization's security operations. These teams often manage security products under a single charter for both on- and off-premises. Teams use intelligence to inform and prioritize efforts continuously.

Infrastructure engineering and automation

Infrastructure engineering and automation teams focus on discipline around design, build, and physical and virtual systems that support product infrastructure. These teams address all aspects of a product or workload, inclusive of security, availability, integrity, capacity, and recoverability of all infrastructure. This includes everything from the servers and storage systems that store data to the networks that connect them to the applications and software that run on them. Infrastructure engineering teams deploy infrastructure and policies using code and deployment automation.

Product teams

A product delivery team is a cross-functional team of people responsible for delivering a software product to the customer. The team typically includes members from the product management, software delivery, engineering, design, quality assurance, and operations departments. Product teams in this model also own security features, security tool implementation into product workflows, and the implementation of security policies into products. Product teams can develop and deliver all sorts of products – like platform services (like IAM), traditional applications, and many other things.

Site reliability engineering

The site reliability engineering (SRE) team is a cross-functional arrangement of system experts responsible for the reliability, performance, availability, scalability, and operational security of a company's software systems. The team can include members from the engineering, operations, security, and DevOps disciplines. The mission of the SRE team is to protect, provide for, and guide the progress of software and systems development.

Cloud strategy and governance

Cloud strategy and governance steering is a cross-functional team responsible for approving and implementing the organization's cloud strategy via projects and products. The team typically includes members from the product, IT, business, risk, compliance and legal departments. These team members are usually stakeholders from both the technology and business organizations that are leading the transformation.

Integrated risk, compliance, audit

The cross-functional risk, compliance (including privacy), and audit teams (inclusive of disciplines like information security, privacy, and resilience) are responsible for working with first-line teams to understand and implement controls to mitigate risks. Internal teams audit the organization's practices to ensure they conform to organization policies and statements about risk while also performing other forms of advisory and audit work.

Often mechanisms, such as risk appetites/tolerances, risk rating, and quantification, developed by these teams are used by product, infrastructure, application, and other teams to prioritize controls, vulnerabilities, incidents, and other work and send them into product and engineering teams to implement. Increasingly, these teams are using continuous monitoring and auditing approaches as well as threat intelligence to monitor risks and prioritize action.

Internal audit teams also conduct audits and assessments using cloud-first services for large-scale data analysis or policy-as-code to evaluate the compliance posture of a workload.

07

Summary

Digital transformation initiatives are both exciting and challenging. While these efforts deliver new technologies, they present opportunities to examine and adjust organization structures and operating models.

They provide a chance to re-examine culture, shift focus to the needs of customers and users, acquire new skills and methods to deliver and manage technology, set shared goals, and distribute work in new ways to new teams.

For more information on cybersecurity, risk governance, and secure transformation, and more ways we can help securely transform your organization, visit our CISO Insights Hub.

Contributors

Our guide for Organizing Security for Digital Transformation comes from experience working with many Google Cloud customers and the deep insights they've shared with us. We are incredibly thankful to their input.

In addition, many authors spent months reviewing and refining the content in this paper. The following Googlers played a significant role in helping us develop, review, and produce this guidance.

Taylor Lehmann
Office of the CISO

David Stone
Office of the CISO

Anton Chuvakin
Office of the CISO

Michele Chubirka
Developer Relations

Nathen Harvey
Developer Relations, DORA

Tom Curry
Office of the CISO

Seth Rosenblatt
Cloud Security Editorial

Bhavana Bhinder
Office of the CISO

Bill Reid
Office of the CISO

Zach Bever
Office of the CISO

Appendix A

Organization descriptions before transformation

Profiles of existing teams and their roles

Security operations

Security operations is the practice of combining security and IT operations to improve collaboration and reduce risks. Security operations teams are responsible for monitoring, detecting, and responding to cyber threats. They also work to prevent security incidents by implementing and maintaining security control. Areas of focus:

Monitor and detect threats – using a variety of tools and techniques to monitor an organization's networks, systems, and applications for signs of malicious activity, including monitoring for intrusions, unauthorized access, and data exfiltration.

Respond to threats – working to respond quickly and effectively to mitigate risk when a threat is detected, involving isolating the affected system, investigating the incident, and addressing the vulnerability that was exploited.

Detect vulnerabilities – working with security engineering and product teams to detect and respond to vulnerabilities in a cloud environment.

Threat intelligence

Threat intelligence teams collect, curate, and analyze relevant threat data from various sources. They identify and track threat actors, their capabilities, and their targets to inform various teams on how to adjust the organization's defenses in response. The teams also share threat intelligence with other organizations to identify and mitigate the threat. Areas of focus:

Collect and analyze threat data – collecting this data from a variety of sources, such as open source intelligence, social media, and dark web forums and then using this data to identify and track threat actors, their capabilities, and targets.

Develop threat models – describing how threat actors may attack an organization, which in turn helps organizations to understand the threats they face and proactively adapt security controls.

Share threat intelligence – working with other organizations to help them protect themselves by way of public reports, private briefings, or through threat intelligence sharing platforms.

Cloud security

Cloud security is the practice of protecting data, applications, and infrastructure that is hosted in the cloud. Cloud security teams are responsible for developing and implementing security policies and procedures, and monitoring and responding to security incidents. Areas of focus:

Develop and implement security policies and procedures – working with business stakeholders to develop and implement security policies and procedures that are specific to an organization's cloud environment, addressing security concerns such as access control, data encryption, and incident response.

Monitor cloud environments for security threats and vulnerabilities – using tools and techniques for detecting unauthorized access, malicious activity, misconfigurations, and data exfiltration.

Secure infrastructure and infrastructure as code – using languages like Terraform and other tools, implement cloud-first security architecture and technologies and ensure technology choices made by product teams continuously improve product resilience.

Educate employees on cloud security best practices – including training employees on how to identify and report security threats.

Security architecture

Security architecture is the practice of designing, developing, and implementing a security framework that protects an organization's assets from cyber threats. Security architecture teams are responsible for defining an organization's security requirements, designing and implementing security controls, and ensuring that the security framework is continuously monitored and updated. Areas of focus:

Define security requirements – working with business stakeholders to define security requirements, including identifying assets, understanding the threats to those assets, and assessing risk tolerance.

Design security controls – designing and implementing controls to protect an organization's assets from cyber threats with a focus on firewalls, intrusion detection systems, encryption, and access control.

Implement security controls – following working with operations teams to implement newly designed security controls, including configuring the controls, testing for effectiveness, and monitoring for compliance.

Incident response

Incident response teams own the process of responding, containing, and resolving security incidents. Incident response teams must respond to security incidents rapidly to minimize the damage and impact. Areas of focus:

Investigate incidents – working to investigate a detected incident to determine the scope and potential impact.

Contain incidents – working to contain an incident to prevent further damage. Involving isolating the affected system, blocking access, and removing the malicious code.

Eradicate threats – evicting bad actors, addressing the immediate vulnerability that was exploited and restoring the affected system to its original state.

Learn from incidents – improving the incident response process, including documenting the incident, analyzing the incident, and developing recommendations for improvement.

Data protection

Data protection is the practice of securing data from unauthorized access, use, disclosure, disruption, modification, or destruction. Data protection teams are responsible for implementing and maintaining controls to protect an organization's data. Areas of focus:

Identify and classify data – focusing on all data that needs to be protected, identifying data type, sensitivity, and value.

Develop data protection standards – developing and recommending security controls to protect the data, including implementing access control, encryption, and backup.

Train teams on data protection – ensuring that users are awareness of data protection requirements.

Monitoring control effectiveness – being prepared to respond to data protection violations and incidents with a plan in place to identify and contain them.

Identity and access management

Identity and access management (IAM) practices ensure that only authorized users have access to an organization's systems and data. Areas of focus:

Define identity and access management policies and procedures – including defining the different types of users, their roles and responsibilities, and the levels of access needed.

Implement identity and access management controls – following the definition of identity and access management policies and procedures, implementing controls to enforce the policies such as implementing access control lists, multi-factor authentication, and password policies.

Monitor and audit identity and access management controls – ensuring effective controls that include regularly reviewing logs and reports to detect any suspicious activity.

Product management

Product management teams define, develop, launch, and maintain a product or service. Efforts often include end user support, integrations, and even support for go-to-market and sales teams looking to expand the products usage. Areas of focus:

Define the product vision – in collaboration with the rest of the team, developing a vision statement of what the product is and what it hopes to achieve.

Build, deliver, and operate products – in collaboration with operations teams, ensuring the product is stable, secure, compliant, and continuously monitored.

Implement security features – ensuring products have security features that are enabled by default and designed into the product in its earliest stages.

Work with engineers and designers – bringing the product vision to life through design feedback, prioritizing features, and managing the product development process.

Manage the product life cycle – including tracking product usage and collecting customer feedback.

Application management and support

Application management is the process of ensuring that software applications are running smoothly and efficiently. It includes tasks such as monitoring application performance, troubleshooting problems, and applying security patches. Application management teams are responsible for ensuring that applications are available to users when they need them and that they are performing at their best.

Application support is the process of providing assistance to users of software applications. This includes tasks such as answering questions, resolving problems, and providing training. Application support teams are responsible for ensuring that users are able to use applications effectively and efficiently. Application management and support teams typically work together to ensure that software applications are running smoothly and efficiently. Application management teams focus on the technical aspects of application management, while application support teams focus on the user-facing aspects of application support. Areas of focus:

Monitor application performance – ensuring that applications are running within acceptable levels through the collection of data on application metrics, such as CPU usage, memory usage, and database activity.

Troubleshoot problems – troubleshooting problems when they occur, identifying the cause and finding a solution through activities such as reviewing logs, analyzing data, and performing tests.

Apply improvements – protecting applications from vulnerabilities by identifying and downloading patches, testing patches, and deploying patches to production environments.

Answer questions – offering support on how to use applications by providing information about application features, troubleshooting problems, and training.

Resolve problems – addressing problems that users may experience with applications by troubleshooting problems, providing workarounds, and escalating problems to application management teams.

Provide training – creating training materials, delivering training sessions, and answering questions from users on how to use applications.

Software engineering

Software engineering is the application of engineering principles to the design, development, testing, and maintenance of software. Teams take a systematic approach to the development of software that ensures that the software is reliable, efficient, and meets the needs of the users.

Note that software engineering teams are responsible for the entire software development life cycle – from requirements gathering to deployment and maintenance. They use a variety of tools and techniques to ensure the software is high quality and meets users' needs. Areas of focus:

Gather requirements – working with stakeholders to gather requirements for the software by identifying the needs of its users and business.

Design software – meeting requirements that have been gathered by creating a detailed plan for how the software will be developed.

Develop software – developing the software according to the design with coding, testing, and debugging.

Test software – ensuring that software meets all requirements and is free of errors.

Deploy software – deploying the software to production so that it is ready to use.

Maintain software – fixing bugs, adding new features, and updating the software to meet changing user needs.

Infrastructure engineering

Infrastructure engineering incorporates the discipline of designing, building, and maintaining the physical and virtual systems that support a company's IT infrastructure. This includes everything from the servers and storage systems that store data, to the networks that connect them and the applications and software that run on them.

Infrastructure engineer teams work with other members of the technology team – such as software developers, system administrators, and security engineers – to ensure that the infrastructure is reliable, scalable, and secure. They also work with business stakeholders to understand the company's needs and to design and implement solutions that meet those needs.

Infrastructure engineers play a vital role in the success of any technology team. They are responsible for ensuring that the infrastructure is reliable, scalable, and secure, which in turn allows greater focus on developing and delivering innovative products and services. Areas of focus:

Design and build new infrastructure systems – build and maintain compute, network, and storage systems in cloud and on premise.

Optimize the performance of infrastructure systems – monitor and adjust systems to increase performance, stability, reliability, capacity, and availability. Respond and correct issues in real time.

Troubleshoot and resolve infrastructure problems – find, diagnose, and correct issues that prevent infrastructure from operating effectively.

Work with other members of the technology team – ensuring that the infrastructure meets the needs of the business.

Upgrade and maintain existing infrastructure systems – maintain infrastructure and infrastructure systems, like power, cooling, energy, and others, such that core infrastructure stays up and running.

Ensure that infrastructure systems are compliant with government regulations and standards – implement controls that ensure infrastructure is deployed and managed according to applicable rules and regulations.

Plan for and implement infrastructure changes – plan, schedule, and execute infrastructure changes.

Enterprise risk

Enterprise risk function ("Risk") is a cross-functional team responsible for identifying, assessing, and managing risks that could impact the achievement of an organization's objectives.

Risk plays a vital role in helping an organization identify, assess, and manage risks. In this way, Risk can help to protect you from financial losses, reputational damage, and other negative consequences. Areas of focus:

Identify and assess risks – pinpointing risks that could impact the organization's objectives, including both internal and external risks such as operational, financial, strategic, and compliance risks.

Develop and implement risk management strategies – managing identified and assessed risks through implementing controls, monitoring risks, and communicating risk information to stakeholders.

Oversee risk management activities – overseeing risk management activities for an organization, including ensuring that risk management is integrated into all aspects of operations.

Report on risk – reporting on the risks that the organization faces and the strategies that are in place to manage those risks across all levels of an organization.

Capture up-to-date information and intelligence about risk the organization is taking on – continuously monitoring risks and controls in the organization. Build systems and prioritization techniques to automatically rate risk and assign response actions to accountable owners (for example, infrastructure, product teams) for things like vulnerabilities, misconfigurations, threats, and others.

Project management office

The project management office (PMO) is responsible for providing guidance, support, and oversight to technology projects. The PMO typically reports to the chief information officer (CIO), chief operating officer (COO), or another senior executive.

The PMO plays a vital role in helping organizations deliver projects on time, on budget, and within scope. By providing guidance, support, and oversight, the PMO helps ensure projects are managed effectively and that project risks are identified and mitigated early on. Areas of focus:

Developing and implementing project management standards and processes – helping the organization manage major transformation projects and give business areas the tools and templates to manage other projects themselves.

Providing training and coaching to project managers – ensuring projects are managed consistently throughout the enterprise.

Tracking and reporting on project progress – ensuring projects stay on track, on time, on budget, and create the value they are out to acquire.

Identifying and resolving project risks – making sure risks to success (or failure) are known at all times.

Overseeing the implementation of project changes – making sure projects are led effectively.

Communicating with stakeholders – updating them on the status of the major activities changing the organization.

Privacy

A privacy team within an organization is responsible for protecting the privacy of data the organization collects from customers, employees, and stakeholders.

The privacy office plays a vital role in helping you determine which privacy laws and regulations are applicable to a business and its operations. The privacy office achieves its objectives by developing and implementing effective privacy policies and procedures, conducting privacy reviews and training, working with regulators to understand and implement necessary protections to comply with legal requirements. Responsibilities can vary depending on the organization's size, industry, and the laws and regulations that apply to it. Areas of focus:

Developing and implementing privacy policies and procedures – giving the organization guidelines and expectations for maintaining the privacy of regulated information.

Responding to data subject requests, such as requests for access, rectification, or erasure of personal data – making sure the customers and individuals whose information is being used to provide a service are aware and that all processing is done within the agreed upon limits and according to applicable laws and regulation.

Communicating with data protection authorities (DPAs) – making sure regulatory expectations are accurate and clear.

Conducting privacy impact assessments (PIAs) – helping product and technology teams understand the risks associated with processing regulated information and handling required safeguards

Investigating and resolving privacy incidents – responding quickly to instances where the privacy of information is compromised.

Compliance

Compliance teams work with their business areas and other teams to help the organization understand how effectively it implements internal controls to mitigate various compliance risks. Similar to audit and advisory teams, compliance teams in our model do not take the place of the corporate compliance departments most organizations have. Compliance professionals in this model are deployed by technology and operations teams looking to proactively manage their compliance risks. Areas of focus:

- **Plan and conduct audits** – including compliance reviews and tests. Facilitate external audits and compliance assessments
- **Identify and assess risks** – focusing on the compliance of all operational policies as well as financial, contracting, safety, quality, and other compliance obligations.
- **Make recommendations for improvements** – focusing on compliance processes and programs.
- **Report on the results of their activities** – reporting regularly on compliance risks and the performance of compliance programs to internal committees.
- **Work with regulators** – ensuring alignment with regulatory expectations and partnership.

Audit and advisory

Audit and advisory teams inspect organization's processes to ensure those processes implement the company's policies and mitigate risk effectively. Audit and advisory teams provides an important role in helping organizations to identify and mitigate risks, improve their efficiency and effectiveness, and comply with policies, laws, and regulations. Separate from internal audit teams, audit and advisory teams in our model are deployed by technology and operations teams looking to proactively manage risk in their functions. Areas of focus:

- **Plan and conduct audits** – including operations, financial statements, and compliance with laws and regulations.
- **Identify and assess risks** – focusing on operations, financial statements, and compliance with laws and regulations.
- **Make recommendations for improvements** – focusing on risk management, control, and governance processes.
- **Report on the results** – delivering findings to management.

Appendix B

The relationship between organizational culture and transformation

01

Going beyond organizational transformation

Change is hard. Moving an organization forward in a security transformation can feel uncomfortable and ambiguous for team members. We've learned that most big changes start with taking stock of where you are starting from, identifying quick wins, and making small changes to attain them. The goal is to keep momentum going.

How does your organization start to think about which operational changes to make? We think this activity starts best by conducting value stream mapping.

Value stream mapping: learning more about how teams perform and interact

More than just understanding organizational layout, it's important to spend time understanding the throughput, quality, handoffs, and tensions that occur between teams in the highest and most important value streams.

Value stream mapping is an activity organizational planners conduct to understand how work gets done. This is considered an essential prerequisite to digital transformation efforts.

With value stream mapping, the team understands how work, including products or features, moves through the business from idea, to work in process, to a final customer where it hopefully creates value. (hopefully!)

Value stream mapping is most effective when:

- The team has visibility into the flow of this work.
- The flow of work, including its current state, is shown on visual displays or dashboards.
- Information about the flow of product development work across the whole value stream is readily available.

A value stream map gives operations the ability to more accurately communicate to an organization how well they're creating value with each task at a point in time and over time. This is necessary to understand constraints and eventually exploit them. In digital transformation, many organizations set goals on achieving operational efficiency and process throughput as a way to achieve scale, lower cost, and offset future expenses.

We believe operational improvements again start with activities like value stream mapping, plus careful process measurement for activities found within the work streams. First, identifying the operations that truly impact speed, safety, cost, and quality in the highest value areas creates an opportunity to stand back and begin to imagine what's truly possible. Then it's time to start experimenting with new technologies.

02

Why culture is key to successful transformation

Value stream mapping helps organizations understand where value could be increased and services and products could be put into the hands of customers more rapidly. However, no matter how rigorous, analysis does not reliably identify or demonstrate how much the beliefs and pressures of the people working in the value stream influence how those processes work and what needs to change to optimize them. If left unaddressed, the culture and their drivers must also either change or be sustained to make sure transformation lands.

Our point of view builds on DevOps Research and Assessment (DORA) research, observations, and principles which were most recently summarized in the Accelerate State of DevOps Report 2023. The report notes that culture is foundational to building technical capabilities, igniting technical performance, reaching organizational performance goals, and helping employees be successful. In fact, culture is a key driver of employees' well-being and organizational performance.

A healthy culture can help reduce burnout, increase productivity, and increase job satisfaction. It also leads to meaningful increases in organizational performance, in software delivery and operational performance, and in-team performance. A healthy organizational culture can help teams be more successful at implementing technical capabilities associated with improved outcomes.

Examining the culture of an organization and its operations is an important initial step in a transformation journey. In the Guide to Cloud Security, we outlined what a strong security culture looked like with traits that included a culture of security by design, by default, of responsibility, awareness, inevitability, review, and sustainability. Now, we're ready to guide organizations deeper into what's needed to achieve a successful digital transformation with the spotlight focused strongly on the organization itself.

Applying Westrum's model to organizational transformation

Westrum's model, originating from Dr. Ron Westrum's study of information flow, posits that organizations with better information flow function more effectively. Westrum outlines three types of organizational cultures: pathological, bureaucratic, and generative.

DORA's research has shown that a performance-oriented, generative culture is a key predictor of software delivery, operational, and organizational performance. The research also indicates this culture leads to a number of other benefits including higher team satisfaction and lower team member burnout rate. Read more in the Accelerate State of DevOps Report 2023.

Pathological (Power-Oriented)	Bureaucratic (Rule-Oriented)	Generative (Performance-Oriented)
Low cooperation	Modest cooperation	High cooperation
Messengers "shot"	Messengers neglected	Messengers trained
Responsibilities shirked	Narrow responsibilities	Risks are shared
Bridging discouraged	Bridging tolerated	Bridging encouraged
Failure leads to scapegoating	Failure leads to justice	Failure leads to inquiry
Novelty crushed	Novelty leads to problems	Novelty implemented
Leaders focus: personal	Bureaucratic objectives	Organization mission

First, generative cultures require trust and cooperation between people who participate in them. Second, generative cultures make higher-quality decisions. Information needed to make decisions flows freely, and teams balance various forms of informal and formal (top-down) decision-making processes which ensure decisions that are hard to undo are scrutinized, and decisions that aren't are made rapidly (or unmade quickly when needed).

The importance of building a generative culture

Teams that recognize the need to continuously improve tend to have higher organizational performance than those that don't. That's the hallmark of a generative culture. A generative culture is one that's high trust and emphasizes the importance of the flow of information.

The Accelerate State of DevOps Report 2023 puts it in compelling terms: organizations with generative cultures have 30% higher organizational performance than those without. This triggers related increases in organization stability, job security, flexibility, knowledge sharing, and work distribution.

Teams with generative cultures have 30% higher organization performance than teams without.

Building a generative culture can take months to years and requires patience, commitment, and visionary leadership to drive it across an entire organization. Building it usually starts inside of small teams, with common goals and the ability to execute their work without much reliance on other teams to deliver at a high rate of performance, whether it be software development or operational performance.
Other factors affecting performance, explained in depth in the Accelerate State of DevOps Report 2023, emphasize the importance of:

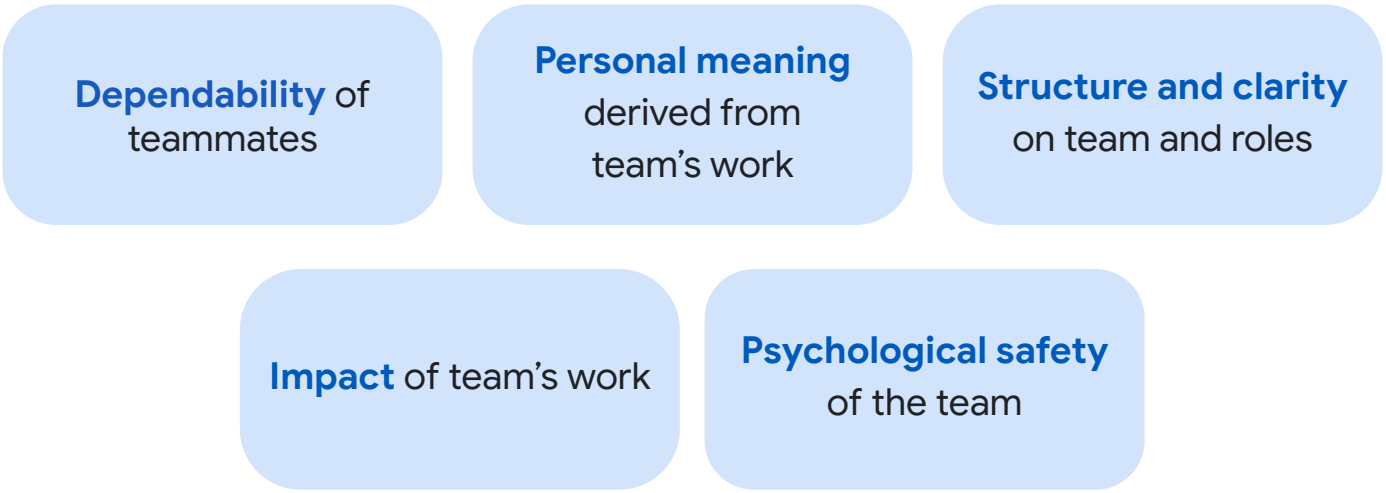
- Building for users (empathy)
- Providing reviews and feedback quickly (code reviews, tight feedback loops, enabled through automation)
- Sharing information and knowledge transfer (enabled through technical practices like trunk-based development and common version control strategies or keeping good quality documentation)
- Leveraging flexible infrastructure with cloud
- Distributing work fairly across a diverse team where everyone belongs

Strong culture drives strong performance and cannot be ignored. Generative cultures aren't the only cultures that will find success, but they are positively correlated with high-performance teams and organizations.

Nurturing generative culture traits

In How to Change a Culture: Lessons From NUMMI, the point is made that the way to change a culture is not to first change how people think, but instead to start by how people behave – in other words, what they do.

We've also observed that it's less about who is on an organization's teams and more about how the teams work together and their ability to learn new skills. Organizations can start by identifying helpful practices to create a generative culture that fosters information flow and trust by working to achieve the five characteristics of an effective team:



03

Strategies for setting and obtaining shared goals

One of the strongest cases for creating a generative culture is that it creates a team environment to foster collaborative support for achievement of shared goals for digital transformation. Teams feel supported when offered the right kind of training and when they have someone who can lead by example.

Focused training empowers team members

The best way to learn a new language is immersion. When it comes to learning the language of digital transformation within organizational teams, the same can be said: jump in and learn new skills and gain new expertise.

Training helps individual team members feel safe and better able to perform their jobs. Training also helps foster a renewed sense of being a “we are in this together” community as colleagues and peers join the training activities. To this end, consider implementing training that:

- Boosts proficiencies in given skill sets with associated certification to recognize newly gained experience
- Host workshops and cloud-enablement days dedicated to specific topics
- Set education paths based on roles, such as access, pipelines, governance and risk, and security operations
- Have teammates teach other teammates to establish a give-back, collaborative environment

Measure established goals

Incorporate and closely monitor industry-standard metrics and methodologies to track the progress of shared goals as well as related performance and risks:

Standard objectives and key results (OKRs) track progress, create alignment, and encourage engagement around measurable goals.

Key performance indicators (KPIs) provide targets for teams to shoot for, milestones to gauge progress, and insights that help people across an organization make better decisions.

Key risk indicators (KRIs) measure the likelihood that the combined probability of an event and its consequences will exceed an organization's risk appetite and could have a negative impact on the ability to succeed.

04

Big picture: focus shared goals on improving security and speed

What are some important goals for cybersecurity teams' digital transformation? One goal should be introducing greater levels of resiliency and security.

One way to achieve transformation is to set goals focused on building specific technical capabilities. Our research, Accelerate State of DevOps Report 2023, indicates that organization's with strengths in four specific capabilities can expect better security and resilience outcomes. Thematically, these goals focus on the following areas:

01

Version control – for all instructions, especially code. Building capabilities deployed through code increasingly helps an organization move fast while documenting what it's doing (so other people can see and learn) as the work gets done.

02

Continuous integration (CI) – for all changes, making sure changes to any system meet the quality, security, and resilience with evidence gathered by automated testing. CI helps make sure changes are of a minimum level of quality and won't break, or stop, the work from being done.

03

Trunk-based development – for all changes, making sure we can always restore a system to a known point of good operation in the event a change or some other complexity is introduced as well as providing a way for teams working on a system built off of a given trunk to understand exactly what is running and what is not.

04

Loosely coupled architecture – for designing systems. Loosely coupled architecture is a design approach in software development where individual components or services within a system have minimal dependencies on each other. This means the components interact mainly through well-defined interfaces (like APIs), exchanging necessary information but otherwise remaining independent.

These technical capabilities should be investigated and considered as goals. Try identifying one high-performing area within an organization and see what measures might be in place today to measure performance. Share these examples widely, publish their results, and inspire others in doing so.

Meeting technical goals yields even better cloud security as a result

Focusing on these four technical capabilities drives good cloud security for several reasons. It sets up organizations to "shift left" to ensure security requirements are present in the earliest stages in the development lifecycle. It also increases the speed of redeployment, deployment, and continuous deployment.

Appendix C

The four stages of organization transformation

What stage are you in?

Here's a detailed look at a breakdown of each stage, activities, and forward management motion with ways to confirm that you are in a particular stage.

Stage 1

Experimentation and Disintegration

Goals: This stage starts with the announcement of your new digital transformation initiative. It signals the time to address your current state, which most likely includes:

- Manual processes stemming from existing heterogeneity for technology infrastructure
- Limited knowledge of cloud architectures with difficulty envisioning what constitutes new workloads and where to start
- Concerns about new skill acquisitions and any future changes in job roles and responsibilities
- Lack of standards for cloud architecture and cloud security
- Team-based automation strategy

How to achieve these goals: To move to the next stage, you need to:

- ❏ Establish strong leadership to articulate clear vision, purpose, support, and expectations
- ❏ Set collaborative goals and define achievable targets that promote cross-team teamwork and achievement
- ❏ Invest in training to prioritize skill development and encourage experimentation
- ❏ Cultivate risk-taking and safety to build programs that promote innovation within a psychologically safe environment

You can also consider kicking off "lighthouse projects" to introduce critical cloud-adoption scaling capabilities, such as version control, continuous integration and continuous delivery/deployment (CI/CD), and loosely coupled architecture patterns.

Dissolution

It's at this point that your organizational structures begin to be challenged with the realization that processes to get work done "the same as before" don't map well in the cloud thanks to slow actions and too many handoffs. There's a risk of duplicating efforts due to lack of governance and direction.

Goals: At this stage, you should be setting shared goals in alignment with your new culture, new organization design, and business outcomes. Actions include:

- Formation of cloud engineering teams with the development of new skills becoming increasingly in demand by teams struggling to adopt
- Emergence of new forms of bureaucracy as the truth behind Conway's Law becomes apparent
- Extremely fast (too fast?) movement of some teams with other teams moving slowly or remaining anchored to existing processes
- Fast-moving teams feeling frustrated by organizational resistance to speed and legacy teams pushing back on new processes (the divide becomes evident)

Steps to achieve these goals: To establish and maintain momentum into the next transformation stage, you should:

- ❑ Reorganize teams to focus on first-mover applications and cloud centers of excellence
- ❑ Transform communication by implementing new flows and collaborative work practices
- ❑ Develop shared roles to foster cross-functional expertise within teams
- ❑ Identify early adopters and find champions in infrastructure, security, compliance, and development
- ❑ Seek external expertise to accelerate adoption with deployment pipelines, CI/CD, and training
- ❑ Prioritize governance with an emphasis on cloud-first services and automation to reduce manual effort

Transformation

Goals: Toil reduction by way of automation is a first principle to any process intersecting with your movement to the cloud. Other hallmarks of this transformation stage include:

- Policies, standards, and procedures are increasingly being executed with code
- Policies are proven implemented and effective through increasingly continuous monitoring
- Most teams are seeing benefits of transformation
- Reliability and resilience of platforms is measurably increasing
- Version control, test automation, CI/CD, and deploying technology with loosely coupled, cloud-first architectures are common practices

Steps to achieve these goals: To begin moving on to the fourth and final integration stage, you should:

- ❏ Establish ownership for the change – appoint change leaders and transformation officers
- ❏ Adopt OKRs that focus remaining non-first-mover-teams efforts on migration
- ❏ Measure based on direct business outcomes and the adjacent commercial benefits of speed, scale, and resilience
- ❏ Incorporate oversight and measurement of process friction
- ❏ Continuously optimize deployment pipelines
- ❏ Select and implement continuous monitoring programs
- ❏ Continue increasing investment and emphasis on automation
- ❏ Assess technical and organizational skills gaps and close with training, mentorship, and experiential learning

Integration

When you successfully reach this stage, governance asks, “Why not cloud?” as the destination for every new workload.

Goals: You should begin to see this kind of tangible progress:

- Team structures optimized with clear paths to acquire support and staffed to deliver on their mission to take advantage of the cloud
- Processes that add friction are met with no support and such proposals are removed quickly via governance
- Automated pipelines block all non-standard approaches except by pre-approved exceptions
- Friction is removed from pipelines / pipeline optimization is a regular practice

Steps to achieve these goals: This marks the ideal opportunity for you to:

- ❑ Inventory and actively retire manual processes for automation
- ❑ Shift governance efforts to focus on burning legacy applications
- ❑ Continuously assess and challenge the need for exceptions to cloud migration