Google Cloud

## Student Slides

# Understanding Google Cloud Security and Operations

## Modules

01 Financial Governance in the Cloud

02 Security in the Cloud

03 Monitoring Cloud IT Services and Operations

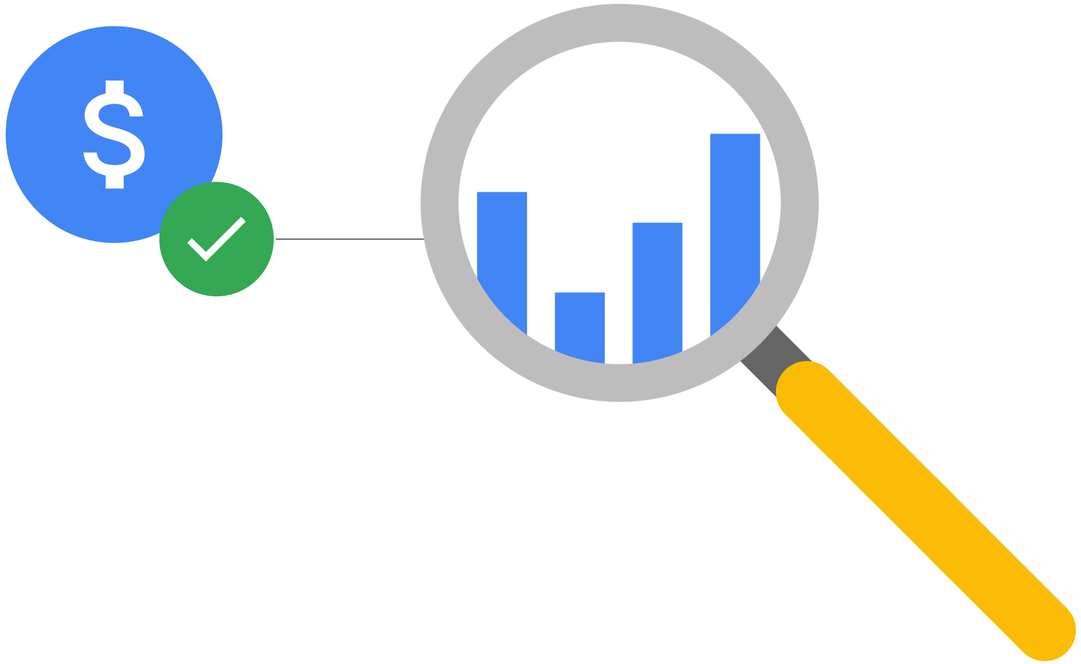
Google Cloud

## Module 1: Student Slides

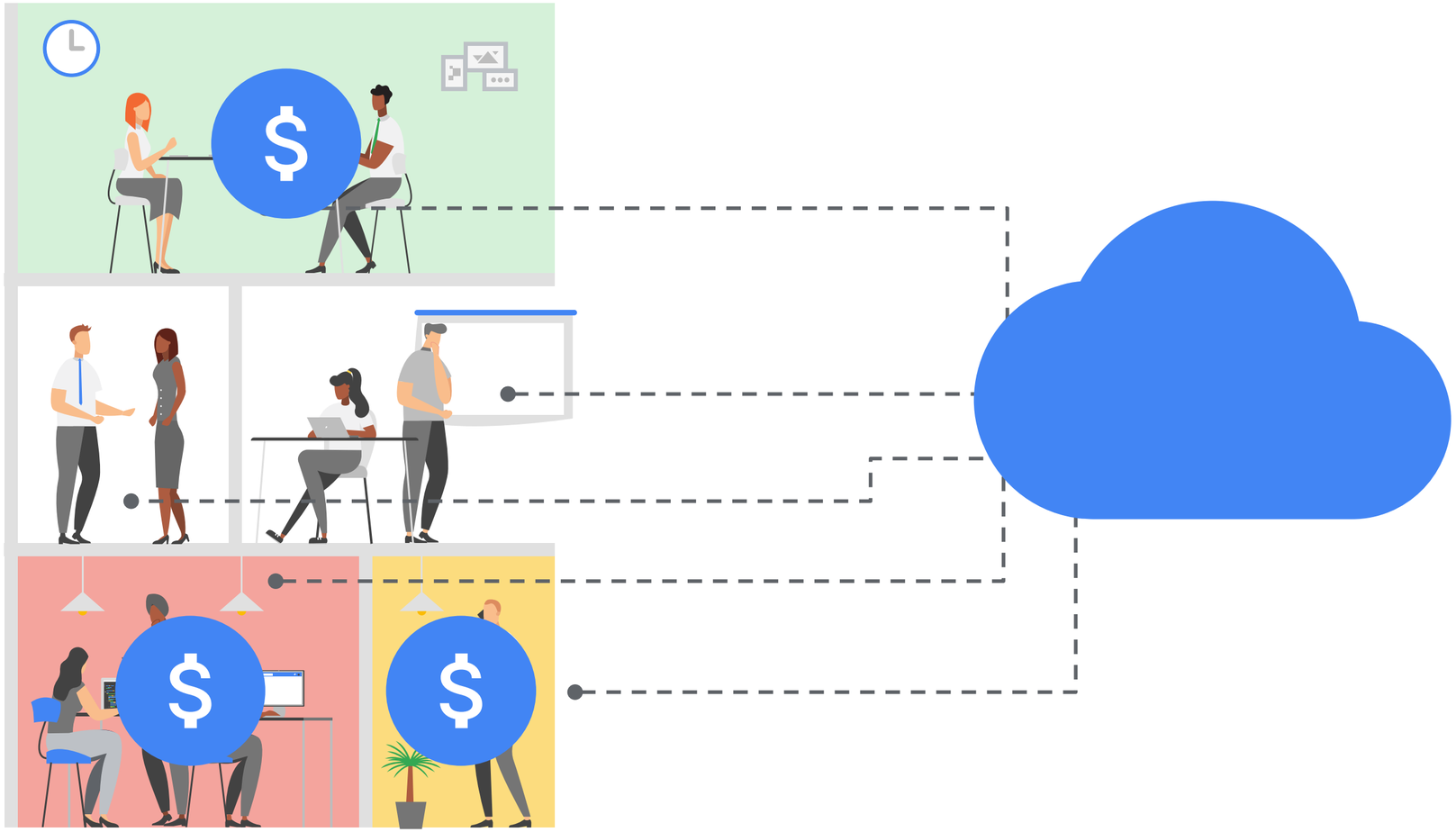
# Financial Governance in the Cloud

## Topics covered

- Cost management changes with cloud
- Total cost of ownership for cloud services
- Core Google Cloud cost management concepts
- Best practices for effective cost management

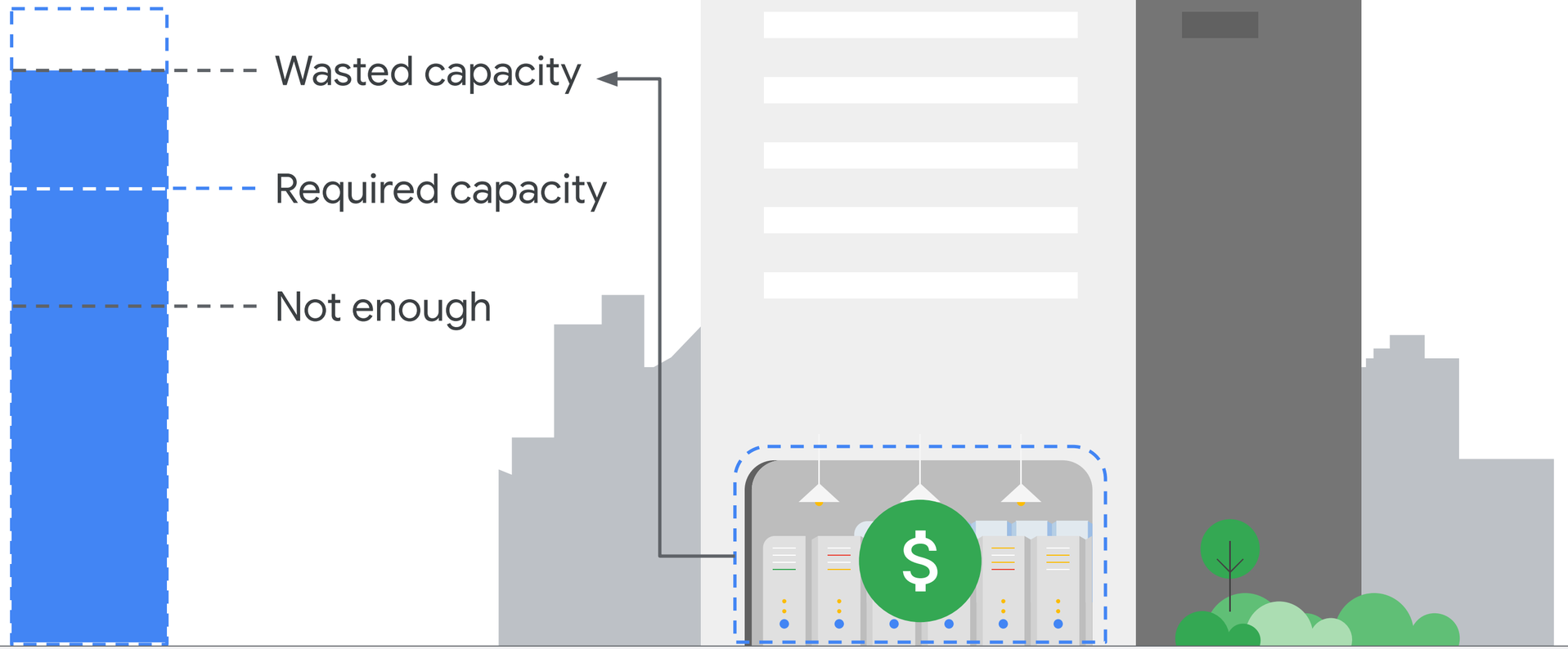


Cloud technology can provide organizations with the means to make more dynamic decisions and accelerate innovation, but managing cloud costs requires vigilance and real-time monitoring in parallel.

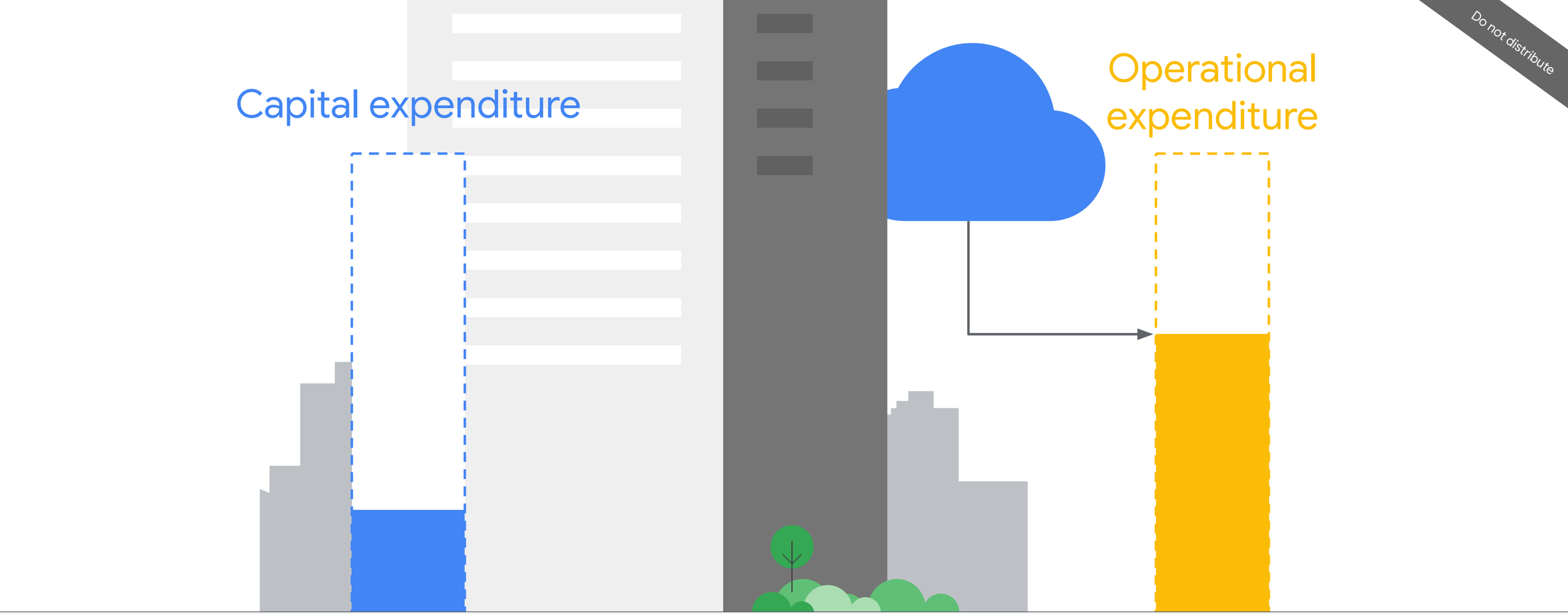


Because almost anyone can now access cloud resources on demand, it involves more people across multiple teams.

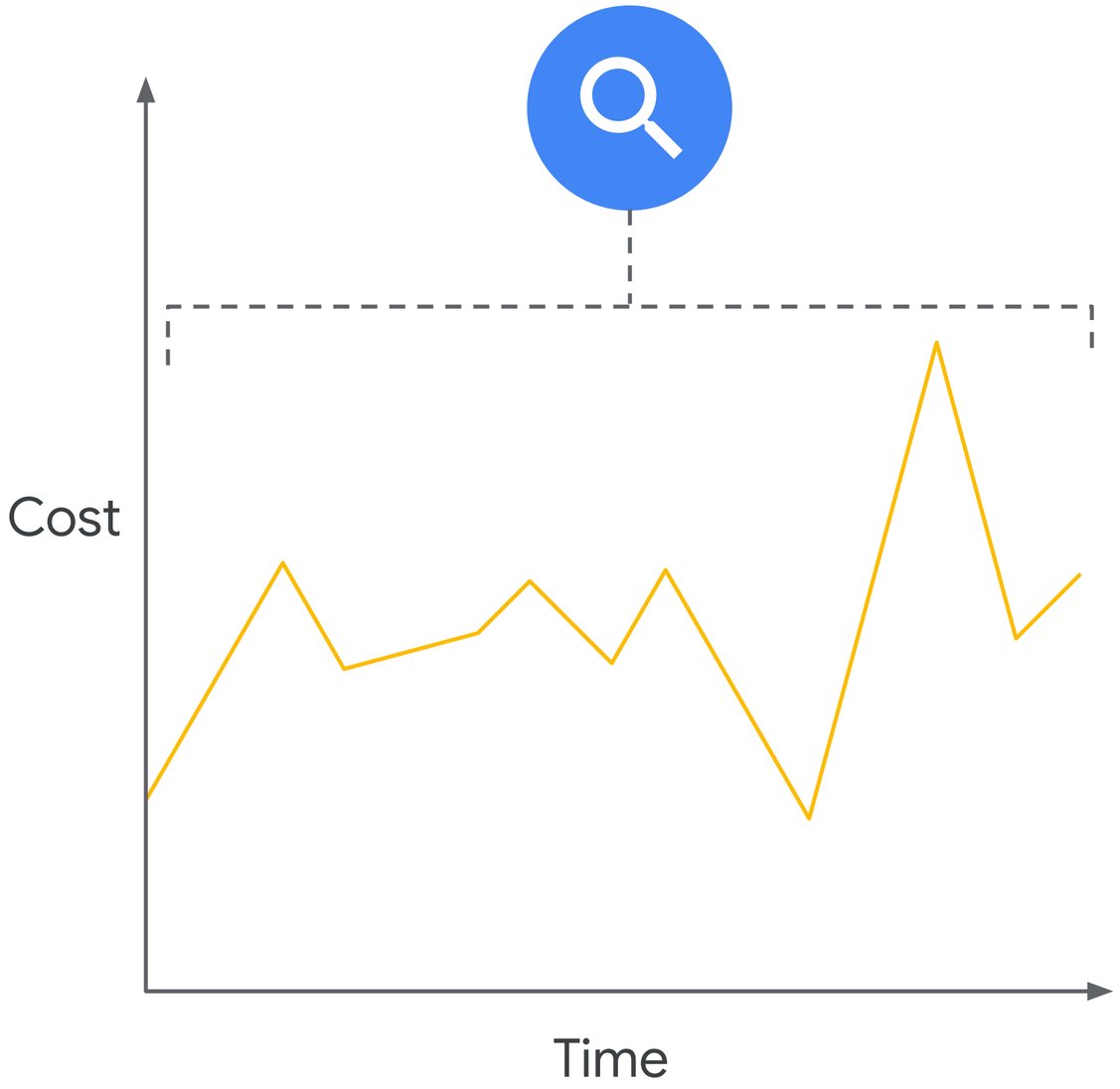
# Capital expenditure



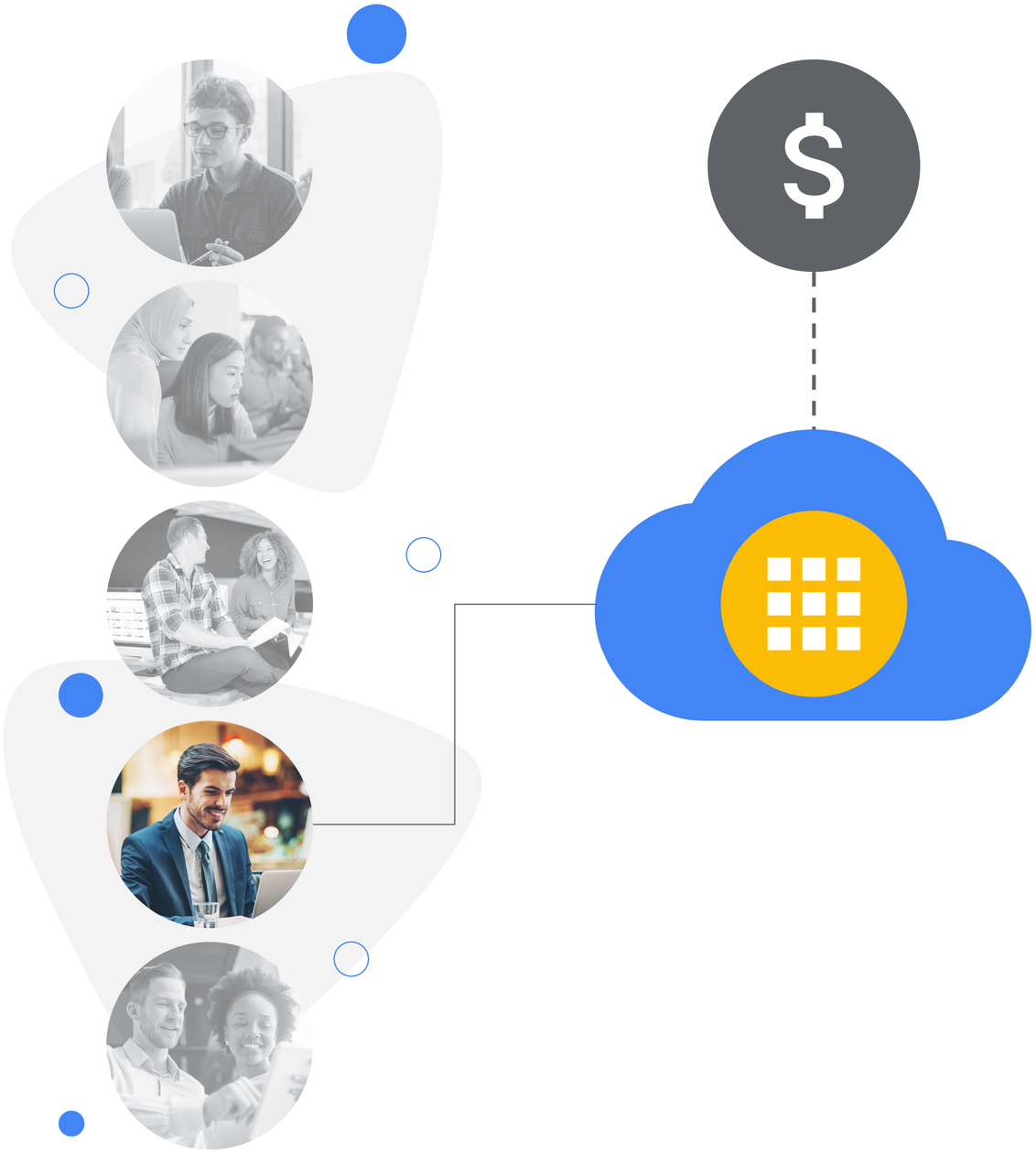

For organizations that build and deploy applications on-premises, there's a heavy emphasis on capital expenditure to set up and maintain their IT infrastructure. It's a careful balancing act between under-purchasing and over-purchasing, so a business doesn't end up with unserved demand or wasted capacity.




When an organization migrates or builds and deploys applications using cloud services, there's a greater emphasis on operational expenditure. They're paying for what they need when they need it.

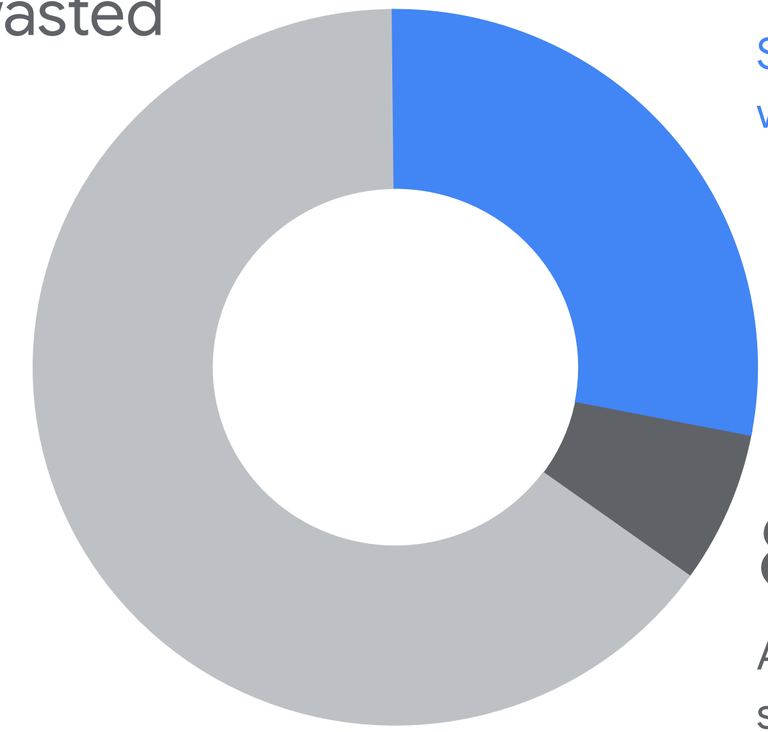



Budgeting is no longer a one-time operational process completed annually. Because of the variable nature of cloud resources and their costs, spending must be monitored and controlled on an ongoing basis.



Given the right permissions, almost any employee can spin up resources in seconds. Often, the accessibility that makes cloud services attractive leads to reduced control and significant overspending.

Up to 35% wasted



**27%**

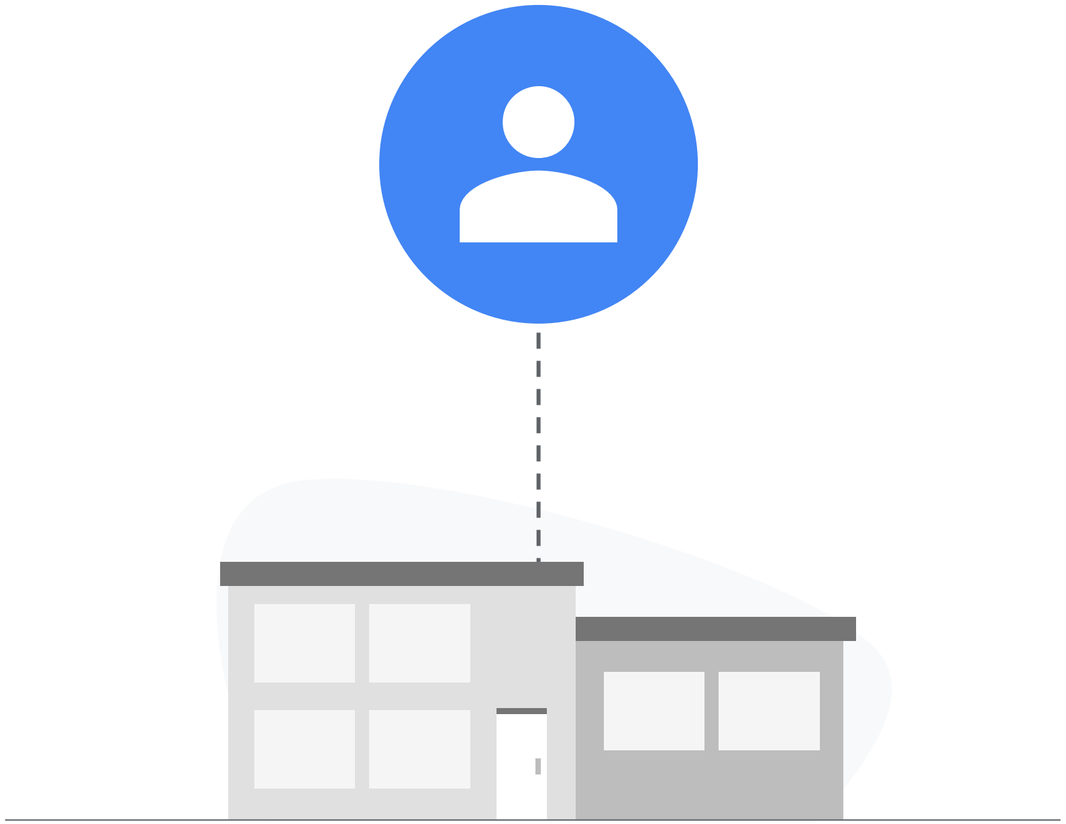
Self-estimated wasted spend

**8%**

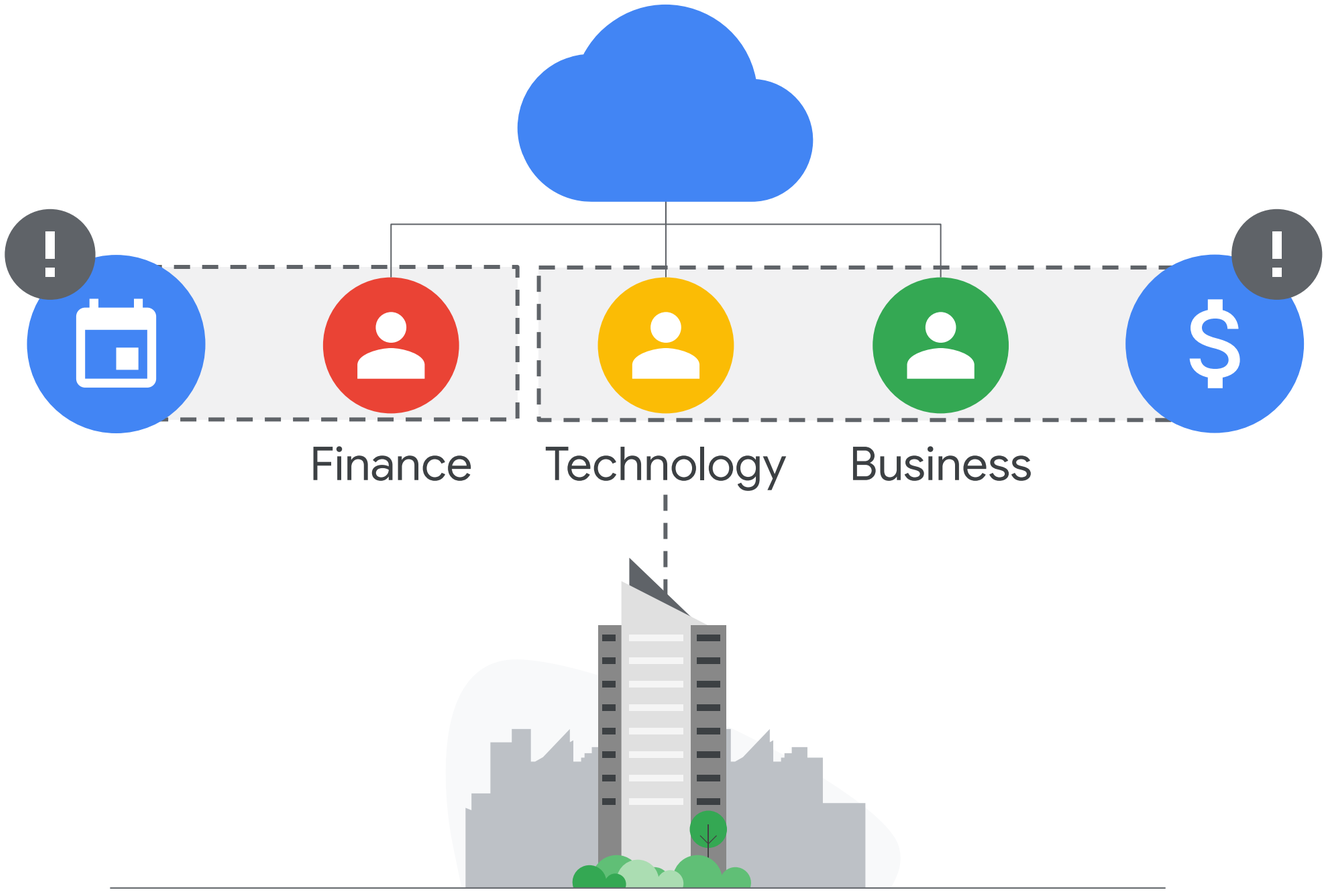
Additional wasted spend measured by Flexera

Source: RightScale 2019 State of the Cloud Report from Flexera.


When cloud usage isn't effectively controlled, it can lead to inefficiencies. According to a Rightscale study from Flexera, businesses surveyed estimated they were wasting 27% of their cloud spend. Businesses were actually wasting 35% of their cloud spend: 8% over their estimates.

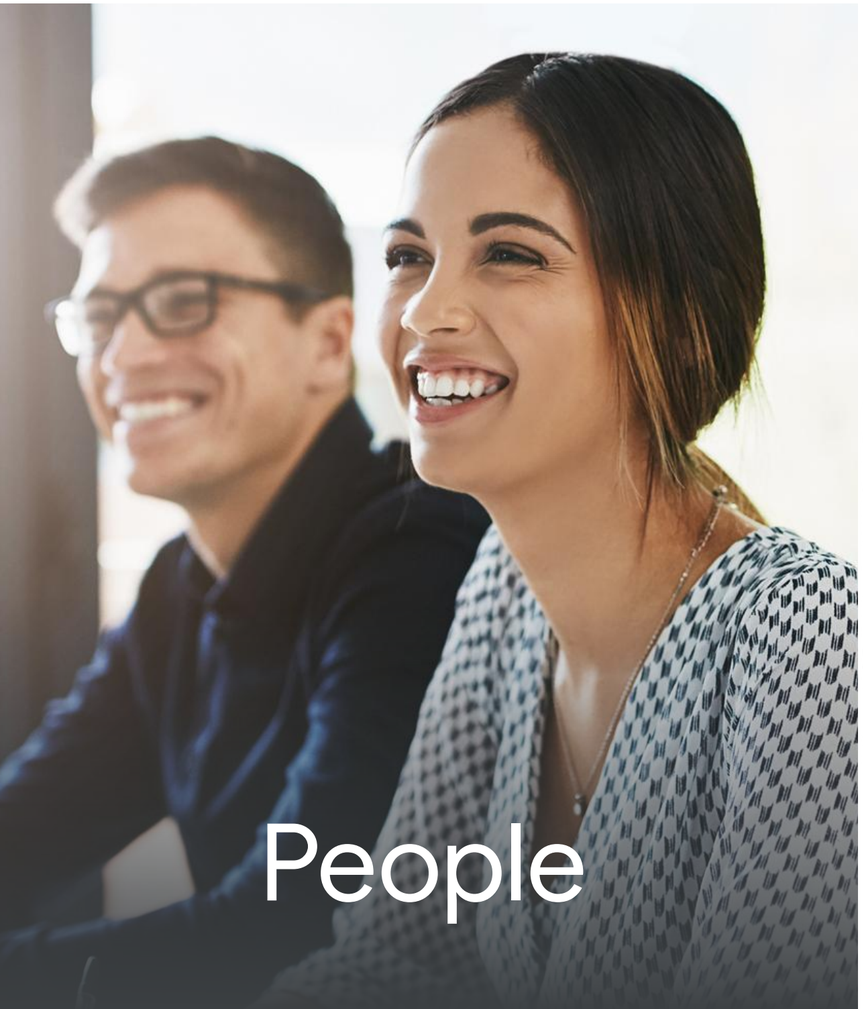


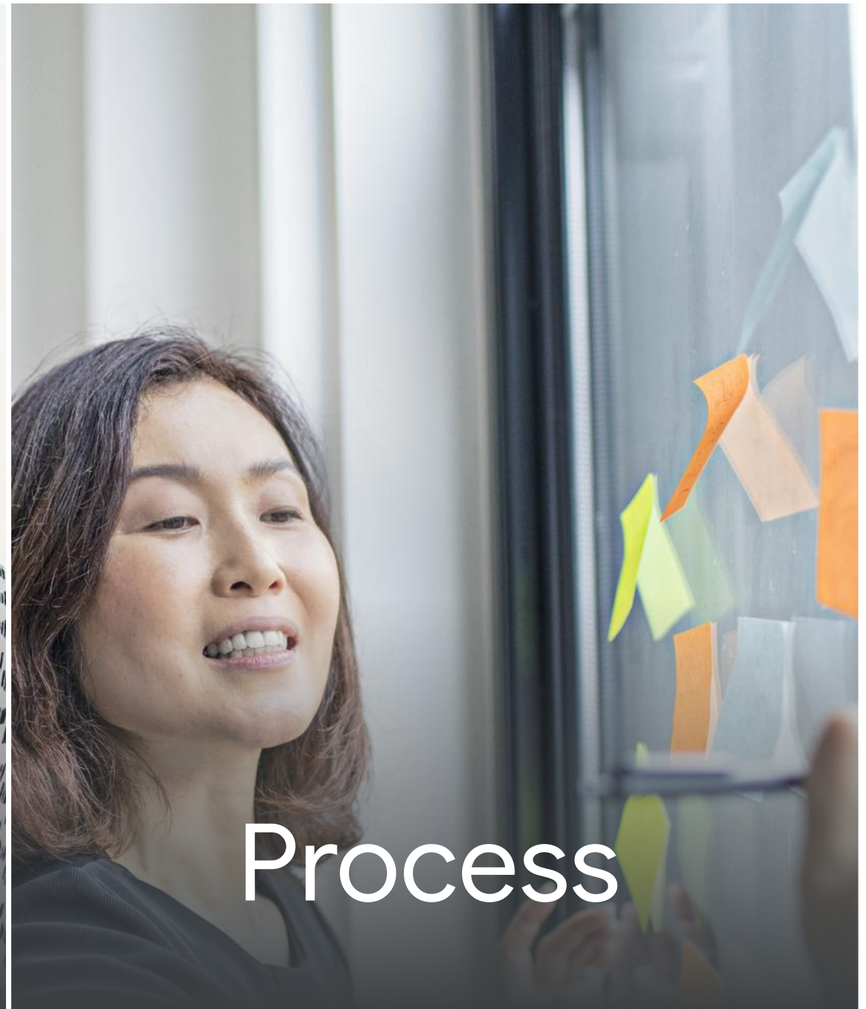
In a small organization, there might be one person or team responsible for managing all aspects of the cloud infrastructure and associated finances, from budgeting to procurement, tracking, optimization, and so on.

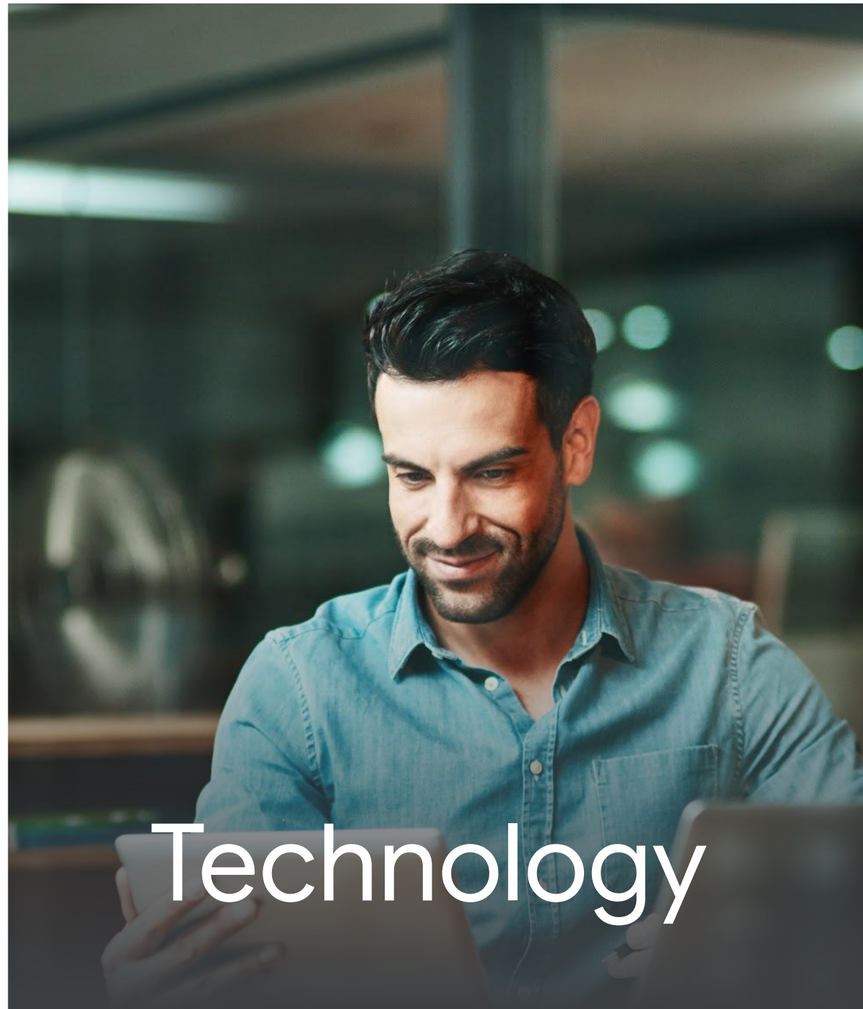



In large organizations, there are people involved across multiple functions. Technology and line-of-business teams are often using cloud resources, but they don't necessarily factor cost into their decision-making. Finance teams control cloud costs, but may struggle to understand or to keep up with cloud spend on a daily, weekly, or monthly basis.

To solve this problem consider
the solution through three lenses:



# People


To manage cloud costs effectively, a partnership across finance, technology, and business functions is required. This partnership would consist of several experts who ensure that best practices are in place across the organization and there is visibility into the ongoing cloud spend.

# Process

When it comes to cloud cost management, consider the following questions:

What cloud resources are being used and by whom?

What are the associated resource costs?

How do these costs measure against the broader business strategy?

# Technology

**Visibility**

**Accountability**

**Control**

**Intelligence**

Google Cloud brings its own native tools to help organizations monitor and manage their costs. In fact, these tools enable organizations to gain greater visibility, drive a culture of accountability for cloud spending, control costs to reduce the risk of overspending, and provide intelligent recommendations to optimize costs and usage.

# Total cost of ownership varies with complexity

**Cost model**
Simple
Infrequent
Predictable

On-premises

Single cloud

Multi-cloud

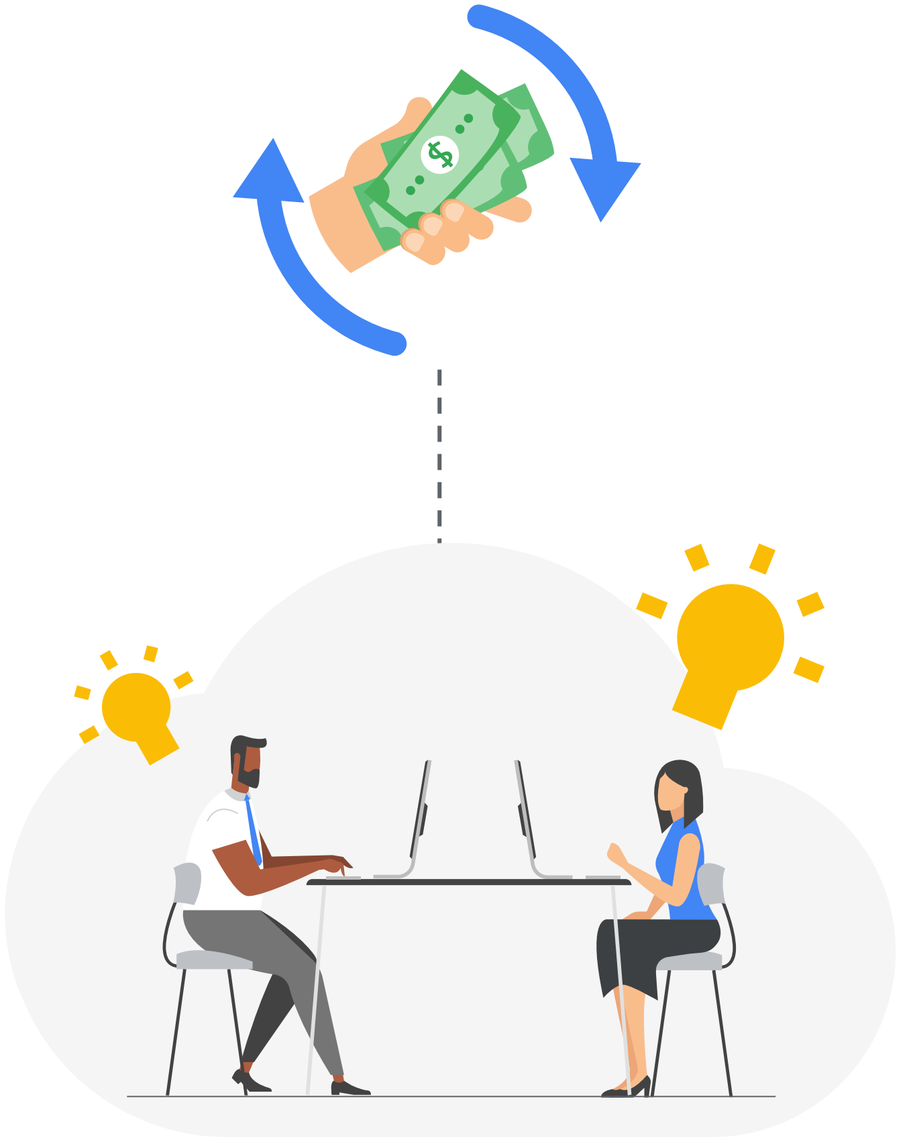
Multi-cloud + on-premises

**Cost model**
Complex
Agile
Unpredictable

Whether an organization is moving to the cloud for the first time or moving from a single cloud provider to multiple providers, how they calculate the total cost of ownership of the IT infrastructure will vary.

Historically, when companies spent a substantial amount of money upfront to set up their IT infrastructure, the capital expenditure would include paying for:

- Space and associated costs
- Storage systems
- Networking
- Hardware
- Software
- Security systems



When organizations run their business using public cloud services, much of their capital expenditure shifts toward a pay-as-you-go OpEx model.

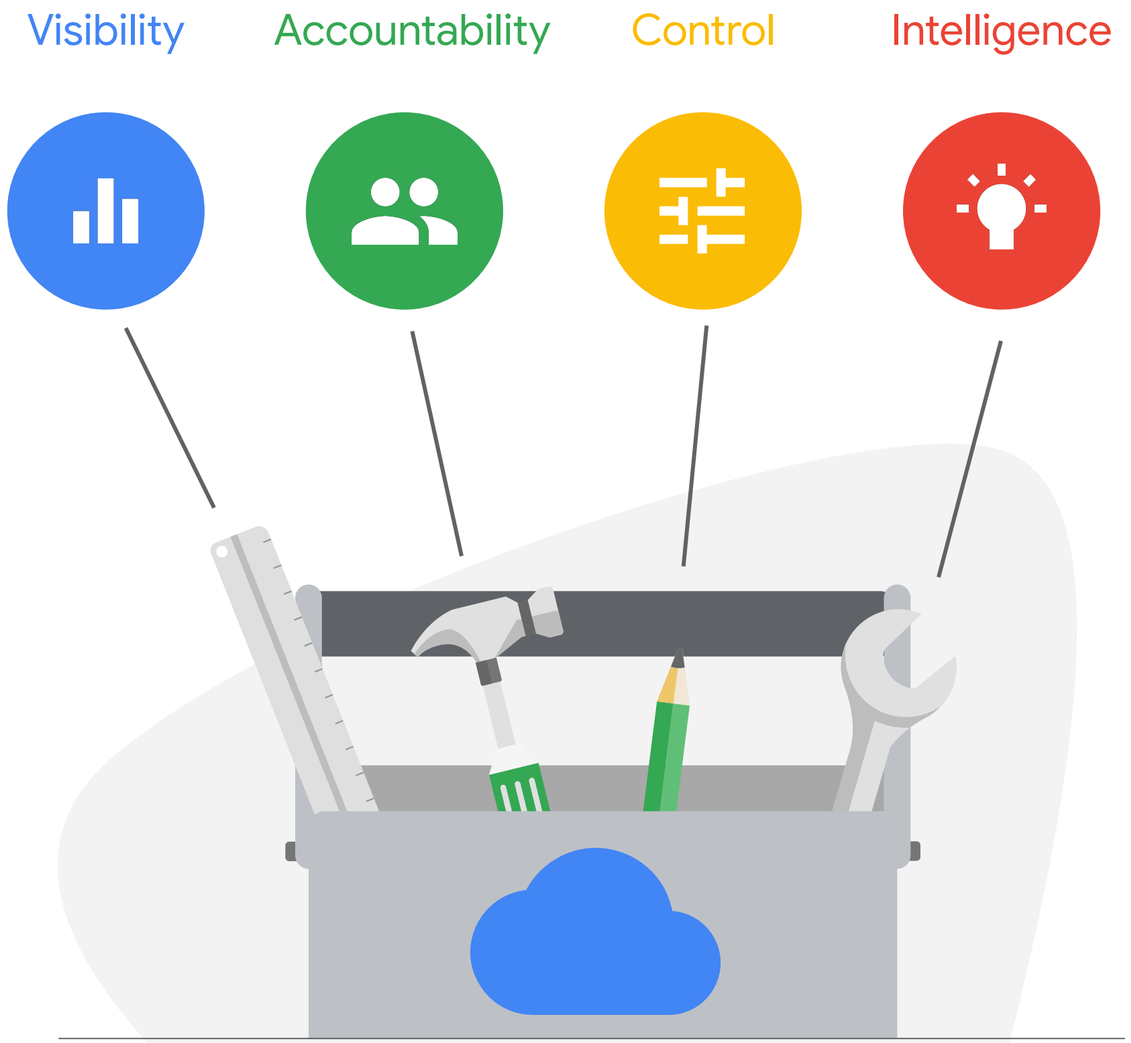

Some organizations may choose to keep some of their business running on-premises and some running on public cloud. The total cost of ownership for them would be more complex.

Best practices and advantages for using available Google Cloud tools for ongoing cost management:

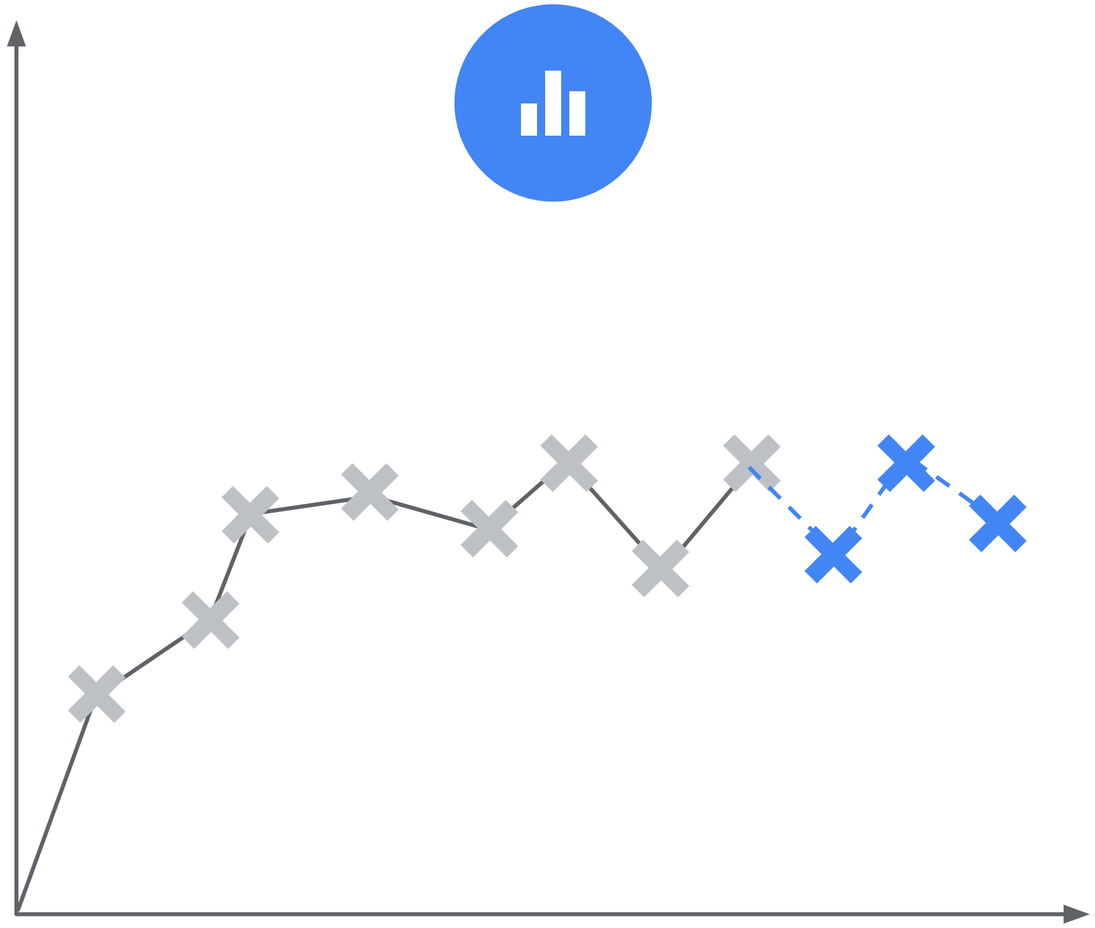
# Best practices

1. Identify the individual or team that will manage costs
2. Learn the difference between invoices and cost tools
3. Use cost management tools for accountability

The goals of the cost management tools are to provide:



# Visibility



Before organizations can optimize their cloud costs, they first need to understand what they're currently spending, whether there are any trends, and what their forecasted costs are. This means they need **visibility** into their cloud costs.

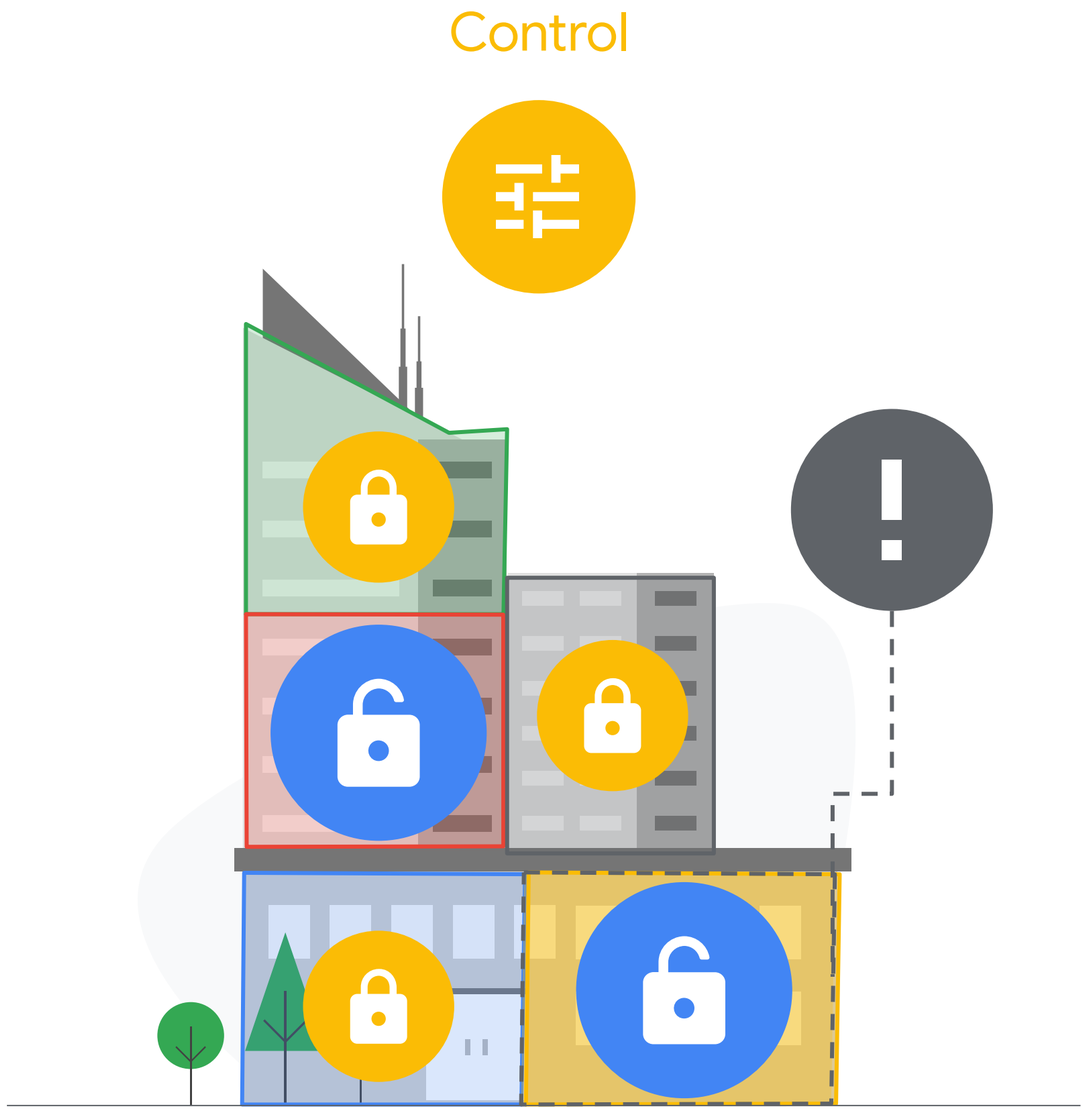
- Built-in reporting tools
- Custom dashboards
- Pricing calculator

cloud.google.com/products/calculator

A central team can monitor current cost trends and identify areas of waste that could be improved using Google Cloud built-in reporting tools, and create custom dashboards to gain greater visibility into their costs. The pricing calculator allows an organization to see how changing usage will affect their costs.

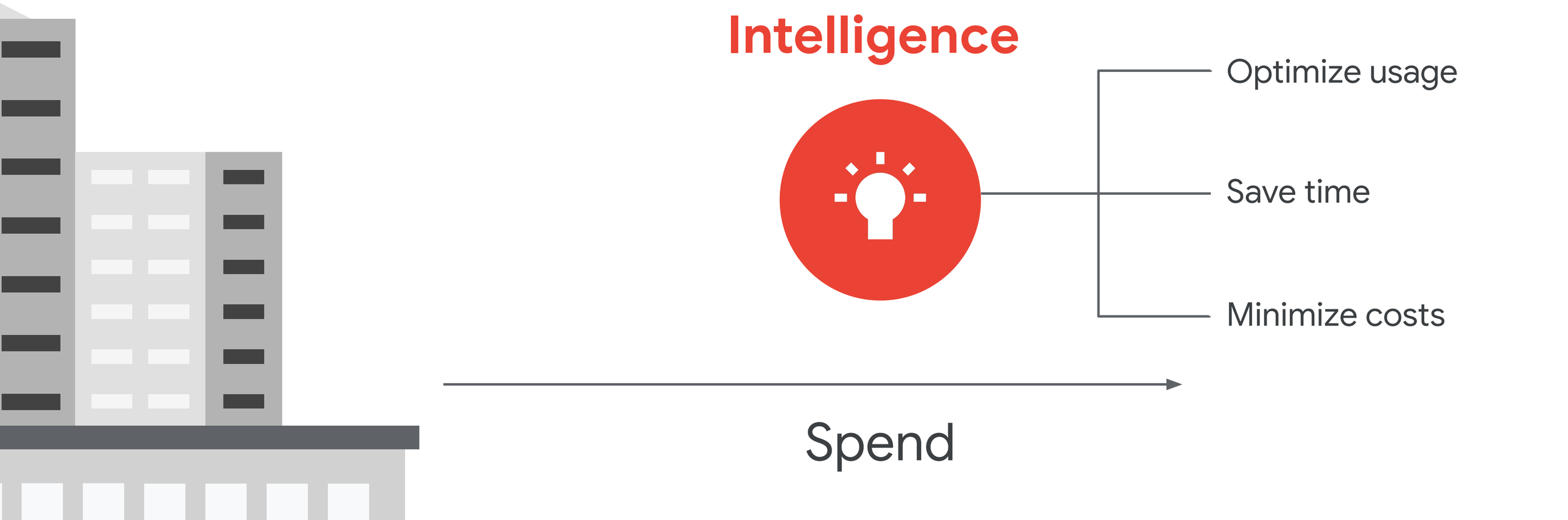
# Accountability


Because cloud spending is decentralized and variable, it's important to establish a culture of **accountability** for costs across the organization. This can be done by defining clear ownership for projects and sharing cost views with the departments and teams that are using cloud resources.




Organizations should also have precise permissions in place to ensure that only authorized individuals in an organization have the power to deploy cloud resources. Creating budgets and alerts to notify key stakeholders when spending is getting off track is an important practice to keep costs under control.

Organizations can make smart spending decisions with **intelligent** recommendations delivered by Google Cloud. These are tailored to each organization and help optimize usage, save time on management, and minimize costs. The recommendations can easily be applied for immediate cost savings and greater efficiency.



Google Cloud

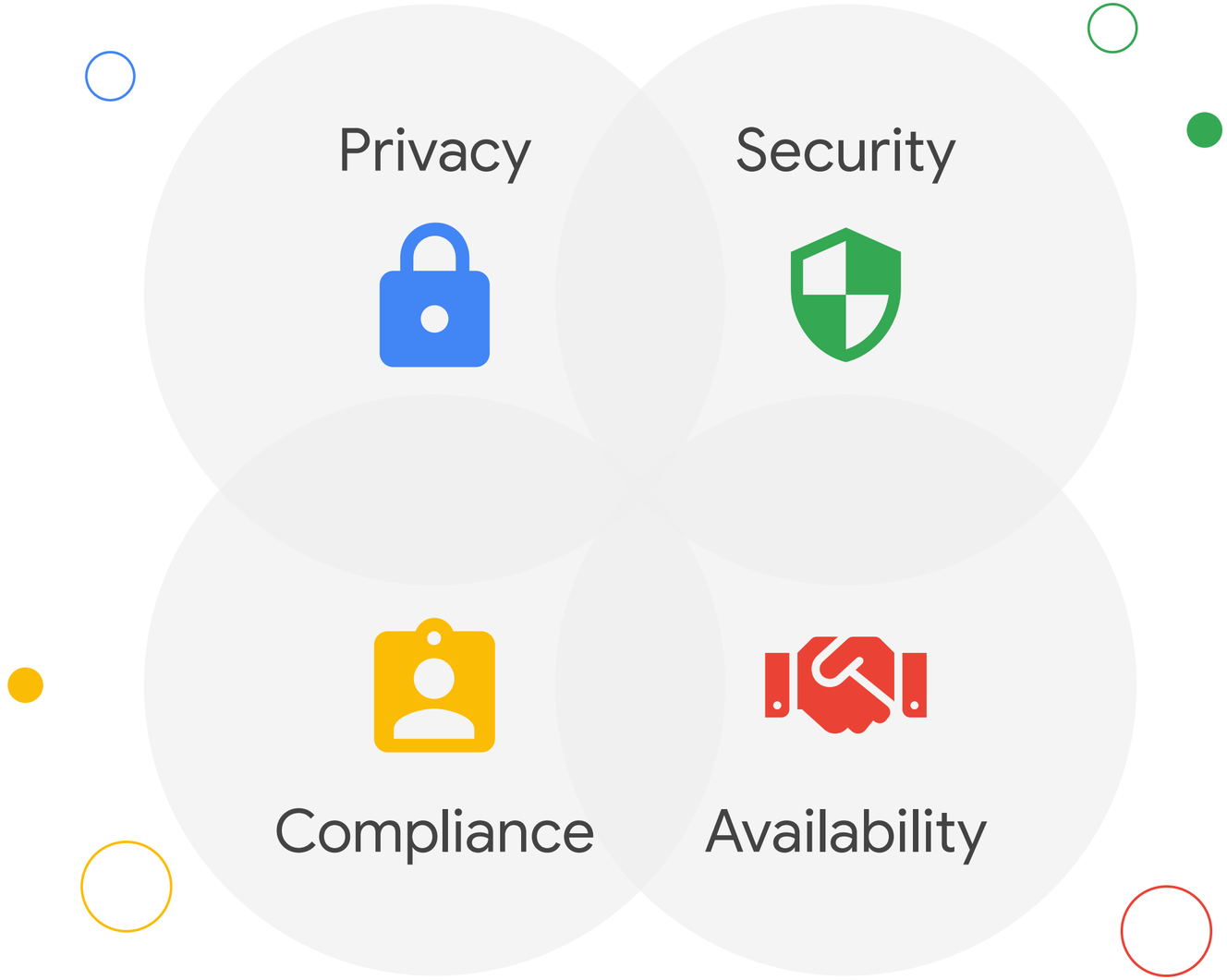
# Module 2: Student Slides

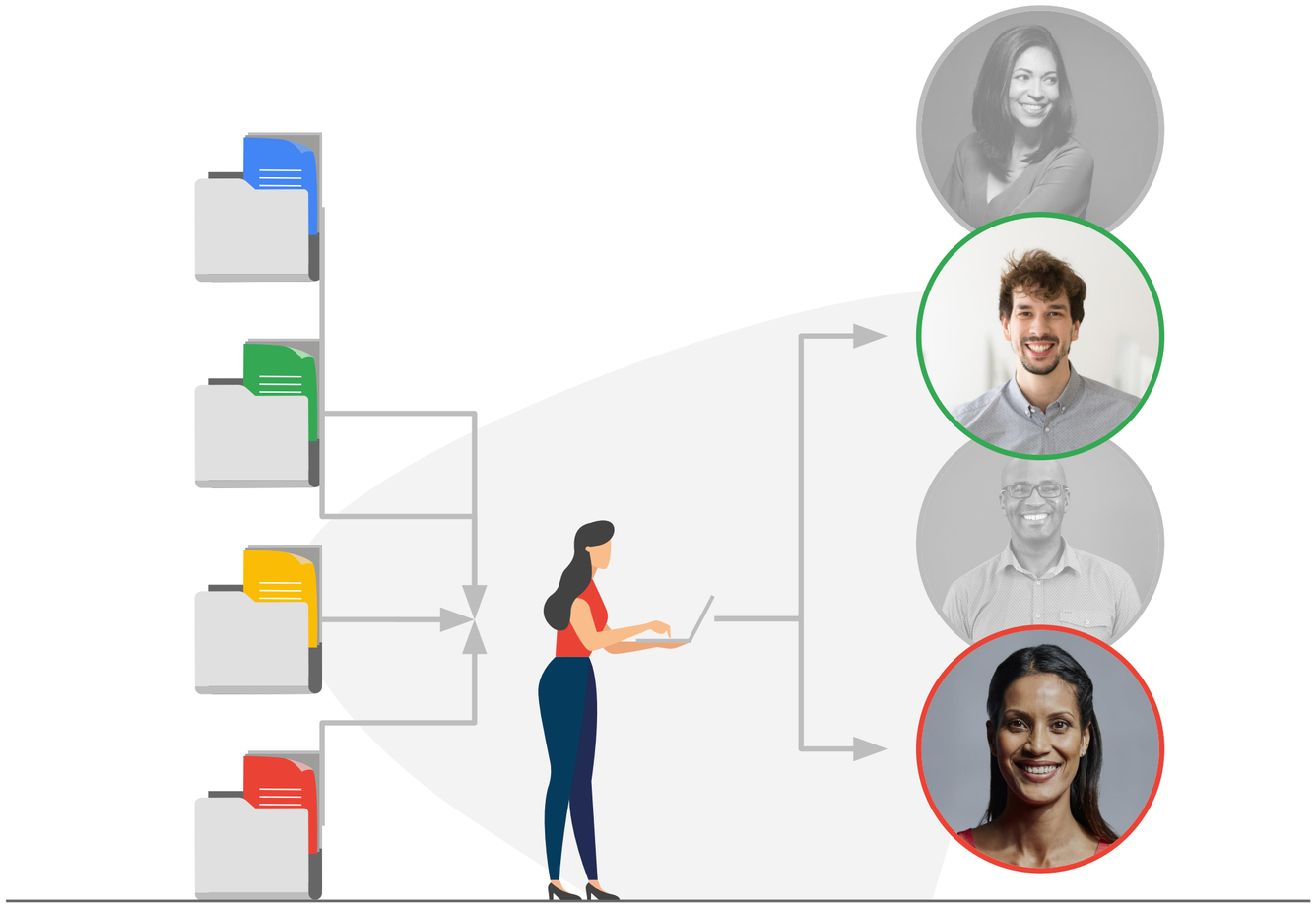
## Security in the Cloud

## Topics covered

- Fundamental terms
- Today's cybersecurity challenges
- The shared responsibility model
- Cloud Identity
- Resource hierarchy

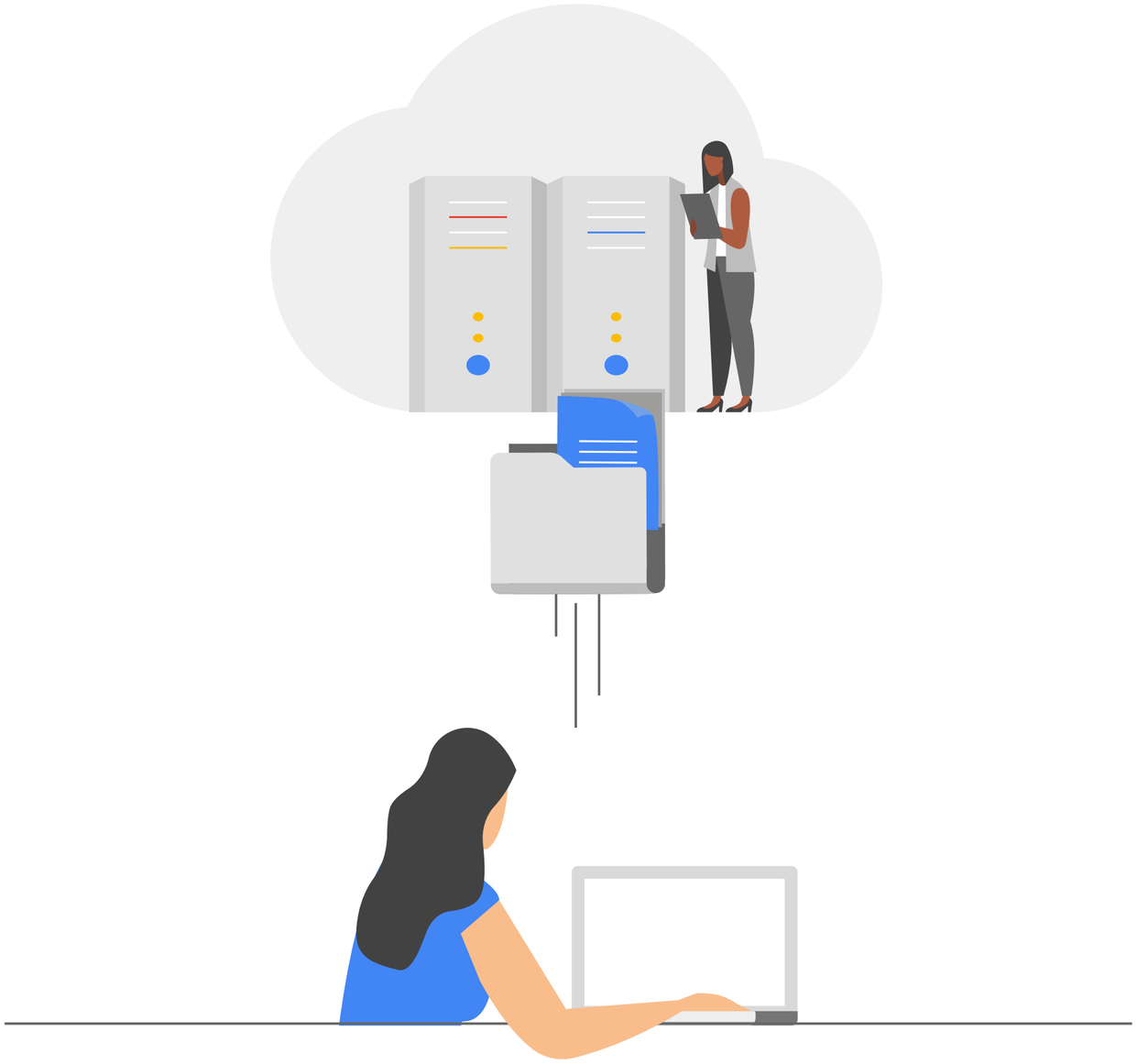
Fundamental terms:



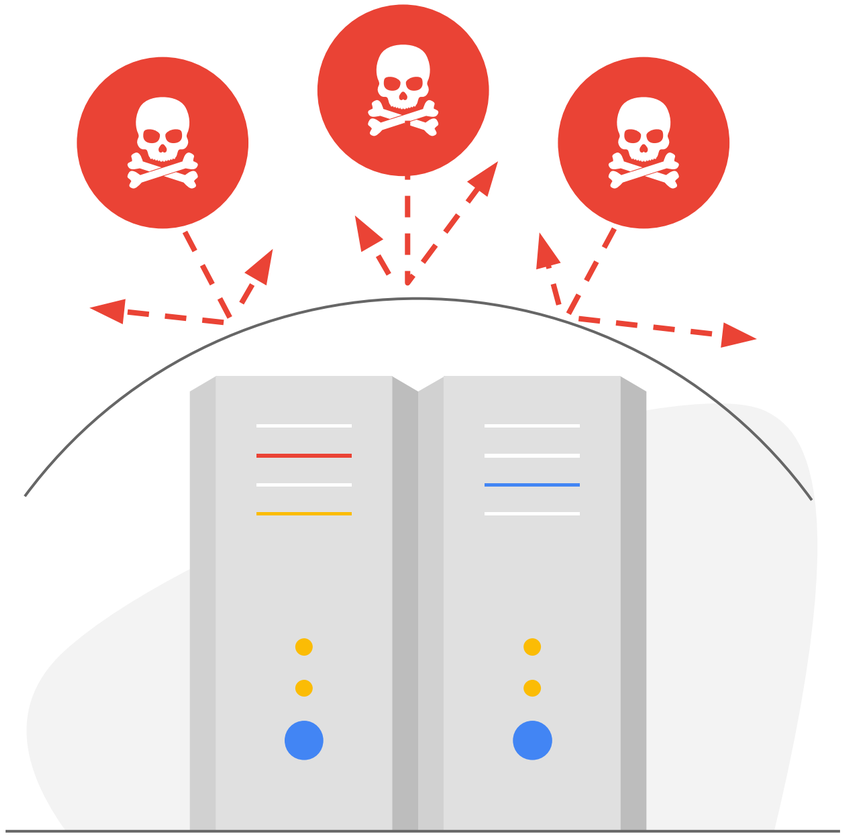


# What is Privacy?

**Privacy**, in the context of cloud technology, refers to the data an organization or an individual has access to and who they can share that data with.



When moving your data to the cloud, the facility and its employees only store or process your data. The data itself remains **private**.

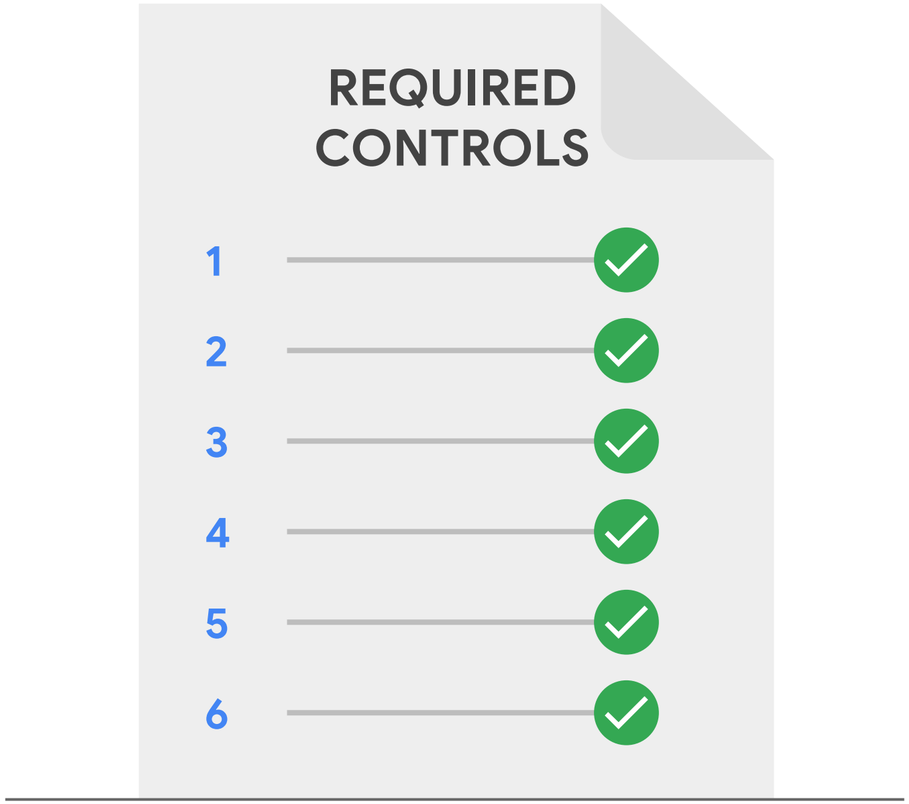


# What is Security?

**Security** in the cloud refers to the policies, procedures and controls put in place to keep data safe.

## What is Compliance?

**Compliance** is about meeting standards set by a third party. This third party might be a regulatory authority, or it might be an international standards organization.




**Compliance** is especially important in highly regulated industries—such as Healthcare or Finance—where there is an abundance of sensitive data.

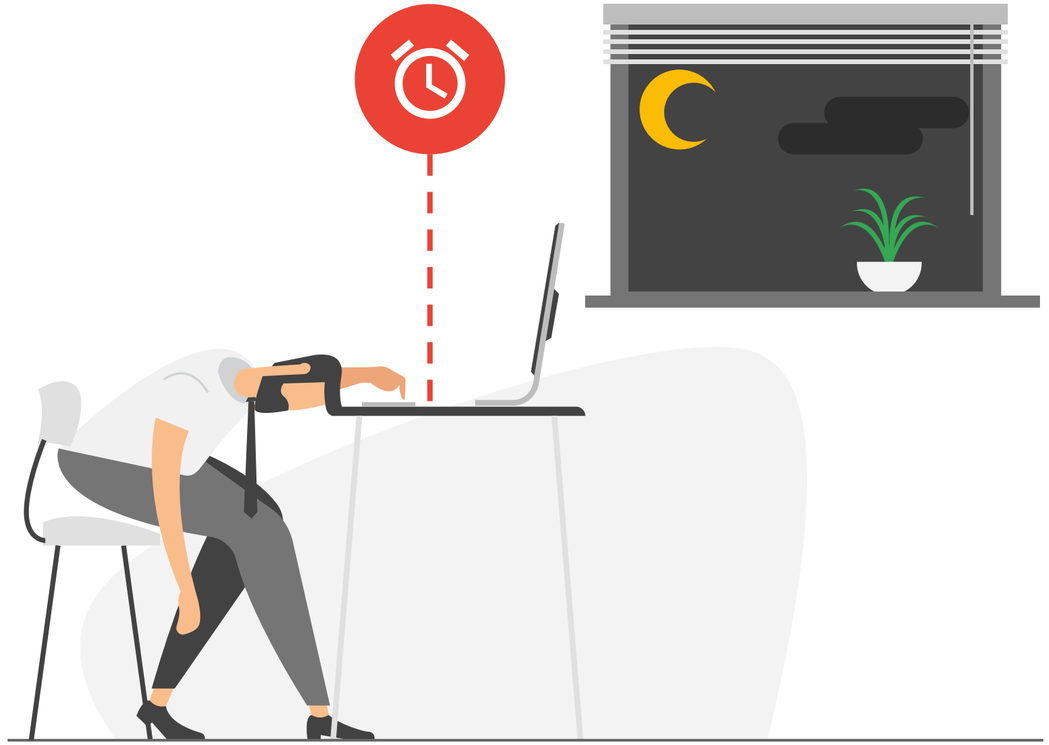
Availability

## What is Availability?

It refers to how much time the cloud service provider guarantees data and services will be running or accessible.

The availability of a service is typically documented as a percentage of time per year. To assess availability of a service, you might ask:

- Does the system work?
- Am I confident that I can access my files anytime I need to, day or night?
- Will I not have access due to system downtime?

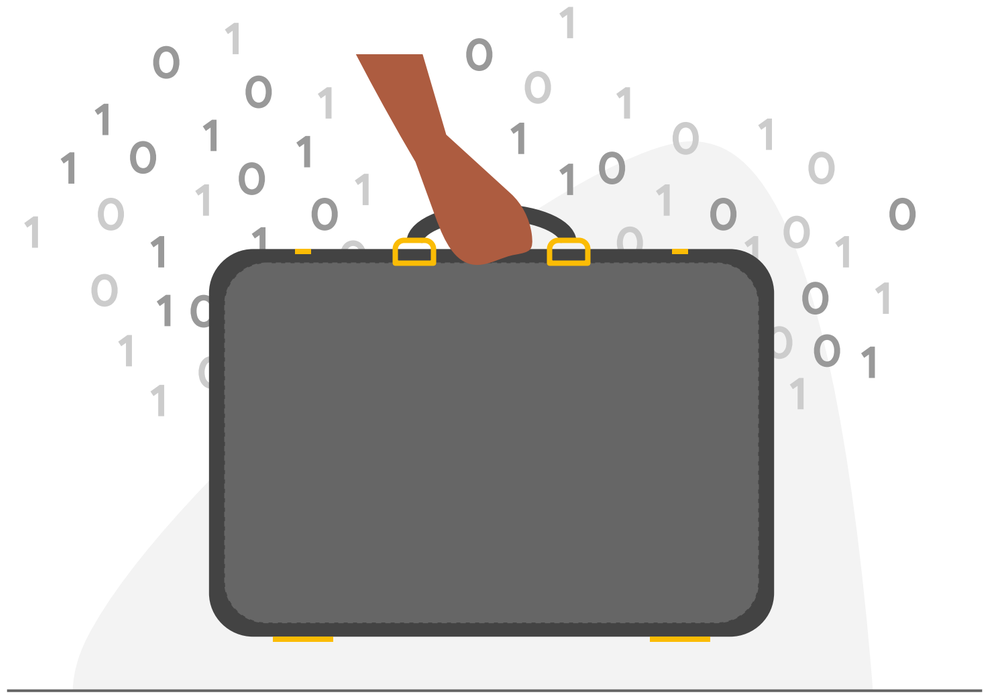


Google Workspace

If you're using, or plan to use, Google Cloud products and services, Google Cloud's commitment to helping you keep your data secure and private is as follows:

1

# You own your data, not Google.



2

# Google does not sell customer data to third parties

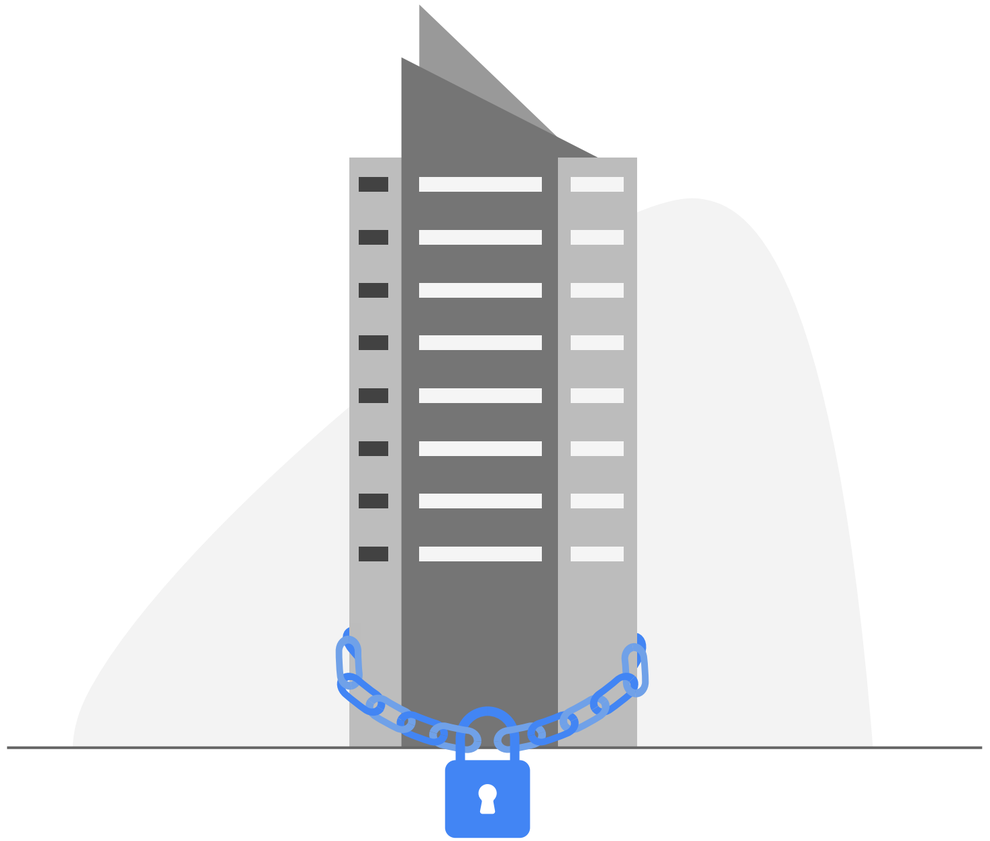
Google Cloud does not use customer data for advertising

3

# All customer data is encrypted by default

4

# Google Cloud guards against insider access to your data

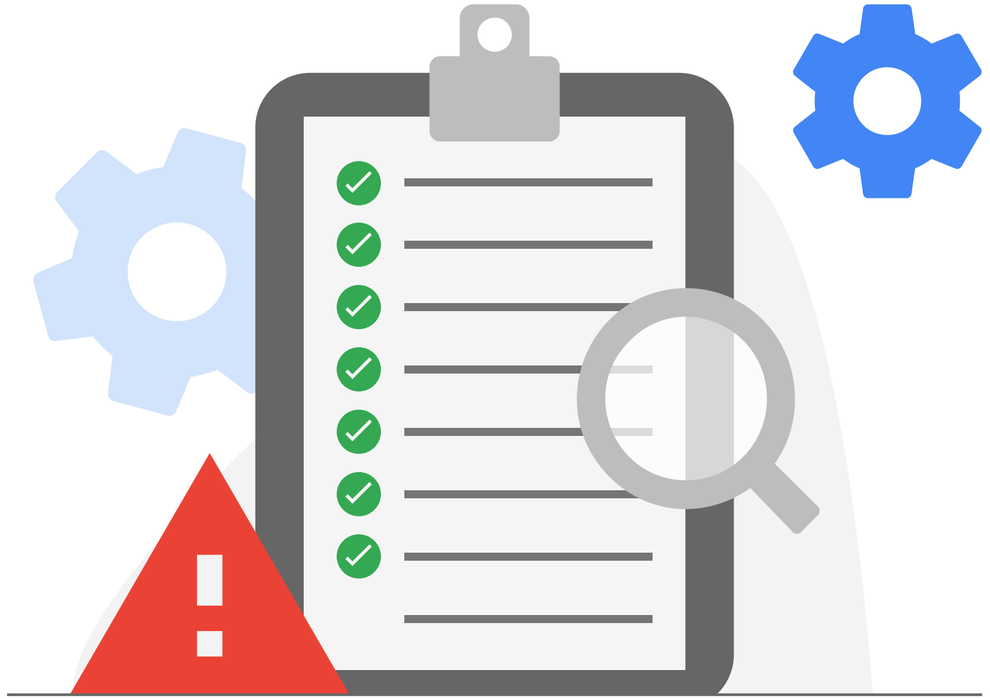


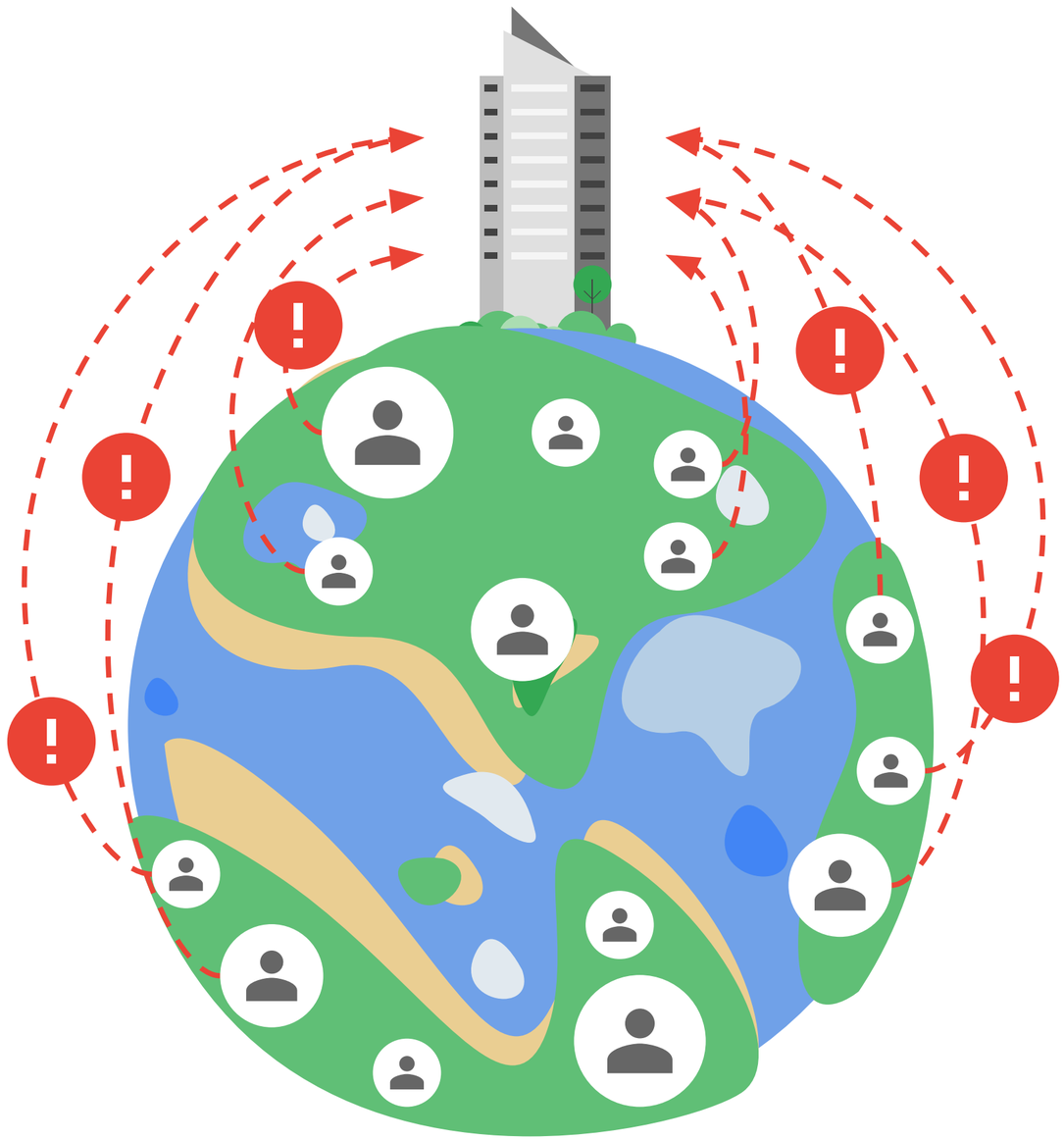
5

# We never give any government entity “backdoor” access to your data

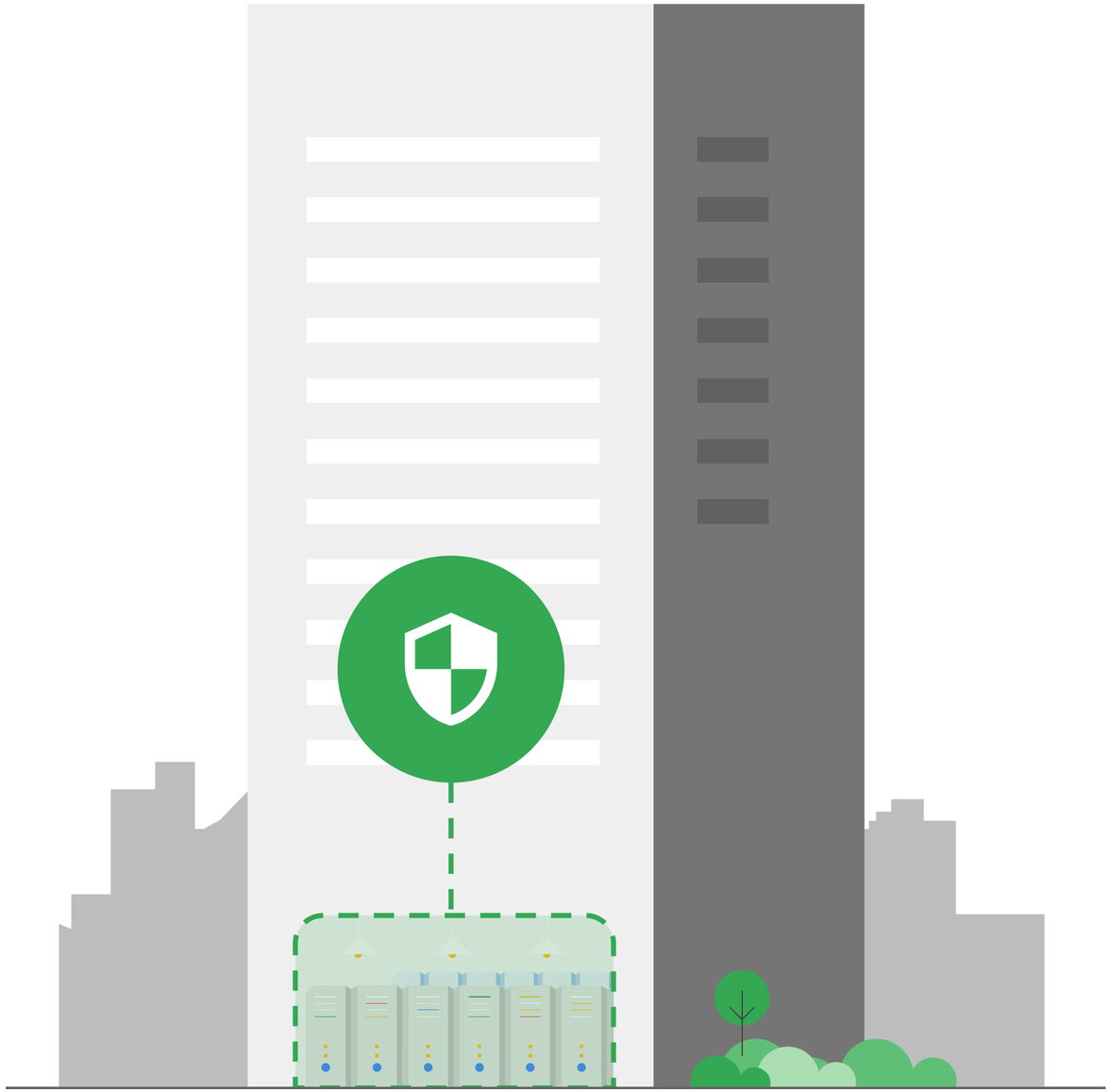
6

# Our privacy practices are audited against international standards

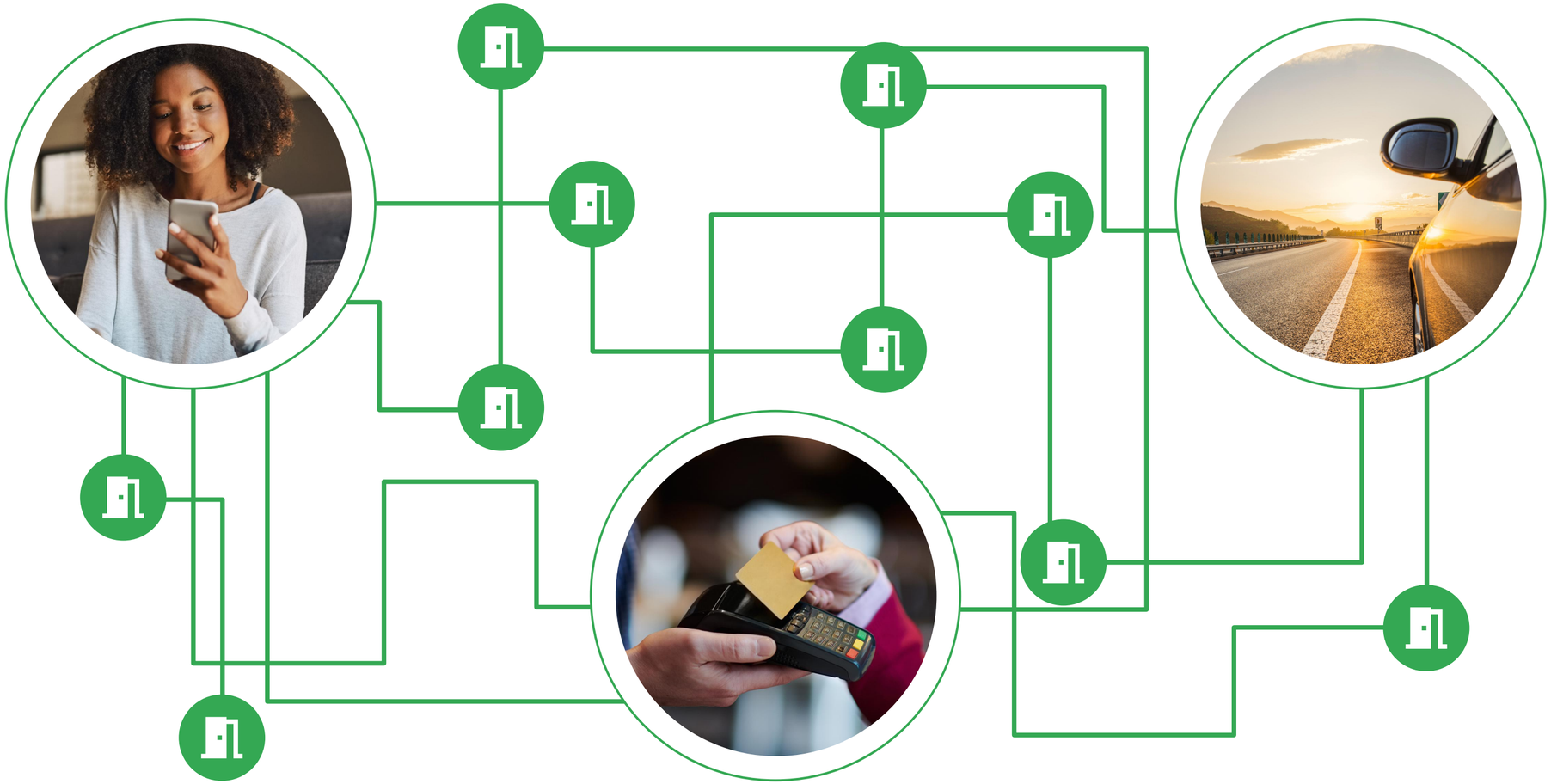




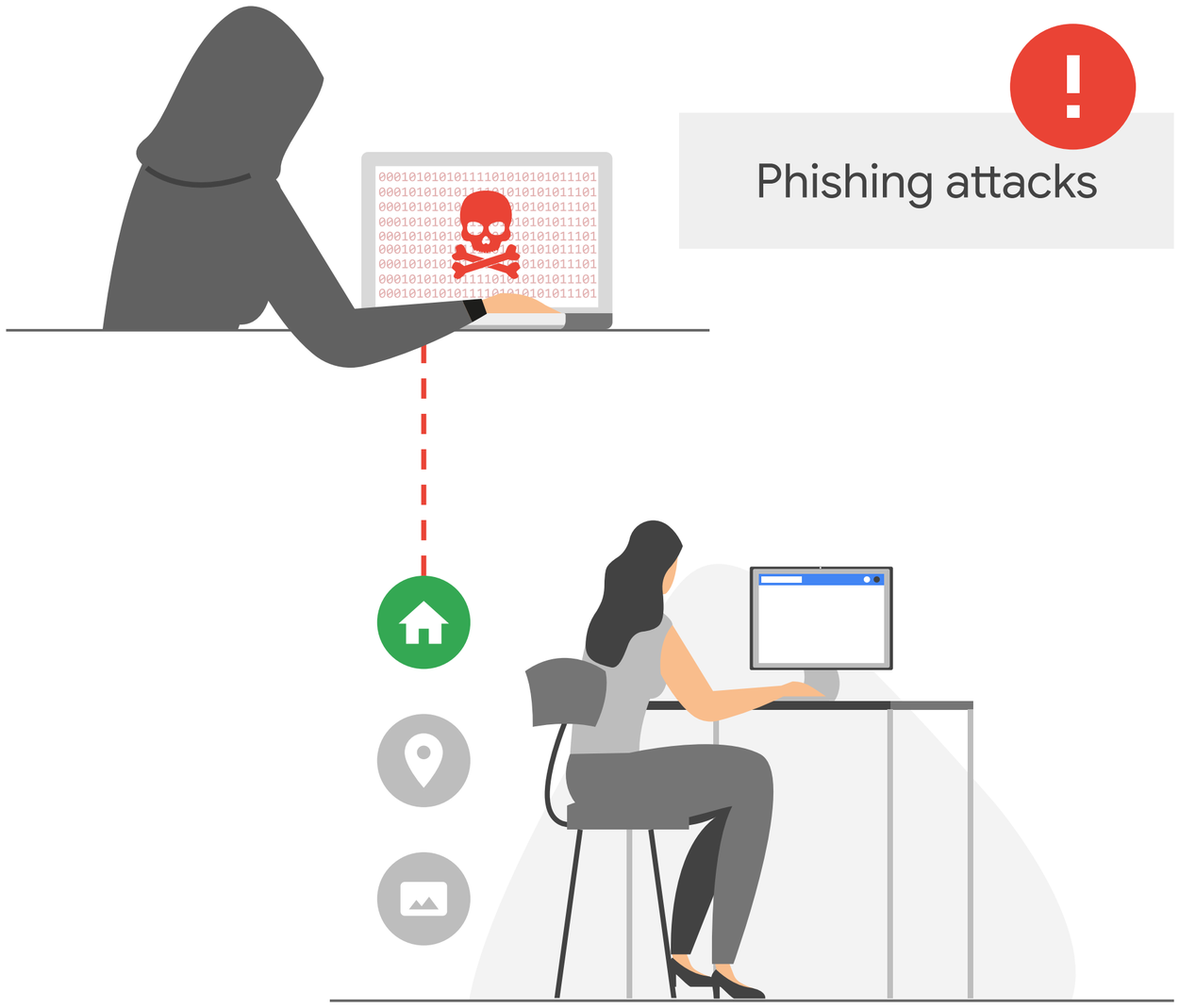
Cyber attacks are bigger than ever. Many groups might use sophisticated methods to gain access to an organization's data. These attacks have become possible because we live online. This means almost every organization is digitally connected to their customers, partners, and even their employees globally.



Traditional on-premises systems or company-owned data centers generally rely on a perimeter-based security approach. The boundary around all of the data is protected by security features. Once someone is inside that security perimeter, they are deemed trustworthy, and therefore have access to everything.

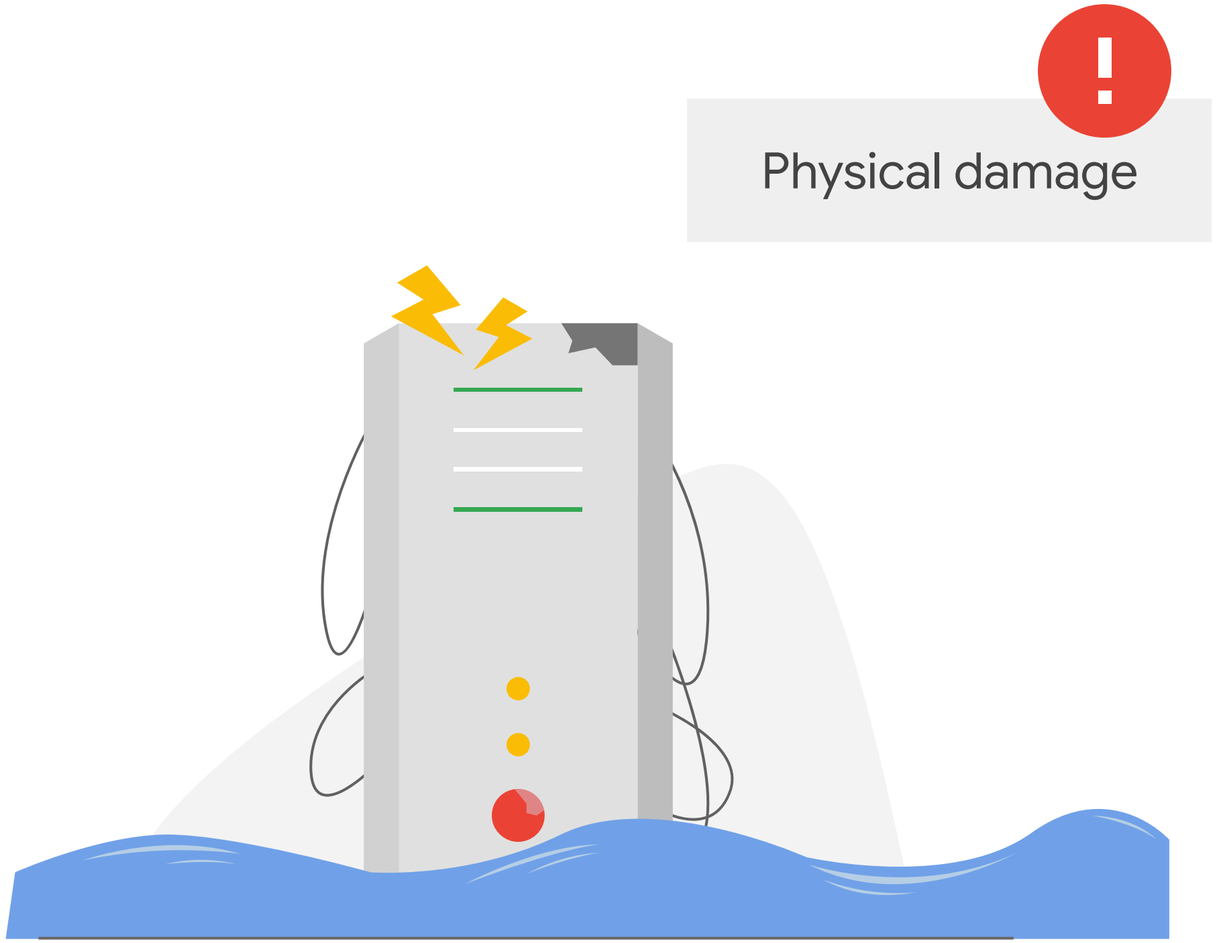


In the Internet of Things era, where everything is connected through sensors that collect data, everything is a node on a network. When everything is a node, each node becomes an entry point. So what are the common cybersecurity threats?



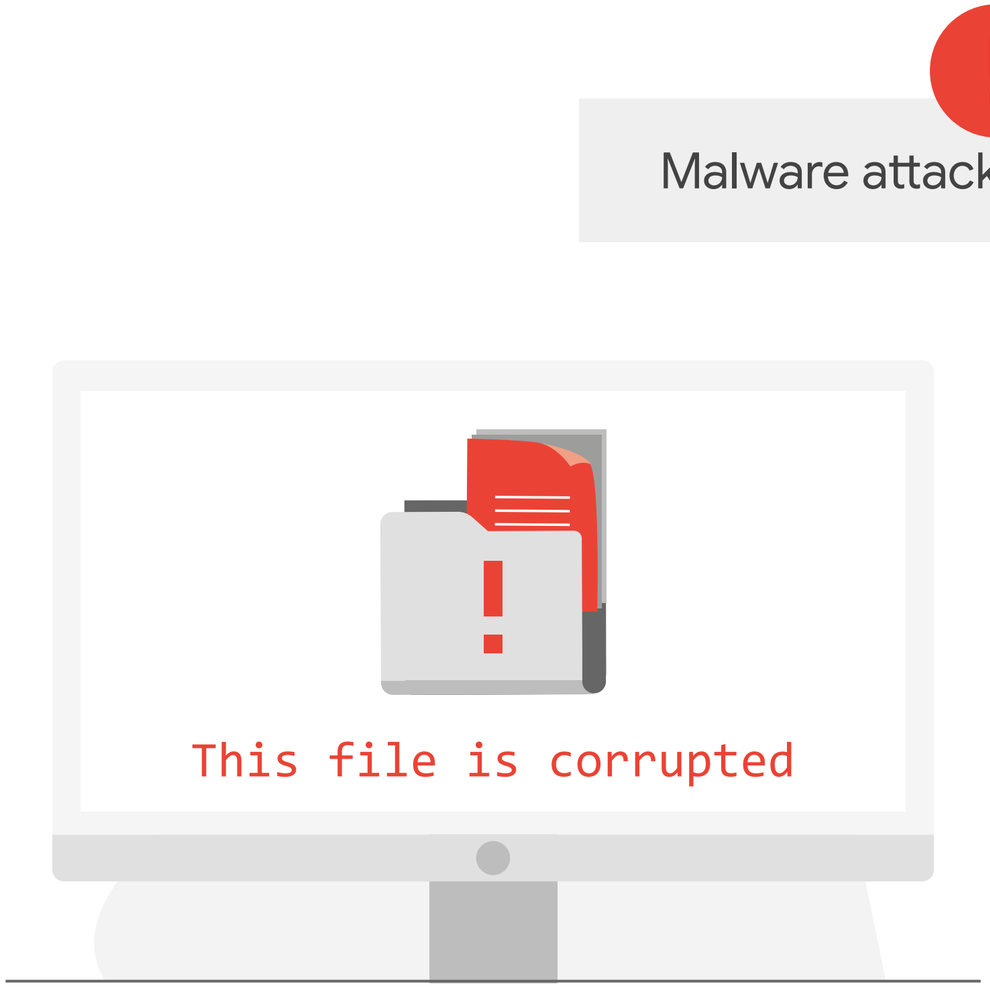

## Criminal Attack

Phishing attackers do research to gather information about you or anyone in your organization, then craft highly targeted emails to trick these people into thinking that the messages are genuine. These people are scammed into downloading malicious attachments, giving up their password, or sharing sensitive data.




## Physical damage

This means that organizations can still be responsible for data losses even when there is damage to the physical hard disk, there are power losses, or natural disasters such as floods, fires, and earthquakes.




# Malware, viruses, and ransomware attacks

Data can be lost, damaged, or destroyed by viruses or malware. Alternatively, a set of files can be rendered unavailable to its intended users via ransomware until the ransom amount is paid.

## Unsecured third-party systems

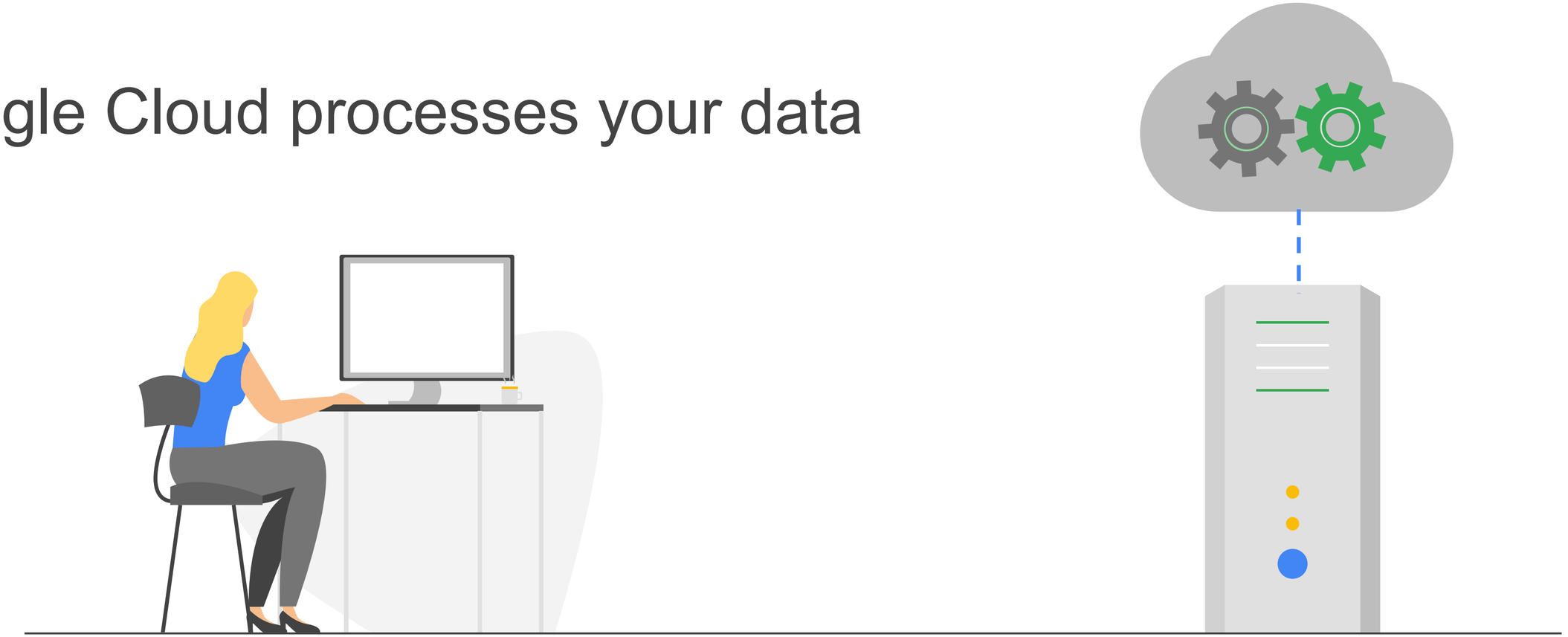
Although third-party systems are often used to address common business needs, without adequate security measures and regular checks, these systems can pose a threat to data security.

## Lack of expert knowledge

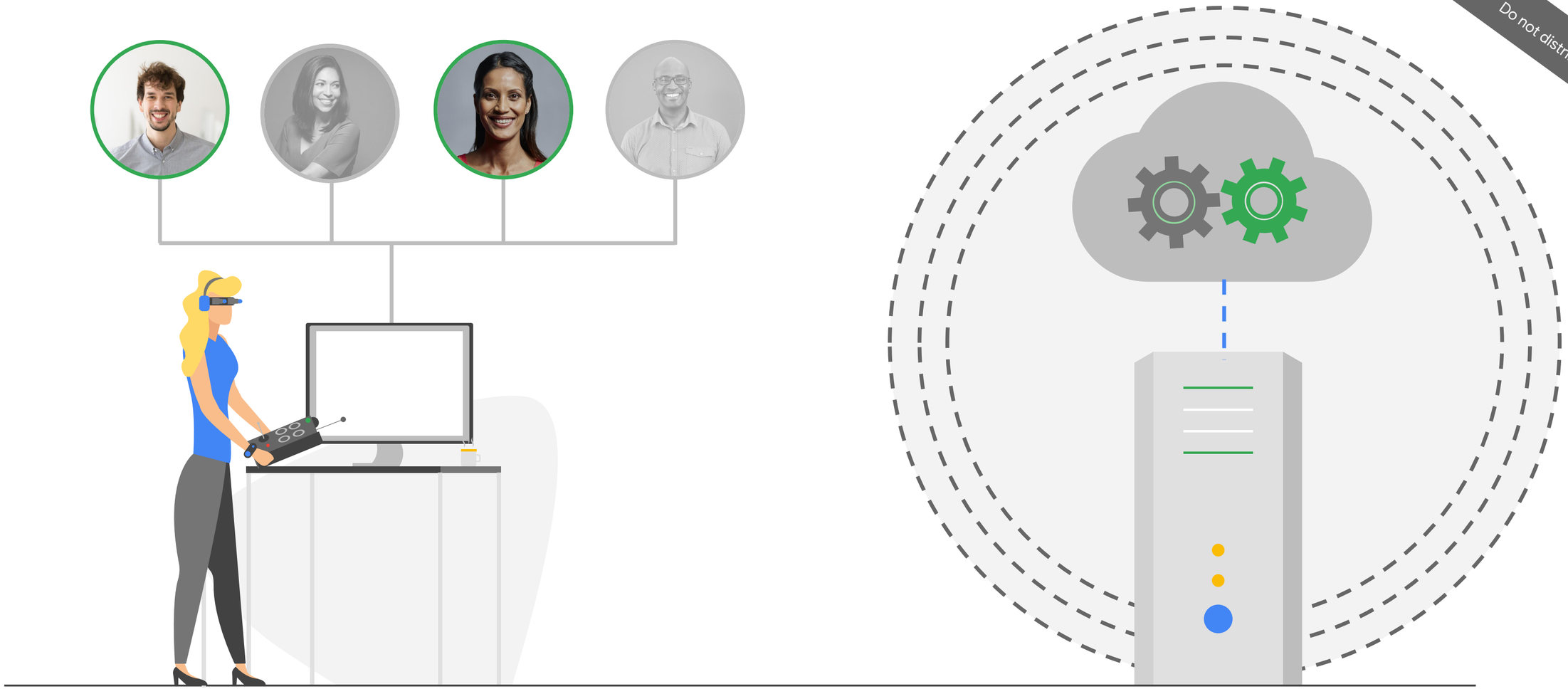
At the rate that technology is changing, investing in the right expertise to assess, develop, implement, and maintain data security plans is essential for businesses to stay ahead of potential data security threats.

When an organization manages its data in its own data centers, that organization is then responsible for **all** aspects of its security.

# Google Cloud processes your data

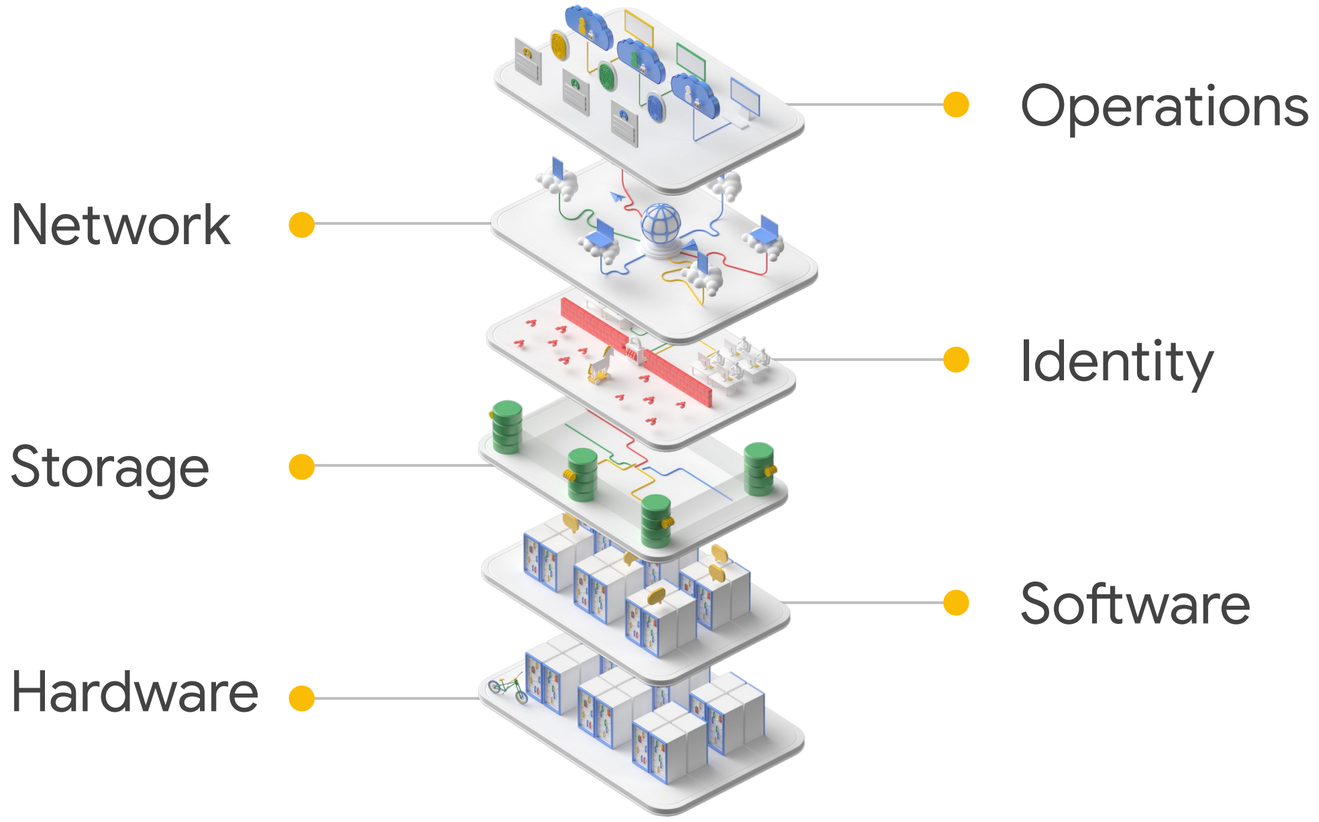


The advantage of using cloud technology is that the responsibility to secure data is shared between a business and the cloud provider.

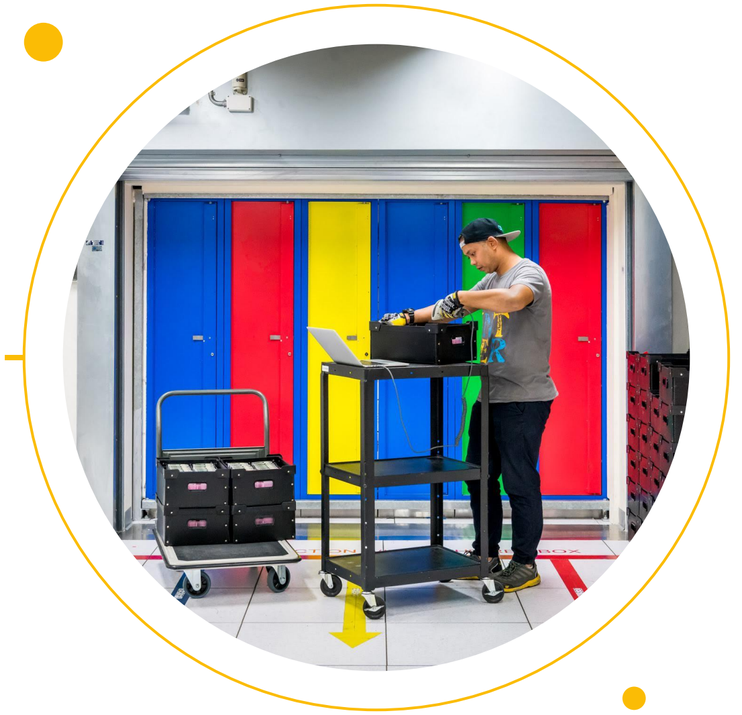


When an organization adopts the cloud, the cloud service provider typically becomes the data **processor**. The organization is the data **controller**.

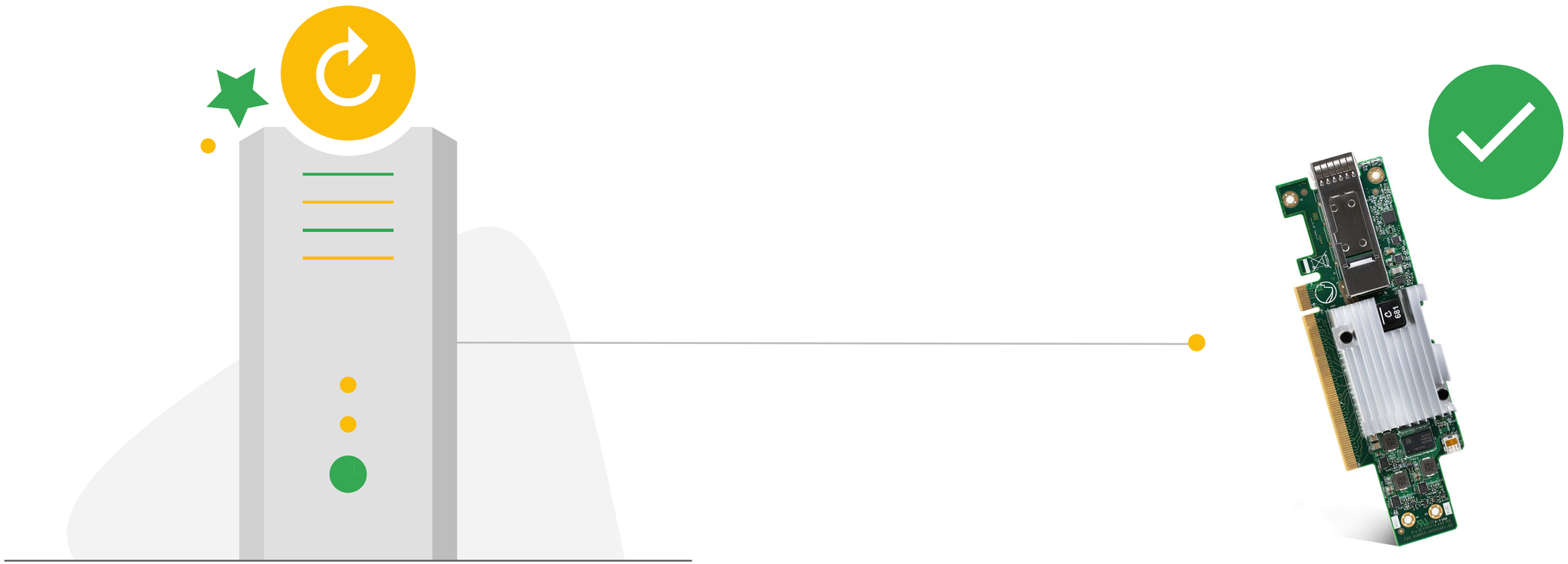
# Google Cloud's multilayer approach to security



# Hardware

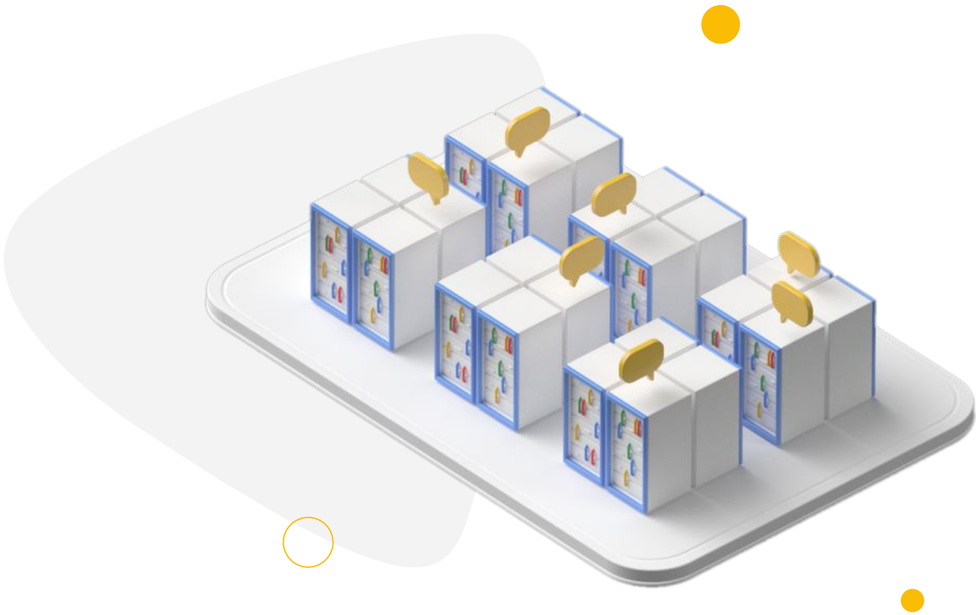


Google designs its own servers, its storage, and its networking gear. It manufactures almost all of its own hardware, and third parties never see the overall process. The hardware is housed in these high-security data centers that are located around the world.



New server builds have a chip, called Titan, embedded.
Titan checks a machine for integrity every time it boots up.

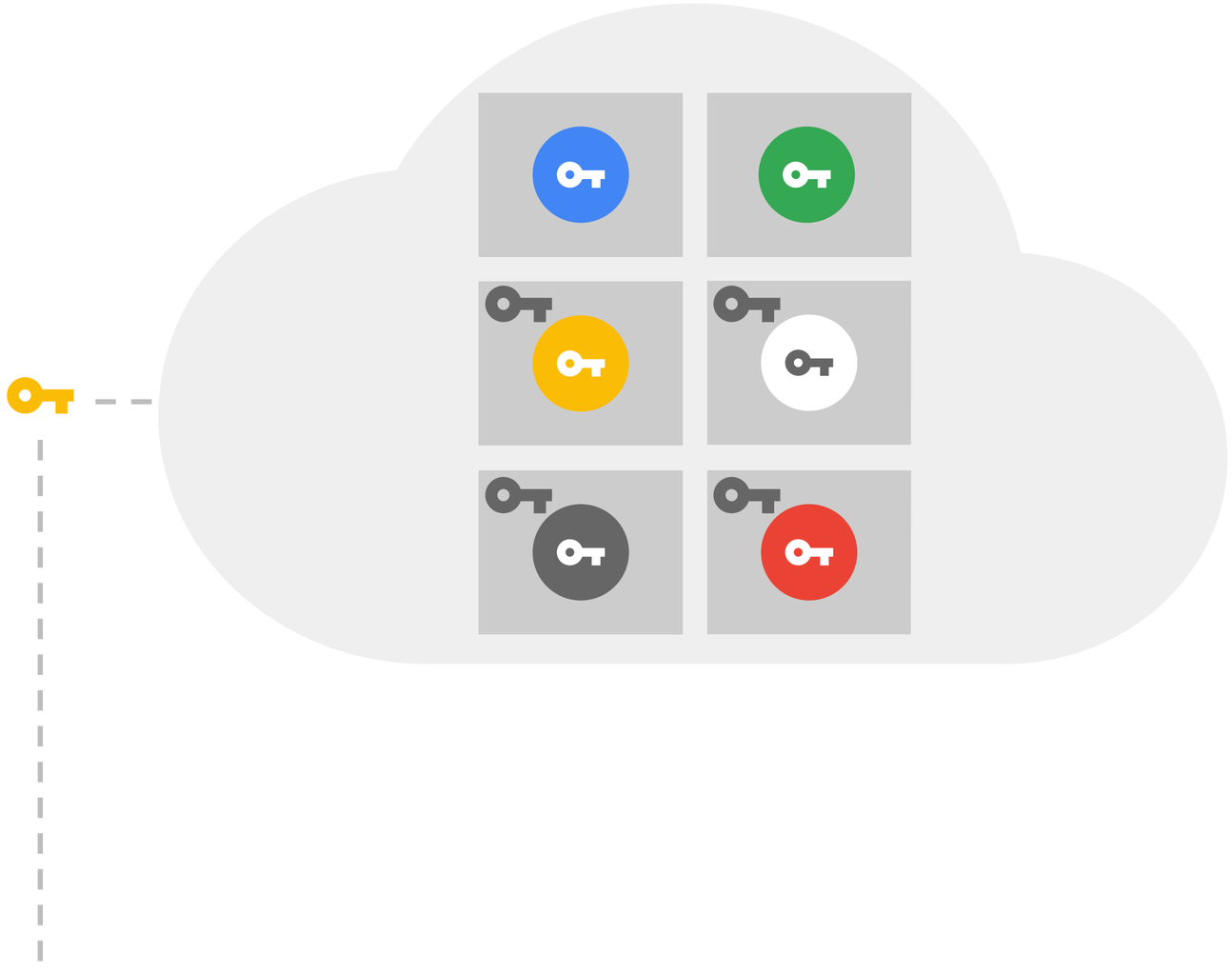
# Software



The Titan microcontroller continues to verify the operating systems and the rest of the deployed software stack. The server is not allowed onto the network and it holds zero data until its health is confirmed.

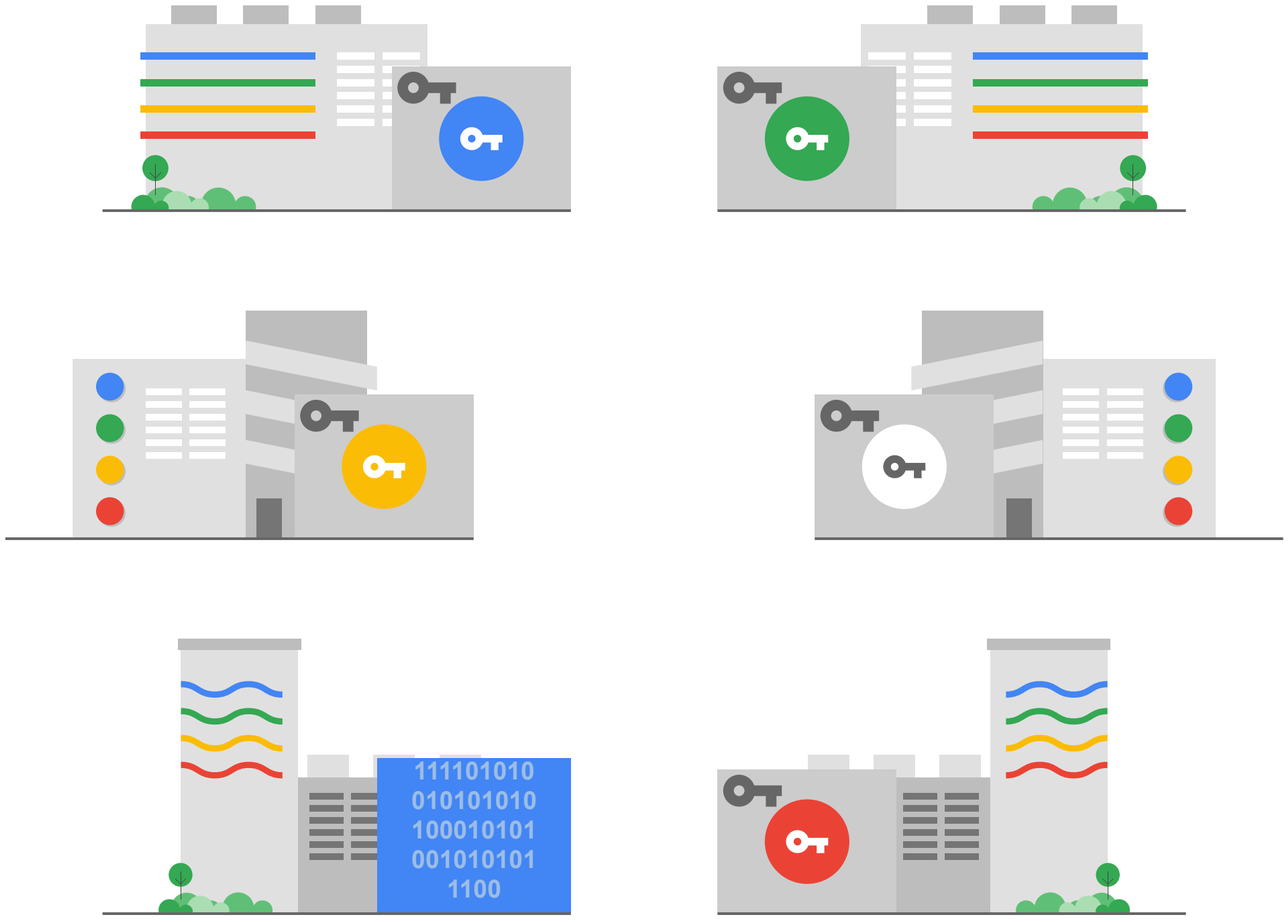
# Storage

Storage is closely connected to the idea of data encryption at rest. Encryption at rest protects data when it is stored on physical media. ALL data at rest is also encrypted by default to help guard against unauthorized access.



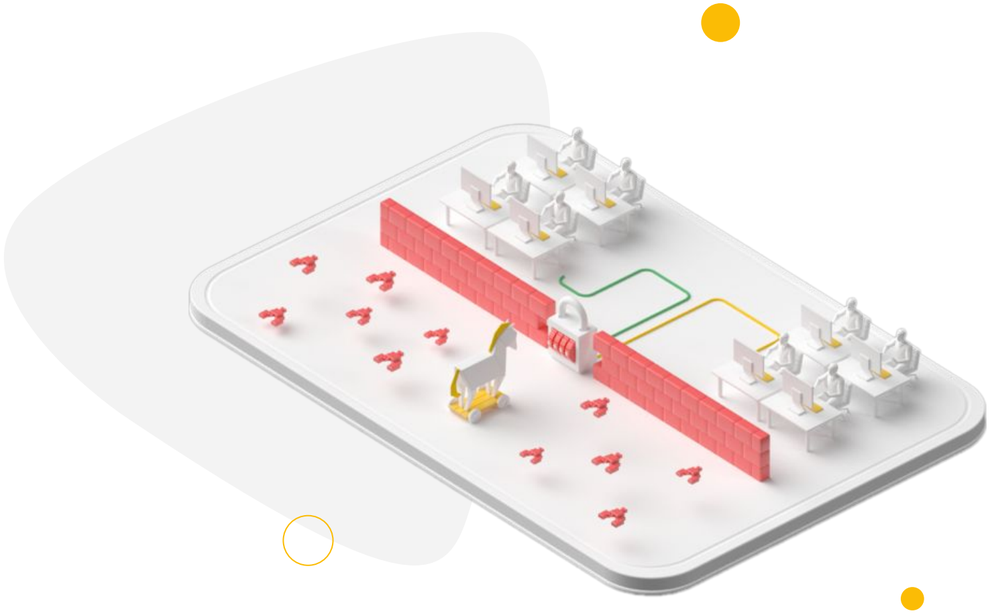
The defense-in-depth process for storing data in Google Cloud is:

1. Data is broken into many pieces in memory.
2. These pieces, or “chunks”, are encrypted with their own data encryption key or ‘DEK’.
3. These DEKs are then encrypted a second time with key encryption key or ‘KEK’.
4. Encrypted chunks and wrapped KEKs are distributed across Google’s infrastructure.




In the unlikely event that someone compromises an encryption key, they could only access one tiny piece of data, which, without all of the other pieces, would be unreadable.

# Identity



Instead of relying on the traditional perimeter approach to security, Google Cloud operates a zero-trust model. This means that every user and every machine that tries to access data or services must strongly authenticate identity at each stage for each file.

# Network

Anyone accessing the cloud does so via a **network**. Encryption in transit protects data as it moves across a network. Multiple layers of defense are in place to help protect customers against network attacks, like DDoS attacks.

# Operations

At Google, a global operations team of more than 900 security experts monitor the system 24 hours a day, 365 days a year. Their role is to detect attacks and other issues and to respond to them.

| | Front end user | Manager | Super user | Admin |
|---|---|---|---|---|
| View logs | ✗ | ✗ | ✓ | ✓ |
| Modify settings | ✗ | ✗ | ✗ | ✓ |
| Modify users | ✗ | ✓ | ✗ | ✓ |
| Modify applications | ✗ | ✓ | ✗ | ✓ |

IT teams need to have a complete understanding of who can access what data. Wherever possible, they need to establish granular access policies. They need to define who can do what, and on what cloud resource.

An Identity Access Management policy, or IAM policy, is made of three parts:

**Who** **can do what** **on which resource**

**Who** can do what on which resource

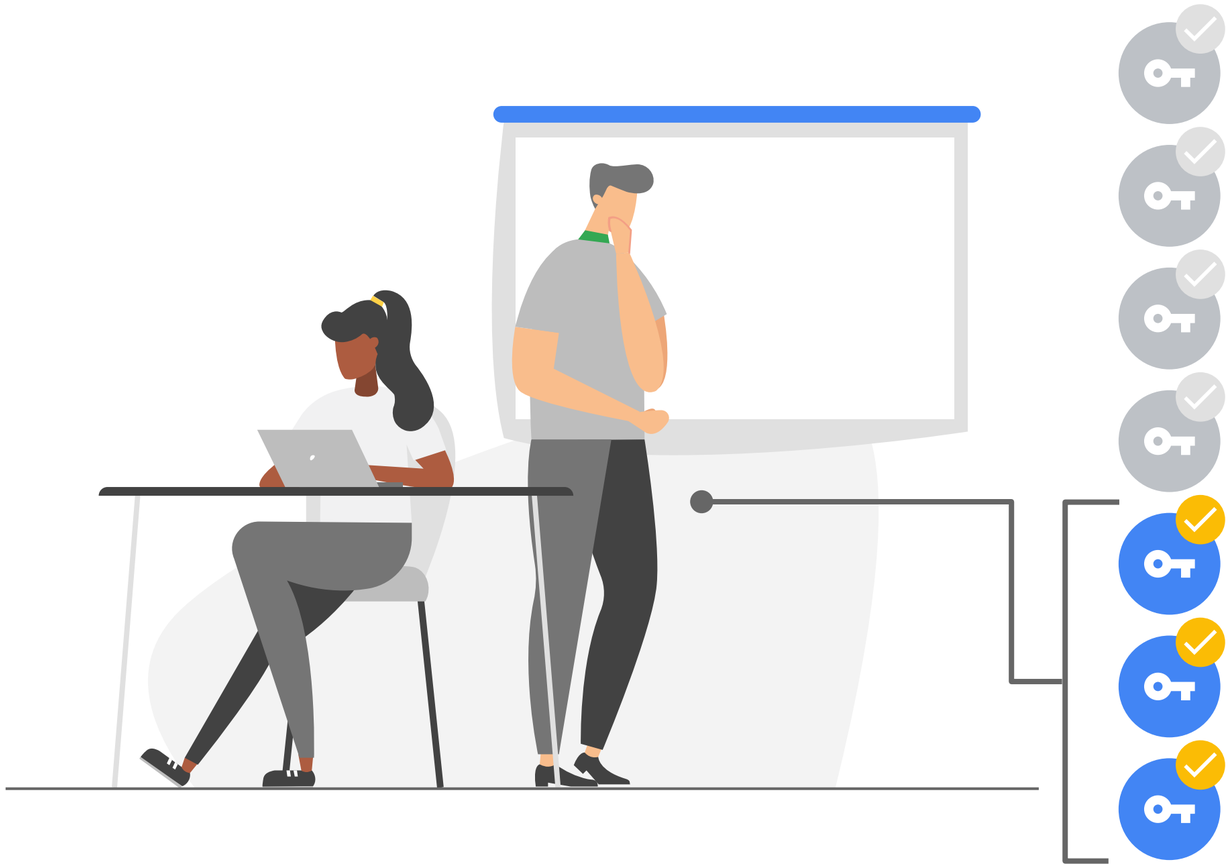
The “who” part of an IAM policy can be a Google account, a Google group, a service account, or a Google Workspace or Cloud Identity domain.

There are three kinds of roles in Cloud IAM:

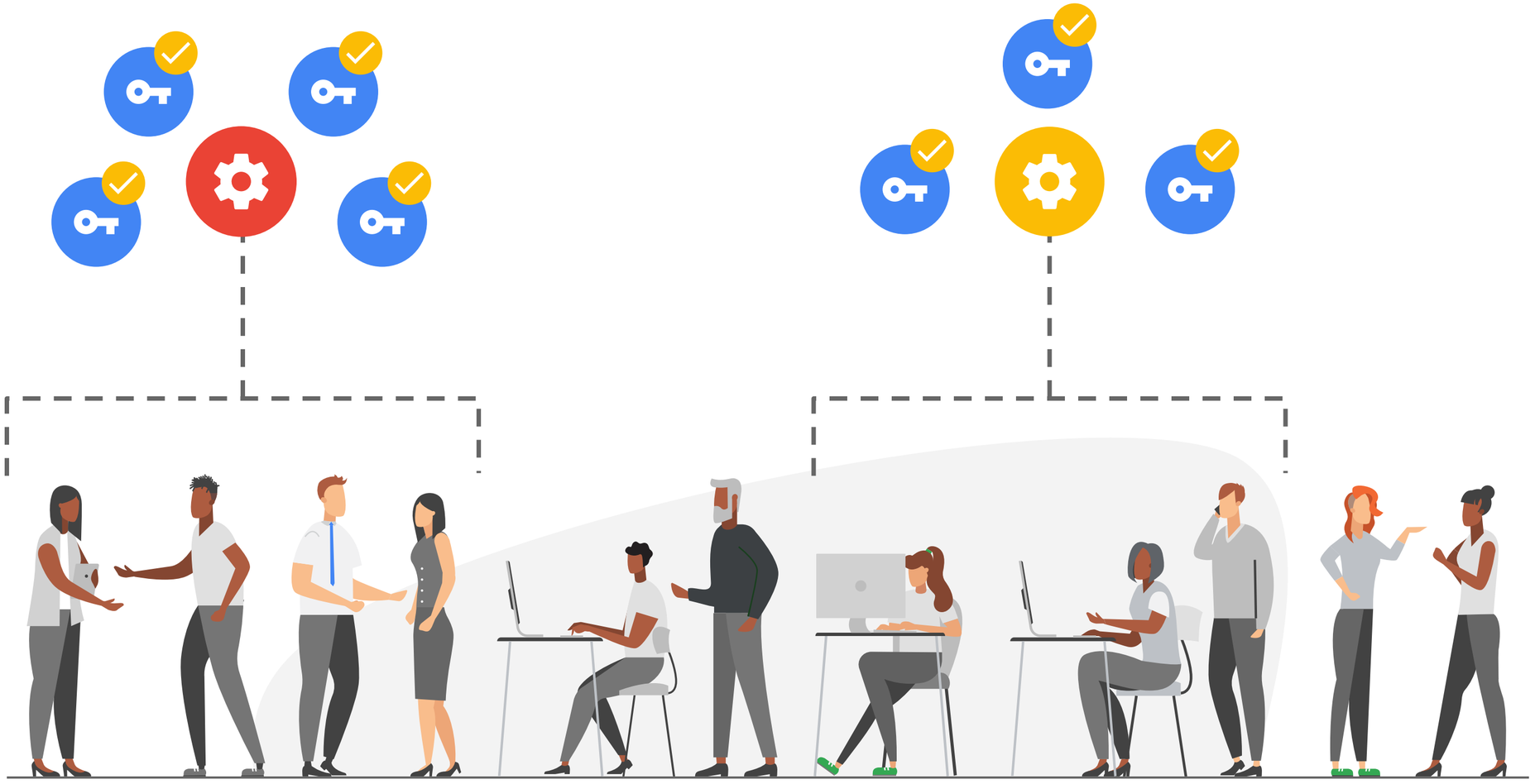

The “can do what” part is defined by an IAM role.

If you’re a viewer on a given resource, you can examine it, but not change its state. If you’re an editor, you can do everything a viewer can do plus change its state. And if you’re an owner, you can do everything an editor can do plus manage roles and permissions on the resource.

# Custom

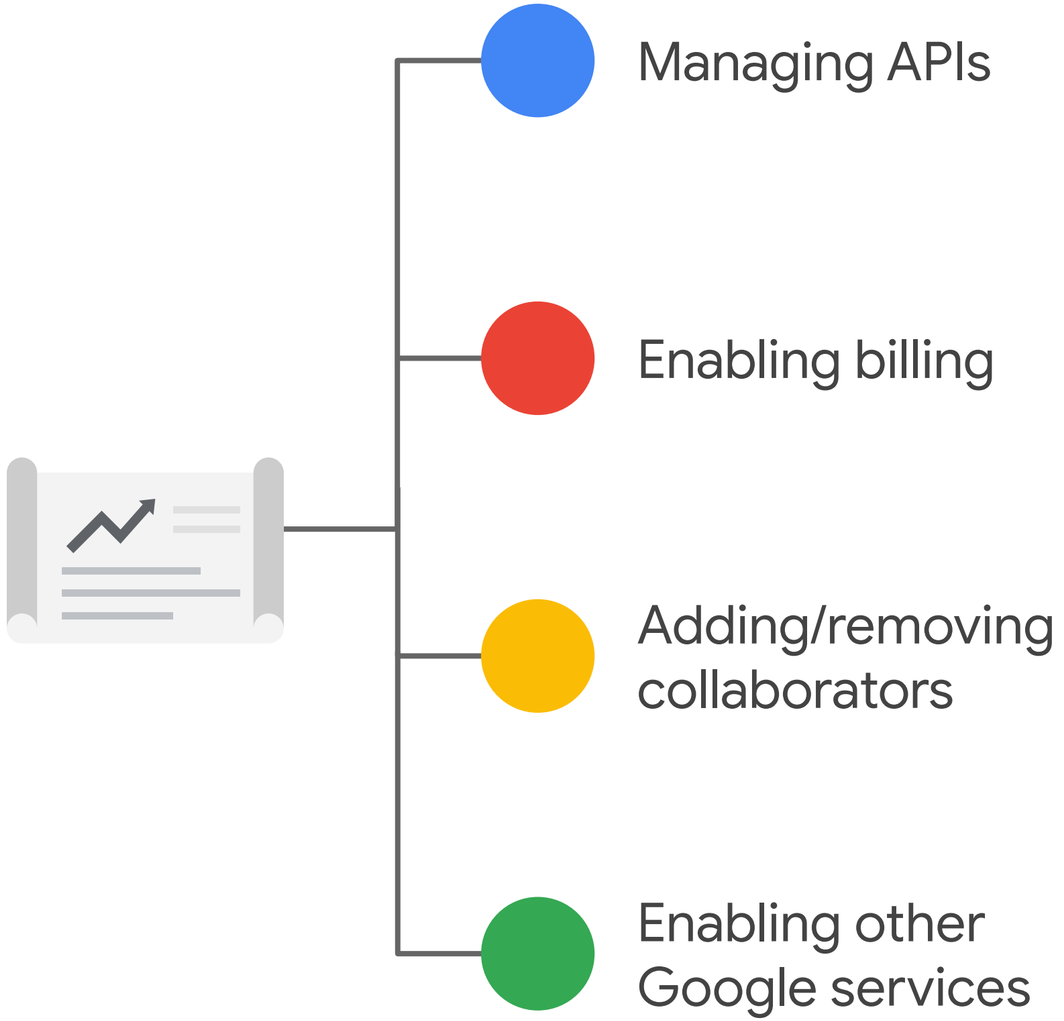


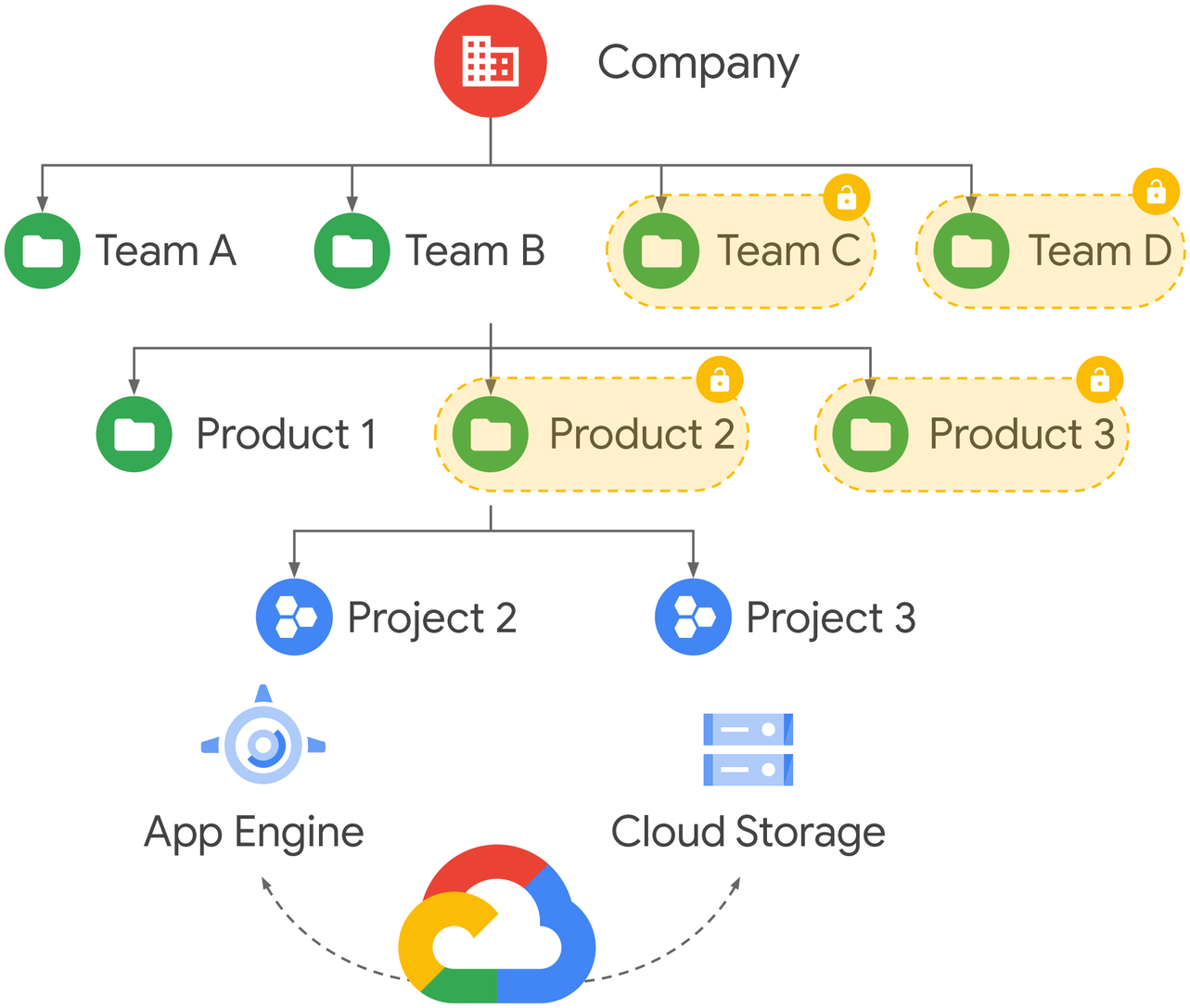
Google Cloud recommends using a “least-privilege” model, in which each person in your organization is given the minimal amount of privilege needed to do their job.



An organization can easily map job functions within the organization to specific groups. Each group can then be given specific roles for specific resources. Users get access only to what they need to do their job, and admins can grant default permissions to entire groups of users.

In the cloud environment, a project is the basis for enabling and using Google Cloud capabilities, like managing APIs, enabling billing, adding and removing collaborators, and enabling other Google
(or Alphabet) services.

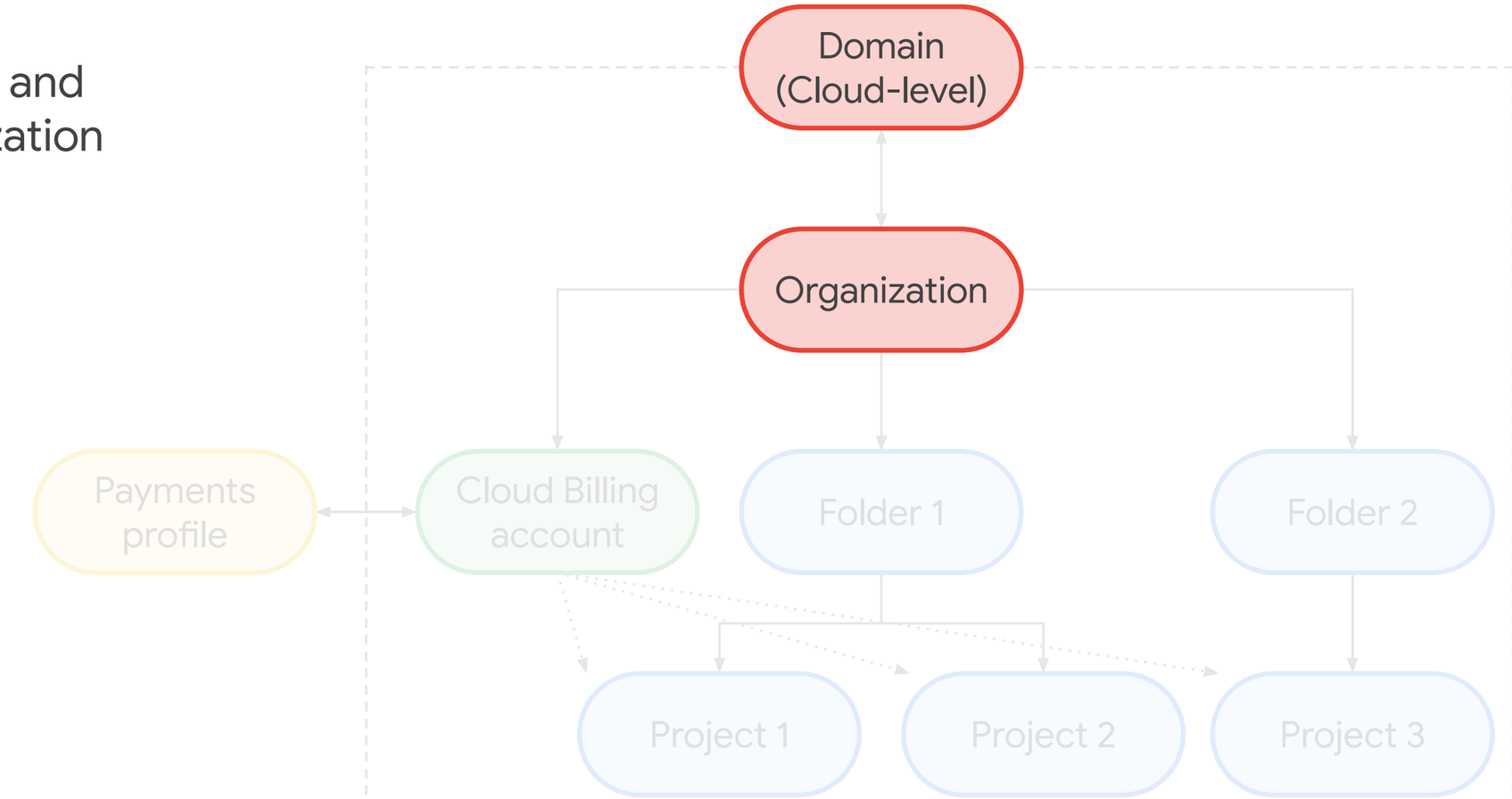





# Resource Hierarchy

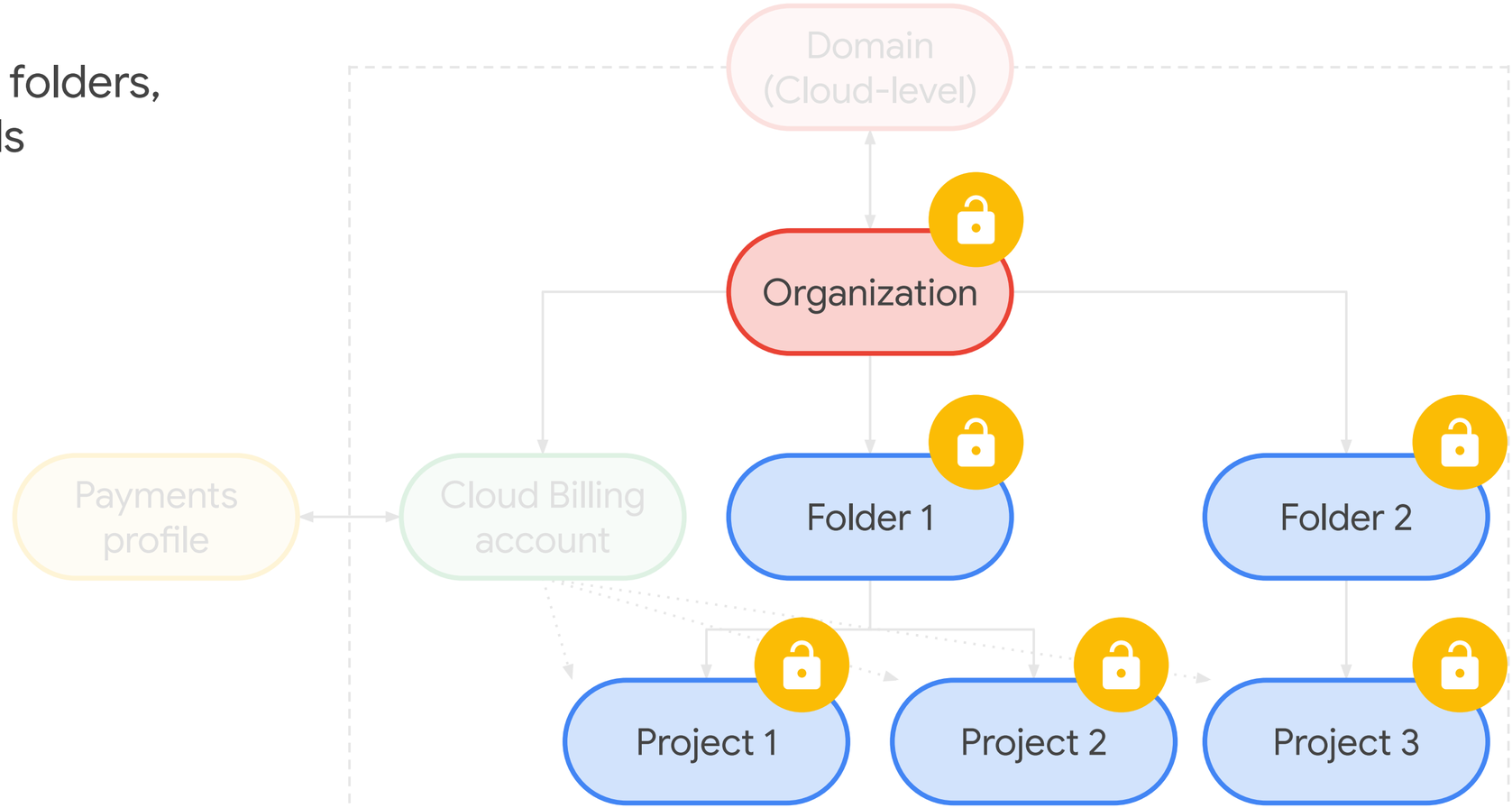
Resource hierarchy refers to the way your IT team can organize your business' Google Cloud environment and how that service structure maps to your organization's actual structure. For example, by teams or by projects or by both. With a resource hierarchy, IT teams can manage access and permissions for groups of related resources.

# Domain and Organization




Everything managed in Google Cloud is under a domain and an organization. The domain is handled through Cloud Identity and helps manage user profiles. The organization is managed through the Cloud Console and lets administrators see and control Google Cloud resources and permissions.

# Projects, folders, and labels




Projects belong to the organization rather than the user that created them. Projects are used for grouping Google Cloud resources like Cloud Storage buckets. It can inherit permissions from any folders above it as well as from the organization at the top, making it easy to set organization-wide rules and policies that cascade down and are enforced throughout the hierarchy.

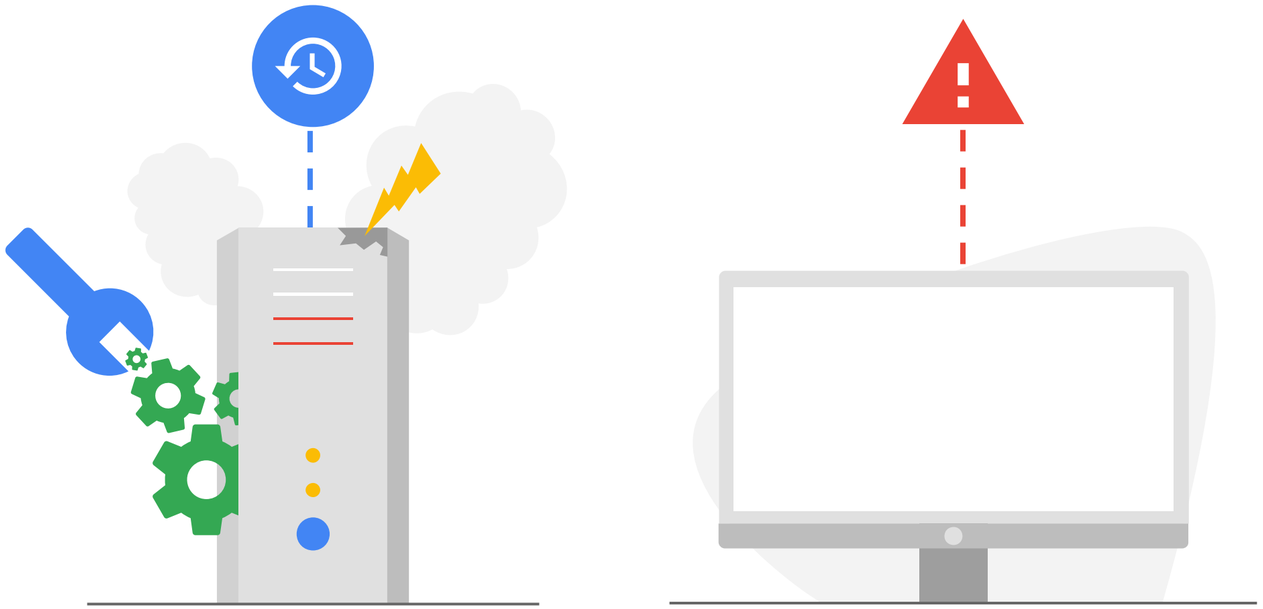
Google Cloud

## Module 3: Student Slides

# Monitoring Cloud IT Services and Operations

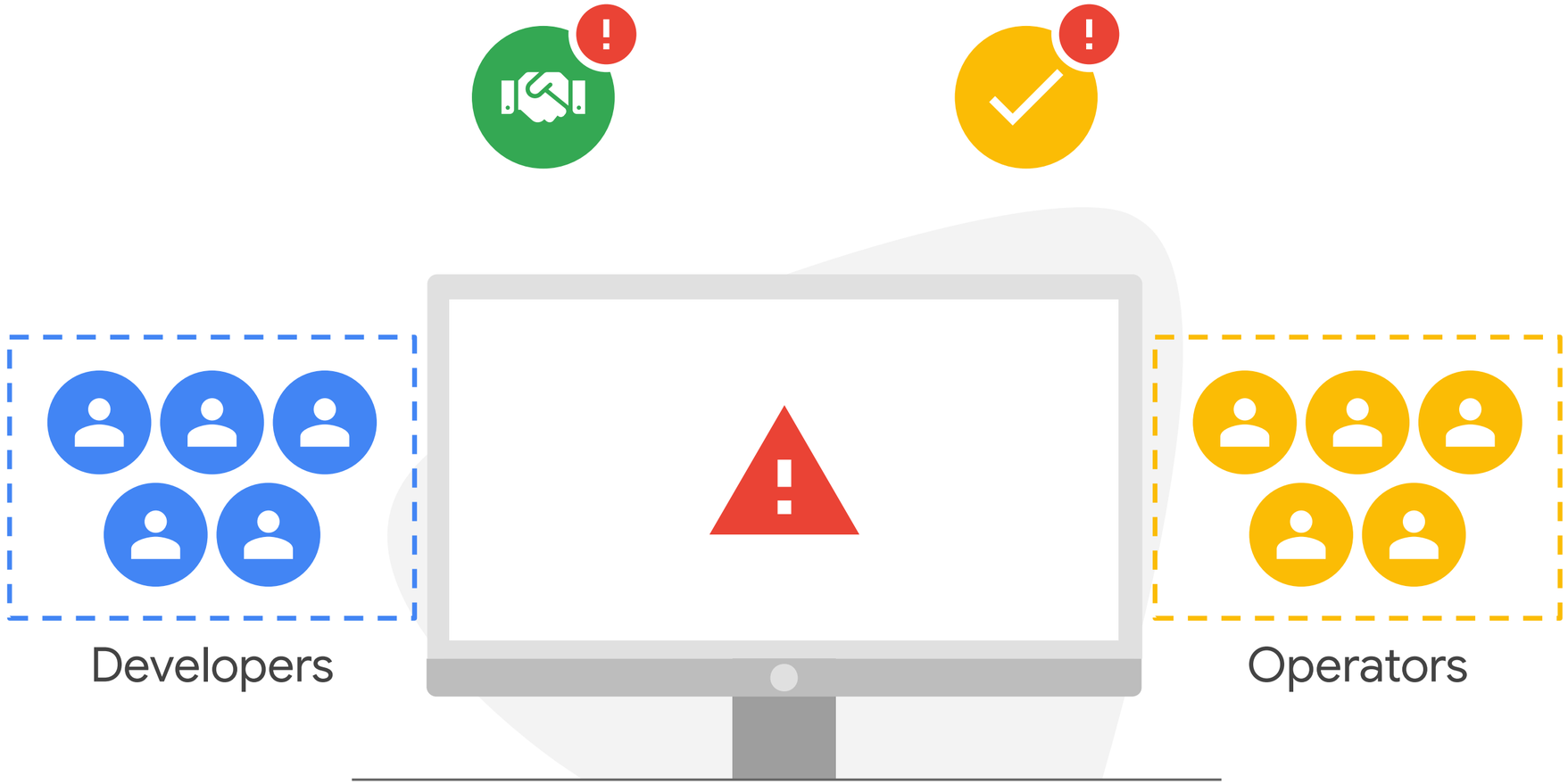
## Topics covered

- IT operational challenges
- DevOps and Site Reliability Engineering
- Google Cloud resource monitoring tools

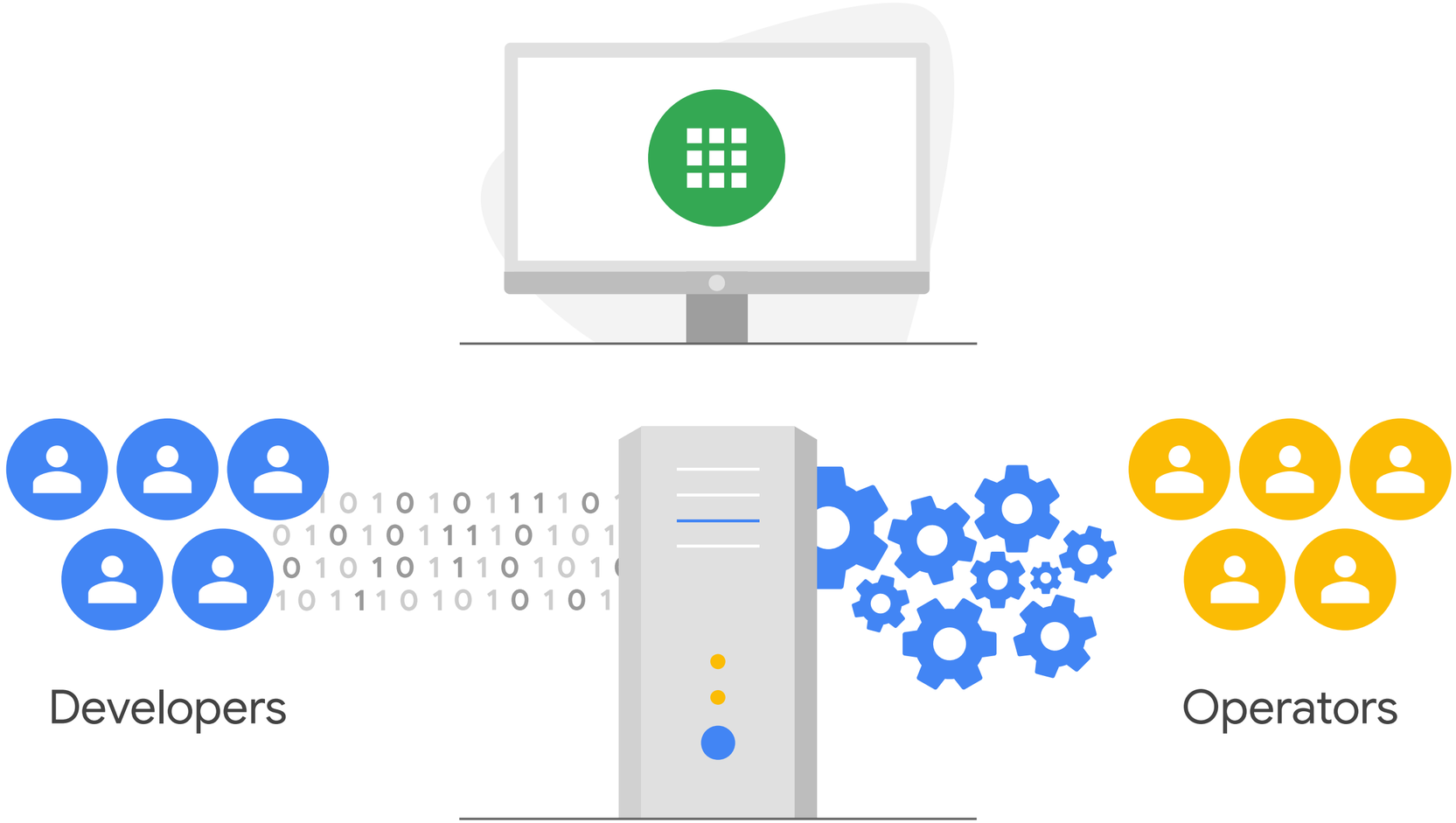


# “Page under construction” or “503 Service Unavailable” messages

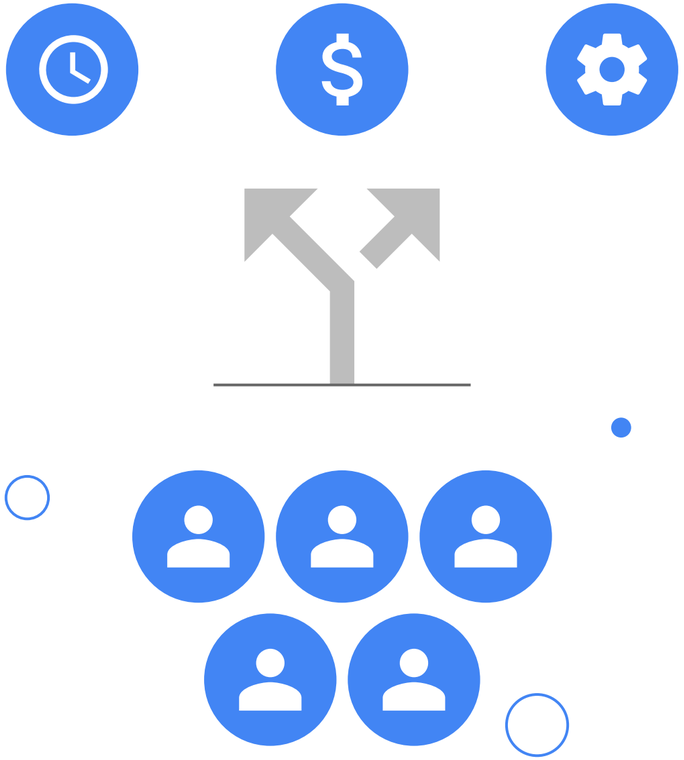
These messages may be the result of planned maintenance, when a company wants to release updates to their website, so they need to take their service offline while changes are being implemented. Or the message on the screen may be the result of an unexpected system failure, and engineers are trying to fix the problem as quickly as possible.



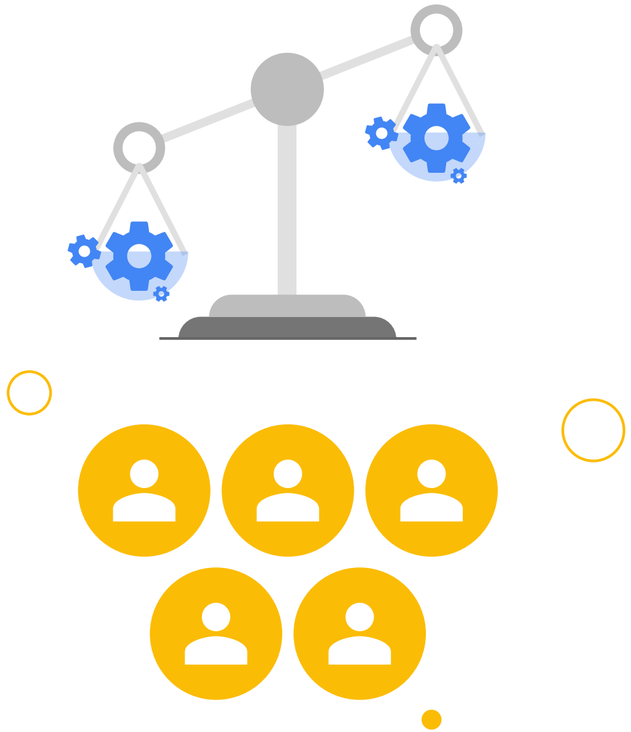

If a service disruption happens unexpectedly, this may be the result of a team structure issue where developers and operators are working in silos. The structure of these teams restricts collaboration and obscures accountability.




Developers are responsible for writing code for systems and applications, and operators are responsible for ensuring that those systems and applications operate reliably.



Developers



Operators

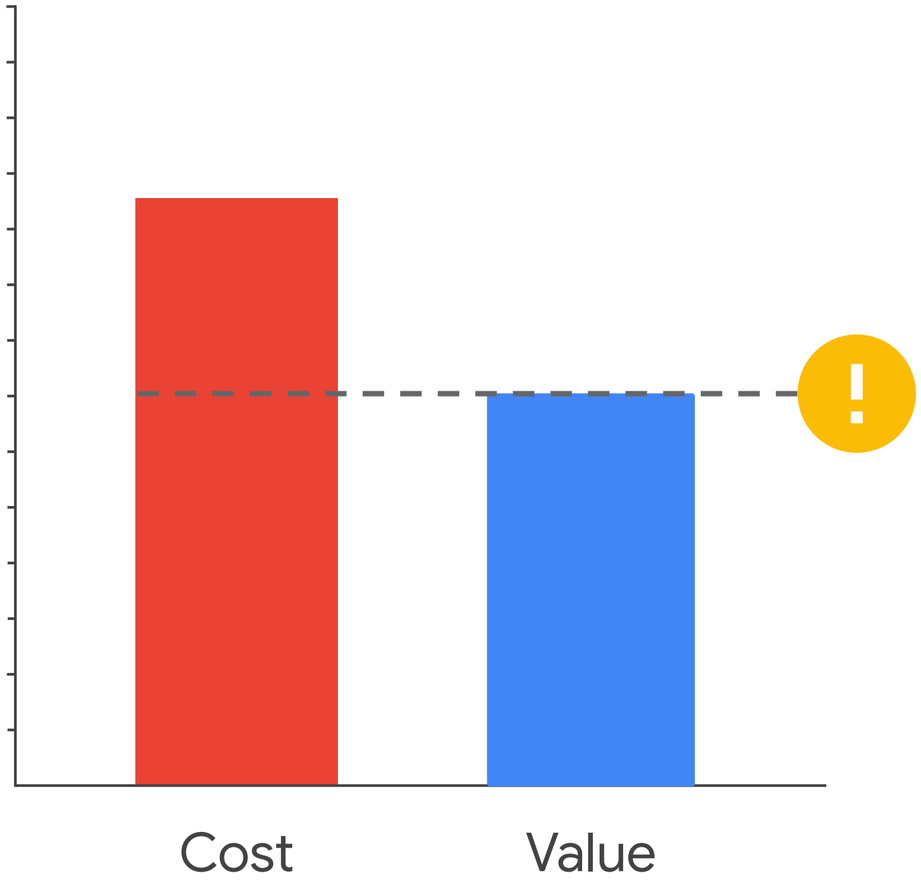
Developers are expected to be agile. Their aim is to release new functions frequently, increase core business value with new features, and release fixes fast for an overall better user experience. In contrast, operators are expected to keep systems stable, and so they often prefer to work more slowly to ensure reliability and consistency.

For organizations to thrive in the cloud, they'll need to adapt their IT operations:

Adjust expectations for service availability

Adopt best practices from DevOps and Site Reliability Engineering

# Reliability




In order to roll out updates, operators have to take a system offline. Ensuring 100% service availability is also incredibly expensive for any business. This means that at some point the marginal cost of reliability exceeds the marginal value of reliability.

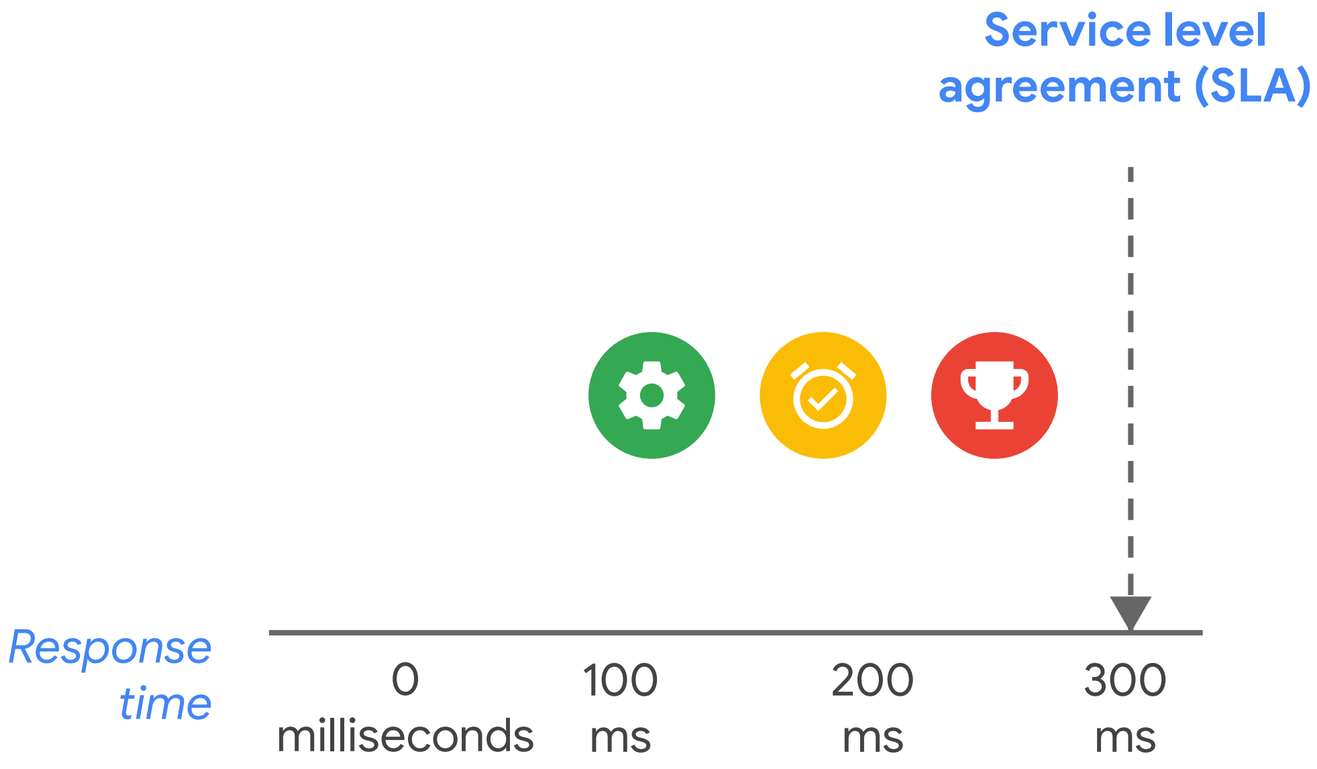
Cloud providers use standard practices to define and measure service availability for customers:

# Standard practices

Service level agreement

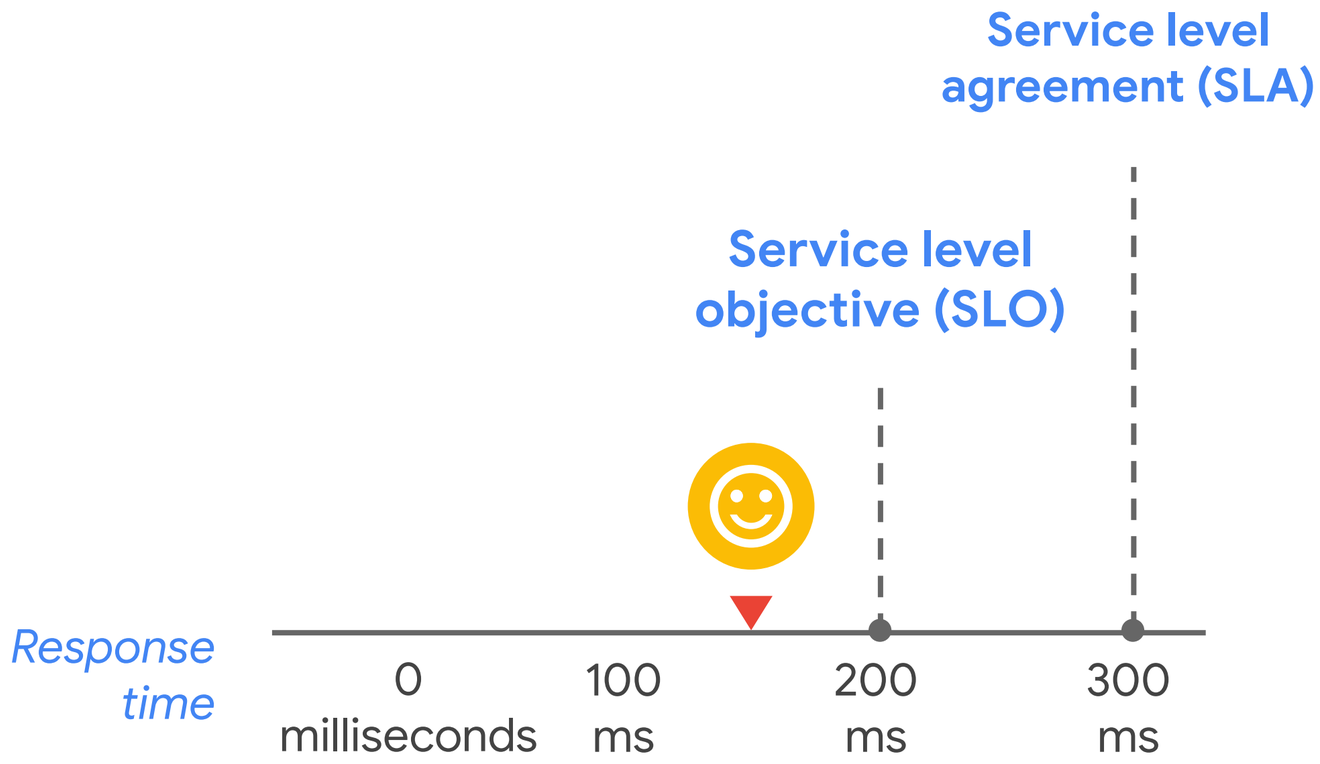
Service level objectives

Service level indicators




# Service level agreement (SLA)

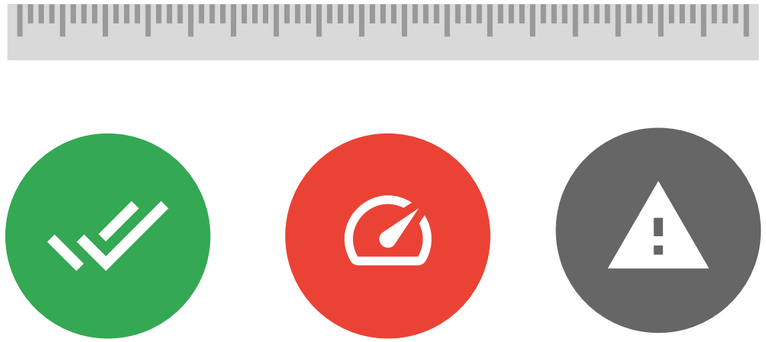
A contractual commitment between the cloud service provider and the customer. The SLA provides the baseline level for the quality, availability, and reliability of that service. If the baseline service is not met by the provider, end users and end customers would be affected. The cloud provider would incur a cost usually paid out to the customer.




## Service level objective (SLO)

A key element within the SLA; the goal for the cloud service performance level, shared between the cloud provider and a customer. If the service performance meets or exceeds the SLO, it means that end users, customers, and internal stakeholders are all happy.

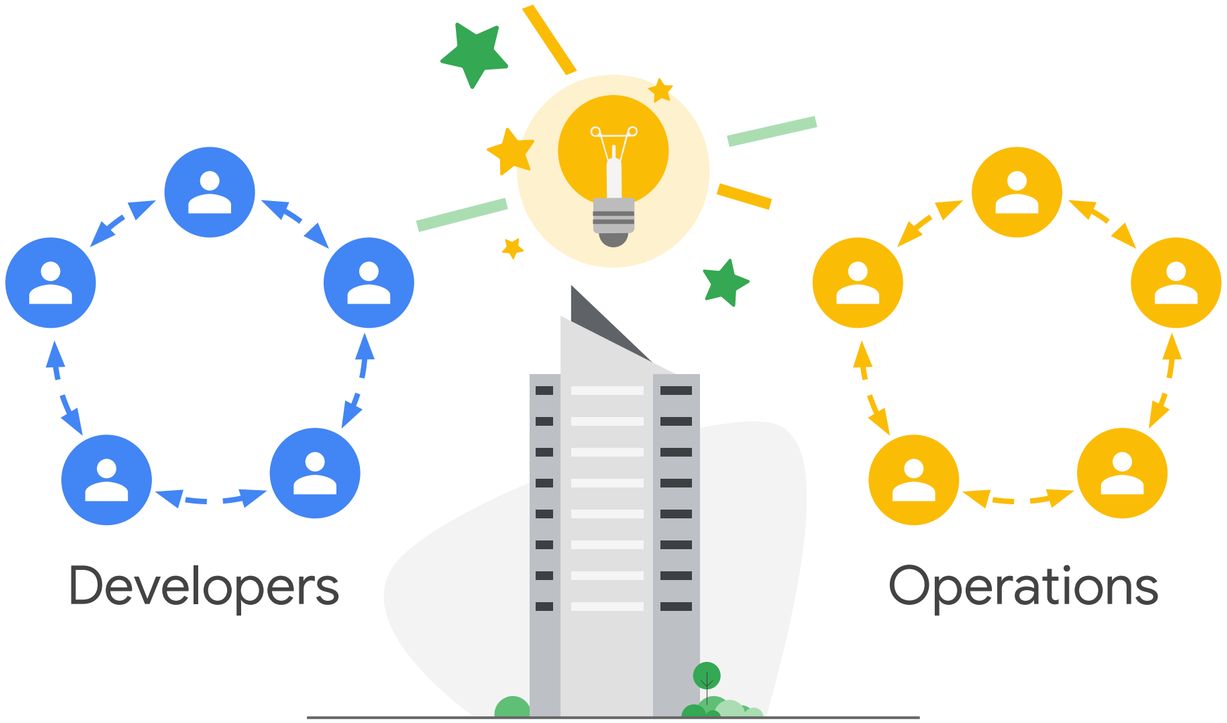
Service level indicator (SLI)



## Service level indicator (SLI)

A measure of the service provided. SLIs often include reliability, latency (which means delays in the system), and errors.

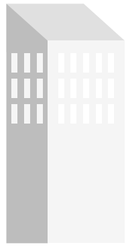

The error budget is typically the space between the SLA and the SLO. This error budget gives developers clarity into how many failed fixes they can attempt without affecting the end user experience.




# DevOps or Developer Operations

A philosophy that seeks to create a more collaborative and accountable culture within developer and operations teams. The philosophy highlights how IT teams can operate, but doesn't give explicit guidance on how an organization should implement practices to be successful.

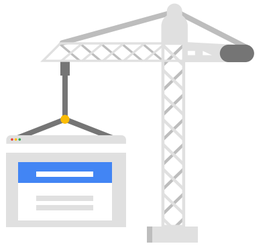
# The five objectives of DevOps:



1. Reduce silos.

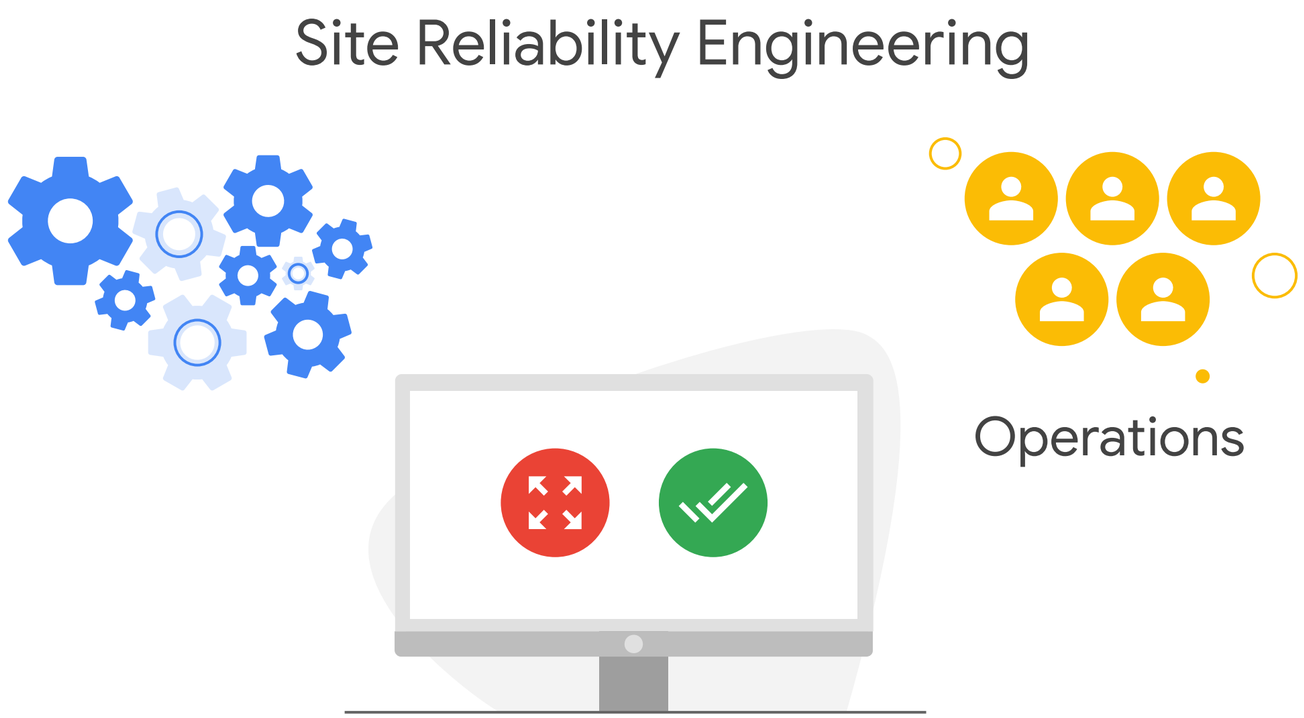
2. Accept failure as normal.

3. Implement gradual change.



4. Leverage tooling and automation.

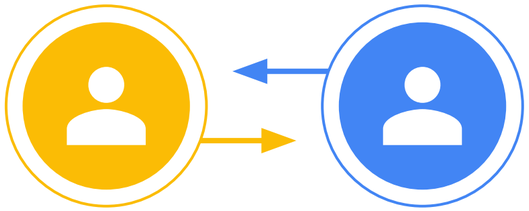
5. Measure everything.



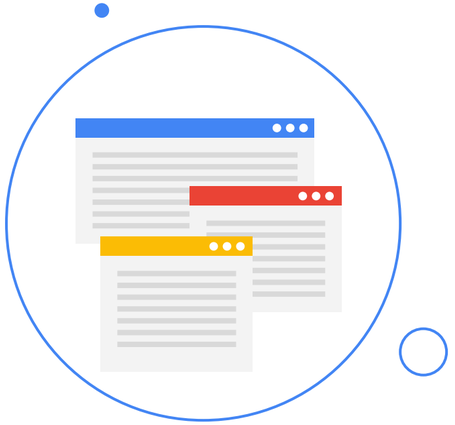

## Site Reliability Engineering (or SRE)

A discipline that applies aspects of software engineering to operations. The goals of SRE are to create ultra-scalable and highly reliable software systems.

## 1 Reduce silos

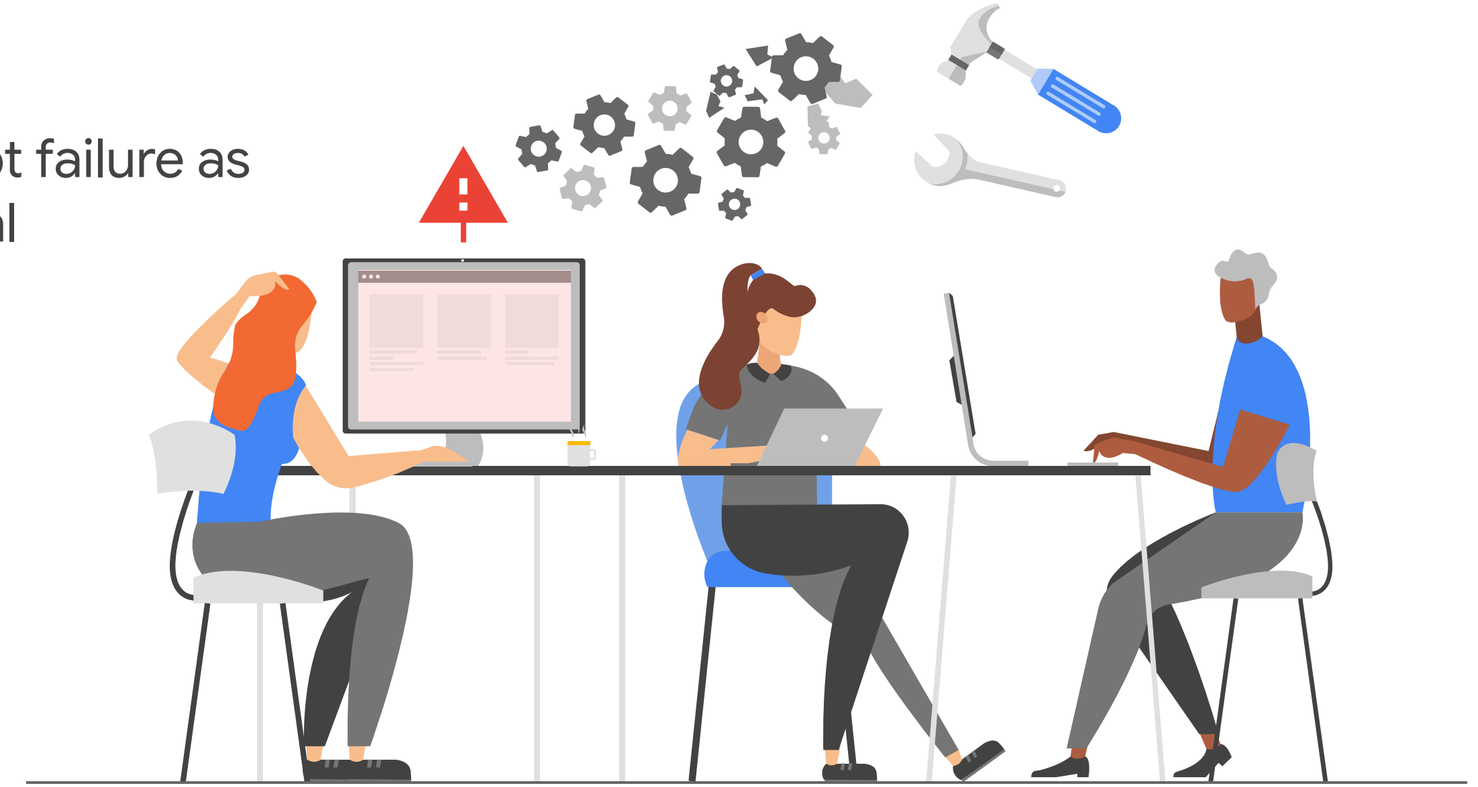


Shared ownership

SRE emphasizes shared ownership of production between developers and operations. Together, they define service level objectives or SLOs, calculate error budgets, determine reliability, and order work priorities.

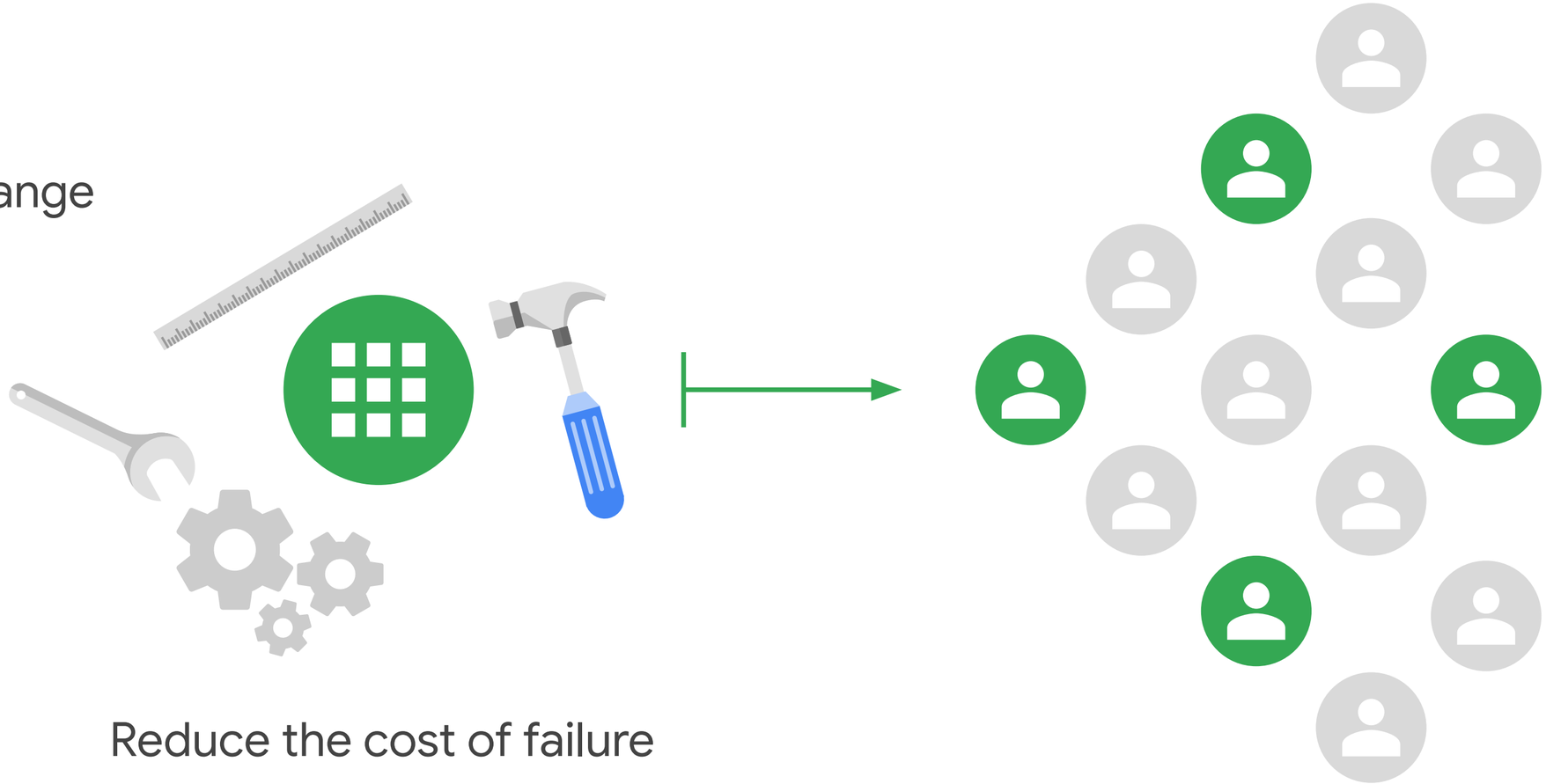
# 2 Accept failure as normal



Iterative, collaborative culture

SREs believe that accepting failure as normal helps to build an iterative, collaborative culture. One way this is done is by holding a blameless “lessons learned” discussion after an incident occurs.

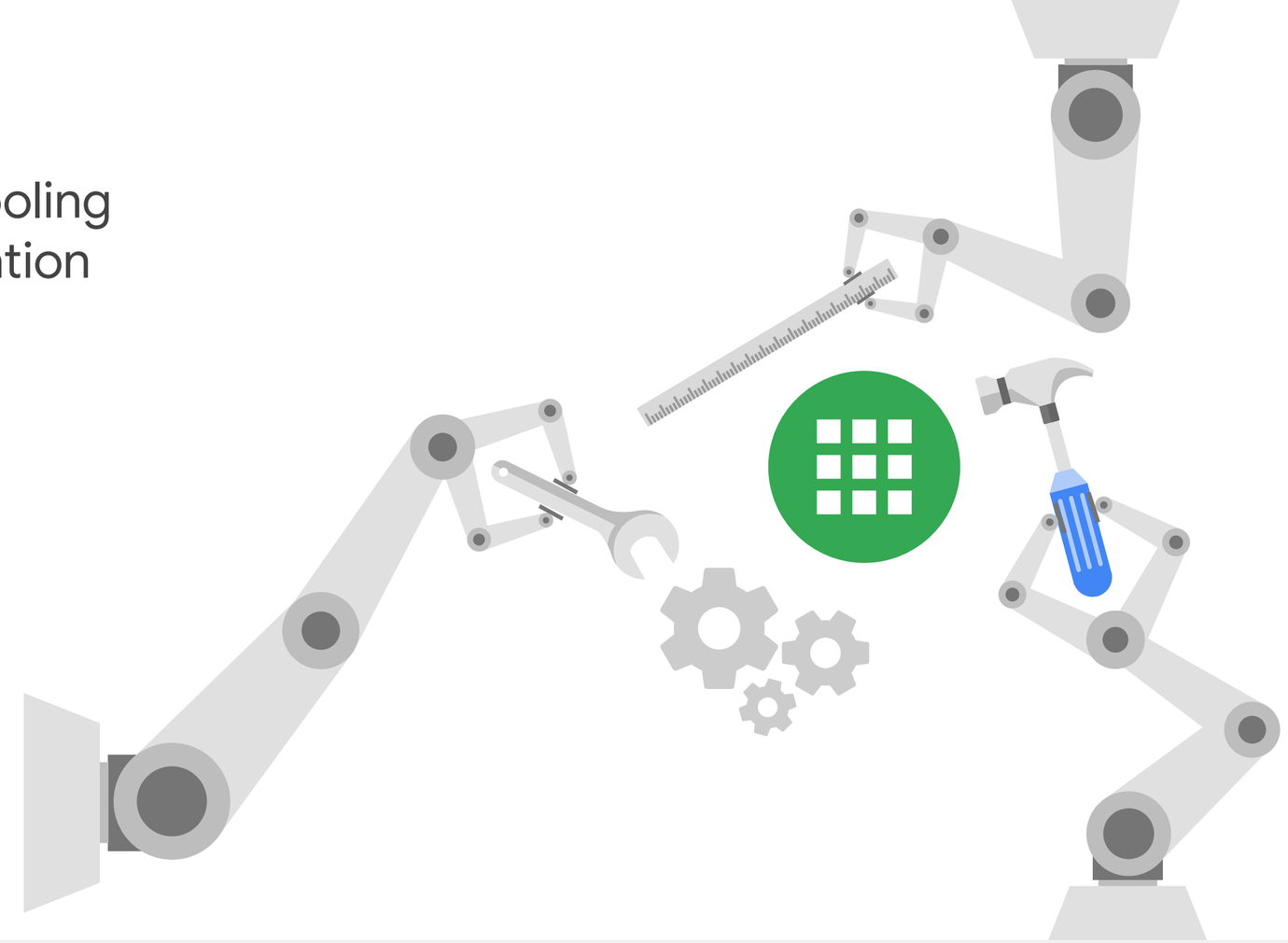
# 3 Implement gradual change



Reduce the cost of failure

When implementing gradual changes, SREs aim to reduce the cost of failure by rolling out changes to a small percentage of users before making them generally available. This promotes more prototyping and launching iteratively.

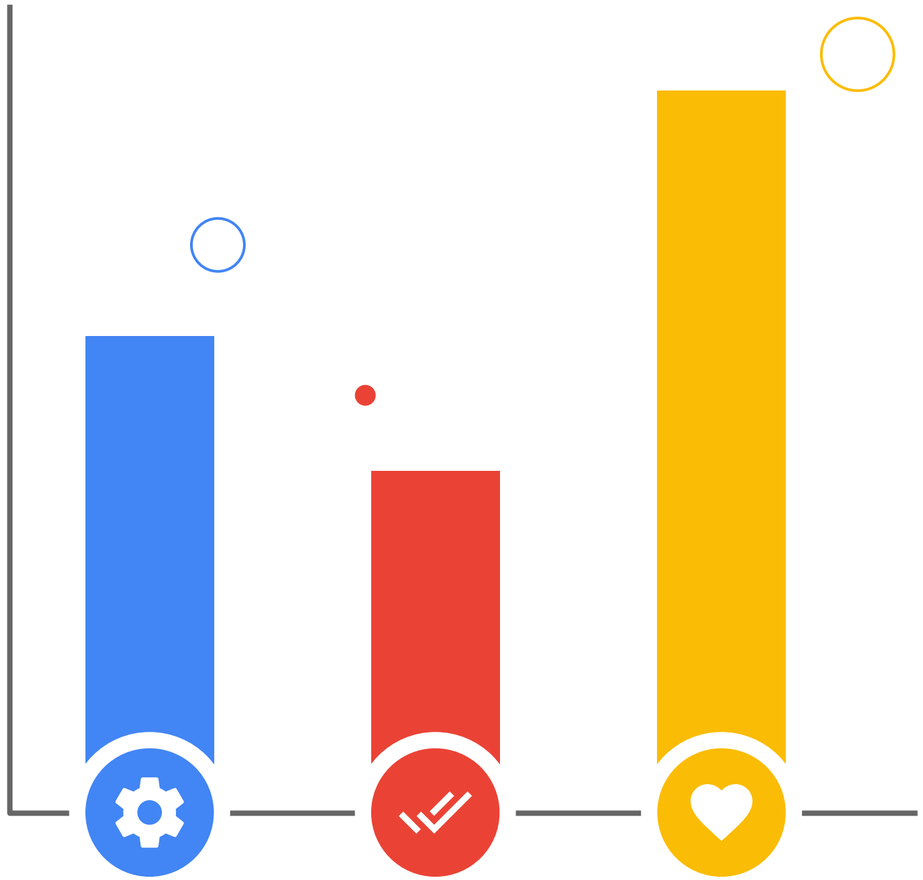
# 4 Leverage tooling and automation



Toil automation

In order to leverage tooling and automation, SREs focus on toil automation.
In software engineering, toil is a type of work that is tied to running a production service. Toil automation, therefore, reduces the amount of manual, repetitive work.

# 5 Measure everything



‘Measure everything’ means tracking everything related to toil, reliability, and the health of their systems.

Goal setting

Transparency

Data-driven decision making

To foster these practices, organizations need a culture of goal setting, transparency, and data-driven decision making. They also need the tools to monitor their cloud environment, and to identify whether they are meeting their service level objectives.

100%

99.999%

SRE shifts the mindset from ‘100% availability’ to 99.99% or 99.999% availability. This means that updates are pushed out iteratively and continually, but only require seconds or minutes of downtime.

The tools included in Google Cloud's operations suite fall into two major categories:

## Operations-focused tools

- Cloud Monitoring
- Cloud Logging
- Error Reporting
- Service Monitoring

## Application performance management tools

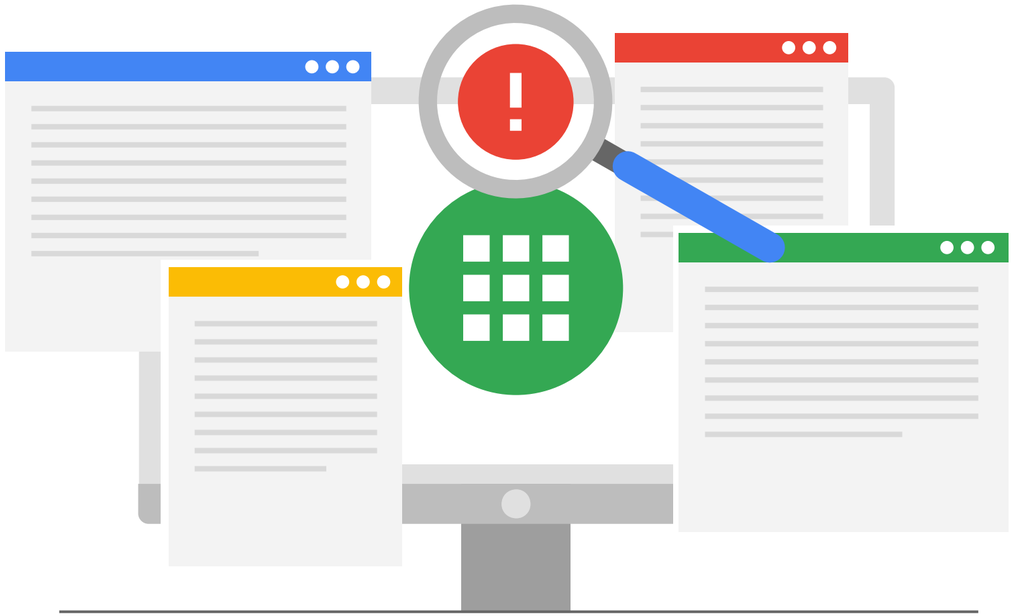
- Cloud Debugger
- Cloud Trace
- Cloud Profiler

Cloud Monitoring

## Cloud Monitoring

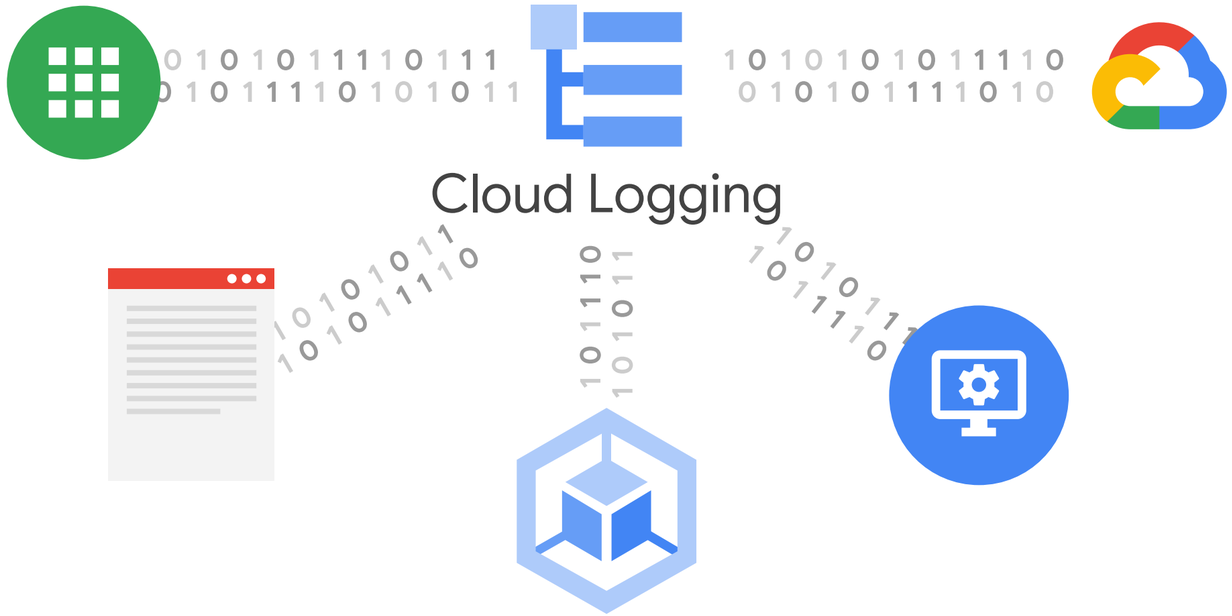
**Cloud Monitoring** is the foundation for Site Reliability Engineering because it provides visibility into the performance, uptime, and overall health of cloud-powered applications.

Developers DevOps System Admins



## Log file

A text file where applications, including the operating system, write events. Log files make it easier for developers, DevOps, and System Admins to get insights and identify the root cause of issues within applications and the infrastructure.




# Google Cloud Logging

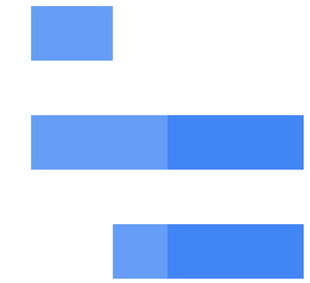
**Google Cloud Logging** is a fully managed service that performs at scale and can ingest application and system log data, as well as custom log data from Google Kubernetes Engine, or GKE, environments, Virtual Machines, and Google Cloud services.


All Google Cloud services, from Google Kubernetes Engine, to BigQuery, to Cloud Spanner, stream metrics and logs into the Google Cloud Logging and Cloud Monitoring components.

Cloud Debugger

## Cloud Debugger

**Cloud Debugger** helps monitor application performance. IT teams can inspect the state of a running application in real time, without stopping or slowing it down. This means that end users are not affected while a developer searches the source code. IT teams can use it to understand the behavior of their code in production and analyze its state to find those hard-to-find bugs.



Cloud Trace

## Cloud Trace

**Cloud Trace** is another Google Cloud solution for monitoring application performance. It is a distributed tracing system that helps developers debug or fix and optimize their code.