**14**

**Defining Security Policies**

Whatever we do in the cloud needs to be secure. Cloud providers only provide tools. You need to define how to use these tools. In order to determine what these tools should do, you need to think about what type of assets you want to protect and how you need to protect them. There are quite a number of security baselines—for example, the baseline as defined by the **Center for Internet Security** (**CIS**), which provides guidelines.

In this chapter, we will learn what a security framework is and why it’s important as a starting point for security policies. We will discover what we need to protect in our cloud environments. Next, we will look at the globally adopted CIS benchmark for Azure, AWS, GCP, Alibaba Cloud, and OCI and learn how to implement CIS using the security suites of these platforms. We will then learn what the difference is between security governance and management, and lastly, study **Cloud Security Posture Management** (**CSPM**) to control our cloud configurations and ensure they are secure and compliant.

In this chapter, we’re going to cover the following main topics:

* Managing security policies
* Understanding security policies
* Understanding security frameworks
* Understanding the dynamics of security and compliance
* Defining the baseline for security policies
* Implementing security policies
* Implementing security policies in Azure, AWS, GCP, Alibaba Cloud, and OCI
* Manage risks with Cloud Security Posture Management

**Understanding security policies**

Let’s start with our traditional on-premises data center—a building traditionally used to host physical equipment that runs applications and stores data. The building is very likely secured by a fence and heavy, locked doors that can only be opened by authorized personnel. Access to the computer floors is also secured. There may be guards in the building or CCTV systems watching over equipment 24 hours a day. The next layer of defense is access to the systems and data. Access to systems is strictly regulated; only authorized and certified engineers may access the systems. It’s all common sense when it comes to running systems in a physical data center.

You will be surprised to see what happens when companies move these systems to cloud environments with IaaS, PaaS, and SaaS solutions. For some reason, companies tend to think that by moving systems to the cloud, those systems are secured intrinsically, by default. That is not the case.

Platforms such as Azure, AWS, GCP, Alibaba Cloud, and OCI are probably the best-secured platforms in the world. They have to be since they are hosting thousands of customers globally on them. But this doesn’t mean that a company will not have to think about its own security policies anymore. The platforms provide a huge toolbox that enables the securing of workloads in the cloud, but what and how to protect these workloads is still completely up to the companies to implement themselves. We will need to establish and enforce our security policies in the cloud, think them through very carefully, and stick to them. That is what this chapter is about.

As with physical data centers, access needs to be regulated first by defining which identities are authorized to enter systems, and next, by determining what these entities are allowed to do in these systems. This is all part of identity and access management, a topic that we will cover in full in *Chapter 15*, *Implementing Identity and Access Management*.

The foundation for security policies is the CIA principle:

* **Confidentiality**: Assets in the IT environment must be protected from unauthorized access.
* **Integrity**: Assets in the IT environment must be protected from changes that are not specified and unauthorized.
* **Availability**: Assets in the IT environment must be accessible to authorized users.

The security policy itself has nothing to do with technology. The policy merely defines the security principles and how these are safeguarded in the organization. The policy does not define what ports must be opened in a firewall or what type of firewall is required. The policy describes the requirement that assets belonging to a certain function in the enterprise must be protected at a certain level.

For example, a business-critical functionality that relies on a specific stack of applications needs to be available at all times and the data loss must be zero. That will lead to an architectural design using mirrored systems, continuous backups, disaster recovery options, and a very strict authorization and authentication matrix for people who must be able to access these systems.

**Understanding security frameworks**

Security policies and forthcoming principles do not stand on their own. Typically, they are defined by industry or public frameworks to which a company must adhere. There are two types of frameworks: mandatory industry frameworks and best practices.

Examples of industry frameworks are the **Health Insurance Portability and Accountability Act** (**HIPAA**) for health care and the **Payment Card Industry** (**PCI**) data security standard for financial institutions. These frameworks were created to protect consumers by setting standards to avoid personal data—health status or bank accounts—being compromised. The cloud architect must have a deep understanding of these frameworks since they define how systems must be designed.

Next to these industry frameworks, there are some overall security standards that come from best practices. Examples are the standards of the **International Organization of Standardization** (**ISO**) and the U.S. **National Institute of Standards and Technology** (**NIST**). Specific to the cloud, we have the framework of the CIS.

Cloud providers have adopted the CIS framework as a benchmark for their platforms, as it is the internationally accepted standard for cybersecurity. The reason is that CIS maps to the most important industry and overall security frameworks such as the ISO, NIST, PCI, and HIPAA. The controls of CIS take the principles from these frameworks into account, but it doesn’t mean that by implementing CIS controls, a company is automatically compliant with the PCI or HIPAA. CIS controls need to be evaluated per company and sometimes per environment.

Basically, there are two levels of CIS controls:

1. Essential basic security requirements that will not impact the functionality of the workloads or services.
2. Recommended settings for environments that require greater security but may impact the workloads or services through reduced functionality.

In summary, CIS provides a security framework based on best practices. These are translated into benchmarks that can be adopted for specific platforms and systems: Azure, AWS, and GCP, and the instances in those clouds using operating systems such as Windows Server or various Linux distributions. These benchmarks lead to settings in the hardening of servers.

CIS offers recommendations for the following:

* Identity and access management
* Storage accounts
* Database services
* Logging and monitoring
* Networking
* Virtual machines
* Application services

Adhering to CIS or any other framework doesn’t necessarily mean that our cloud environments are compliant by default. We will elaborate on this in the next section.

**Understanding the dynamics of security and compliance**

Security and compliance are two completely different things, yet they are closely related to each other. Security policies are required to achieve compliance. We will get into the relationship a bit further in this section.

First, let’s get a good definition of security. **Security** involves all activity to protect the assets of a company and the users of their systems. This activity can be defined in security controls: physical, technical, and administrative. Typically, we don’t have to worry about physical controls in the cloud. Microsoft, Amazon, Google, Alibaba, and Oracle will make sure that their data centers and all the hardware that’s in them are well protected. However, we do have to worry about technical and administrative controls. We need to take action to, for instance, implement antivirus and antimalware software on workloads that we host in the cloud—these are technical controls. Administrative controls are procedures, protocols, and processes. They need to be in place too.

If we have taken actions to implement technical and administrative controls, then we can achieve compliance. However, the controls must be aligned with cloud usage standards and laws, which might be specific to industries, regions, or countries. These laws and rules are documented in frameworks.

In short, cloud security and compliance are two essential aspects of any organization’s IT infrastructure. Ensuring that your organization’s data and systems are secure and compliant with relevant regulations is essential for protecting a business and its customers. The question is, does the cloud help to make the IT infrastructure more secure? By moving to the cloud, organizations outsource the management and maintenance of infrastructure to a third-party provider, the cloud platform. This can free up valuable time and resources for your organization, but it also means that you need to rely on the security measures put in place by the cloud provider.

To ensure the security of your data and systems, it is essential to choose a cloud provider that has strong security measures in place. This includes physical security measures, such as data center security and employee background checks, as well as technical measures, such as encryption and access controls. As we already concluded, the major cloud providers have these physical controls well in place.

Next, we come to compliance. Different industries and countries have their own specific regulations and requirements when it comes to the storage and handling of sensitive data. For example, the **General Data Protection Regulation** (**GDPR**) in the European Union sets strict guidelines for the protection of personal data, while the HIPAA in the United States regulates the handling of medical information.

To ensure compliance with these regulations, it is essential to choose a cloud provider that has demonstrated its commitment to compliance. This may involve obtaining certifications, such as SOC 2 for security or the PCI DSS for handling credit card information, or undergoing regular audits to ensure that their practices align with relevant regulations.

It is also important for organizations to have their own processes and controls in place to ensure compliance with relevant regulations. This may include implementing access controls to ensure that only authorized individuals have access to sensitive data, regularly reviewing and updating policies and procedures, and providing training to employees on how to handle sensitive data.

The relationship between cloud security and compliance is dynamic and critical at the same time. Ensuring that your organization’s data and systems are secure and compliant with the relevant regulations is essential to protect your business and its customers. By carefully evaluating the security measures and compliance commitments of your cloud provider and implementing your own controls, you can ensure that your organization’s IT infrastructure is secure and compliant.

It all starts with setting the baselines for our security. In the next section, we will learn how to define this baseline.

**Defining the baseline for security policies**

It just takes a few mouse clicks to get a server up and running on any cloud platform. But in an enterprise that’s migrating or creating systems in the cloud, there’s a lot for an architect to think about—securing environments being the top priority. It is likely that IaaS, PaaS, and SaaS solutions will be used to build our environment. It could grow in complexity where a lack of visibility could lead to vulnerabilities. So, with every service enrolled in the cloud environment, we really need to consider how best to secure each service. Every service needs to be compliant with the security baseline and the policies defined in that baseline.

What are the steps to create policies and the baseline?

1. **Check regulations**: Every company is subject to regulations. These can be legal regulations such as privacy laws or industry compliance standards. Make sure the regulations and compliance frameworks your company needs to adhere to are understood. Be sure to involve internal legal departments and auditors. This is the starting point in all cases.
2. Also, check which security frameworks cloud providers have adopted. The major platforms—Azure, AWS, GCP, Alibaba, and OCI—are compliant with most of the leading compliance and security frameworks, but this may not be the case for smaller providers, for instance, specific SaaS solutions. Be aware that with SaaS, the provider controls the full stack: operating systems, hardware, network infrastructure, application upgrades, and patches. You have to be sure that this is done in a compliant way for your company.
3. **Restrict access**: This is what is often referred to as **zero trust**, although the term is even more related to network segmentation. But zero trust is also tightly connected to access management. We will have to design a clear **Role-Based Access Control (RBAC)**model. Users have specific roles granting authorization to execute certain actions in cloud environments. If they don’t have the appropriate role or the right authorization, they will not be able to execute actions other than the ones that have been explicitly assigned to that particular role. One term that is important in this context is **least privilege—**users only get the role and associated authorizations to perform the minimum number of actions that are really required for the daily job and nothing more.
4. **Secure connections**: Cloud environments will be connected to the **wide area network** (**WAN**) of a company and the outside world, the internet. The network is the route into cloud environments and must be very well secured. What connections are allowed, how are they monitored, what protocols are allowed, and are these connections encrypted? But also, how are environments in the cloud tenant segmented, and how do systems in the tenant communicate with each other? Are direct connections between workloads in the cloud tenant allowed or does all traffic need to go through a centralized hub?
5. The security baseline should contain strict policies for all connectivity: direct connections, VPNs, in-transit encryption, traffic scanning, and network component monitoring. Again, we should think about the zero-trust principle; network segmentation is crucial. The architecture must be designed in such a way that users can’t simply hop from one segment of the environment to another. Segments must be contained and workloads inside the segments must be protected. A zero-trust architecture typically has zones defined, for instance, a private zone where only inbound traffic is allowed or a public zone that has connections to the outside world. These zones are strictly separated from each other by means of a variety of security elements, firewalls, security groups, or access control lists.
6. **Protect the perimeter**: This is about protecting the outside of the cloud environment, the boundary. Typically, the boundary is where the connections terminate in the cloud environment. This can be a hub, and that’s where the gateways, proxy servers, and firewalls will be hosted. Typically, it also hosts the bastion host or jump server as a single point of entry, where a user is allowed to gain access to the workloads in the environment.
7. **Protect the inside**: There will be workloads in our cloud: servers, applications, containers, and functions. Although there is boundary protection with gateways and firewalls, we must also protect our workloads, especially, but not limited to, the critical ones. These workloads must be hardened, reducing the vulnerability of systems with mandatorily applied security settings, such as removing software components or disabling services that are not required to run on a system.
8. **Perform frequent audits**: This is a step that falls within managing security policies, which will be covered in the last section of this chapter. Security policies need to be constantly assessed. Hackers don’t sit on their hands and will constantly think of ways to look for vulnerabilities. Therefore, it’s necessary to continuously assess and audit policies and evaluate identified vulnerabilities. How critical are those vulnerabilities and what are the odds that our environments will get breached? Are we protected well enough? But also, how fast can action be taken if a vulnerability gets exploited and we need to mitigate the consequences? This is not something that should be discussed once a month but instead should be at the forefront of our minds at all times, for everyone developing or managing cloud environments.

We will need to define the scope of our security policies. One way to do that is by thinking in layers, derived from defense-in-depth as a common methodology to design security architectures. Each layer comprises protective measures against specific threats. These layers are as follows:

* **Network layer**: As already stated in the previous section, the network is the entrance into our cloud environment. Networks need to be protected from unauthorized people getting in. Technologies to protect a network from threats are firewalls, **Intrusion Detection Systems** (**IDSes**) and **Intrusion Prevention Systems** (**IPSes**), **Public Key Infrastructure**(**PKI**), and network segmentation, preferably adhering to zero-trust principles.
* **Platform layer**: Typically, this is the layer of the operating system. Systems should be fully patched with the latest fixes for (possible) vulnerabilities and hardened. Also, pay attention to ports that are opened on a system. Any port that is not required should be disabled.
* **Application layer**: This layer is not only about an application but also about middleware and APIs communicating directly with the application. Application code must be secured. Static code analysis can be very helpful and is strongly advised. Static program analysis is performed without actually executing software, validating the integrity of source code so that any attempt to change code or software parameters is detected.
* **Data layer**: This is the holy grail for hackers, the ultimate target of almost every hacker. If a hacker succeeds to get through the first three layers—network, platform, and application—then the next layer is the data itself. We will extensively discuss data security in *Chapter 16*, *Defining Security Policies for Storing Data*. All critical data should be encrypted, in transit and at rest.
* **Response layer**: This is the layer for all security monitoring, typically the layer for **Security Information and Event Management** (**SIEM**) and **Security Orchestration, Automation, and Response**(**SOAR**) systems. This is the layer where all suspicious activity is captured, analyzed, and translated into triggers to execute mitigating actions.

Security policies must be defined and applied at each layer. Now, let’s look at some best practices for security policies:

* **Access**: Only use named accounts to allow access to systems, including just-in-time access. Be extremely selective when granting global admin rights, implement RBAC, and use multi-factor authentication. In the next chapter, we will go into this subject in more detail.
* **Perimeter or boundary protection**: Implement firewalls or use the native firewalls from the cloud platforms. A recommended practice is to have the firewall set to “block all” as the default and then open up ports as per the requirements of a certain workload or functionality. Only have ports open when there’s a valid reason.
* **PKI**: Public and private keys are used to verify the identity of a user before data is transferred. Breached passwords are still the number one root cause for compromised systems and data leaks. Therefore, it’s recommended not to use passwords but instead keys, securely stored in a key vault. All major cloud providers offer PKI services and key vault solutions.
* **Logging and audit trails**: Be sure that you know what happens in your cloud environment, at all times. Even with the most rigid security policy, a company should never fully rely on security measures alone. Monitoring and an audit trail are highly recommended (or required, even) best practices.

Now it’s time to discover how these policies should be implemented using the native security suites in Azure, AWS, and GCP.

**Implementing security policies**

We have studied the compliance and security frameworks, and we’ve defined our security baseline. Now we need to implement it in our cloud environments. In this section, we will explore implementations in the major clouds, using native security platforms. Since CIS is widely and globally adopted as the baseline for security policies, all sections will explore specific settings that CIS benchmarks recommend for the different platforms. Links to the benchmarks are provided in the *Further reading* section of this chapter. CIS not only provides recommendations but also documents how policies should be implemented.

For example, in GCP, there is a recommendation to “*ensure Cloud Audit Logging is configured properly across all services and all users from a project*.” CIS benchmarks also guide users to find where a setting needs to be configured and how—in this example, by going to audit logs at <https://console.cloud.google.com/iam-admin/audit> or by configuring it from the command line:

gcloud organizations get-iam-policy ORGANIZATION\_ID

gcloud resource-manager folders get-iam-policy FOLDER\_ID

gcloud projects get-iam-policy PROJECT\_ID

The format in the CIS benchmarks is always the same, for all cloud platforms.

**Implementing security policies in Microsoft Defender for Cloud**

For starters, we have to understand what defines a policy, and this is basically the principle that applies to other clouds as well. A policy defines:

* **Mode**: Stating what resource types will be evaluated against the policy.
* **Parameters**: This sets the action a policy will/should have, for example, allow or deny.
* **Policy rule**: Typically a rule appears as an if-then statement. If a specific condition is met, then a specific action must be taken.
* **Effect**: This specifies the expected outcome when a policy is applied.

Microsoft Defender for Cloud is a native service of Azure where we can specify security policies. Microsoft Defender for Cloud automatically, at no cost, enables any of your Azure subscriptions not previously onboarded by you or another subscription user. Within minutes of launching Defender for Cloud for the first time, you might see:

* Recommendations for ways to improve the security of your connected resources.
* An inventory of your resources that are now being assessed by Defender for Cloud, along with the security posture of each.

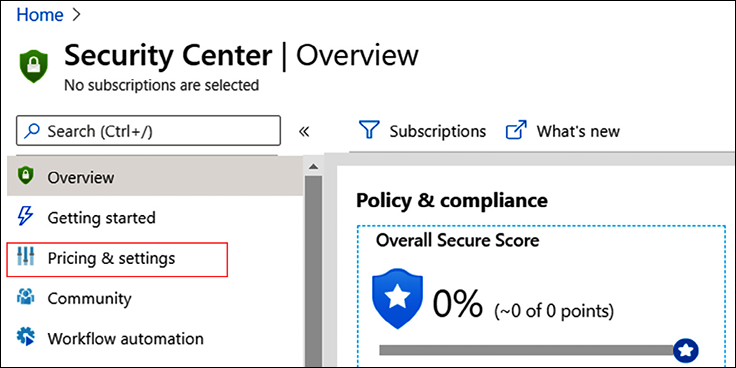
Then, you can enable enhanced security features for unified security management and threat protection across your hybrid cloud workloads.

We don’t need to install or configure anything; from the Azure console, Defender for Cloud can be accessed immediately by simply enabling it. It then starts monitoring workloads that you have deployed in Azure: virtual machines, databases, storage accounts, networking components, and other Azure services.

By default, every Azure subscription has the Microsoft cloud security benchmark assigned. This is the successor of **Azure Security Benchmark** (**ASB**), which was rebranded in October 2022. However, additional policies will need to be configured in Defender for Cloud. You have dozens of regulatory standards you can apply (PCI, SOC, CIS, NIST, or ISO). As Microsoft Defender for Cloud is a multi-cloud product, you have different options for the cloud you are protecting (Azure, AWS, or GCP). You can even create your own custom security initiatives.

CIS lists some recommendations specific to Azure Security Center. The most important one is to activate the standard pricing tier in Security Center—this enables threat detection for all networks and VMs in the Azure tenant. Every CIS recommendation to implement a policy comes with an explanation.

Enabling the standard pricing tier and adjusting settings is done through the **Defender for Cloud**blade in the portal at <https://portal.azure.com/#home>, as shown in the following screenshot:



*Figure 14.1: Overview of the Security Center blade in the Azure portal*

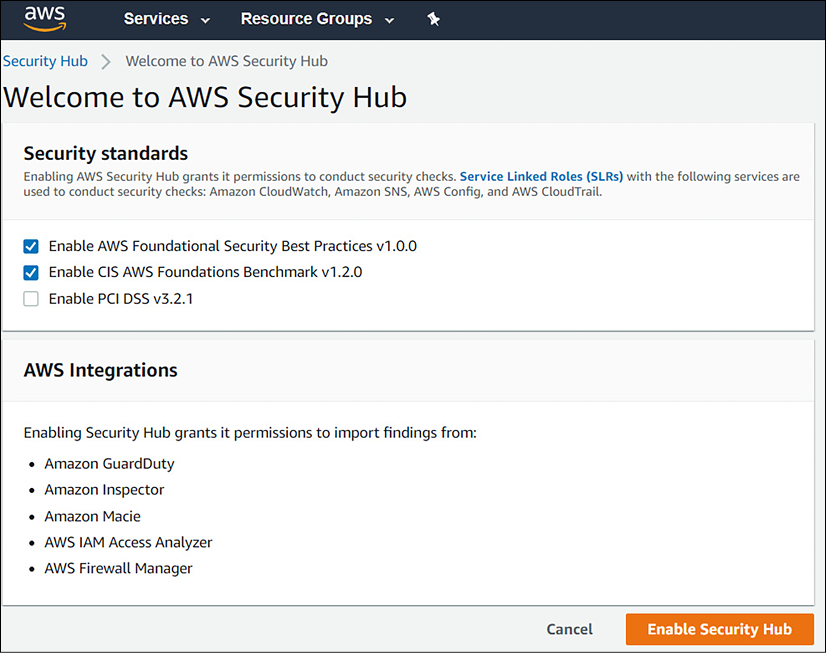
Getting started with Defender for Cloud is best done by visiting <https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security>.

Azure has more than just Azure Security Center—Azure Sentinel, a native SIEM and SOAR solution. Sentinel is an intelligent defense-in-depth solution, and it is especially useful when activating its MITRE ATT&CK® security framework. ATT&CK is a knowledge base that is constantly updated with the latest threats and known attack strategies. A group of developers under the name of BlueTeamLabs have published templates and code to implement ATT&CK in Sentinel. It’s worthwhile taking a look at this at <https://github.com/BlueTeamLabs/sentinel-attack>.

**Implementing security policies in AWS Security Hub**

AWS offers a single security dashboard with AWS Security Hub. The solution aggregates monitoring alerts from various security solutions, such as CloudWatch and CloudTrail, but also collects findings from Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS IAM Access Analyzer, and AWS Firewall Manager. CloudTrail, however, is the key element in Security Hub. CloudTrail constantly monitors the compliance of accounts that are used in the AWS environment. It also performs operational auditing and risk auditing, meaning it keeps track of all activity that is started from the console in your environment, enables analysis of changes to resources, and detects unusual activity. It’s fair to say that CloudTrail is the engine underneath Security Hub.

Security Hub makes it easy to start monitoring all activity in your AWS environment. It’s accessible from the AWS console, as shown in *Figure 14.2*:



*Figure 14.2: Accessing Security Hub in the AWS console*

There are a couple of things that need explaining in the preceding screenshot. The top part of the screen shows the security baselines that can be selected—**Enable AWS Foundational Security Best Practices v1.0.0** and **Enable CIS AWS Foundations Benchmark v1.2.0** have been ticked by default. The third one is the PCI DSS framework. **PCI DSS** stands for **Payment Card Industry Data Security Standard** and is specific to financial institutions.

In the lower part of the screen, we see all the integrations that Security Hub offers:

* **GuardDuty**: Amazon’s solution for threat detection.
* **Inspector**: This tool assesses applications for exposure, vulnerabilities, and deviations from best practices valid for these applications.
* **Macie**: This solution monitors the data security and data privacy of your data stored in Amazon S3 storage.
* **IAM Access Analyzer**: This tool keeps track of accounts accessing environments in AWS and whether these accounts are still compliant with security policies.
* **Firewall Manager**: This tool enables centralized management of all firewalls in the AWS environment.

By clicking the **Enable Security Hub** button, the aforementioned baselines with the named integrations will be enrolled.

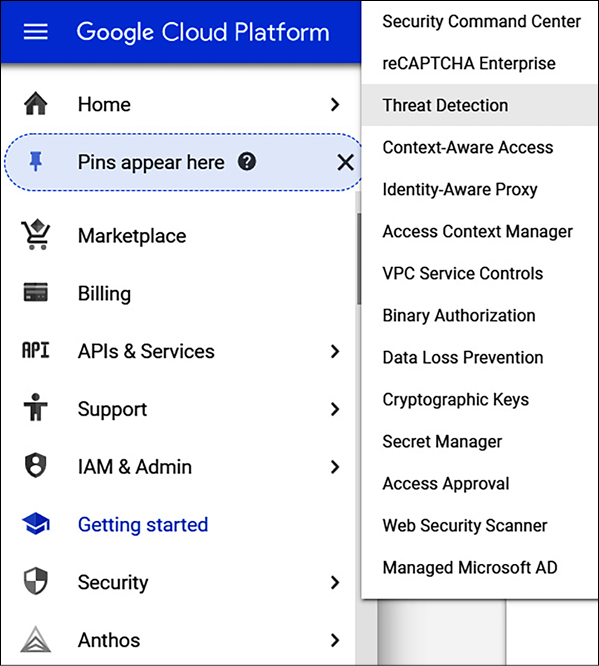
The CIS baseline should definitively be implemented as the worldwide accepted standard for securing online environments. Specific to AWS, CIS includes the following recommendations for settings to control security policies:

* Ensure that CloudTrail is enabled in all regions
* Ensure that CloudTrail log file validation is enabled
* Ensure that an S3 (storage) bucket used to store CloudTrail logs is not publicly accessible
* Ensure that CloudTrail logs are integrated with CloudWatch logs
* Ensure that AWS Config is enabled in all regions
* Ensure that S3 bucket access logging is enabled on a CloudTrail S3 bucket
* Ensure that CloudTrail logs are encrypted at rest using **Key Management Services**—**Customer Master Keys**(**KMS CMKs**)
* Ensure that rotation for customer-created CMKs is enabled
* Ensure **Virtual Private Cloud** (**VPC**) flow logging in all VPCs

Obviously, these are not all the settings; these are the most important settings to get the logging and monitoring of security policies right. In the *Further reading* section, we include links to the various CIS benchmarks for the major clouds.

**Implementing security policies in GCP Security Command Center**

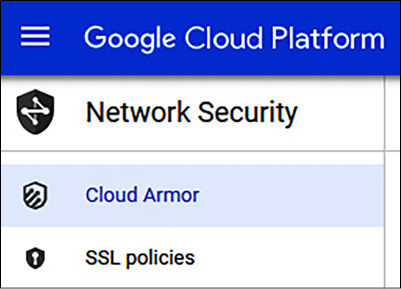
In GCP, we will have to work with Security Command Center. You can manage all security settings in Security Command Center and view the compliancy status from one dashboard. The concept is the same as AWS Security Hub—Security Command Center in GCP comprises a lot of different tools to manage security in GCP environments. In the GCP cloud console, we’ll see **Security** in the main menu. Hovering over the **Security** subheading will pop up the products and tools that are addressed in **Security Command Center**, as shown in the following screenshot:



*Figure 14.3: Launching Security Command Center in the cloud console of GCP*

Security Command Center does an inventory and discovery of all assets in the GCP environments and, next, starts monitoring them in terms of threat detection and prevention. One special feature that needs to be discussed here is Google Cloud Armor. Cloud Armor started as a defense layer to protect environments in GCP from **Distributed Denial-of-Service** (**DDoS**) and targeted web attacks. Cloud Armor has since been developed into a full security suite in GCP to protect applications, using the functionality of **Web Application Firewalls** (**WAFs**).

Cloud Armor can be launched from the GCP console at <https://console.cloud.google.com/>. You won’t find it under **Security Command Center** but under **Network Security**, as shown in *Figure 14.4*:



*Figure 14.4: Menu of Cloud Armor in GCP*

We can specify security policies in Cloud Armor, but GCP already includes a list of policies that can be evaluated. These preconfigured policies are based on the **OWASP** CRS—the **Open Web Application Security Project**, a community that strives to find methodologies and practices to constantly improve the protection of online applications. **CRS** stands for **Core Rule Set**. Cloud Armor includes the top 10 OWASP threats in rule sets. The number one threat is the injection of hostile code in order to breach an application and get access to data. In *Chapter 16*, *Defining Security Policies for Storing Data*, we will explore OWASP in more detail since this is all about securing applications and data.

However, OWASP does overlap with CIS, but OWASP merely identifies the threats, whereas CIS makes recommendations for avoiding vulnerabilities and assesses the chances of threats really being exploited. Misconfigured security, for example, is number 6 in the top 10 of OWASP. Insufficient logging and monitoring conclude the top 10. Both are heavily addressed by CIS.

The CIS 2.2.0 benchmark for GCP was released in March 2020. Specifically, for logging and monitoring, CIS recommends the following settings to audit security policies:

* Ensure that Cloud Audit Logging is configured properly across all services and users in a project.
* Ensure that sinks are configured for all log entries.

A sink will export copies of all the log entries.

* Retention policies on log buckets must be configured using Bucket Lock.
* Ensure that log metric filters and alerts exist for project ownership assignments and changes.
* Ensure that log metric filters and alerts exist for audit configuration changes.
* Ensure that log metric filters and alerts exist for custom role changes.
* Ensure that log metric filters and alerts exist for VPC Network Firewall rule changes.
* Ensure that log metric filters and alerts exist for VPC Network Route changes.
* Ensure that log metric filters and alerts exist for VPC Network changes.
* Ensure that log metric filters and alerts exist for cloud storage IAM permission changes.
* Ensure that log metric filters and alerts exist for SQL instance configuration changes.

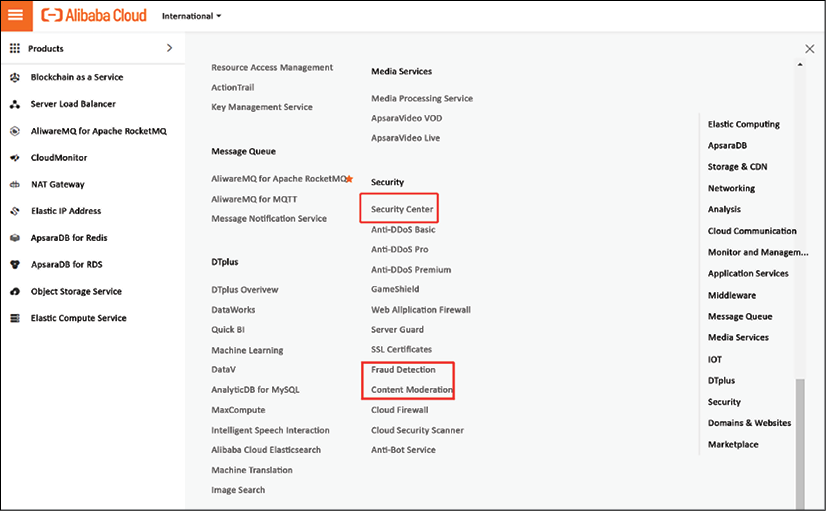
As with Azure and AWS, these are the settings to audit security policies against the CIS benchmark. In the *Further reading* section, we include links to the various CIS benchmarks for the major clouds.

**Implementing security policies in Alibaba Cloud**

The main product in Alibaba Cloud is Security Center. This is the place where we can define and store security policies for assets that we host in Alibaba Cloud. Security Center offers extensive services for:

* Defining and guarding the security baseline
* Asset control
* Compliancy check
* Ransomware alerts
* Mining alerts
* Tamper-proofing
* AccessKey pair leaks
* Attack-source tracing
* Cloud security configuration monitoring
* Cloud asset risk monitoring

A nice feature is that users can have a 7-day trial in Security Center. But this does not cover everything in terms of security. Alibaba offers a wide range of additional services, including “business security.” Fraud detection offers real-time analysis and identification of risks. One more service that is worthwhile mentioning is **Content Moderation**—a service that enables the detection of pornography, violence, and terrorism in images, text, audio, and videos. It includes daily updates on compliance intelligence. All these services are listed under **Security** in the console, as shown in *Figure 14.5*:



*Figure 14.5: Security menu in Alibaba Cloud*

There are three levels in Security Center, including a free tier, but then services are limited to setting policies for abnormal login, cloud platform configuration assessment, and vulnerability checks. The advanced tier is charged at approximately 10 USD per server per month, but it does provide sophisticated protection against viruses, ransomware, and cryptomining. Advanced also includes intrusion detection. The enterprise level is the most complete offering, with AccessKey leak detection, attack awareness, and attack tracking among other services. Enterprises are recommended to contact Alibaba Cloud for financial offerings.

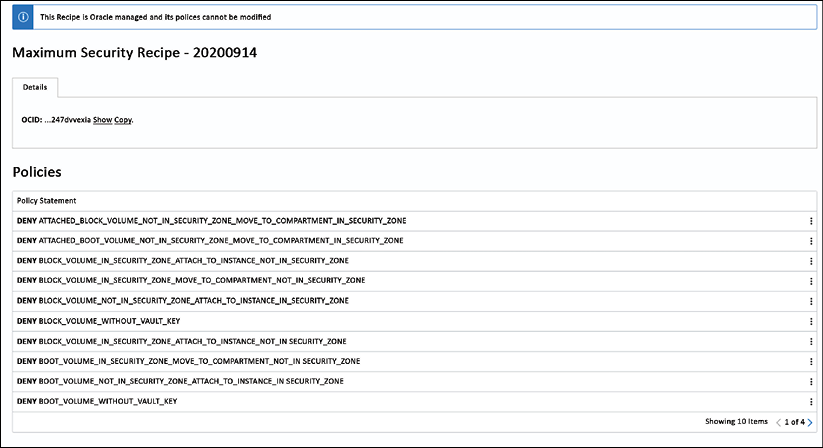
Naturally, there is a CIS benchmark (version 1.0.0) for Alibaba Cloud too, which we recommended reviewing.

**Implementing security policies in OCI**

The best place to start to understand how security policies work in OCI is the **Consensus Assessment Initiative Questionnaire** (**CAIQ**) for OCI, available to read at <https://www.oracle.com/a/ocom/docs/oci-corporate-caiq.pdf>. This is an extensive document that lists the security practices in OCI. It lists all the control domains and how Oracle addresses security issues in each domain. We picked the first topic in the list as an example, asking if Oracle adheres to industry standards such as the OWASP Software Assurance Maturity Model to build security in systems and the Software Development Life Cycle. Oracle’s answer to that one is **Oracle Software Security Assurance** (**OSSA**).

Obviously, this is not an implementation of the security policies for our specific environment. The CAIQ is a good starting point to define these policies, adhering to the best practices of OCI.

In OCI, we define policies in a security zone. Creating a security zone is done through a recipe, a collection of the policies in that zone. There’s already a predefined recipe called the Maximum Security Recipe, managed by Oracle, which can’t be modified. It’s shown in *Figure 14.6*:



*Figure 14.6: Maximum Security Recipe in OCI*

We can, however, add recipes with specific security policies, following a categorization. These categories are:

* Restrict resource movement, preventing resources to be moved outside of the zone
* Restrict resource association, ensuring that all components of a specific resource are in the same zone
* Deny public access
* Require encryption
* Ensure data durability concerning automatic backups
* Ensure data security, preventing data from being copied outside the zone
* Use only configurations approved by Oracle

More detailed information about security zones in OCI can be found at <https://docs.oracle.com/en-us/iaas/security-zone/using/security-zone-policies.htm>. Be aware that a security zone is not the same as a tenant or a compartment in OCI; a zone is associated with a single compartment that has the same name as the zone. The compartment holds the resources, and the security zone holds the policies that the resources have to comply with.

How do we keep track of policies in OCI? With Cloud Guard. This tool detects misconfigured resources and activity across tenants that are considered suspicious. Cloud Guard can be easily launched from the **Security** menu in the console. Recipes can now be entered in Cloud Guard.

The latest version of the CIS benchmark for OCI is CIS Oracle Cloud Infrastructure Foundations Benchmark version 1.2.0.

**Managing security policies**

It doesn’t stop with implementing security policies. We need to have governance in place to manage the policies. Governance is required at two levels:

1. The security policies themselves, auditing these against the compliance frameworks that a business has to adhere to.
2. The technical implementation of the security policies, keeping the monitoring up to date, and making sure that all assets are indeed tracked against the policies.

The first level is the domain of people concerned with the security governance in a business, typically, a **Chief Information Security Officer** (**CISO**) or **Chief Information Officer** (**CIO**). They need to set directions for security policies and make sure that the business is compliant with the security strategy, industry, and company frameworks. The CISO or CIO is also responsible for assurance from internal and external auditing.

Level two is more about security management, concerning how to deal with security risks in the IT landscape, including the cloud environments. To make it simple—security governance is about making policies; security management is about (technically) implementing and enforcing policies. So, security engineers should worry about the management of security monitoring tools that were covered in this chapter. They will need to understand how to implement rule sets in Microsoft Defender for Cloud, AWS Security Hub, and Google Security Command Center. They will also need to know what to do in the event of an alert being raised in these systems, who should follow up, and what actions need to be taken. Those will be technical actions, such as isolating an environment when it’s breached. The configuration of rules in the security suites is also in their hands.

However, the security policies themselves need to be defined from a higher level in a business. The CISO or CIO will hardly ever completely understand how to program a security console, but they will know what needs to be protected from a business perspective. Obviously, the strategic level of CISO/CIO can’t do anything without input from the tactical level—the security architects and engineers. They will all have to work closely together.

**Manage risks with Cloud Security Posture Management**

We discussed methodologies to implement security policies in the various clouds. Now, we also have to make sure that these policies are followed to ensure that our environments stay compliant. That’s the key function of CSPM:

* Detect cloud misconfigurations
* Remediate cloud misconfigurations, preferably through automation
* Manage best practices for different cloud configurations and services
* Check the cloud health status against a security control framework and compliance standards
* Monitor cloud services, including storage solutions, encryption, and account permissions

CSPM is designed to detect and remediate risks that might be caused by bad configurations of cloud services. Since we work in multi-cloud, we have to find tools that can scan multiple environments in clouds. Some of these tools are also able to check against regulatory frameworks such as the HIPAA, alert, and even automatically remediate issues. Palo Alto Networks’ Prisma and Trend Micro’s Cloud One Hybrid Cloud Security are two such tools, but there are many more. Since CSPM is an evolving market, more providers are expected to enter this domain.

The best practices are:

* Understanding the risk profile of an organization; different organizations have different risk profiles, based on factors such as the type of data they handle, the regulatory environment they operate in, and their overall security posture. Understanding your organization’s risk profile will help you prioritize your efforts and allocate resources appropriately.
* Implementing a strong governance framework by establishing clear policies, procedures, and controls for your cloud environment. This should include things like access controls, data classification, and incident response plans.
* Implementing CSPM, which provides continuous monitoring and assessment of your cloud environment and enables fast identification of potential risks. Other tools, such as **cloud access security brokers** (**CASBs**) and SIEM systems, can also help you identify and mitigate risks.
* An obvious point that can’t be stressed enough: make sure to keep your cloud environment, including all hardware and software, up to date with the latest patches and security updates. This can help you protect against known vulnerabilities and reduce the risk of attacks.
* Monitoring and reviewing your risk posture regularly. This can involve conducting regular risk assessments, reviewing security logs, and staying up to date with the latest threats and vulnerabilities.

One of the crucial elements of keeping environments secure is only granting access to authorized users and services. Good IAM is key. That’s the central topic of the next chapter.

**Summary**

In this chapter, we discussed the basics of security frameworks as a starting point to define policies for cloud environments. We learned that there are different frameworks and that it depends on the industry to determine the compliance requirements of a business. Then, we must decide which security controls to set to ensure that our cloud environments are compliant too.

One framework that is globally accepted and commonly used for clouds is CIS. We learned that the CIS benchmarks for these cloud platforms not only greatly overlap but also have specific settings that need to be implemented in the respective security suites—Microsoft Defender for Cloud, AWS Security Hub, Google’s Security Command Center, Alibaba Cloud, and OCI’s Security Zones.

In the last section, we learned how we can keep control of security policies and our environments compliant by implementing CSPM and studying some best practices.

In the next chapter, we will dive into identity and access management, since that’s where security typically starts—who is allowed to do what, how, and maybe even when in our cloud environments? In *Chapter 17*, *Implementing and Integrating Security Monitoring,* we will further explore the use of the monitoring tools that we discussed briefly in this chapter.

**Questions**

1. We’ve discussed the CIA principle. What does it stand for?
2. Name the attributes that are included as a minimum in a policy.
3. Where do we implement security policies in OCI?
4. What does a CSPM tool do?

**Further reading**

You can refer to the following links for more information on the topics covered in this chapter:

* The CIS framework: <https://www.cisecurity.org/>
* The CIS Benchmark for Azure: [https://learn.microsoft.com/en-](https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark)
* The CIS framework: <https://www.cisecurity.org/>
* The CIS Benchmark for Azure: <https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark>
* The CIS Benchmark for AWS: <https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf>
* The CIS Benchmark for GCP: <https://www.cisecurity.org/benchmark/google_cloud_computing_platform/>
* The CIS Benchmark for Alibaba: <https://www.cisecurity.org/benchmark/alibaba_cloud>
* The CIS Benchmark for OCI: <https://www.cisecurity.org/benchmark/oracle_cloud>
* Link to the OWASP community pages: [https://owasp.org/www-project-top-ten/#:~:text=The%20OWASP%20Top%2010%20is%20the%20reference%20standard,software%20development%20culture%20focused%20on%20producing%20secu](https://owasp.org/www-project-top-ten/#:~:text=The%20OWASP%20Top%2010%20is%20the%20reference%20standard,software%20development%20culture%20focused%20on%20producing%20secure%20code)