Google Cloud

Security control implementation

As you've learned, security controls are important safeguards that help reduce risk. You've also learned about the steps that can be taken to choose and implement controls for specific risks and threats. In this reading, you'll learn more about best practices for implementing security controls and examine an example of how to document security controls that you've already implemented.

Best practices for implementing security controls

- Conducting risk assessment
- Identifying security control
- Selecting solutions
- Developing an implementation plan
- Testing and validating controls
- Monitoring and maintaining controls

Conduct risk assessment

There are both qualitative and quantitative risk assessment approaches. As a security professional, one of the most important parts of risk assessment is understanding the asset that you're trying to protect. The asset could be data, a process, or people. Remember you also need to understand threat actors and the potential vulnerabilities they could exploit, including the likelihood and impact of a successful attack.

Threat modeling is a good way to start considering the likelihood and impact of risk. Some common threat models include: Process for Attack Simulation and Threat Analysis (PASTA), Trike, the Common Vulnerability Scoring System (CVSS), Attack Trees, Security Cards, and hybrid Threat Modeling Method (hTMM). Each of these methodologies provides a different way to assess the threats to organizational assets.

Identify security controls

Once you've identified potential threats and the likelihood of any related risks, you can identify which security controls are best.

Some examples of common security controls for cloud computing include:

- Usernames and passwords (simple authentication)
- Two-factor authentication
- Antivirus software

- Firewalls
- DDoS (Distributed Denial of Service) attack protection
- Intrusion prevention and detection systems
- Cloud security posture management system (CSPM) controls

So, how do you know which controls to use? You might decide to use a layered approach or use a framework like NIST CSF to identify appropriate controls. For example, if you were using NIST as a reference, you might start by taking a control from each of the functions (Identify, Protect, Detect, Respond, and Recover).

Develop an implementation plan

An implementation plan is an action plan that turns your security control strategy into specific tasks. Your implementation plan should be very clear about how you'll make sure that the required controls are implemented. A good implementation plan considers how each particular control will be rolled out. You'll have to consider any training or communication that needs to happen, the financial cost, and the technical requirements that must be met to apply the control.

One of the most common difficulties in an implementation plan is getting organizational buy-in. Buy-in refers to willingness and support. You must have buy-in and support from other parts of the organization, including IT, for controls to be successful. The concept of organizational buy-in is important because controls are technical, procedural, and administrative. This means they require other members of the organization to take part in implementation in order to make them effective.

Test and validate

Controls need to be tested in order to confirm or validate that they are meeting risk or compliance goals. You need to ensure that the controls are effective and operational. It is important to define and measure what success is, and to conduct ongoing assessments while considering any potential new threats. Sometimes, there may be a change in the impact or likelihood of a threat, and that may require ongoing adjustment of a control, or a change in the control approach.

Monitor and maintain

Once security controls have been successfully implemented, it's important to continually monitor and maintain controls to help reduce risk.

Security controls documentation example

The table on the last page of this reading is an example of what a control mapping spreadsheet might look like. In this example there are five columns. The first column describes the security control. The second column assigns a risk level ranging from low, medium, or high. Following that, the next column offers a space for you to outline the reasoning for why the control was chosen. And, the final column documents the source, standard, or framework as applicable.

Note: The template for documenting controls may differ depending on organizational and compliance needs.

Key takeaways

Using best practices to identify and implement security controls will ensure that you have the necessary controls in place to meet compliance and organizational needs. Documenting your controls in a clear chart or spreadsheet will help you to show evidence and rationale for the controls that you have chosen.

Resources for more information

Check out these resources for more information on implementing controls:

- Multi-factor authentication for more information on enforcing multi-factor authentication controls.
- Threat Modeling to learn more about the different threat models.

Google Cloud

Security controls documentation table

Security Control	Level Low/Medium/High	Rationale	Source
Access Control: Ensure the Owner, Editor, and Viewer roles are not assigned in Cloud IAM	M	Adhering to the principle of least privilege helps to reduce the risk of exploitation if user credentials are compromised by an outside attacker or malicious insider.	
Access Control: Establish Google Groups to represent separation of duties	M	Adhering to the principle of least privilege helps to reduce the risk of exploitation if user credentials are compromised by an outside attacker or malicious insider.	Establish Google Groups to represent separation of duties
Access Control: Grant access to Groups, adhering to the principle of least privilege	M	Adhering to the principle of least privilege helps to reduce the risk of exploitation if user credentials are compromised by an outside attacker or malicious insider.	Grant access to Groups,
Identify: Building an asset list using Cloud Asset Inventory is a control or Policy analyzer.	M	These tools will identify what programs are running and which policies are in place in the cloud environment.	NIST CSF
Protect: VPC-Service Controls	H	VPC service controls will prevent non-allowed IP addresses from making any connection or performing actions on the resources.	NIST CSF
Detect: Use SCC to understand vulnerabilities and changes in cloud posture relative to a benchmark.	H	Detect and reduce vulnerabilities.	NIST CSF
Respond: Use Chronicle to initiate a threat hunt to determine the scope and nature of the attack.	M	Chronicle will help to determine the scope and nature of the attack.	NIST CSF
Recover: Backup and restore using Terraform.	M	Backup and restore to rebuild an environment to a known good state.	NIST CSF