Google Cloud

Control mapping for risk management

Throughout your journey, you learned about controls, and how to implement them to manage risk and meet compliance obligations. In this reading, you'll learn more about mapping controls, and explore an example of a control map.

Introduction to control mapping

Control mapping can help you identify control gaps, along with overlap between various control sets. Control mapping is an important part of the risk management and compliance process. By assessing controls and mapping them, risk teams can help save both time and effort.

Getting started

As a security professional, you may have to create a control map. Control maps are spreadsheets that identify, document, and evaluate the controls in place within an organization. Control maps can look different depending on organizational and business needs.

To create a control map, build a spreadsheet that details your controls, and collects evidence from your cloud environment that these controls are in place.

Your control mapping spreadsheets should include evidence of controls that your organization has put in place across whole sets of control frameworks, standards, and regulations. Evidence collection is the process of gathering and documenting data, records, and other compliance processes to demonstrate adherence to rules, regulations, and standards. In the control map, evidence is an explanation of the control that it is in place, and how this control meets the requirement. For example, if a cybersecurity framework requires multi-factor authentication (MFA), you'll want to ensure that your organization uses security keys or other tools that meet this requirement. Some ways to gather evidence include: consulting with your team, reviewing existing control maps, reviewing security policies and procedures, testing and validation reports, and risk assessments.

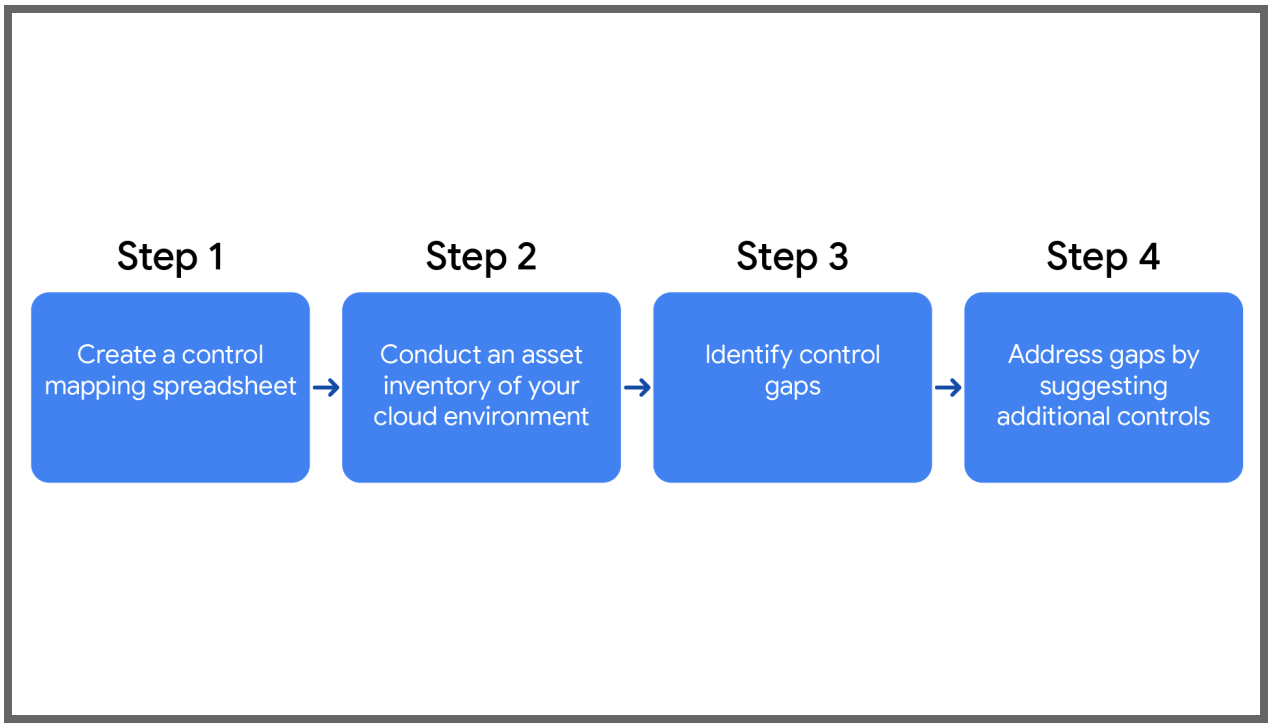
New regulations often require specific control mapping configurations. When a new regulation is introduced, you can compare its control requirements to the controls that you already have mapped. You can also make note of the differences between new and existing regulations, and then add any missing controls to fill the gaps, or remove any mappings for obsolete controls. For example, if a new regulation requires new passwords for staff every 30 days instead of every 45 days, your security team would need to implement this control in order to meet the

new regulation and fill the gap. Then, you can update the control map explaining how this requirement has been met by your team.

Pro tip: You don't have to start from scratch! There are lots of free resources available. You can start with the detailed controls from an existing control map like the NIST SP 800-53 to build your control mapping sheet in Excel or Google Sheets. There are also helpful, no cost resources that provide crosswalks between frameworks and regulations, including mappings of NIST SP800-53 to ISO 27001 and NIST SP 800-53 to NIST 1.1 CSF.

Here are the steps to creating both a control map and map controls:

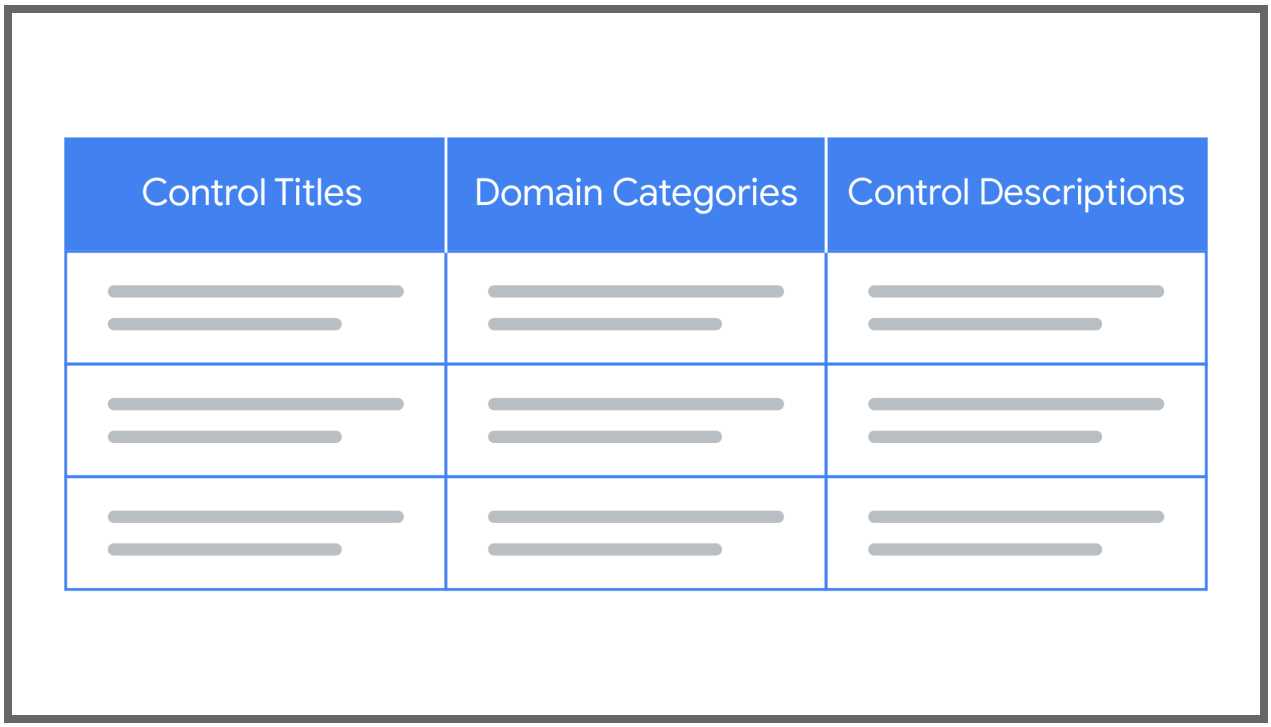
1. Create a control mapping spreadsheet.
2. Conduct an asset inventory of your cloud environment.
3. Identify control gaps.
4. Address gaps by suggesting additional controls.



Create a control mapping spreadsheet

Here are the steps to creating and recording evidence in your control map in more detail.

First, create a spreadsheet that includes security control titles, domain categories, and descriptions to identify related controls. This graphic is an example of a spreadsheet that has been set up to map controls. Remember, you can use resources like the NIST SP 800-53 control catalog to help you get started.



Conduct an asset inventory

Next, conduct an inventory of all cyber and virtual assets in your organization's cloud environment. The Google Cloud Asset Inventory can be a helpful tool for conducting an inventory. You can input the inventory into a separate spreadsheet. You can also use this inventory to determine the best controls to use to protect your assets and maintain compliance.

Map your controls to a framework

Then, evaluate your current controls, and map them to your organization's or framework's requirements. The PCI DSS Shared Responsibility Matrix document outlines compliance guidance across four product categories that are core to PCI DSS® compliance. These include: Compute, Networking, Storage, and Security & Identity. This document breaks down the division of responsibilities between the cloud service provider and the customer or user. Documents like these can help you create and organize your control maps. Remember, compliance obligations may differ depending on organization, industry, and location.

Identify and address gaps

Lastly, analyze your control map to identify gaps that need to be addressed. You can do this by reviewing the control requirements from frameworks, regulations, and organizational policy that you've included in your map, and identify which requirements have not been met. Once

you've identified the missing controls, you can address these gaps by suggesting additional controls to your team. Once these controls have been implemented by your organization, you can add the evidence to your control map to explain how the gap has been filled with additional controls.

Key takeaways

Implementing controls to meet organizational and compliance needs can be a difficult task. But, mapping controls saves you time and effort, and can help your organization maintain a strong and compliant security posture.

After you've mapped your controls and identified any gaps, you can move on to choosing specific controls or other solutions to close the gaps you've identified. This will help to reduce risk and meet compliance obligations.

Resources for more information

Review this resource to learn more:

- Example of a NIST SP 800-53 spreadsheet