

# Course 2 resources and citations

---

## Module 1: Introduction to frameworks within security domains

### Resources

Helpful resources and tips

- [Google Docs Editors Help: Google Docs Help Center](#)
- [Google Docs Editors Help: Google Sheets Help Center](#)
- [Google Docs Editors Help: How to use Google Slides](#)
- [Hands-on labs overview](#)

Learn more about security and compliance with Google whitepapers

- [Google Cloud: Cloud Security Podcast](#)
- [Google Cloud: Google security overview](#)
- [Google Cloud: Security whitepapers](#)
- [Google Security Blog: MiraclePtr: protecting users from use-after-free vulnerabilities on more platforms](#)

Learn more about security controls

- [NIST: Control Catalog spreadsheet](#)
- [NIST: Control Map spreadsheet](#)
- [NIST: SP 800-53 controls and SP 800-53B control baselines: Resources for implementers](#)

Use existing frameworks to demonstrate compliance

- [AICPA: 2017 Trust Services Criteria: See what's changed](#)
- [Department of Health and Human Services: Security Standards: Technical Safeguards](#)
- [Google Cloud: SOC 2 – Compliance](#)
- [HITRUST for HIPAA](#)

Control mapping for risk management

- [NIST: Control Map spreadsheet](#)

Security control implementation

- [Carnegie Mellon University: Threat modeling: 12 available methods](#)
- [Google Cloud: Enforce uniform MFA to company-owned resources](#)

## Citations

Introduction to cloud security domains

- Holladay, H.G. (2022, November 21). [How to write a cloud security policy for your business](#). *Kirkpatrick Price Blog*.
- OpenStack. (2023, September 26). [Security boundaries and threats](#).
- SCA Editor. (2020, September 9). [What are the 5 domains of the NIST cybersecurity framework?](#) *SCA security*.
- Sharma, V. (2024, January 18). [CCSP domains: Requirements for CCSP qualification](#). *Knowledgehut blog*.
- Skoutaris, E.(2020, October 16). [What is the cloud controls matrix \(CCM\)?](#) *Cloud Security Alliance blog*.

## Explore compliance and security

- Auditboard. (2022, April 25). [Security vs compliance: Where do they align?](#)
- Coretelligent. (2023, May 19). [Security vs. Compliance: Differences & similarities \(2023\)](#).
- Cyber Risk Management. (2023, November). [Security vs. compliance: What's the difference?](#) Trava Security blog.
- Miller, A. (2021, June 25). [IT security vs IT compliance: What's the difference?](#) Security & Compliance blog.
- National Institute of Standards and Technology. (n.d.). [Cybersecurity framework](#).

## Learn more about security and compliance with Google whitepapers

- Google Cloud. (n.d.). [Security & Identity Google Cloud Blog](#).

## Security controls and compliance

- Exabeam. (n.d.). [Cloud security controls: Key elements and 4 control frameworks](#).
- National Institute of Standards and Technology. (n.d.). [Security control](#). Computer Security Resource Center.
- Walkowski, D. (2019, August 22). [What are security controls?](#) F5 Labs.

## Learn more about security controls

- Joint Task Force. (2020, September). [Security and privacy controls for information systems and organizations](#) (Special Publication 800-53r5). National Institute of Standards and Technology.
- Peacock, J. (n.d.). [NIST SP 800-53 control families explained](#). Cybersaint.

## Risk and compliance

- Cyber Risk Management. (2023, November). [Security vs. compliance: What's the difference?](#) Trava Security blog.
- javaTpoint. (n.d.). [What are the security risks of cloud computing.](#)
- SecurityScorecard. (2021, August 25). [Compliance vs risk management: What you need to know.](#)

## The three areas of compliance: People, process, and technology

- Computer Science Research Education Group. (n.d.). [Computer security 10.3: Technology, people, process and compliance.](#) University of Canterbury, NZ.
- Manage Engine Academy. (n.d.). [The three Ps of compliance.](#)
- Plutora. (2020, September 8). [People, process, technology: The PPT framework, explained.](#)

## Use existing frameworks to demonstrate compliance

- HIPAA Journal. (2023, July 31). [HIPAA compliance guidelines.](#)
- PCI DSS "©2006–2023 PCI Security Standards Council, LLC. All Rights Reserved."
- Yawn, A.J. (2022, January 24). [SOC 2 Trust Services Categories.](#) SANS Institute.

## Overview of the Google Cloud Security Command Center

- Google Cloud. (n.d.). [Security command center.](#)
- Google Cloud. (2024, January 17). [Configuring security command center.](#)

## Cloud security controls

- Swanagan, M. (2020, December 7). [Types of security controls explained.](#) PurpleSec.
- Exabeam. (n.d.). [Cloud security controls: Key elements and 4 control frameworks.](#)

Explore steps to implement security controls

- Buchanan Technologies. (n.d.). [5 key steps to performing a cloud security assessment](#).
- Google Cloud. (2020, February 5). [Enforce uniform MFA to company-owned resources](#).
- XM Cyber. (n.d.). [What is a security control?](#)

Security control implementation

- Shah, J. (2019, December 9). [What to do, and How to do it — 5 Steps to Implementing IT Security Controls](#). *Medium*.
- XM Cyber. (n.d.). [What is a Security Control Validation?](#)

## Module 2: Risk management and security frameworks, regulations, and standards

### Resources

Risk management and security frameworks

- [Google Cloud: Security and resilience framework](#)
- [Cloud Security Alliance: What is the Cloud Controls Matrix \(CCM\)?](#)

Compare and contrast risk management frameworks

- [NIST: Control Map spreadsheet](#)
- [AICPA: Mapping of SOC 2 Trust Services to HITRUST](#)

Google's Secure AI Framework

- [Google: Introducing Google's Secure AI Framework](#)
- [Google: Secure AI Framework Approach](#)

Learn more about data protection and privacy regulations

- [PIPEDA Fair Information Principle 1 – Accountability](#)
- [PIPEDA Fair Information Principle 2 – Identifying Purposes](#)
- [PIPEDA Fair Information Principle 3 – Consent](#)
- [PIPEDA Fair Information Principle 4 – Limiting Collection](#)
- [PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention](#)
- [PIPEDA Fair Information Principle 6 – Accuracy](#)
- [PIPEDA Fair Information Principle 7 – Safeguards](#)
- [PIPEDA Fair Information Principle 8 – Openness](#)
- [PIPEDA Fair Information Principle 9 – Individual Access](#)
- [PIPEDA Fair Information Principle 10 – Challenging Compliance](#)
- [PIPEDA in brief](#)
- [What is GDPR, the EU’s new data protection law?](#)

Security frameworks, regulations, laws, and standards

- [NIST: Control Map spreadsheet](#)
- [General Data Protection Regulation \(GDPR\)](#)
- [Department of Health and Human Services: HIPAA Administrative Simplification](#)
- [HIPAA Journal: HIPAA Compliance Guidelines](#)
- [ISO standards](#)
- [NIST: Cybersecurity framework](#)
- [Official PCI Security Standards Council site](#)

- [PIPEDA legislation and related regulations](#)
- [Department of Health and Human Services: Security Standards: Technical Safeguards](#)
- [Google Cloud: SOC 2 – Compliance](#)
- [The California Privacy Rights Act of 2020](#)
- [Department of Health and Human Services: The HIPAA Privacy Rule](#)

What is Google Cloud Risk Manager?

- [Google Cloud: Access control with IAM](#)
- [Google Cloud: Automatically generating reports](#)
- [Google Cloud: Cloud Asset Inventory](#)
- [Center for Internet Security: New CIS Benchmark for Google Cloud Computing Platform](#)
- [Google Cloud: Remediating findings](#)
- [Google Cloud: Security Command Center](#)
- [Google Cloud: Vulnerability findings](#)

## Citations

### Introduction to risk management frameworks

- Kosutic, D. (n.d.). [What is ISO 27001? A quick and easy explanation](#). Advisera.
- National Institute of Standards and Technology. (n.d.). [Cybersecurity framework](#).
- National Institute of Standards and Technology. (2023, December 13). [NIST Risk Management Framework](#). Computer Security Resource Center.
- AICPA & CIMA. (n.d.). [SOC 2® - SOC for service organizations: Trust services criteria](#).
- Stevenson, R. (2022, August 26). [Risk Management Framework \(RMF\): Overview + Best Practices](#). Drata.

### Risk management and security frameworks

- National Institute of Standards and Technology. (2021, May 14). [Examples of framework profiles](#). NIST Cybersecurity Framework.
- StandardFusion. (2023, May 23). [Guide to ISO 27001 Compliance - Part 3](#).

### Google's Secure AI Framework

- Hansen, R. & Venables, P. (2023, June 8). [Introducing Google's secure AI framework](#). Google blog.

### Data protection and privacy

- Intersoft Consulting. (n.d.). [General data protection regulation \(GDPR\)](#).
- TutorialsPoint. (2022, March 22). [Distinguish between data privacy and data protection](#).

### Learn more about data protection and privacy regulations

- Klosowski, T. (2021, September 6). [The State of Consumer Data Privacy Laws in the US \(And Why It Matters\)](#). Wirecutter.



## Data protection and privacy scenarios

- National Institute of Standards and Technology. (2019, April 30). [\*NIST Privacy Framework: An enterprise risk management tool \(Discussion Draft\)\*](#).
- National Institute of Standards and Technology. (2019). [\*Hypothetical NIST privacy framework use case profiles\*](#).

## Industry-specific regulations and standards

- Centers for Disease Control and Prevention. (2022, June 27). [\*Health insurance portability and accountability act of 1996 \(HIPAA\)\*](#). Public Health Professionals Gateway.
- Gorman, J., & Redding, J. (2023, February 21). [\*FedRAMP is law! So what? Infusion Points\*](#).
- Hartwig, B. (2021, May 20). [\*CCPA vs CalOPPA: Which one applies to you and how to ensure data security compliance\*](#). Infosec.
- Nadeau, M. (2020, June 12). [\*General Data Protection Regulation \(GDPR\): What you need to know to stay compliant\*](#). CSO Online.
- The Office of the National Coordinator for Health Information Technology. (n.d.). [\*Guide to privacy and security of health information\*](#). HealthIT.

## Apply industry-specific requirements

- Centers for Disease Control and Prevention. (2022, June 27). [\*Health insurance portability and accountability act of 1996 \(HIPAA\)\*](#). Public Health Professionals Gateway.
- Gorman, J., & Redding, J. (2023, February 21). [\*FedRAMP is law! So what? Infusion Points\*](#).
- Hartwig, B. (2021, May 20). [\*CCPA vs CalOPPA: Which one applies to you and how to ensure data security compliance\*](#). Infosec.
- Nadeau, M. (2020, June 12). [\*General Data Protection Regulation \(GDPR\): What you need to know to stay compliant\*](#). CSO Online.

- The Office of the National Coordinator for Health Information Technology. (n.d.). [Guide to Privacy and Security of Health Information](#). HealthIT.

#### Risk management industry standards

- de Groot, J. (2023, May 8). [What is PCI compliance? 12 requirements & more](#). Digital Guardian.
- Gallop, D. (n.d.). [PCI DSS compliance levels and requirements for your business](#). Carbide Secure blog.
- PCI security standards council. (n.d.). [Official PCI Security Standards Council site](#).
- PCI Security Standards Council. (n.d.). [Document library](#).
- PCI Security Standards Council. (2018, July). [PCI DSS quick reference guide: Understanding the payment card industry data security standard version 3.2.1](#).
- Scurti, H. (2022, October 4). [Level 1 PCI compliance: What it is & what you need to know](#). EBizCharge.
- VikingCloud. (n.d.). [VikingCloud—Bringing security and compliance together](#).
- Yacono, L. (2023, January 5). [A beginner's guide to PCI compliance](#). CIMCOR.

#### What is Google Cloud Risk Manager?

- Google Cloud. (n.d.). [Quickstarts](#).
- Google Cloud. (n.d.). [Risk Protection Program](#).

## Module 3: The compliance lifecycle

### Resources

Learn more about controls for workloads and services

- [Google Cloud: BigQuery overview](#)
- [Google Cloud: Customer-managed encryption keys \(CMEK\)](#)
- [Google Cloud: Enterprise foundations blueprint](#)
- [Google Cloud: Harden your cluster's security](#)
- [Google Cloud: Hardening MySQL overview](#)
- [Google Cloud: Introduction to data governance in BigQuery](#)
- [Google Cloud: Overview of access control](#)
- [Google Cloud: Three security and scalability improvements for Cloud SQL for SQL Server](#)

Audits and security assessments

- [AICPA & CIMA: System and Organization Controls: SOC Suite of Services](#)
- [HITRUST Alliance: External Assessors](#)
- [InvGate: What is the difference between assessment and audit?](#)

Best practices Google Cloud resource hierarchy

- [Google Cloud: Organize resources using labels](#)
- [Google Cloud security best practices center](#)
- [Google Cloud: Understanding allow policies](#)

## Citations

### Overview of compliance lifecycle

- F5. (2022). [Four steps of the compliance lifecycle](#).
- PCI Security Standards Council. (2008) [Getting started with PCI data security standard](#).
- Silveira, P., Rodriguez, C., Birukou, A., Casati, F., Daniel, F., D'Andrea, V., Worledge, C., and Taheri, Z. (2011). *Aiding compliance governance in service-based business processes*. Researchgate. 10.4018/978-1-61350-432-1.ch022.

### Cloud security controls

- Baykara, S. (2021, December 9). [Cloud security controls: What you need to know](#). PCI DSS GUIDE.
- Center for Internet Security. (n.d.). [Mapping and compliance](#).
- Davies, K. (2022, August 24). [Cloud Controls Matrix: How to secure your journey to the cloud](#). Contino.
- PCI Security Standards Council. (n.d.). [Official PCI security standards council site](#).
- Sahoo, N. (2021, June 15). [What are compensating controls in PCI DSS?](#) Payments Journal.

### Control mapping

- Center for Internet Security. (2023, January). [CIS controls: Version 8](#).
- MITRE Engenuity: Center for Threat Informed Defense. (n.d.). [Google Cloud Platform security control mappings to MITRE ATT&CK®](#).

### Learn more about controls for workloads and services

- Google Cloud. (2023, December 20). [Enterprise foundations blueprint](#).

## Review a compliance report

- Ross, W. L., & Copan, W. (2020, September). [Security and privacy controls for information systems and organizations](#) (NIST Special Publication 800-53, Rev. 5). National Institute of Standards and Technology.

## Cloud security audits

- Exabeam. (n.d.). [Cloud security audits: Step by step](#).
- Finney, J. (2022, November 9). [Cloud compliance audits: What you need to know](#). Linford & Co. LLP Blog.
- TeamMate. (2022, November 30). [How to audit the cloud: 4 tips to help internal auditors get started](#). Wolters Kluwer.

## Audits and security assessments

- Varghese, J. (2023, October 23). [All you need to know about Security Audit Report](#). Astra Blog.

## Prepare for and audit

- Exabeam. (n.d.). [Cloud security audits: Step by step](#).
- Google Cloud. (n.d.). [What is cloud architecture?](#)
- Lucidscale. (n.d.). [How to prepare for a cloud audit](#).
- RSI Security (2022, September 19). [Best practices for auditing the cloud](#). RSI Security Blog.

## Cloud security control inheritance

- Ford, J. (2022, September 27). [What is compliance inheritance?](#) Project Hosts: Security Compliant Clouds.
- Tracy, R. (2020, May 5). [Control Inheritance – Easing the burden of compliance and reducing audit fatigue](#). Telos Corporation Blog.
- Google Cloud. (2023, August 8). [Google Cloud Architecture Framework: Security, privacy, and compliance](#).

## Cloud resource hierarchy and security controls

- Google Cloud. (2024, January 22). [Using resource hierarchy for access control](#).
- Google Cloud. (2024, January 22). [Introduction to the Organization Policy Service](#).

## Best practices for Google Cloud resource hierarchy

- Google Cloud. (2024, January 22). [Resource hierarchy](#).
- OWASP. (n.d.). [Threat modeling](#). OWASP Cheat Sheet Series.

## Negative organizational impacts of non-compliance

- Arcserve. (2023, December 20). [7 most infamous cloud security breaches](#). Arcserve Cybersecurity Blog.
- Cybersecurity and Infrastructure Security Agency, United States Digital Service, & Federal Risk and Authorization Management Program. (2022, June). [Cloud security technical reference architecture](#).
- IT Glue. (2021, August 5). [Consequences of non-compliance](#). IT Glue Blog.

#### Policy as code and infrastructure as code

- Duplocloud. (2022, December 6). [The 7 biggest benefits of infrastructure as code](#). *DuploCloud Blog*.
- Palo Alto Networks. (n.d.). [What is policy-as-code?](#)

#### Key considerations when writing policy as code

- Synopsys. (n.d.). [Policy-as-code](#).

#### Review and update a risk management policy

- Ross, W. L., & Copan, W. (2020, September). [Security and privacy controls for information systems and organizations](#) (Special Publication 800-53, Rev. 5). National Institute of Standards and Technology.

## Module 4: Cloud tools for risk management and compliance

### Resources

#### Vulnerability management

- [CVE: About the CVE Program](#)
- [NIST: National vulnerability database – Homepage](#)
- [OWASP Top 10 API Security Risks – 2023](#)
- [VulDB: Vulnerability database – Homepage](#)

## Cloud security management (CSPM) resources

- [Netskope: Cloud security posture management \(CSPM\)](#)
- [Gartner Peer Insights: Cloud security posture management tools reviews and ratings](#)
- [Check Point: CloudGuard for cloud native security](#)
- [Palo Alto Networks: DevSecTalks](#)
- [Palo Alto Networks: Prisma Cloud](#)
- [UC Berkeley: Prisma Cloud Security](#)
- [CrowdStrike: Cloud Workload Protection](#)
- [CSO: Review: CrowdStrike Falcon breaks the EDR mold](#)
- [Orca Security: Demo](#)

## Cloud tools for risk management

- [Google Cloud: IAM overview](#)
- [Google Cloud: Policy Analyzer for IAM policies](#)

## Guide to Guide to risk assessment and compliance management with Security Command Center

- [Google Cloud: Manage and monitor for compliance](#)

## Use reports to remediate findings

- [Google Cloud: Firewall](#)
- [Google Cloud: Policy Analyzer for IAM policies](#)
- [Google Cloud: Managing reports](#)
- [Google Cloud: Risk Manager conceptual overview](#)



## Digital sovereignty and sovereign clouds

- [Google Cloud: T-Systems Sovereign Cloud Powered by Google Cloud](#)

## Organizational policy constraints, inheritance and violation

- [Google Cloud: Access control for folders with IAM](#)
- [Google Cloud: Access control for organization resources with IAM](#)
- [Google Cloud: Access control for projects with IAM](#)
- [Google Cloud: Resource hierarchy](#)
- [Google Cloud: Resource hierarchy: IAM Inheritance](#)
- [Google Cloud: Understanding constraints](#)
- [Google Cloud: Understanding hierarchy evaluation](#)

## Interview tip: Provide examples

- [Interview Warmup](#)

## Citations

### Vulnerability management frameworks

- Center for Internet Security. (n.d.). [CIS Critical Security Controls](#).
- CVE. (n.d.). [History](#).
- MITRE Engenuity. (n.d.). [Cybersecurity: Center for threat-informed defense](#).
- National Institute of Standards and Technology. (2023, April 21). [Getting started](#).
- OWASP. (n.d.). [OWASP Top 10:2021](#).

## Vulnerability management

- National Institute of Standards and Technology. (n.d.). [National Vulnerability Database](#).
- Palo Alto Networks. (n.d.). [What is the MITRE ATT&CK framework?](#)
- RSI Security. (2023, May 29). [Comparing vulnerability management frameworks](#). *RSI Security Blog*.

## Introduction to multicloud CSPMs

- Check Point. (n.d.). [CloudGuard for Cloud Security Posture Management](#).
- Crowdstrike. (n.d.). [Cloud workload protection](#).
- Google Cloud. (n.d.). [What Is multicloud?](#)
- Netskope. (n.d.). [The NETSKOPE Cloud Security Platform](#).
- Orca Security. (n.d.). [Cloud security posture management \(CSPM\)](#).
- Palo Alto Networks. (n.d.). [Prisma cloud](#).

## Security Command Center

- Goldstein, E. (2021, September 7). [Cloudy with a chance of migration: Helping agencies make the move to the cloud](#). Cybersecurity & Infrastructure Security Agency.
- Google Cloud. (n.d.). [Security Command Center](#).
- Google Cloud Tech. (2022, October 7) [How to detect threats in your Google Cloud environment with Security Command Center](#) [Video]. YouTube.
- Google Cloud Tech. (2022, October 10) [Getting started with Security Command Center](#) [Video]. YouTube.
- Google Cloud. (2024, January 22). [Security Command Center overview](#).
- Horev, R. (2021, July 29). [5 GCP security tools you should know about](#). *Vulcan Cyber Blog*.

## Security Command Center, Risk Manager, Policy Analyzer, Assured Workloads

- Center for Internet Security. (n.d.). [New CIS benchmark for Google Cloud Computing Platform](#).
- Google Cloud. (n.d.). [Assured workloads](#).
- Google Cloud. (2024, January 22). [Customer-managed encryption keys \(CMEK\)](#).
- Google Cloud. (2024, January 22). [Risk Manager conceptual overview](#).
- Google Cloud. (2024, January 22). [Understanding allow policies](#).

## Cloud tools for risk management

- Google. (n.d.). [reCAPTCHA](#).
- Google Cloud. (2024, January 22). [Beyond Corp Enterprise overview](#).
- Google Cloud. (2024, January 22). [Chronicle SIEM overview](#).
- Google Cloud. (2024, January 22). [Cloud IDS overview](#).
- Google Cloud. (2024, January 22). [Cloud Logging overview](#).
- Google Cloud. (2024, January 22). [Identity-Aware Proxy Overview](#).
- Google Cloud. (2024, January 22). [Introduction to Cloud Asset Inventory](#).
- Google Cloud. (2024, January 22). [Overview of Cloud Identity](#).
- Google Cloud. (2024, January 22). [Overview of VPC Service Controls](#).
- Palo Alto Networks. (n.d.) [What is SOAR?](#)

## Guide to risk assessment and compliance management with Security Command Center

- Google Cloud. (2024, January 22). [Overview of Security Health Analytics](#).
- Google Cloud. (2024, January 22). [Vulnerability findings](#).

## Understand Google Cloud's Risk Protection Program

- Federal Trade Commission. (2018, October 5). [Cyber insurance](#).
- Google Cloud Tech. (2022, October 24). [What is the risk protection program?](#) [Video]. YouTube.
- Munich RE. (n.d.). [Cloud protection +: Innovative cyber insurance solution for Google Cloud customers](#).
- Venables, P. & Potti, S. (2021, March 2). [Announcing the Risk Protection Program: Moving from shared responsibility to shared fate](#). *Google Cloud Blog*.

## The value of shared fate in cloud risk protection programs

- Chuvakin, A. & Rosenblatt, S. (2023, March 22). [Lessons from the future: Why shared fate shows us a better cloud roadmap](#). *Google Cloud Blog*.
- Venables, P. & Potti, S. (2021, March 2). [Announcing the Risk Protection Program: Moving from shared responsibility to shared fate](#). *Google Cloud Blog*.

## Digital sovereignty and sovereign clouds

- Karlstad, W. (2022, April 19). [Why sovereign cloud is a hot topic – 5 tips, and the background](#). CIO.

## Organizational policies in the cloud

- Google Cloud. (2024, January 22). [Introduction to the Organization Policy Service](#).
- Google Cloud. (2024, January 22). [Organization policy constraints](#).
- Google Cloud. (2024, January 22). [Resource hierarchy](#).

## Organization policy service

- Peacock, T. & Chuvakin, A. (Hosts). (2022, February 7). [\*Policy intelligence: More fun and useful than it sounds!\*](#) [Audio podcast]. Cloud Security Podcast. (51).
- Google Cloud. (2021, November 5). [\*Preventing security requirements violations with Google Cloud\*](#) [Video]. YouTube.
- Google Cloud. (2024, January 22) [\*Using constraints.\*](#)
- Google Cloud. (2022, October 11). [\*How Goldman Sachs bolstered their security posture through policy management and controls\*](#) [Video]. Youtube.

## Organizational policy constraints, inheritance and violation

- Google Cloud. (2024, January 22). [\*Organization policy constraints.\*](#)