

Certificate resources and citations

Course 1 resources and citations

Module 1: Introduction to cloud computing

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](#)
- [QWIKlabs Help: Common problems with labs/lab troubleshooting](#)

Google's trusted infrastructure

- [Google Cloud: Google Infrastructure Security Design Overview](#)

Cloud benefits and limitations

- [Google Cloud: Advantages and Disadvantages of Cloud Computing](#)

Serverless computing

- [Google Cloud: Serverless](#)
- [Journal of Cloud Computing: Serverless computing: a security perspective](#)

Citations

Composition of the cloud

- Cloud Flare. (n.d.) [What is latency? How to fix latency.](#)
- Google Cloud. (n.d.). [What is Cloud Storage?](#) Retrieved January 18, 2024.
- Google Cloud. (2023, September 1) [Building blocks of reliability in Google Cloud.](#)
- Think with Google. (n.d.). [Consumer insights: Mobile site abandonment after delayed load time.](#) Google.

Cloud deployment models

- Google Cloud. (n.d.). [What is Cloud Storage?](#) Retrieved January 18, 2024.
- Google cloud. (n.d.) [What is private cloud?](#) Retrieved January 18, 2024.
- IBM. (n.d.) [What is private cloud?](#)

Google's trusted infrastructure

- Google Cloud. (2022, September). [Default encryption at rest.](#)

Cloud benefits and considerations

- Google Cloud. (n.d.) [Advantages of cloud computing.](#)
- IBM. (n.d.) [What are the benefits of cloud computing?](#)
- Salesforce. (n.d.) [12 benefits of cloud computing.](#)

Cloud benefits and limitations

- Google Cloud. (n.d.). [What is cloud computing?](#)

Ephemerality and cloud resources

- Google Cloud. (n.d.) [*The advantages of cloud computing.*](#)
- Google Cloud. (n.d.) [*Best practices for operating containers.*](#)
- IBM. (n.d.) [*What is cloud computing?*](#)

Virtualization and virtual machines

- Google Cloud. (n.d.) [*What is a virtual machine?*](#)
- IBM. (n.d.) [*What is virtualization?*](#)
- Infosec Institute. (2012, December). [*Virtualization security.*](#)
- Scarfone, K. (2011, January) [*Guide to security for all visualization technologies*](#) (Special Publication 800-125). National Institute of Standards and Technology.

Serverless computing

- Google Cloud. (n.d.). [*Cloud functions.*](#)
- Google Cloud. (n.d.). [*Serverless computing.*](#)
- Jonas, E., Schleier-Smith, J., Sreekanti, V., Tsai, C.-C., Khandelwal, A., Pu, Q., Shankar, V., Carreira, J., Krauth, K., Yadwadkar, N., Gonzalez, J. E., Popa, R. A., Stoica, I., & Patterson, D. A. (2019, February 9). [*Cloud programming simplified: A Berkeley view on serverless computing.*](#) Cornell University.

Containerization

- Buchanan, I. (n.d.) [*Containers vs. virtual machines.*](#) Atlassian.
- Docker. (n.d.) [*What is a container?*](#)
- Google Cloud. (n.d.) [*What are containers?*](#)
- Intel. (n.d.) [*Containers in the Cloud: An easier way to deploy workloads.*](#)

Cloud storage benefits

- Huang, C., Huang, L., Qin, Z., Yuan, H., Zhou, L., Varadharajan, V., & Kuo, C. (2014, May 23). [Survey on securing data storage in the cloud](#). APSIPA Transactions on Signal and Information Processing, 3, e7.
- IBM. (n.d.) [What is cloud storage?](#)
- Jones, M. T. (2010). [Anatomy of a cloud storage infrastructure](#). IBM developerWorks.
- Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). [A systematic review on cloud storage mechanisms concerning e-healthcare systems](#). *Sensors*, 20(18), 5392.

Types of storage in the cloud

- Google Cloud. (n.d.) [Buckets](#).
- Google Cloud. (n.d.) [What is object storage?](#)
- Harris, J. (2014, February 26). [Bridging the divide between unstructured and structured data](#). *Berkeley School of Information Blog*.
- IBM. (n.d.) [What is cloud storage?](#)

Google's storage options

- Google Cloud.(2024, January 17). [Storage classes](#).

Module 2: Security in the cloud

Resources

Controls that contribute to security depth

- [Google Cloud: NIST Cybersecurity Framework & Google Cloud](#)

Platform as a service

- [Google Cloud: What is Platform as a Service \(PaaS\)?](#)

Firewalls for network security

- [Google Cloud: Network controls in GCP vs. on-premises: Not so different after all](#)

Citations

Cloud defense in depth

- Envid, I., & Kiner, E. (2019, June 20). [Google Cloud networking in depth: Three defense-in-depth principles for securing your environment](#). *Google Cloud Blog*.
- Google Cloud. (2023, August). [Google security overview](#) [Whitepaper].
- Mahalkari, A., Tailor, A., & Shukla, A. (2016). [Cloud computing security, defense in depth detailed survey](#). *International Journal of Computer Science and Information Technologies*, 7(3), 1145-1151.
- Zhang, K., & Somani, Z. (2022, August 26). [How to avoid cloud misconfigurations and move towards continuous compliance](#). *Google Cloud Blog*.

Controls that contribute to security depth

- Google Cloud. (2020, April). [NIST Cybersecurity Framework & Google Cloud](#) [Whitepaper].

The shared responsibility model

- Alvarenga, G. (2022, November 14). [Shared responsibility model](#). CROWDSTRIKE.
- CloudPassage. (2020, August 26). [Shared responsibility model explained](#). *Industry Insights Blog*.
- Google Cloud. (2023, August 21). [Share responsibility and shared fate on Google Cloud](#).
- National Cyber Security Centre. (n.d.) [Cloud security guidance](#).
- Oracle. (n.d.). [What is cloud security?](#)

Shared responsibility challenges

- CloudPassage. (2020, August 26). [Shared responsibility model explained](#). *Industry Insights Blog*.
- Google Cloud. (2023, August 21). [Share responsibility and shared fate on Google Cloud](#).
- Kaczorowski, M. (2019, March 29). [Exploring container security: The shared responsibility model in GKE](#). *Google Cloud Blog*.

Shared responsibility and cloud migration

- Google Cloud. (2023, August 21). [Share responsibility and shared fate on Google Cloud](#).

The shared fate model

- Chuvakin, A., & Rosenblatt, S. (2023, March 22). [Lessons from the future: Why shared fate shows us a better cloud roadmap](#). *Google Cloud Blog*.
- Google Cloud. (2023, August 21). [Share responsibility and shared fate on Google Cloud](#).
- Google Cloud. (2023, August 31). [Landing zone design in Google Cloud](#).

An overview of IaaS, PaaS, and SaaS

- Cloudflare. (n.d.) [*What is identity as a service?*](#)
- Google Cloud. (n.d.). [*PaaS vs IaaS: What's the difference?*](#)
- Google Cloud. (n.d.). [*What is IaaS?*](#)
- Google Cloud. (n.d.). [*What is PaaS?*](#)
- Google Cloud. (2023, August 21). [*Share responsibility and shared fate on Google Cloud.*](#)
- National Cyber Security Centre. (n.d.). [*Cloud security shared responsibility model.*](#)

Infrastructure as a service

- Google Cloud. (n.d.). [*What is IaaS?*](#)
- Google Cloud. (2023, October 9). [*Migrate to Google Cloud.*](#)
- National Cyber Security Centre. (n.d.). [*Cloud security shared responsibility model.*](#)

Platform as a service

- Cloud Information Center. (n.d.). [*Platform as a service \(PaaS\).*](#)
- Google Cloud. (2023, August 21). [*Share responsibility and shared fate on Google Cloud.*](#)

Software as a service

- Google Cloud. (n.d.). [*Software as service \(SaaS\).*](#)
- Splunk. (2022, November 17) [*Shadow it.*](#)

IAM policies provide security depth

- Google Cloud. (2024, January 17). [IAM overview](#).
- Google Cloud. (2024, January 17). [Use IAM Securely](#).
- Okta. (2023, September 15). [What is LDAP & how does it work?](#)
- Red hat. (2022, June 3). [What is lightweight directory access protocol \(LDAP\) authentication?](#)

IAM in the cloud

- Google Cloud. (2023, August 8). [Manage identity and access](#).
- Google Cloud. (2024, January 17). [Service accounts overview](#).
- Google Cloud. (2024, January 17). [Workforce identity federation](#).

Explore the Google Cloud console

- Google Cloud. (n.d.). [Cloud identity](#).
- Google Cloud. (n.d.). [Cloud Identity](#) [Whitepaper].
- Google Cloud. (n.d.). [Google Cloud console](#).

Networking fundamentals

- Eisenbud, D.E., Yi, C, Contavalli, C, Smith, C, Kononov, R., Mann-Hielscher E., Cilingiroglu, A., Cheyney, B., Shang, W & Hosein, J.D. (n.d.). [Maglev: A fast and reliable software network load balancer](#). Google Inc., UCLA, SpaceX.
- Google Cloud. (2024, January 17). [Cloud Load Balancing overview](#).
- VMware. (n.d.). [What is software-defined networking \(Sdn\)?](#)

Firewalls for network security

- Google Cloud. (2024, January 17) [VPC firewall rules](#).
- Palo Alto Networks. (n.d.) [What is a firewall as a service?](#)
- Palo Alto Networks. (n.d.) [What is firewall as a service? What is a public cloud firewall?](#)

Key concepts of virtual private clouds

- Cloudflare. (n.d.) [What is a virtual private cloud \(VPC\)?](#)
- IBM. (n.d.). [What is a virtual private cloud \(VPC\)?](#).
- Kuehler, J & Mollison, G. (2018, October 3). [Network controls in GCP vs. on-premises: Not so different after all](#). *Google Cloud Blog*.
- Palo Alto Networks. (n.d.). [What is network segmentation?](#)

Module 3: The security lifecycle

Resources

Terraform as an IaC tool

- [HashiCorp: Resource Blocks](#)

Citations

An overview of DevSecOps

- Buchanan, I. (n.d.). [History of Devops](#). Atlassian.
- Cloud Security Alliance. (n.d.). [Devsecops](#).
- Sanders, G., Morrow, T., Richmond, N., & Woody, C. (2021). [Integrating zero trust and DevSecOps](#) [White paper]. Carnegie Mellon University, pp. 1-37.
- Software Engineering Institute. (n.d.). [DevSecOps](#). Carnegie Mellon University.

- Synopsys. (n.d.). [DevSecOps](#).

DevSecOps in action

- Department of Defense. (2021, September). [DevSecOps fundamental guidebook: DevSecOps tools & activities](#).
- Sanders, G., Morrow, T., Richmond, N., & Woody, C. (2021, July). [Integrating zero trust and DevSecOps](#) [White paper]. Carnegie Mellon University.

Software pipelines

- Lucidchart. (2017, November 2). [The pros and cons of waterfall methodology](#).
- Red Hat. (2022, May 11) [What is a CI/CD pipeline?](#)
- Synopsys Editorial Team. (2017, March 27). [Top 4 software development methodologies](#). Synopsys blog.

The CI/CD pipeline

- Amazon Web Services. (n.d.). [What is continuous delivery?](#)
- Gitlab. (n.d.) [What is CI/CD?](#)
- Google Cloud. (n.d.). [DevOps capabilities](#).
- Palo Alto Networks. (n.d.) [What is the CI/CD pipeline?](#)
- Red Hat. (2022, May 11) [What is a CI/CD pipeline?](#)

Software pipelines and Google's Cloud Build

- Google Cloud. (2024, January 17). [Overview of Cloud Build](#).

Introduction to the software supply chain

- Google Cloud. (2024, January 17) [Software supply chain security](#).

- Schmitt, J. (2023, June 26). [Software supply chain: What it is and how to keep it secure](#). *CircleCI Blog*.
- Temple-Raston, D. (2021, April 16). [A “worst nightmare” cyberattack: The untold story of the solarwinds hack](#). NPR.
- Williams, J. (2020, December 15). [What you need to know about the solarwinds supply-chain attack](#). *SANS Institute Blog*.

Levels of the software supply chain

- Google Cloud. (2024, January 17) [Artifact Registry overview](#).
- Google Cloud. (2024, January 22) [Software supply chain threats](#).
- SLSA. (n.d.). [SLSA specification](#).

Strengthen the supply chain with Software Delivery Shield

- Google Cloud. (n.d.). [Software delivery shield](#).
- Google Cloud. (2024, January 17). [Overview of Assured Open Source Software](#).
- McGrath, M. (2022, October 11). [Software Delivery Shield protects the software supply chain](#). *Google Cloud Blog*.

Infrastructure as code (IaC) in the cloud

- Gitlab. (n.d.) [What does infrastructure as code mean?](#)
- Klein, J., & Reynolds, D. (2018). [Infrastructure as code—Final report](#). Carnegie Mellon University.
- Kumara, I., Garriga, M., Romeu, A. U., Di Nucci, D., Palomba, F., Tamburri, D. A., & Van Den Heuvel, W. (2021). [The do's and don'ts of infrastructure code: A systematic gray literature review](#). *Information & Software Technology*.
- Palo Alto. (n.d.) [What is IaC security?](#)

An overview of policy as code

- HashiCorp. (n.d.) [Policy as code](#).
- Palo Alto. (n.d.) [What is Policy as Code?](#)
- Synopsys. (n.d.). [Policy-as-code](#).
- Zhang, X. (2023, April 7). [Realize policy-as-code with Pulumi through CrossGuard on Google Cloud](#). *Google Cloud Blog*.

Terraform as an IaC tool

- Google Cloud. (2024, January 17). [Deploy a basic Flask web server by using Terraform](#).
- Hashicorp. (n.d.). [What Is Infrastructure as Code with Terraform?](#)

IaC in the GitOps framework

- Gitlab. (n.d.) [Merge requests](#).
- Gitlab. (n.d.) [What is GitOps?](#)
- Neytchev, J. (n.d.) [GitOps with Prisma Cloud Code Security](#). Palo Alto.
- Red Hat. (2023, March 10). [What is GitOps?](#)
- Weaveworks (2021, July 13) [The history of GitOps](#).

Module 4: Cloud security analyst roles and responsibilities

Resources

Useful Google Cloud tools

- [Google Cloud: Cloud Functions documentation](#)
- [Google Cloud: Cloud Identity](#)
- [Google Cloud: Cloud Shell documentation](#)
- [Google Cloud: Compute Engine documentation](#)
- [Google Workspace: How teams of all sizes connect, create, and collaborate](#)

Introduction to artificial intelligence

- [Google Cloud: Generative AI examples](#)
- [Google Cloud: Introduction to Generative AI](#)

Guide to Virtual Private Cloud (VPC)

- [Google Cloud: gcloud compute networks](#)

Citations

Introduction to the cloud security analyst's role

- CompTIA. (2022, October). [Complete Guide to IT Risk Management](#).
- Cyber Threat Intelligence team. (n.d.). [What is cyber threat intelligence?](#) C/IS.
- National Institute of Standards and Technology. (2023, November 7). [NIST Risk Management Framework](#).

Cloud security analyst job responsibilities

- Google Cloud. (2024, January 18). [Security Command Center overview](#).

Core cloud security analyst responsibilities

- Kumar, A., Umurzoqovich, R. S., Duong, N. D., Kanani, P., Kuppusamy, A., Praneesh, M., & Hieu, M. N. (2022, November). [An intrusion identification and prevention for cloud computing: From the perspective of deep learning](#). *Optik*, 270, 170044.

The security ecosystem

- Google cloud. (n.d.). [Professional Cloud Security Engineer](#).
- Haller, K. (2022, May 18). [A cloud security architect's to-do list](#). Data Center Knowledge.
- Palo Alto Networks. (n.d.). [Cloud security is a shared responsibility](#).
- Strategy of Security. (n.d.). [Cybersecurity ecosystem](#).

Communicate with stakeholders

- Giallonardo, R. (2019, February 22). [Privacy and security in cloud computing](#). *Medium*.
- National Institute of Standards and Technology. (n.d.). [Stakeholder](#). Computer Security Resource Center.

Core skills for cloud cybersecurity analysts

- Cybersecurity Guide Contributors. (2023, October 23). [Become a security analyst: Skills and steps](#). Cybersecurity guide.

Common tools in the cloud analyst's toolkits

- Cloud Identity Help. (n.d.). [View VirusTotal reports from the investigation tool](#). Google.
- CompTIA. (n.d.). [What is Wireshark and how is it used?](#)
- Google. (n.d.). [reCaptcha: Tough on bots easy on humans](#).
- Hashicorp (n.d.). [Terraform](#).
- Lucidchart. (2018, July 17). [Improving your organization's web security testing](#).

Introduction to artificial intelligence

- Google Cloud. (n.d.). [What is artificial intelligence \(AI\)?](#)
- Google Cloud. (n.d.). [What is machine learning \(ML\)?](#)
- Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023, August 1). [From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy](#). *IEEE Access*, 11, 80218–80245.

Cloud Shell overview

- Google Cloud. (n.d.). [Cloud shell](#).
- Google Cloud. (2023, December 6). [gcloud compute networks subnets create](#).
- Google Cloud. (2024, January 17). [Cloud code for cloud shell limitations and restrictions](#).
- Google Cloud. (2024, January 18). [gcloud CLI overview](#).

Guide to Virtual Private Cloud (VPC)

- Google Cloud. (2023, October). [Global, regional, and zonal resources](#).
- Google Cloud. (2023, November). [Virtual Private Cloud \(VPC\) overview](#).

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](#)
- [QWIKlabs Help: Common problems with labs/lab troubleshooting](#)

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*](#).

Course 3 resources and citations

Module 1: Access control and identity management

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](#)
- [QWIKlabs Help: Common problems with labs/lab troubleshooting](#)

Guide to firewall rules

- [VPC firewall rules](#)
- [View logs by using the Logs Explorer](#)

Citations

Core principles of identity management

- Bhargav-Spantzel, A., Squicciarini, A.C., & Bertino, E. (2007). [Trust negotiation in identity management](#). *IEEE Security and Privacy Magazine*, 5(2), 55–63.
- Choudhary, S., & Singh, N. (2022). [Analysis of security-based access control models for cloud computing](#). *International Journal of Cloud Applications and Computing*, 12(1), 1–19.
- Kandukuri, B. R., Ramakrishna, P. V., & Rakshit, A. (2009). [Cloud security issues](#). 2009 IEEE International Conference on Services Computing.
- Le Luo Guan, Lin, J., Luo, B., Jing, J., & Wang, J. (2015). [Protecting private keys against memory disclosure attacks using hardware transactional memory](#). IEEE Symposium on Security and Privacy.
- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). [Security and Privacy Challenges in Cloud Computing Environments](#). *IEEE Security & Privacy*, 8(6), 24–31.
- White, G. L., Mediavilla, F. A. M., & Shah, J. R. (2011). [Information privacy](#). *International Journal of Information Security and Privacy*, 5(1), 50–66.

Uses for identity management measures

- Cloudflare Learning Center. (n.d.). [What is an identity provider \(IdP\)?](#) Cloudflare.
- Google Cloud. (2020, February 5). [Enforce uniform MFA to company-owned resources](#).
- Google Cloud (2024, January 22). [Access control best practices](#).
- Google Cloud. (2024, January 22). [Role-based access control \(RBAC\) overview](#).

- Google Cloud. (2024, January 22). [Role-based access control \(RBAC\) user guide](#).
- Google Cloud. (2023, February 27). [Single sign-on](#).
- Google Workspace Admin Help. (n.d.). [Security best practices for administrator accounts](#). Google.
- OneLogin. (n.d.). [SAML explained in plain english](#).
- Salstonstall, M., & Vergadia, P. (2021, February 8). [Security keys and zero trust](#). Google Cloud Blog.

Authentication, authorization and auditing (AAA)

- CISCO. (2023, February 2). [Compare TACACS + and RADIUS](#).
- Google Cloud. (2024, January 22). [Authenticate by using API keys](#).
- Lalchandani, N., Jiang, F., Jeong, J.J., Zolotavkin, Y., & Doss, R. (2021, December 21). [Evaluating the current state of application programming interfaces for verifiable credentials](#). 2021 18th International Conference on Privacy, Security and Trust (PST).
- Trnka M., Abdelfattah A.S., Shrestha A., Coffey M., & Cerny T. (2022, February 10) Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors (Basel)*, 22(4):1361. doi: 10.3390/s22041361.

Credential handling and service accounts

- Cisco Umbrella. (n.d.). [Cybersecurity threat trends report](#).
- Cloudflare. (n.d.). [What is mutual TLS \(mTLS\)?](#)
- Google Identity. (2023, November 7). [OAuth 2.0 for client-side web applications](#). Google for developers.
- IBM. (2022, December, 13). [OpenID Connect overview](#).
- OWASP. (n.d.). [Secrets management cheat sheet](#). OWASP Cheat Sheet Series.

Access controls in the cloud

- Amazon Web Services. (n.d.). [AWS Identity and Access Management](#).
- Ferraiolo, D. F., & Kuhn, R. (1992). [Role-based access controls](#). *15th National Computer Security Conference (1992)*, 554-563.
- Google Cloud. (n.d.). [Identity and Access Management documentation](#).
- Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2015, February). [Attribute-based access control](#). *Computer*, 48(2), 85-88.
- Joint Task Force. (2013, April). [Security and privacy controls for federal information systems and organizations](#) (Special Publication 800-53, Revision 4). National Institute of Standards and Technology.
- OpenVPN. (n.d.). [What is a VPN?](#)
- Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). [Role-based access control models](#). *Computer*, 29(2), 38-47.

Cloud access control in action

- Device42. (n.d.). [A guide to cloud asset management](#).
- Google Cloud. (n.d.). [VPC service controls](#).
- Google Cloud. (2024, January 22). [Access Context Manager overview](#).
- Google Cloud. (2024, January 22). [Access control overview](#).
- Google Cloud. (2024, January 22). [Compute Engine IAM roles and permissions](#).
- Google Cloud. (2024, January 22). [IAM basic and predefined roles reference](#).
- Google Cloud. (2024, January 22). [IAM overview](#).
- Google Cloud. (2024, January 22). [Introduction to the Organization Policy Service](#).
- Google Cloud. (2024, January 22). [Reauthenticating users](#).

- Google Cloud. (2024, January 22). [Shared VPC](#).
- Google Cloud. (2024, January 22). [Virtual Private Cloud \(VPC\) overview](#).
- Google Cloud. (2024, January 22). [VPC firewall rules](#).
- Kulkarni, S., Dixon, F., Nachmany, A., & Erukulla, R. (2023, February 10). [Access control review: Addressing challenges and ensuring compliance in cloud service consumers](#). Cloud Security Alliance.
- Mollison, G., & Hohpe, G. (2019, January 10). [Identity and authentication, the Google Cloud way](#). *Google Cloud Blog*.
- National Institute of Standards and Technology. (n.d.). [B.4 Authenticators and verifiers](#) (Special Publications 800-63B).
- National Security Agency. (2020, January 22). [Mitigating cloud vulnerabilities](#).
- OWASP. (2021). [A01:2021 – Broken Access Control](#). OWASP Top 10: 2021.

Perimeter protection

- Cloud Security Alliance. (2020). [CSA security guidance for critical areas of focus in cloud computing](#).
- Mell, P., & Grance, T. (2011, September). [The NIST definition of cloud computing](#) (Special Publication 800-145). National Institute of Standards and Technology.
- Meng, G., Liu, Y., Zhang, J., Pokluda, A., & Boutaba, R. (2015, July 22). [Collaborative security](#). *ACM Computing Surveys*, 48(1), 1-43.
- Scarfone, K., & Mell, P. (2007, February). [Guide to intrusion detection and prevention systems \(IDPS\)](#) (Special Publication 800-94). National Institute of Standards and Technology.
- Yasar, K., & Letkovich, B. (2018). [Firewall](#). TechTarget.

Trust boundaries

- Dotson, C. (2019, April 23). [Practical cloud security](#). O'Reilly.
- Google Cloud. (2024, January 22). [Configure firewall rules](#).
- Google Cloud. (2024, January 22). [VPC firewall rules](#).
- National Institute of Standards and Technology. (n.d.) [Cybersecurity Framework](#).
- National Institute of Standards and Technology. (2011). [Chapter 14: Cloud security essentials and architecture](#).
- O'Keefe, M. (2019, January 22). [Welcome to the service mesh era: Introducing a new Istio blog post series](#). *Google Cloud Blog*.
- OWASP. (n.d.). [OWASP risk assessment framework](#).
- Peacock, T., & Chuvakin, A. (2023, May 22). [How to implement trust boundaries for access control](#) (122) [Audio podcast]. Cloud Security Podcast.

Guide to firewall rules

- Google Cloud. (2024, January 22). [Firewall Rules Logging](#).
- Google Cloud. (2024, January 22). [Virtual Private Cloud \(VPC\) overview](#).
- Google Cloud. (2024, January 22). [VPC Flow Logs](#).

Common attack vectors

- Chen, T. M., & Abu-Nimeh, S. (2011, April). [Lessons from Stuxnet](#). *Computer*, 44(4), 91-93.
- Mirkovic, J., & Reiher, P. (2004). [A taxonomy of DDoS attack and DDoS defense mechanisms](#). *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.
- Scarfone, K., & Mell, P. (2007, February). [Guide to intrusion detection and prevention systems \(IDPS\)](#) (Special Publication, pp. 800-94). National Institute of Standards and Technology.

- Stallings, W. (2017). *Network security essentials: Applications and standards (6th ed.)*. Pearson.
- Symantec. (2019, February). [Internet security threat report \(ISTR\)](#). Vol. 24.

Zero trust

- Cybersecurity Action Team. (2022, March). [Applying the NCSC zero trust principles on Google Cloud](#) [Whitepaper]. Google Cloud.
- Grance, T., & Jansen, W. (2011, December 9). [Guidelines on security and privacy in public cloud computing](#) (Special Publication 800-144). National Institute of Standards and Technology.
- Palo Alto Networks. (n.d.). [What is a zero trust architecture](#).
- Pratt, M. (2023, March 7). [What is zero trust? A model for more effective security](#). CSO Online.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August). [Zero trust architecture](#) (Special Publication 800-207). National Institute of Standards and Technology.
- Vigliarolo, B. (2020, May 29). [Zero trust security: A cheat sheet](#). TechRepublic.

Zero trust policies and complementary controls

- CrowdStrike. (n.d.). [CrowdStrike Zero Trust](#).
- Forrester. (n.d.). [Revolutionize your security with Forrester's zero trust model](#).
- Gartner. (n.d.). [Implementing zero trust security in the public sector](#).
- Google Cloud. (n.d.). [What is zero trust?](#)
- Google Cloud. (2024, January 22). [Create and manage access control lists \(ACLs\)](#).
- Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020). [Zero trust architecture](#) (Special Publication 800-207). National Institute of Standards and Technology.

- Wired. (n.d.). [The future of trust starts with “zero”](#).

Core principles of identity management

- Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2007). [Trust negotiation in identity management](#). *IEEE Security and Privacy Magazine*, 5(2), 55-63.
- Choudhary, S., & Singh, N. (2022). [Analysis of security-based access control models for cloud computing](#). *International Journal of Cloud Applications and Computing*, 12(1), 1-19.
- Kandukuri, B. R., Ramakrishna, P. V., & Rakshit, A. (2009). [Cloud security issues](#). 2009 IEEE International Conference on Services Computing.
- Le Luo Guan, Lin, J., Luo, B., Jing, J., & Wang, J. (2015). [Protecting private keys against memory disclosure attacks using hardware transactional memory](#). IEEE Symposium on Security and Privacy.
- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). [Security and privacy challenges in cloud computing environments](#). *IEEE Security and Privacy Magazine*, 8(6), 24-31.
- White, G. L., Mediavilla, F. A. M., & Shah, J. R. (2011). [Information privacy](#). *International Journal of Information Security and Privacy*, 5(1), 50-66.

Module 2: Threat and vulnerability management

Citations

Introduction to threat management

- IBM. (n.d.). [Cybersecurity services](#).
- National Cybersecurity Alliance. (n.d.). [CyberSecure My Business](#).
- National Institute of Standards and Technology. (2018, April 16). [Framework for improving critical infrastructure cybersecurity](#).

- Verizon. (2020). [2020 data breach investigations report](#).

Threat and vulnerability management assessments

- Alvarenga, G. (2022, January 11). [What is a cloud security assessment?](#) Crowdstrike.
- Haber, M.J. (2022, September 16). [How to solve complex cloud security problems with AI](#). Cloud Security Alliance.

Asset and resource management

- Center for Internet Security. (n.d.). [CIS Critical Security Control 1: Inventory and control of enterprise assets](#).
- Gartner. (n.d.). [IT asset management \(ITAM\)](#). Gartner Glossary.
- National Institute of Standards and Technology. (2018, April 16). [Framework for improving critical infrastructure cybersecurity](#).
- SANS Institute. (2023, June 9). [CIS Controls v8](#).

Steps for asset management

- Alonso, J., Orue-Echevarria, L., Casola, V., Torre, A.I., Huarte, M., Osaba, E., & Lobo, J.L. (2023, January 12). [Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review](#). *Journal of Cloud Computing*, 12(6).
- Google Cloud. (n.d.). [Cloud Asset Inventory](#).
- Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017, April 22). [A risk management framework for cloud migration decision support](#). *Journal of Risk and Financial Management*, 10(2), 10.
- National Institute of Standards and Technology. (2018, April 16). [Framework for improving critical infrastructure cybersecurity](#).

On-the-job asset management applications

- Archer, D. (2023, July 12). [The importance of effective asset management in today's cloud environment](#). *CPO Magazine*.
- Device 42. (n.d.). [A guide to cloud asset management](#).
- Google Cloud. (n.d.). [Identity and access management documentation](#).
- Google Cloud. (2023, August 4). [Manage your assets](#).
- Google Cloud. (2024, January 22). [Introduction to Cloud Asset Inventory](#).
- Google Cloud. (2024, January 22). [Review and apply role recommendations for projects, folders, and organizations](#).
- Hitachi Vantara. (n.d.). [What is cloud access management \(CAM\)?](#)
- IBM Cloud Education. (2022, May 6). [What is IT asset management \(ITAM\)?](#) *IBM Blog*.
- Smart, E. (2023, January 10). [Why asset management is crucial for cyber teams in 2023](#). appNovi.
- Rossi, E. (2022, December 21). [Introducing cybersecurity asset management](#). *Qualys Security Blog*.

Vulnerability remediation and posture management

- Almorsy, M., Grundy, J., & Müller, I. (2016, September 5). [An analysis of the cloud computing security problem](#). Cornell University.
- Cloud Security Alliance. (2017, July 26). [Security guidance for critical areas of focus in cloud computing v4.0](#).
- Mell, P., & Grance, T. (2011). [The NIST definition of cloud computing](#) (Special Publication 800-145). National Institute of Standards and Technology.

- Zissis, D., & Lekkas, D. (2012, March). [Addressing cloud computing security issues](#). *Future Generation Computer Systems*, 28(3), 583-592.

Vulnerability remediation and posture management in software development

- Cloud Security Alliance. (2017, July 26). [Security guidance for critical areas of focus in cloud computing v4.0](#).
- National Institute of Standards and Technology. (2018, April 16). [Framework for improving critical infrastructure cybersecurity](#).
- OWASP. (n.d.). [OWASP top ten](#).
- Scarfone, K., & Souppaya, M. (2013, July). [Guide to enterprise patch management technologies](#) (Special Publication 800-40 Revision 3). National Institute of Standards and Technology.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Boston, MA: Cengage Learning.
- Zalewski, M. (2017). *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks*. San Francisco, CA: No Starch Press.

Posture management tools and techniques

- Farber, S. (2022, August 2). [Mastering data security posture management: A practical guide to DSPM](#). Dig Security.
- Gillis, A.S. (2023, July). [Cloud security posture management \(CSPM\)](#). TechTarget.
- Murphy, T., & Smith, S. (2022, May 6). [Know your cloud security acronyms: An overview of CWPP, CSPM, CIEM, and CNAPP](#). Orca Security Blog.
- Puzas, D. (2023, April 17). [What is cloud security posture management \(CSPM\)?](#) CrowdStrike.

- Smith, A. (2023, May 3). [Top takeaways from the Gartner innovation insight: Data security posture management](#). *Laminar Security Blog*.
- Snyk. (n.d.). [4 steps of the vulnerability remediation process](#).
- Van der Vaart, L. (2021, June 10). [7 steps to improve your cloud security posture management](#). *VMware Cloud Blog*.

IT automation tools for posture management

- Ansible. (n.d.). [Ansible community documentation](#).
- Ansible Galaxy. (n.d.). [Welcome to Galaxy](#).
- Fowler, M. (2010, March 1). [Blue green deployment](#).
- Humble, J., & Farley, D. (2015). *Continuous delivery: Reliable software releases through build, test, and Deployment Automation*. Addison-Wesley.
- Puppet. (n.d.). [Explore product documentation](#).
- Puppet Forge. (n.d.). [Welcome to Puppet Forge](#).
- Red Hat. (n.d.). [Red Hat Ansible Automation Platform](#).

IT automation tools for security configuration management

- Cybersecurity & Infrastructure Security Agency (n.d.) [Secure by design](#).
- Donahue, P.R., & Connolly, E. (2023, April 20). [Secure by default: Recommendations from the CISA's newest guide, and how Cloudflare follows these principles to keep you secure](#). *The Cloudflare Blog*.
- Gillis, A.S. (2023, July). [Cloud security posture management \(CSPM\)](#). TechTarget.
- Moline, J. (2023, June 23). [What is SCM \(security configuration management\)?](#) Tripwire.
- National Institute of Standards and Technology. (n.d.) [Security configuration management \(SecCM\)](#). Computer Security Resource Center.

- Souppaya, M. & Scarfone, K. (2022, April). [*Guide to enterprise patch management planning: Preventive maintenance for technology*](#) (Special Publication 800-40r4). National Institute of Standards and Technology.

Guide to web application security scanning

- Google Cloud. (2024, January 22). [*Setting up custom scans using Web Security Scanner*](#).
- Hitachi Vantara. (n.d.). [*What is cloud access management \(CAM\)?*](#)

Patching and rehydration

- Antonopoulos, N., Gillam, L., & Springerlink Online Service. (2017). *Cloud Computing : Principles, Systems and Applications*. Springer International Publishing.
- Chapple, M., & Seidl, D. (2021). *CompTIA Security+ SY0-601 Exam Cram (6th ed.)*. Pearson IT Certification.
- Hashizume, K., Rosado, D.G., Fernández-Medina, E., & Fernandez, E.B. (2013, February 27). [*An analysis of security issues for cloud computing*](#). *Journal of Internet Services and Applications*, 4(5).
- Modi, C., Patel, D., Borisaniya, B., Patel, H., & Rajarajan, M. (2013, January). [*A survey of intrusion detection techniques in Cloud*](#). *Journal of Network and Computer Applications*, 36(1), 42-57.
- Singh, S., Jeong, Y. S., & Park, J. H. (2016, November). [*A survey on cloud computing security: Issues, threats, and solutions*](#). *Journal of Network and Computer Applications*, 75, 200-222.
- Zhang, Q., Cheng, L., & Boutaba, R. (2010, April 20). [*Cloud computing: State-of-the-art and research challenges*](#). *Journal of Internet Services and Applications*, 1, 7-18.

Compare and contrast: Patching and rehydration

- Balalaie, A., Heydarnoori, A., & Jamshidi, P. (2016). [Microservices architecture enables devops: Migration to a cloud-native architecture](#). *IEEE Software*, 33(3), 42–52.
- Google Cloud. (2023, February 28). [Best practices for operating containers](#).
- Leitner, P., Wittern, E., Spillner, J., & Hummer, W. (2019, March). [A mixed-method empirical study of Function-as-a-Service software development in industrial practice](#). *Journal of Systems and Software*, 149, 340–359.

Rehydration keeps systems up-to-date

- Google Cloud. (2023, May 8) [Best practices and reference architectures for VPC design](#).
- Google Cloud. (2024, January 26) [Overview of Web Security Scanner](#).
- Myres Training. (n.d.). [What is rehydration in AWS](#).
- Scappman. (2022, August 5). [Top 5 challenges of patch management](#).

Trends in vulnerability and threat management

- Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016, March). [Integration of cloud computing and Internet of Things: A survey](#). *Future Generation Computer Systems*, 56, 684–700.
- Buczak, A. L., & Guven, E. (2016). [A survey of data mining and machine learning methods for cybersecurity intrusion detection](#). *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
- Costello, K. & Rimol, N. (2020, October 19). [Gartner identifies the top strategic technology trends for 2021](#). Gartner.
- Gai, K., Qiu, M., & Sun, X. (2018, February). [A survey on FinTech](#). *Journal of Network and Computer Applications*, 103, 262–273.

- Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A., & Khan, S.U. (2015, January). [The rise of “big data” on cloud computing: Review and open research issues](#). *Information Systems*, 47, 98-115.
- Li, Z., Xu, K., Wang, H., Zhao, Y., Wang, X., & Shen, M. (2019, May 30). [Machine-learning-based positioning: A survey and future directions](#). *IEEE Network*, 33(3), 96-101.
- Pan, J. & McElhannon, J. (2018, February). [Future edge cloud and edge computing for Internet of Things applications](#). *IEEE Internet of Things Journal*, 5(1), 439-449.

Trends in security: Artificial Intelligence (AI), machine learning (ML), and Internet of things (IoT)

- Cisco. (n.d.). [What Is Device Security?](#)
- Corde, C. & Lichtenstein, S. (2023, April 24). [Introducing AI-powered investigation in Chronicle Security Operations](#). *Google Cloud Blog*.
- Google Cloud. (n.d.). [What is artificial intelligence \(AI\)?](#)
- IBM. (n.d.). [What is SOAR?](#)
- Oracle. (n.d.). [What is IoT?](#)
- Potti, S. (2023, April 24). [Supercharging security with generative AI](#). *Google Cloud Blog*.
- Roeckl, A. (2022, September 23). [What is Internet of Things \(IoT\) security?](#) CrowdStrike.
- Segal, E. (2020, March 31). [The impact of AI on cybersecurity](#). IEEE Computer Society.

Reports and assessments for threat and vulnerability management

- Assante, M.J. & Lee, R.M. (2015, October 5). [The industrial control system cyber kill chain](#) [White Paper]. SANS Institute.
- National Institute of Standards and Technology. (2018, April 16). [Framework for improving critical infrastructure cybersecurity](#).

Module 3: Resilience and stability in cloud computing

Resources

Guide to automating deployment with Terraform

- [HashiCorp: Terraform Language Documentation](#)
- [HashiCorp: Google Cloud Platform provider](#)
- [GitHub: HCL Native Syntax Specification](#)

Citations

Cloud-native design and architecture principles

- Google Cloud (2023, February 28). [Best practices for operating containers](#).
- Google Cloud (2023, November 13) [Manage traffic and load for your workloads in Google Cloud](#).
- Google Cloud (2024, January 26) [Managing infrastructure as code with Terraform, Cloud Build, and GitOps](#).
- Grey, T. (2019, June 19). [5 principles for cloud-native architecture – What it is and how to master it](#). *Google Cloud Blog*.
- Intel (n.d.). [What is cloud automation?](#)
- Jones, C. (2022, February 1). [What does “Cloud Managed Services” even mean?](#) Red River.
- Palmore, M.K. & Holmes, W. (2022, April 13) [The journey to the cloud mitigates enterprise risk](#). *Google Cloud Blog*.
- Red Hat (2022, May 11). [What is open source software?](#)
- Red Hat (2023, December 21). [Stateful vs. stateless](#).

- Security Compass (2021, September 16). [How can you identify your internet-facing applications?](#)

Cloud-native architecture for security

- Google Cloud (2023, August 21). [Shared responsibilities and shared fate on Google Cloud.](#)
- Hughes, C.(2021, June 20). [The shared responsibility model explained and what it means for cloud security.](#) CSO.
- Kubernetes (2023, September 7). [Overview of cloud native security.](#)
- Tasleem, S. & Vijayaraghavulu, P. (2020, October). [A multi-level security mechanism for cloud storage system.](#) *International Journal of Innovative Research in Technology*, 7(5), 140-148.

TTL policies and expiration

- Google Cloud. (2024, January 26) [Manage data retention with TTL policies.](#)
- Google Cloud. (2024, January 26) [Time to live \(TTL\) overview.](#)
- Scylla. (n.d.). [Time to live \(TTL\) value.](#)

Introduction to ephemerality and immutability

- Aima, A. (2020, February 5). [Storage options in Google Cloud Platform - Rundown.](#) *DataDrivenInvestor*.
- Cyral Inc. (n.d.). [Immutability for cloud infrastructure \(and for turning pets into cattle\).](#) *Cyral Inc Blog*.
- Dadgar, A. (2018, November 15) [What is mutable vs. immutable infrastructure?](#) HashiCorp.
- Google Cloud (2024, January 26). [Create short-lived credentials for a service account.](#)

- Moore, M. (2022, April 12). [The principle of ephemerality](#). Chainguard.
- Peacock, T., & Chuvakin, A. (Host). (2022, May 31). [Cyber defense matrix and does cloud security have to DIE to win?](#) (67)[Audio podcast episode]. Cloud Security Podcast.
- Posey, B. (2021, June 9). [How immutable object storage can help protect data](#). TechTarget.

Automation in cloud security

- HashiCorp (n.d.). [Configuration syntax](#).
- Hashicorp (n.d.) [Initialize Terraform configuration](#).
- Intel. (n.d.). [What is cloud automation?](#)
- Rajasekar, P. (2022, August 3). [Why automation and scalability are the most important traits of your Kubernetes platform](#). Google Cloud Blog.
- Red Hat. (2022, July 25). [What is cloud automation?](#)

Infrastructure as code, policy as code, and DevSecOps

- Buchanan, I. (n.d.). [Infrastructure as code - How infrastructure as code manages complex infrastructure](#). Atlassian.
- Clegg, T. (2022, March 25). [GUIs, CLI, APIs: Learn basic terms of infrastructure-as-code](#). The New Stack.
- IBM (n.d.) [What is IT infrastructure?](#)
- Karam, T. (2022, January 19). [Securing DevOps: The ABCs of security-as-code](#). Cloud Security Alliance Blog.
- Lee, B. (2020, February 21). [Using Open Policy Agent \(OPA\) to develop policy as code for cloud infrastructure](#). Cloud Security Alliance Blog.

- National Institute of Standards and Technology (n.d.) [Application programming interface \(API\)](#). Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.) [Infrastructure as code](#). Computer Security Resource Center.
- Paloalto Networks (n.d.). [What is policy-as-code?](#)
- Red Hat (2022, May 11). [What is infrastructure as code \(IaC\)?](#)
- Tech at GSA. (n.d.) [Building a DevSecOps culture - from a technical perspective](#).
- Wilson, B. (2023, March 14). [Infrastructure as code vs. configuration management vs. infrastructure provisioning](#). DevOps Cube.
- Zhang, X. (2023, April 7). [Realize policy-as-code with Pulumi through CrossGuard on Google Cloud](#). Google Cloud Blog.

Automation to improve cloud security efficiency

- Bigelow, S.J. & Montgomery J. (2021, July). [Cloud automation](#). TechTarget.
- Ghanizada, I. (2022, December 9). [IT prediction: the vast majority of security operations workloads will be automated](#). Google Cloud Blog.
- Ghanizada, I. & Chuvakin, A. (n.d.) [Autonomic security operations: 10x transformation of the Security Operations Center](#). Google Cloud.
- Martinez, R., & Shin, P. (2023, January 20). [Building an automated serverless deployment pipeline with Cloud Build](#). Google Cloud Blog.
- Shackleford, D. (2021, January 29). [4 steps toward cloud security automation](#). TechTarget.

AI and automation in security

- Barret, C., Boyd, B., Burzstein, E., Carlini, N., Chen, B., Choi, J., Chowdhury, A.R., Christodorescu, M., Datta, A., Feizi, S., Fisher, K., Hashimoto, T., Hendrycks, D., Jha, S., Kang, D., Kerschbaum, F., Mitchell, E., Mitchell, J., Ramzan, Z., ... Yang, D. (2023, December 29). [Identifying and mitigating the security risks of generative AI](#).
- Boutin, Chad. (2022, March 16). [There's more to AI bias than biased data](#). National Institute of Standards and Technology.
- Dhoni, P., & Kumar, R. (2023, August 18). [Synergizing generative AI and cybersecurity: Roles of generative AI entities, companies, agencies, and government in enhancing cybersecurity](#). TechRxiv.
- IBM Data and AI team. (2023, October 16). [Shedding light on AI bias with real world examples](#). IBM Blog.
- Pothukuchi, A.S., Kota, L.V., & Mallikarjunaradhya, V. (2023, August 8). [Impact of generative AI on the software development lifecycle \(SDLC\)](#). International Journal of Creative Research Thoughts, 11(8).

Infrastructure as code and cloud-native security

- Ferrari, M., & Glissmann, J. (2019, April 5). [Want repeatable scale? Adopt infrastructure as code on GCP](#). Google Cloud Blog.
- Google Cloud. (2024, January 26). [Using recommendations for infrastructure as code](#).
- Hughes, C. (2021, July 8). [Securing infrastructure as code: Perils and best practices](#). CSO.
- OWASP. (n.d.). [Infrastructure as code security cheatsheet](#). OWASP Cheat Sheet Series.
- Stevens, A. (2021, November 11). [Automating Cloud Security](#). Infosecurity Magazine.
- Zamot, M. (2019, July 1). [How to use infrastructure as code](#). OpenSource.

Benefits of policy as code

- Hashimoto, M., & Dadgar, A. (2020, January 6). [How policy as code imbues DevOps with speed & protection](#). Hashicorp.
- Paloalto. (n.d.). [What is policy as code?](#)
- Pathak, A. (2024, January 2). [Policy-as-code: How to understand and implement it in 2024](#). Geekflare.
- Sebek, M. (2022, March 31). [7 benefits of policy as code](#). Progress Chef Blog.

Terraform for IaC management

- Chen, M. (2022, June 20) [The 3 phases of infrastructure automation](#). HashiCorp Blog.
- Clegg, T. (2023, June 8). [Securing your multi-cloud Terraform pipelines with policy-as-code](#). Pluralsight Blog.
- IBM (n.d.). [What is Terraform?](#)
- Kosaka, G. (2021, April 17). [An introduction to secure infrastructure as code \(IaC\) using Terraform](#). SUSE Blog.
- Morris, K. (2021, January 19). [Infrastructure as Code, 2nd Edition](#). O'Reilly.
- Oracle. (2022, May 10). [What is Infrastructure as Code \(IaC\)?](#) Developer Resource Center.
- Red Hat (2022, May 11). [What is infrastructure as code \(IaC\)?](#)
- Ruddy, K. (2020, June 29). [Managing policy as code with Terraform and Sentinel](#). Hashicorp.
- Terraform (n.d.) [Policies API](#). Hashicorp.
- Terraform (n.d.) [Policy enforcement](#). Hashicorp.
- Terraform (n.d.). [State](#). Hashicorp.

- Terraform (n.d.). [The core Terraform workflow](#). Hashicorp.
- Szymanski, S. (2023, October 12). [What are Terraform modules and how to use them: Tutorial](#). Spacelift Blog.

Terraform and cloud security automation

- Google Cloud. (2023, December 20). [Enterprise foundations blueprint](#).
- Google Cloud. (2024, January 26). [Best practices for using Terraform](#).
- Martinez, R. (2021, November 29) [Getting started with the security foundations blueprint automation repo](#). Google Cloud Blog.
- Matharu, Y. & Coulter, T. (2022, December 16). [Introduction to policy as code with automation](#). Red Hat.
- Terraform (n.d.) [Policies and policy sets](#). Hashicorp.
- Terraform (n.d.) [Policy enforcement](#). Hashicorp.
- Terraform (n.d.) [Running Terraform in automation](#). Hashicorp.
- Terraform (n.d.) [Terraform cloud security model](#). Hashicorp.
- Terraform (n.d.) [What is Terraform?](#) Hashicorp.

Guide to automating deployment with Terraform

- Isla, D. (2018, October 31). [GoogleCloudPlatform/terraform-google-examples](#). Github.
- Terraform. (n.d.). [What is Terraform?](#) HashiCorp.

Containers vs. virtual machines

- Google Cloud (n.d.) [What are containers?](#)
- Google Cloud (n.d.). [What is a virtual machine?](#)
- Intel (n.d.) [Containers and the cloud: An easier way to deploy workloads](#).

- VMware (n.d.). [What is a hypervisor?](#)

A brief guide to containers

- Google Cloud (n.d.). [Containers vs VMs.](#)
- Google Cloud (n.d.). [What are containers?](#)
- Google Cloud (2024, January 26). [Deploy an app in a container image to a GKE cluster.](#)

Containers' importance in cloud

- Dhaduk, H. (2022, May 26). [14 containerization use cases: Hit a home run with containers.](#) *Simform Blog*.
- Google Cloud (n.d.). [Containers vs VMs.](#)
- Google Cloud (n.d.). [What are containers?](#)
- Google Cloud (n.d.). [What is microservices architecture?](#)

Container benefits and considerations

- Awan, A. (2019, August 5). [Security concerns around rapid container growth.](#) *The New Stack*.
- Despoudis, T. (2019, June 14). [How to lock down the kernel to secure the container.](#) *The New Stack*.
- Docker (n.d.). [About storage drivers.](#)
- Docker (n.d.). [Multi container apps.](#)
- Docker (n.d.). [Docker manifest.](#)
- Flockport (n.d.). [Understanding layers and containers.](#)
- Google Cloud (2023, February 28). [Best practices for building containers.](#)
- Google Cloud (n.d.). [What are containers?](#)

- Kumar, A. (2023, October 19). [Multi container pods in Kubernetes](#). K21 Academy.
- National Institute of Standards and Technology (n.d.) [Container runtime](#). Computer Security Resource Center.
- Nvidia docs hub. (n.d.). [Preparing to use Docker containers](#).
- Red Hat (2022, May 11). [What is a Linux container?](#)
- Rice, L. (2020, May 12). [Container Security: Chapter 1](#). O'Reilly.
- Sanche, D. (2018, January 2). [Kubernetes 101: Pods, nodes, containers, and clusters](#). Google Cloud – Community.
- The Hacker News. (2022, May 23). [Yes, containers are terrific, but watch the security risks](#).
- Ubuntu Manuals. (2019). [Focal \(1\): Containers storage](#).
- Velayudhan, N. (2021, September 1). [What are container runtimes?](#) Opensource.
- [x]cube LABS (2023, February 23). [The advantages and disadvantages of containers](#).

Techniques to secure containers

- Google Cloud. (2023, February 28). [Best practices for building containers](#).
- Kaczorowski, M. (2018, March 29). [Exploring container security: An overview](#). Google Cloud Blog.
- Google Cloud (n.d.) [What are containers?](#)
- Google Cloud (n.d.). [What is Kubernetes?](#)
- IBM (n.d.). [What are containers?](#)
- National Institute of Standards and Technology. (n.d.) [Role-based access control \(RBAC\)](#). Computer Security Resource Center.

- Paloalto. (n.d.). [What is container security?](#)
- Red Hat (2021, September 10). [A layered approach to container and kubernetes security](#) [Whitepaper].
- Red Hat (2023, April 6). [Understanding containers.](#)
- Souppaya, M., Morello, J., & Scarfone, K. (2017, September). [Application container security guide](#) (Special Publication 800-190). National Institute of Standards and Technology.
- VMware (2022). [10 things you must do to secure containers now.](#)
- VMWare (n.d.). [What is Kubernetes security?](#)
- Wright, L. (n.d.). [Examples of managed services.](#) Core Blog.

Container drift

- Fruhlinger, J. (2022, July 19). [What is an SBOM? Software bill of materials explained.](#) CSO Online.
- Lehmann, T. & Rosenblatt, S. (2022, June 23). [How SLSA and SBOM can help healthcare's cybersecurity resiliency.](#) Google Cloud Blog.
- Howe, R. (2023, March 22). [Container drift: Where age isn't just a number.](#) Security Intelligence.
- Kellermann, M. (n.d.). [The Dirty Pipe vulnerability.](#) M4All.
- Korren, T. (2020, March 19). [Blocking attacks in runtime with drift prevention.](#) Aquqasec Blog.
- Losh, C. (2021, August 26). [Detect container drift in your Kubernetes deployments.](#) Trend Micro.
- Nwankwo, E. (2022, October 4). [Drift Detection.](#) Palo Alto live Community Blog.

- Pelletier, J. (2021, May 18). [Configuration drift in Kubernetes - What it is and why it matters](#). *Fairwinds Blog*.
- Sysdig. (n.d.). [Managing container security with container scanning and more](#).
- The Linux Foundation. (2021, June 15). [What is an SBOM?](#)
- Toulas, B. (2022, November 24). [Docker Hub repositories hide over 1.650 malicious containers](#). *Bleeping Computer*.

Security in containers

- Donston-Miller, D. (2021, August 24). [Containers vs. virtual machines: Why you don't always have to choose](#). *Red Hat*.
- Google Cloud (n.d.). [Containers vs. VMs](#).
- Guo, J. (2017, August 9). [Demystifying container vs. VM-based security: Security in plaintext](#). *Google Cloud Blog*.
- Iradier, Á. (2021, October 14). [Container security best practices: Comprehensive guide](#). *Sysdig Blog*.
- Kaczorowski, M. (2018, March 29). [Exploring container security: An overview](#). *Google Cloud Blog*.
- Kubernetes. (2023, August 24). [Using RBAC authorization](#).
- Kubernetes. (2023, November 3). [User namespaces](#).
- Lidder, U. (2023, July 19). [Enhancing cloud security: Four vital practices for Kubernetes security](#). *Cloud Security Alliance Blog*.
- Sheps, A. (2023). [What is container security?](#) *Cloud Native Wiki*.
- Security Guidance Working Group. (2021, August 19). [Five recommendations for securing cloud containers](#). *Cloud Security Alliance Blog*.

- The Google Cloud content marketing team. (2021, May 23). [Cloud computing 101: Frequently asked questions](#). *Google Cloud Blog*.
- OWASP (n.d.). [OWASP DevSecOps Guideline – v-0.2](#).
- Scanlon, T. & Laughlin, R. (2020, April 6). [7 quick steps to using containers securely](#). *SEI Blog, Carnegie Mellon University*.

Serverless functions and security

- Cloudflare (n.d.). [Serverless computing vs. containers – How to choose](#).
- Hamerman, O. (2023, February 9). [Containers and serverless – Rivals or cohorts?](#) *InfoQ*.
- Jacques, N. (2021, March 16). [A guide to serverless functions and how to deploy them](#). *SitePoint*.
- Khani, A. (2021, March 11). [Multi-cloud security best practices for serverless functions](#). *VMware Blog, Broadcom*.
- Mayaan, G.D. (2022, January 3). [The basics of serverless user authentication](#). *Cloud Native Now*.
- Red Hat (2022, May 11). [What is serverless?](#)
- Watts, S. (2023, July 10). [The serverless functions beginner's guide](#). *Splunk Blog*.

Container orchestration

- Beda, J. (2015, January 22). [What makes a container cluster?](#) *Google Cloud Platform Blog, Google*.
- Gilbert, C. (2019, September 4). [5 Kubernetes RBAC mistakes you must avoid](#). *Red Hat Blog*.
- Google Cloud. (n.d.) [What is container orchestration?](#)
- IBM (n.d.) [What is container orchestration?](#)

- Magnezi, K. (2020, July 15). [GKE best practices: Designing and building highly available clusters](#). *Google Cloud Blog*.
- McCune, R. (n.d.). [Container orchestration is key. What your security team needs to know](#). *Tech Beacon*.
- Opentext (n.d.). [What is policy orchestration?](#)
- Red Hat (2021, June 22). [What is Kubernetes role-based access control \(RBAC\)?](#)
- Red Hat (2022, May 10). [What is container orchestration?](#)
- Red Hat (2022, October 10). [What is high availability and disaster recovery for containers?](#)
- Sysdig. (n.d.). [Designing a secure container orchestration and containerized architecture strategy](#).
- Tolety, K. (2022, April 22). [Building Kubernetes high availability clusters: Easy guide 101](#). *Hevodata*.
- Velimirovic, A. (2021, December 9). [Orchestration vs. automation: Overlapping, but different IT concepts](#). *phoenixNAP Blog*.
- VMware (n.d.). [What are Kubernetes pods?](#)
- VMware (n.d.). [What is container orchestration?](#) *Broadcom*.
- VMware (n.d.). [What is Kubernetes Security?](#) *Broadcom*.

Module 4: Data protection and privacy

Citations

Introduction to the three states of data

- Cloudflare (n.d.). [What happens in a TLS handshake? / SSL handshake](#).
- Confidential Computing Consortium (n.d.). [About the Confidential Computing Consortium](#).
- Fitzgibbons, L. (2019, February). [Data in use](#). TechTarget.
- Google Cloud (n.d.). [Confidential VM documentation](#).
- Google Cloud (2022, September). [Default encryption at rest](#).
- Google Cloud (2022, September). [Encryption in transit](#) [Whitepaper].
- IBM (n.d.). [What is confidential computing?](#)
- Inpher (n.d.). [What is fully homomorphic encryption?](#)
- Rjaibi, W. (2022, April 18). [The next frontier for data security: Protecting data in use](#). *Security Intelligence*.
- SSL Support Team. (2023, June 12). [Private and public keys](#). SSL.

Data encryption

- Google Cloud. (n.d.). [What is encryption?](#)
- Google Cloud (2022, September) [Encryption in transit](#) [Whitepaper].
- Kong, J.H., Ang, L.M., & Seng, K.P. (2015, March). [A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments](#). *Journal of Network and Computer Applications*, 49, 15-50.
- Mouha, N. (2021, July). [Review of the advanced encryption standard](#) (Internal report 8319). National Institute of Standards and Technology.

- National Institute of Standards and Security. (2023, February 6). [Elliptic curve cryptography](#). Computer Security Resource center.
- Rimkienė, R. (2023, November 15). [What is AES encryption and how does it work?](#) Cyber News.
- Tyson, M. (2022, February 24). [Understand the RSA encryption algorithm](#). Infoworld.

Data encryption at rest, in transit, and in use

- Alfatec (2022, June 27). [What is a centralized key management system?](#)
- Cloudflare (n.d.). [What is a cryptographic key?](#)
- Google Cloud (2022, September) [Default encryption at rest](#).
- Google Cloud (2023, August 15). [Client-side encryption with Tink and Cloud KMS](#).
- Google Cloud (2024, January 26). [Setting up access control](#).
- National Institute of Standards and Technology. (2023, May 9). [Advanced Encryption Standard \(AES\)](#) (NIST FIPS; 197).
- Velimirovic, A. (2021. November 4). [Data encryption at rest explained](#). phoenixNAP Blog.

Asymmetric versus symmetric encryption

- Adee, R. & Mouraditis, H. (2022, February). [A dynamic four-step data security model for data in cloud computing based on cryptography and steganography](#). Sensors, 22(3), 1109.
- Arampatzis, A. (2023, July 25). [When should you use symmetric vs asymmetric encryption?](#) Venafi Blog.
- Google Cloud. (n.d.). [What is encryption and how does it work?](#)
- Google Cloud. (2022, September). [Default encryption at rest](#).
- Google Cloud. (2022, September). [Encryption in transit](#) [Whitepaper].

- National Institute of Standards and Technology. (2023, May 9). [Advanced Encryption Standard \(AES\)](#) (NIST FIPS; 197).

Data classification and tagging

- Buckbee, M. (2023, May 26). [What is data classification? Guidelines and process.](#) *Varonis Blog*.
- Google Cloud. (2024, January 26). [Tags and tag templates.](#)

Protection of personally identifiable information (PII)

- Google Cloud (2024, January 26) [Classification, redaction, and de-identification.](#)
- National Institute of Standards and Technology. (n.d.) [Data loss.](#) Computer Security Resource Center.

Cryptographic keys for data protection

- Cloudflare. (n.d.). [How does public cryptography work?](#)
- Cloudflare. (n.d.). [What is a cryptographic key?](#)
- Cloud Security Alliance. (n.d.). [Cloud key management.](#)
- Google Cloud. (n.d.). [Cloud key management.](#)
- Google Cloud. (n.d.). [What is encryption?](#)
- Google Cloud. (2024, January 26). [Destroy and restore key versions.](#)
- Google Cloud. (2024, January 26). [Key rotation | Cloud KMS documentation.](#)
- National Institute of Standards and Technology. (n.d.). [Domain parameter.](#) Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.) [Key.](#) Computer Security Resource Center.

Data governance for security and data quality

- Collibra. (2023, October 18). [The 6 data quality dimensions with examples](#).
- Google Cloud. (n.d.) [What is data governance?](#)
- Herzberg, B. (2021, November 11). [The datamasters: Data owners vs. data stewards vs. data custodians](#). *Satori Blog*.
- Montvilas, T. (2022, January 7). [How to approach data governance to avoid poor data quality](#). *Forbes*.
- Oracle (n.d.). [What is data management?](#)
- OvalEdge Team. (2022, September 8). [Data governance and data quality: Working together](#). *OvalEdge Blog*.
- Sarfin, R.L. (2021, May 12). [Data quality dimensions: How do you measure up?](#) *Precisely Blog*.

Data sovereignty and data governance

- Chia, A. (2023, July 11). [Data sovereignty vs. data residency: Uncovering the differences](#). *Splunk Blog*.
- Cloudflare (n.d.). [What is data localization?](#)
- Cloudian (n.d.). [What is data sovereignty? Challenges and considerations](#).
- Google Cloud (2024, January 26). [Data residency overview](#).

Data sovereignty challenges and strategies

- Bertucci, D. (2022, April 5). [Data sovereignty: Everything you need to know](#). *Auvik Blog*.
- Chia, A. (2023, July 11). [Data sovereignty vs data residency: Uncovering the differences](#). *Splunk Blogs*.

- Mohanty, P.R. (2023, August 24). [Data sovereignty in the AI age: Gupshup's innovative approach](#). *Gupshup Blog*.
- Spanning Cloud Apps. (n.d.). [Data sovereignty: Definition, requirements and how to ensure it](#). *Spanning Blog*.
- Tan, A. (2023, May 1). [Tackling the challenges of data sovereignty in a multi-cloud world](#). *Computer Weekly, Tech Target*.
- Karlstad, W. (2022, April 19). [Why sovereign cloud is a hot topic – 5 tips, and the background](#). *CIO*.

Data discovery to support data governance

- Chuvakin, A. & Ellis, S. (2020, October 20). [Improving security, compliance, and governance with cloud-based DLP data discovery](#). *Google Cloud Blog*.
- Imperva. (n.d.). [Data discovery](#).

Data retention policies

- Druva (n.d.). [Data retention policy definition](#).
- Eliaçık, E. (2022, March 30). [Everything you need to know about data retention policy](#). *Dataconomy*.
- Google Cloud. (2024, January 26). [Data deletion on Google Cloud](#).
- Marker, A. (2019, July 17). [The essentials of data retention: Policies, plans, and templates](#). *Smartsheet*.
- Onna. (2020, October). [The best data retention policy template to get you started](#). *Onna Blog*.
- Proofpoint (n.d.). [What is a data retention policy?](#)
- Qureshi, A. (n.d.). [Data retention policy 101: Best practices, examples & more \[with template\]](#). *Intradyn Blog*.

Plan for business continuity

- Google Cloud. (n.d.). [What is encryption?](#)
- Google Cloud. (2023, November 22). [Disaster recovery planning guide.](#)
- Google Cloud. (2024, January 29). [Business continuity planning and disaster recovery.](#)
- Theimer, M. (2021, October 31). [Business continuity and disaster recovery in the cloud.](#) *Cloud Security Alliance Blog.*

Create a business continuity plan

- Cisco (n.d.). [What is business continuity?](#)
- Posey, B. (2022, May 31). [Business continuity in the cloud: Benefits and planning tips.](#) *TechTarget.*
- Sathyanarayanan, K. (2023, June 6). [Disaster recovery and business continuity preparedness for cloud-based startups.](#) *ISACA Now Blog.*
- Theimer, M. (2021, October 31). [Business continuity and disaster recovery in the cloud.](#) *Cloud Security Alliance Blog.*

Business continuity scenario

- Glickman, H. (2021, March 10). [Architecting for failure and the future of resilience: How to ensure you're prepared for risks now and five years down the line.](#) *Forbes.*
- Google Cloud (2023, January 16). [Architecting disaster recovery for cloud infrastructure outages.](#)
- Google Cloud (2023, November 22). [Disaster recovery planning guide.](#)
- Marker, A. (2020, November 11). [The beginner's guide to business continuity management in the cloud.](#) *Smartsheet.*
- Roddie-Fonseca, M. (2023, July 5). [Ransomware in the cloud.](#) *SANS Blog.*

- Theimer, M. (2021, October 31). [Business continuity and disaster recovery in the cloud](#). *Cloud Security Alliance Blog*.
- Torres, G. (2022, March 5). [The key components of a business continuity plan](#). *Zerto Blog*.

Course 4 resources and citations

Module 1: Detection foundations

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](#)
- [QWIKlabs Help: Common problems with labs/lab troubleshooting](#)

Essential SecOps skills

- [Google Cloud: Google on SecOps](#)
- [Google Cloud: Welcome to the Google Cloud Security Community](#)
- [YouTube: Google Cloud SecOps](#)

AI in SecOps: Red teams

- [Google: Why red teams play a central role in helping organizations secure AI systems](#)

Log types: A breakdown

- [Google Cloud: Sample audit log entry](#)
- [Google Cloud: Samples for Google Workspace Login Audit](#)

Alert and log optimization

- [Google Cloud: Alerting overview](#)
- [Google Cloud Whitepaper: Google Cloud security foundations guide](#)

Guide to event threat detection

- [Google Cloud: Overview of Event Threat Detection](#)
- [Google Cloud: Query findings in the Google Cloud console](#)

Determine the difference between normal activity and an incident

- [Google Cloud: Configuring Security Command Center](#)
- [Google Cloud: Findings – Security](#)
- [Google Cloud: IAM & Admin](#)
- [Google Cloud: Logs explorer](#)

Citations

SecOps and its components

- Google Cloud. (n.d.). [Cloud Logging](#).
- Google Cloud. (n.d.). [Cloud Monitoring](#).
- Google Cloud. (n.d.). [Identity and Access Management \(IAM\)](#).
- Joint Task Force. (2013, April). [Security and privacy controls for federal information systems and organizations](#) (Special Publication 800-53 revision 4). National Institute of Standards and Technology.

- Kent, K., & Souppaya, M. (2006, September). [*Guide to computer security log management: Recommendations of the National Institute of Standards and Technology*](#) (Special Publication 800-92). National Institute of Standards and Technology.
- Google Cloud. (2024, January 22). [*Overview of Web Security Scanner*](#).
- Google Cloud. (n.d.). [*Security Command Center*](#).

Essential SecOps skills

- Lange, K., (2023, May 31). [*What Is SecOps? Security Operations defined*](#). *Splunk Blog*.
- Google Cloud. (2024, January 22). [*Vulnerability findings*](#).

Vulnerability management techniques

- Angafor, G. N., Yevseyeva, I., & He, Y. (2020). [*Game-based learning: A review of tabletop exercises for cybersecurity incident response training*](#). *SECURITY AND PRIVACY*, 3(6), e126.
- Joint Task Force. (2012, September). [*Guide for conducting risk assessments*](#) (Special Publication 800-30 Revision 1). National Institute of Standards and Technology.
- Murdoch, D. (2016). *Blue team handbook: Incident response edition: A condensed field guide for the cyber security incident responder*. Createspace Independent Publishing.
- National Cyber Security Centre (NCSC), UK. (2016, September 23). [*Vulnerability management*](#).
- Rehberger, J. (2020). *Cybersecurity Attacks – Red Team Strategies*. Packt Publishing Ltd.
- Tenable. (n.d.). [*Solutions for vulnerability management*](#).
- Weidman, G. (2014). *Penetration testing: A hands-on introduction to hacking*. No Starch Press.

Vulnerability scanning, penetration testing, and tabletop exercises

- Google Cloud. (2024, January 22). [About Patch](#).
- Google Cloud. (2024, January 22). [Overview of Web Security Scanner](#).
- Google Cloud. (2024, January 22). [Rapid Vulnerability Detection overview](#).
- Google Cloud. (2024, January 22). [Vulnerability findings](#).

AI in SecOps: Red teams

- Mandiant. (n.d.). [Red team assessment](#).
- Venables, P. (2023, July 26). [The Prompt: Insights from our AI Red Team's first report \(Q&A\)](#). Google Cloud Blog.

Incident detection basics

- Evans, E. (2020, August 24). [Incident detection and response in Google Cloud Platform \(GCP\)](#). CSNP.
- Google Cloud. (2024, January 22). [Overview of Event Threat Detection](#).
- Google Cloud. (2024, January 23). [Alerting overview](#).
- Minherz. (2023, October 12). [Make actionable alerts using Google Cloud](#). Google Cloud - Community.
- New Relic. (2023, August 7). [Effective alerting in practice](#) [Whitepaper].

Phases of incident response and management

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). [Computer security incident handling guide](#) (Special Publication, 800-61, Revision 2). National Institute of Standards and Technology.
- Google Google Cloud. (2022, September). [Data incident response process](#).

- Mell, P., & Grance, T. (2011, September). [The NIST definition of cloud computing](#) (Special Publication 800-145). National Institute of Standards and Technology.
- Scarfone, K., & Mell, P. (2007, February). [Guide to intrusion detection and prevention systems \(IDPS\)](#) (Special Publication 800-94). National Institute of Standards and Technology.

Incident response plans

- Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). [Computer security incident handling guide](#) (Special Publication 800-61, Revision 2). National Institute of Standards and Technology.
- European Network and Information Security Agency (ENISA). (2010, December 20). [Good practice guide for incident management](#).
- Kral, P. (2012, February 21). [Incident handler's handbook](#) [White paper]. SANS Institute.
- Verizon. (n.d.). [2023 Verizon Data Breach Investigations Report](#). Verizon Business.

More about incident response phases

- Google Cloud. (2022, September). [Data incident response process](#).

Intrusion detection systems

- Google Cloud. (n.d.). [Cloud Monitoring](#).
- Google Cloud. (n.d.). [Security](#).
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019, July 17). [Survey of intrusion detection systems: Techniques, datasets and challenges](#). *Cybersecurity*, 2(1).

Signature and anomaly-based detection

- Google Cloud. (n.d.). [Cloud Monitoring](#).
- Google Cloud. (n.d.). [Security](#).
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019, July 17). [Survey of intrusion detection systems: Techniques, datasets and challenges](#). *Cybersecurity*, 2(1).

Logs for analysis and monitoring

- Chuvakin, A. A. (2013). *Logging and Log Management: the Authoritative Guide to Dealing With Syslog, Audit Logs, Events, Alerts and Other It Noise*. Syngress Media Inc.
- Google Cloud. (n.d.). [Chronicle – Suite](#).
- Google Cloud. (n.d.). [Cloud Logging](#).
- Google Cloud. (2024, January 22). [Reading and writing application logs](#).
- Google Cloud. (2024, January 23). [Cloud Audit Logs overview](#).
- Kent, K., & Souppaya, M. (2006, September). [Guide to computer security log management](#) (Special Publication 800-92). National Institute of Standards and Technology.

Log types: A breakdown

- Cloud Identity Help. (n.d.). [Admin log events](#).
- Cloud Identity Help. (n.d.). [User log events](#).
- Google Cloud. (2023, June 13). [gcloud logging sinks create](#).
- Google Cloud. (2024, January 23). [Cloud Audit Logs overview](#).
- Google Cloud. (2024, January 23). [Route logs to supported destinations](#).
- Google Cloud. (2024, January 23). [Routing and storage overview](#).

Log management: The skills needed for success

- Chuvakin, A. A., Schmidt, K., & Phillips, C. (2012). *Logging and Log Management: The authoritative guide to understanding the concepts surrounding logging and log management*. Syngress Media Inc.
- Kent, K., & Souppaya, M. (2006, September). [Guide to computer security log management](#) (Special Publication 800-92). National Institute of Standards and Technology.
- Tracy, M., Jansen, W., Scarfone, K., & Winograd, T. (2007, September). [Guidelines on securing public web servers](#) (Special Publication 800-44 Version 2). National Institute of Standards and Technology.

Alerts and notifications

- Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, March 14). [AD-IoT: Anomaly detection of IoT cyberattacks in Smart City using machine learning](#). *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0305–0310.
- Alsubhi, K., Al-Shaer, E., & Boutaba, R. (2008, August 26). [Alert prioritization in intrusion detection systems](#). *NOMS 2008 - 2008 IEEE Network Operations and Management Symposium*.
- Spathoulas, G. P., & Katsikas, S. K. (2010). [Reducing false positives in intrusion detection systems](#). *Computers & Security*, 29(1), 35–44.

Alert search techniques

- Alsulami, B., Almalawi, A., & Fahad, A. (2022, June 6). [A review on machine learning based approaches of network intrusion detection systems](#). *International Journal of Current Science Research and Review*, 05(06), 2159–2177.
- Cotroneo, D., Paudice, A., & Pecchia, A. (2019). [Empirical analysis and validation of security alerts filtering techniques](#). *IEEE Transactions on Dependable and Secure Computing*, 16(5), 856–870.

- Maheyazah Md Siraj, Mohd Aizaini Maarof, & Mohd, Z. (2009, January). [Intelligent alert clustering model for network intrusion analysis](#). *International Journal of Advances in Soft Computing and its Applications*, 1(1), 33–48.
- Manganaris, S., Christensen, M., Zerkle, D., & Hermiz, K. (2000). [A data mining analysis of RTID alarms](#). *Computer Networks*, 34(4), 571–577.

Alert and log optimization

- Google Cloud. (2024, January 23). [Alerting overview](#).

Guide to event threat detection

- Google Cloud. (2024, January 22). [Overview of Event Threat Detection](#).
- Google Cloud. (2024, January 22). [Work with findings in the Google Cloud console](#).

Module 2: Detection in practice

Resources

Lockheed Martin's Cyber Kill Chain® in practice

- [Lockheed Martin: Cyber Kill Chain](#)

Guide to false positive analysis

- [Google Cloud: Best practices for using service accounts](#)

Explore false positives through incident detection

- [Google Cloud: Findings – Security](#)

IoCs for threat detection

- [Google Cloud: How to hunt the cloud: Lessons and experiences from years of threat hunting](#)

- [Google Cloud: Overview of Event Threat Detection](#)
- [Google Cloud: Strategic Threat Hunting with SOAR and Threat Intel](#)

Query tools: RegEx and YARA-L

- [Google Cloud: Creating a custom regex detector](#)

Citations

Introduction to Lockheed Martin's Cyber Kill Chain®

- Hornetsecurity. (n.d.). [Cyber Kill Chain](#).
- Howard, R., & Olsen, R. (2020). [Implementing intrusion kill chain strategies](#). *Cyber Defense Review*.
- Kauhanen, J. [Host] (2021, March 11). [Looking at phishing through the intrusion kill chain \(051\)](#) [Audio podcast]. Cyber Security Sauna.
- Lockheed Martin. (n.d.). [Cyber Kill Chain](#).
- Spring, J. and Hatleback, E. (2017, January 4). [Thinking about intrusion kill chains as mechanisms](#). *Journal of Cybersecurity*, 3(3), 185-197.

False positive analysis

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August) [Computer security incident handling guide](#) (Special Publication 800-61 Revision 2). National Institute of Standards and Technology.
- KirstenS, Wichers, Jkcurucar, kingthorin. (n.d.). [Intrusion detection](#). OWASP.
- Maqbool, Z., Aggarwal, P., Pammi, V. S. C., & Dutt, V. (2020, January 28). [Cyber security: Effects of penalizing defenders in cyber-security games via experimentation and computational modeling](#). *Frontiers in Psychology*, 11, 11.
- National Institute of Standards and Technology. (n.d.). [False positive](#). Computer Security Resource Center.

- Proofpoint. (2023, February 3). [What is alert fatigue?](#)
- The Hacker News. (2022, August 9). [The truth about false positives in security.](#)

Lockheed Martin's Cyber Kill Chain® in practice

- MITRE ATT&CK. (n.d.). [Cloud Matrix.](#)

Guide to false positive analysis

- Google Cloud. (2024, January 22). [Service accounts overview.](#)

Introduction to security monitoring

- Exabeam. (n.d.). [What is cloud security monitoring?](#)
- Google Cloud. (n.d.). [Cloud Logging.](#)
- Google Cloud. (2024, January 22). [Overview of Event Threat Detection.](#)
- Sharif, A. (2023, March 14). [What is cloud monitoring?](#) Crowdstrike.
- Vergadia, P. (2022, July 13). [Security monitoring in Google Cloud.](#) Google Cloud Blog.

Security monitoring key concepts

- Blumira. (n.d.). [What is cloud security monitoring? A complete guide.](#)
- Cooney, C. (2022, May 3). [Proactive monitoring vs. reactive monitoring.](#) Coralogix Blog.
- Exabeam. (n.d.). [What is cloud security monitoring?](#)
- Google Cloud. (n.d.). [Operations suite.](#)
- Google Cloud. (2022, July 13). [Security monitoring in Google Cloud.](#) Google Cloud Blog.
- Lawrence, M. (n.d.). [What is proactive monitoring?](#) Chron.
- Vinoth, K.P. (2023, September 26). [Why proactive monitoring matters: Benefits and best practices.](#) Knowledge Hut.

Tools for proactive security monitoring

- Google Cloud. (n.d.). [Security Command Center](#).
- Google Cloud. (2020, November 18). [Security talks: Improve your security posture with the security command center](#) [Video]. YouTube.
- Google Cloud. (2024, January 22). [Overview of Event Threat Detection](#).

Indicators of compromise (IoCs)

- Cybersecurity & Infrastructure Security Agency. (n.d.). [Using indicators of compromise \(IOC\) for incident response](#) [Powerpoint slides].
- Cybersecurity & Infrastructure Security Agency. (2023, January 26). [Protecting against malicious use of remote monitoring and management software](#).
- Evans, E. (2020, August 24). [Incident detection and response in Google Cloud Platform \(GCP\)](#). CSNP.
- FBI. (2022, March 7). [RagnarLocker ransomware indicators of compromise](#).
- Google Cloud. (2024, January 24). [Investigating and responding to threats](#).
- Gwalani, R. (2021, October 11). [Investigate threats surfaced in Google Cloud's Security Command Center using Chronicle](#). Medium.
- Johnson, C., Badger L., Waltermire, D., Snyder, J., & Skorupka, C. (2016, October). [Guide to cyber threat information sharing](#) (Special Publication 800-150). National Institute of Standards and Technology.
- National Security Agency. (2019, August). [Continuously hunt for network instructions](#).

Essentials of threat hunting

- Chang, B. & Correa, R. (2022, August 17). [Announcing curated detections in Chronicle SecOps Suite](#). Google Cloud Blog.

- IBM. (n.d.). [What is threat hunting?](#)
- Kaplan, D. (2022, September 12). [Threat hunting](#). *Chronicle Blog*.
- MITRE ATT&CK. (n.d.). [Frequently asked questions](#).
- Trellix. (n.d.). [What is cyber threat hunting?](#)

IOCs for threat detection

- Daszczyszak, R., Ellis, D., Luke, S., & Whitley, S. (2019, March). [TTP-based hunting](#). MITRE.
- Mandiant. (2023). [M-Trends 2023](#).
- SANS. (2016, February 16). [The Who, what, where, when, why and how of effective threat hunting](#) [Whitepaper].
- Secwriter. (2023, June 23). [Unleashing the power of threat hunting in the cloud](#). *CyberDom*.

Aggregations and correlations

- National Institute of Standards and Technology. (n.d.). [Aggregation](#). Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). [Correlation](#). Computer Security Resource Center.

Introduction to query tools

- Google Cloud. (2024, January 22). [Overview of the YARA-L 2.0 language](#).
- Google Cloud. (2024, January 23). [Build queries by using the Logging query language](#).
- Google Cloud. (2024, January 23). [Logging query language](#).

Query tools: RegEx and YARA-L

- Google Cloud. (2024, January 22). [Creating a custom regex detector](#).
- Google Cloud. (2024, January 22). [Yara-L best practices](#).

Module 3: Incident response management and attack mitigation

Resources

Guide to log queries, exports, and analysis

- [Google Cloud: Query syntax](#)

Analyze audit logs using BigQuery

- [Google Cloud: Welcome to BigQuery studio!](#)
- [Google Cloud: Stream findings to BigQuery for analysis](#)
- [Google Cloud: Quotas and limits](#)

Documentation in practice

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

Incident response partners

- [Google Cloud Chronicle: Welcome to Chronicle](#)
- [Mandiant: Cyber threat defense solutions](#)
- [MITRE ATT&CK](#)
- [VirusTotal](#)

Playbooks' role in incident response

- [Google Cloud: Chronicle documentation](#)
- [NIST: NIST Cybersecurity Framework](#)

Citations

The importance of evidence preservation

- Borkar, P. (2023, May 2). [Incident response: 6 steps and teams and tools that make them happen](#). Exabeam.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). [Computer security incident handling guide](#) (Special Publication 800-61 Revision 2). National Institute for Standards and Technology.
- Connectwise. (n.d.). [Tier 1 vs. tier 2 vs. tier 3 cybersecurity](#).
- Google Cloud. (2022, September). [Data incident response process](#).

Digital evidence preservation: Techniques and best practices

- Digicert. (n.d.). [What is an electronic timestamp?](#)
- Guttman, B., White, D. R., & Walraven, T. (2022, September). [Digital evidence preservation](#) (Interagency Report 8387). National Institute of Standards and Technology.
- Jabeen, S. (2023, December 20). [What are the best practices for protecting digital evidence?](#) Vidizmo.
- Namer, A. (2021, August 18). [How to conduct live network forensics in GCP](#). Google Cloud Blog.
- Palter, J. (2021, April 19). [Preserving digital evidence the right way: Your 10-step guide](#). Real Time Networks Blog.
- United Nations Office on Drugs and Crime (UNODC). (2019, March). [Handling of digital evidence](#).

How security teams preserve evidence

- Grispos, G., Storer, T., & Glisson, W.B. (2012). [Calm before the storm: The challenges of cloud computing in digital forensics](#). *Interdisciplinary Informatics Faculty Publications*, 44.
- U.S. Department of Education (ED), Office of the Chief Information Officer (OCIO), & Information Assurance Services (IAS). (2021, January 13). [Standard RS.CO: Computer crime incident reporting](#). Department of Education.

Incident response in Google Cloud

- Google Cloud. (n.d.). [Chronicle SIEM](#).
- Google Cloud. (2022, September). [Data incident response process](#).
- Google Cloud. (2024, January 22). [Chronicle SOAR overview](#).
- Stubbs, J., Menn, J. & Bing, C. (2019, June 26). [Inside the West's failed fight against China's 'Cloud Hopper' hackers](#). Reuters.

Incident response best practices with Chronicle SOAR

- Exabeam. (n.d.). [Incident response automation and security orchestration with SOAR](#).
- Google Cloud. (n.d.). [Chronicle documentation](#).
- Google Cloud. (2024, January 22). [Cases overview](#).
- Google Cloud. (2024, January 22). [Create Entities \(Mapping & modeling\)](#).
- Google Cloud. (2024, January 22). [Getting started with Chronicle SOAR](#).
- Google Cloud. (2024, January 22). [What's on the Playbooks screen?](#)
- Red Hat. (2022, May 11). [What is SOAR?](#)

Incident identification

- AT&T Cybersecurity. (n.d.). [Security Incidents: Types of attacks and triage options](#). Insider's guide to incident response: Expert tips.
- Cybersecurity & Infrastructure Security Agency. (2020, September 24). [Technical approaches to uncovering and remediating malicious activity](#).
- Kleitman, S., Law, M. K. H., & Kay, J. (2018, October 26). *It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling*. PLoS One, 13(10). 10.1371/journal.pone.0205089.

Coordination for incident response

- Google Cloud. (2022, September). [Data incident response process](#).
- Site Reliability Engineering (SRE). (2017). [Example incident state document](#). Google.
- Vankirk, S. (2022, September 2). [Protect your company with our cyber incident management expert advice](#). Cybersecurity Exchange.

Guide to log queries, exports, and analysis

- Google Cloud. (2024, January 23). [Cloud Audit Logs overview](#).
- Google Cloud. (2024, January 23). [Routing and storage overview](#).

Documentation fundamentals

- Borkar, P. (2023, May 2). [Incident response: 6 steps and teams and tools that make them happen](#). Exabeam.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). [Computer security incident handling guide](#) (Special Publication 800-61 Revision 2). National Institute for Standards and Technology.
- Connectwise. (n.d.). [Tier 1 vs. tier 2 vs. tier 3 cybersecurity](#).

- Google Cloud. (2022, September). [Data incident response process](#).

Elements of successful documentation

- California Department of Technology. (n.d.). [Incident response plan example](#) [Word doc].
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). [Computer security incident handling guide](#) (Special Publication 800-61 Revision 2). National Institute for Standards and Technology.
- Login. Gov handbook. (n.d.). [Incident response guide](#). U.S. General Services Administration.
- Google Cloud. (2022, September). [Data incident response process](#).
- Office of Inspector General. (2023, January). [P@s\\$w0rds at the U.S. Department of the Interior: Easily cracked passwords, lack of multifactor authentication, and other failures put critical DOI systems at risk](#) (2021-ITA-005). U.S. Department of the Interior.

Documentation in practice

- Cloud.gov. (2023, December 11). [Security incident response guide](#).
- Google Cloud. (n.d.). [Google Cloud Armor](#).
- Google Cloud. (2022, September). [Data incident response process](#).

Actionable alert identification

- Davis, J., & Cheung, J. (2020, August 6). [Logs-based security alerting in Google Cloud: Detecting attacks in Cloud Identity](#). *Google Cloud Blog*.
- Evans, E. (2020, August 24). [Incident detection and response in Google Cloud Platform \(GCP\)](#). CSNP.
- GitLab. (2024, January 24). [Incident management](#). The GitLab Handbook.

- Google Cloud. (n.d.). [Operations suite](#).
- Google Cloud. (2024, January 22). [Overview of Event Threat Detection](#).
- Google Cloud. (2024, January 23). [Alerting overview](#).
- Google Cloud. (2024, January 23). [Behavior of metric-based alerting policies](#).
- Google Cloud. (2024, January 23). [Using Security Health Analytics](#).
- Minherz. (2023, October 12). [Make actionable alerts using Google Cloud](#). *Google Cloud - Community*.
- New Relic. (2023, August 7). [Effective alerting in practice](#) [White paper].

Security orchestration with playbooks

- Chronicle SOAR. (n.d.). [Working with Playbooks](#).
- Nyre-Yu, M. (2020). [Identifying expertise gaps in cyber incident response: Cyber defender needs vs. technological development](#). (SAND2020-5902C). Sandia National Lab.
- Tankard, C. (2020). [Pandemic underpins need for SOAR](#). *Network Security*, 2020(5), 20–20.
- Trustradius. (n.d.). [Chronicle SOAR](#).

Incident response orchestration vs. automation

- Deacon-Smith, R. & Atamel, M. (2021, April 21). [Choosing the right orchestrator in Google Cloud](#). *Google Cloud Blog*.
- CloudBolt Software. (n.d.). [Comparing cloud automation and orchestration processes](#).
- Cyware Labs. (2021, March 5). [What is the difference between security orchestration and security automation?](#) *Security orchestration and response*.

Playbooks' role in incident response

- Google Cloud. (n.d.). [Chronicle documentation – SOAR](#).
- Google Cloud. (2022) [Top security playbooks 2022-2023](#) [Whitepaper]. 3rd Edition.
- Nichols, M. (2023, December 7). [What is SOAR and how does it improve threat detection and remediation?](#) Red Scan.
- Team ZCySec. (n.d.). [9 SOAR playbook examples for SOC processes](#). ZCybersecurity.

Module 4: Incident recovery

Resources

System recovery steps and scenarios

- [Dark reading: Homepage](#)
- [Infosecurity magazine: Homepage](#)
- [National Institute of Standards and Technology \(NIST\): Computer Security Resource Center](#)
- [SecurityWeek: Homepage](#)
- [SysAdmin, Audit, Network and Security \(SANS\) Institute: Homepage](#)

Guide to backups and VM recovery

- [Google Cloud: Backup and DR Service overview](#)

Recover VMs with Google Backup and DR Service

- [Google Cloud: Backup and DR Service overview](#)
- [Google Cloud: Backup/recovery appliance types](#)

- [Google Cloud: Create a production to snapshot policy](#)
- [Google Cloud: Supported regions](#)

Disaster recovery planning in Google Cloud: Build a DRP

- [DevOps: Cloud disaster recovery best practices](#)
- [Google Cloud: Backup and DR Service documentation](#)
- [Google Cloud: Disaster recovery planning guide](#)
- [Medium: Disaster recovery on Google Cloud for data \(Part 1\)](#)
- [TechTarget: Cloud disaster recovery \(cloud DR\)](#)

Disaster recovery planning in Google Cloud: Implement a DRP

- [DevOps: Cloud disaster recovery best practices](#)
- [Google Cloud: Backup and DR Service documentation](#)
- [Google Cloud: Disaster recovery planning guide](#)
- [Medium: Disaster recovery on Google Cloud for data \(Part 1\)](#)
- [TechTarget: Cloud disaster recovery \(cloud DR\)](#)

Create and manage effective BCDR plans

- [Google Cloud: Cloud Architecture Center](#)
- [Google Cloud: Disaster recovery planning guide](#)
- [Google Cloud: Site reliability engineering \(Sre\)](#)

Interview tip: End responses with positive takeaways

- [Interview Warmup](#)

Citations

Recovery plans in action

- Alabama Department of Labor. (n.d.). [Unemployment Insurance Program disaster recovery plan](#) [White Paper].
- Cybersecurity & Infrastructure Security Agency. (n.d.). [Online toolkit: Partnering to safeguard k-12 organizations from cybersecurity threats](#).
- Github. (n.d.). [Playbook: Ransomware](#).
- Google Cloud. (2023, November 22). [Disaster recovery planning guide](#).
- National Cyber Security Center. (n.d.). [NCSC CAF guidance](#).
- Parsons, M. (2023, October, 17). [IT DRP : How best to plan your company's recovery from a cyber crisis](#). C-Risk.
- Ready (2023, September 7). [IT disaster recovery plan](#). U.S. Department of Homeland Security.
- VMware. (n.d.). [What is disaster recovery?](#)

Information recovery and system restoration

- Alabama Department of Labor. (n.d.). [Unemployment Insurance Program disaster recovery plan](#) [White Paper].
- Google Cloud. (n.d.). [What is disaster recovery?](#)
- MSP360. (2021, January 11). [Cloud disaster recovery: Planning and approaches](#). MSP360 Blog.

System recovery steps and scenarios

- Fearn, N. (2023, December 5). [How to recover systems in the event of a cyber attack](#). *Computer Weekly*.
- ISO. (2012). [ISO/IEC 27037:2012: Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence](#).
- National Institute of Standards and Technology. (n.d.). [Digital evidence](#).
- National Institute of Standards and Technology. (2020, September). [Security and privacy controls for information systems and organizations](#) (Special Publication 800-53, Revision 5).

Business continuity and disaster recovery (BCDR) basics

- AWS. (n.d.). [Business continuity plan \(BCP\)](#).
- Bartock, M., Cichonsk, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016, December). [Guide for cybersecurity event recovery](#) (Special Publication 800-184). National Institute of Standards and Technology.
- Elephant Drive. (n.d.). [Ultimate guide for beginners: Data backup and recovery explained](#).
- Google Cloud. (n.d.). [Backup and disaster recovery](#).
- Swanson, M. (2010). [Contingency planning guide for federal information systems](#) (Special Publication 800-34, Revision 1) [PowerPoint Slides]. National Institute of Standards and Technology.
- Vergadia, P. (2019, October 28). [Disaster recovery on Google Cloud: An overview](#). *Google Cloud - Community*.

The role of BCDR tools

- Hanna, T. (n.d.). [The 15 best business continuity software and tools for 2024](#). Solutions Review.
- Moore, J., Bigelow, S.J., & Crocetti, P. (n.d.). [What is BCDR? Business continuity and disaster recovery guide](#). Techtarget.
- Rao, S. (2020, April, 23). [Disaster recovery and business continuity plan on Google Cloud](#). Unified Data Sciences.

BCDR in Google Cloud

- Google Cloud. (n.d.). [Backup and disaster recovery](#).
- Google Cloud. (2024, January 22). [Backup plans](#).
- Google Cloud. (2024, January 22). [Set up and plan a Backup and DR Service deployment](#).
- Google Cloud. (2024, January 24). [Backup and DR Service overview](#).

Guide to backups and VM recovery

- Google Cloud. (2024, January 22). [Backup plans](#).
- Google Cloud. (2024, January 22). [Define backup policies](#).

Recovery options and measures of success

- Google Cloud. (n.d.). [Backup and disaster recovery](#).
- Google Cloud. (2023, January 16). [Architecting disaster recovery for cloud infrastructure outages](#).
- IBM. (2023, September 18). [Business continuity and disaster recovery overview](#). IBM Cloud Framework for Financial Services.

- Swanson, M. (2010). [Contingency planning guide for federal information systems](#) (Special Publication 800-34, Revision 1) [PowerPoint Slides]. National Institute of Standards and Technology.

Components of a disaster recovery plan (DRP)

- Google Cloud. (n.d.). [Backup and disaster recovery](#).
- Ready (2023, September 7). [IT disaster recovery plan](#). U.S. Department of Homeland Security.
- Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., & Lynes, D. (2010, May). [Contingency planning guide for federal information systems](#) (Special Publication 800-34 Revision 1). National Institute of Standards and Technology.

Disaster recovery planning in Google Cloud: Build a DRP

- Cybary. (2022, December 15). [CISSP study guide: Disaster recovery - hot, cold, and warm sites](#). *Cybary Blog*.
- Google Cloud. (2023, January 16). [Architecting disaster recovery for cloud infrastructure outages](#).
- Google Cloud. (2023, November 22). [Disaster recovery planning guide](#).
- Google Cloud. (2024, January 22). [Optimize Security Command Center](#).
- National Institute of Standards and Technology. (n.d.). [Cold site](#). Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). [Hot site](#). Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). [Warm site](#). Computer Security Resource Center.

Disaster recovery planning in Google Cloud: Implement a DRP

- Cybary. (2022, December 15). [CISSP study guide: Disaster recovery - hot, cold, and warm sites](#). *Cybary Blog*.
- Google Cloud. (2023, January 16). [Architecting disaster recovery for cloud infrastructure outages](#).
- Google Cloud. (2023, November 22). [Disaster recovery planning guide](#).
- Google Cloud. (2024, January 22). [Optimize Security Command Center](#).
- National Institute of Standards and Technology. (n.d.). [Cold site](#). Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). [Hot site](#). Computer Security Resource Center.
- National Institute of Standards and Technology. (n.d.). [Warm site](#). Computer Security Resource Center.

Business continuity and disaster recovery plans

- Ready (2023, September 7). [IT disaster recovery plan](#). U.S. Department of Homeland Security.
- Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., & Lynes, D. (2010, May). [Contingency planning guide for federal information systems](#) (Special Publication 800-34 Revision 1). National Institute of Standards and Technology.
- Google Cloud. (n.d.). [What is disaster recovery?](#)
- Google Cloud. (2024, January 22). [Business continuity planning and disaster recovery](#).
- Grachis, G. (2018, August 16). [Are you prepared for hurricane season? Disaster recovery and business continuity plan best practices](#). CSO Online.

- National Institute of Standards and Technology. (n.d.). [Business continuity plan \(BCP\)](#). Computer Security Resource Center.
- Theimer, M. (2021, October 31). [Business continuity and disaster recovery in the cloud](#). *Cloud Security Alliance Blog*.

Create and manage effective BCDR plans

- Ailsa. (2023, February 1). [Ultimate guide: Google Cloud backup and restore](#). CBackup.
- Google Cloud. (2023, January 16). [Architecting disaster recovery for cloud infrastructure outages](#).
- Google Cloud. (n.d.). [Cloud Build](#).
- Google Cloud. (n.d.). [Cloud Monitoring](#).
- Google Cloud. (n.d.). [Identity and Access Management \(IAM\)](#).
- Google AdSense Help. (n.d.). [Overview of the Policy center](#). Google Cloud.
- Johnson, C. (n.d.) [Building resilience: A step-by-step guide to creating a BCDR plan](#). Axcient.
- Marker, A. (2021, October 17). [Business continuity and disaster recovery: Their differences and how they work together](#). Smartsheet.
- Sullivan, E. (2018, December). [Essential guide to business continuity and disaster recovery plans](#). TechTarget.

Disaster recovery plan stakeholders

- Bartock, M., Cichonsk, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016, December). [Guide for cybersecurity event recovery](#) (Special Publication 800-184).
- Cloudian. (n.d.). [Disaster recovery plan examples and essential elements for your plan](#).
- Google Cloud. (2023, November 22). [Disaster recovery planning guide](#).

- ITtoolkit. (n.d.). [*How to take a team approach to disaster recovery planning*](#).
- National Institute of Standards and Technology. (2018, April 16). [*Framework for improving critical infrastructure cybersecurity*](#).
- Spring, J.M., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2020, December), [*Prioritizing vulnerability response: A stakeholder-specific vulnerability categorization*](#). Carnegie Mellon University.

Course 5 resources and citations

Module 1: Cloud-security focused career resources

Resources

Tips for resume preparation

- [Coursera: How to make a resume: 2024 resume writing guide](#)
- [Google Docs](#)
- [Purdue University: Résumé Workshop](#)

Update your resume

- [Glassdoor: Home page](#)
- [Indeed: Home page](#)
- [Linkedin: Job search](#)

Citations

The cloud security hiring process

- Google Cloud. (n.d.) [Professional cloud security engineer](#).
- National Initiative for Cybersecurity Careers and Studies (NICCS). (2023, November 17). [Cyber Career Pathways Tool](#). Cybersecurity and Infrastructure Security Agency (CISA).
- U.S. Bureau of Labor Statistics. (2022, September 8). [Information security analysts](#). Occupational Outlook Handbook.

GenAI's role in skill development

- Barret, C., Boyd, B., Burzstein, E., Carlini, N., Chen, B., Choi, J., Chowdhury, A., Christodorescu, M., Datta, A., Feizi, S., Fisher, K., Hashimoto, T., Hendrycks, D., Jha, S., Kang, D., Kerschbaum, F., Mitchell, E., Mitchell, J., Ramzan, Z.,... Yang, D. (2024, January 1). [Identifying and mitigating the security risks of generative AI](#). arXiv: 2308.14840.
- Dhoni, P., & Kumar, R. (2023, August 18). [Synergizing generative AI and cybersecurity: Roles of generative AI entities, companies, agencies, and government in enhancing cybersecurity](#). TechRxiv.
- Makhija, V., & Fender, S. (2023, April 24). [Introducing AI-powered risk summaries in Security Command Center](#). Google Cloud Blog.

Portfolios to share project work with employers

- Do, A. (2023, March 13). [Building your brand through your portfolio: Best practices and examples](#). DePaul University Career Center's Blog.
- Izuakor, C (Dr.). (2023, October 19) [Break in: How to get into cybersecurity and build a rewarding career](#). Cybersecurity Guide.
- John, R. (2023, Jan 7). [How to build a cybersecurity portfolio website](#) [Video]. YouTube.
- Kaspersky, J. (2023, January 26). [How to build a cyber security portfolio?](#) Red Team Security Blog.

Refine your resume

- Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). [Resume & application tips](#). Retrieved May 23, 2023.
- National Institute of Standards and Technology. (2018, August 6). [NICE tutorials](#). Information Technology Laboratory.

Tips for resume preparation

- Purdue University Writing Lab. (n.d.). [Résumé Workshop](#). [Purdue OWL®]

Prepare for interviews

- Columbia University Center for Career Education. (n.d.). [Prepare for a software or technical interview](#).
- Marquette University. (n.d.) [Interviewing guide](#). Career Services Center.
- Petersen, R., Santos, D., Smith, M.C., Wetzels, K.A., & Witte, G. (2020, November). [Workforce framework for cybersecurity \(NICE framework\)](#) (Special Publication 800-181). National Institute of Standards and Technology.

Prepare for a cloud security job interview

- Columbia University Center for Career Education. (n.d.). [Prepare for a software or technical interview](#).
- Oliver, V. (2021, November 11). [10 Common job interview questions and how to answer them](#). *Harvard Business Review*.
- Petersen, R., Santos, D., Smith, M.C., Wetzels, K.A., & Witte, G. (2020, November). [Workforce framework for cybersecurity \(NICE framework\)](#) (Special Publication 800-181). National Institute of Standards and Technology.

Module 2: The capstone project

Resources

Incorporate your project into a portfolio

- [GitHub: Creating an account on GitHub](#)
- [GitLab: Sign up](#)
- [Google Drive: Access your Google Drive](#)
- [Google Sites Help: How to use Google Sites](#)

Module 3: Put your Google Cybersecurity Certificate to work

Resources

Showcase your work

- [Applied Digital Skills: Create a resume in Google Docs](#)
- [Applied Digital Skills: Create a resume in Google Docs](#)
- [Big Interview: Grow with Google user guide](#)
- [Enhancv: Search resume examples](#)
- [Linkedin: Add and remove skills on your profile](#)
- [Linkedin: Edit the About section on your profile](#)
- [Linkedin: Manage licenses & certifications](#)

Prepare for your job search

- [Glassdoor: Home page](#)
- [Indeed: Home page](#)

- [Interview Warmup](#)
- [Linkedin: Job search](#)