# Course 2 overview
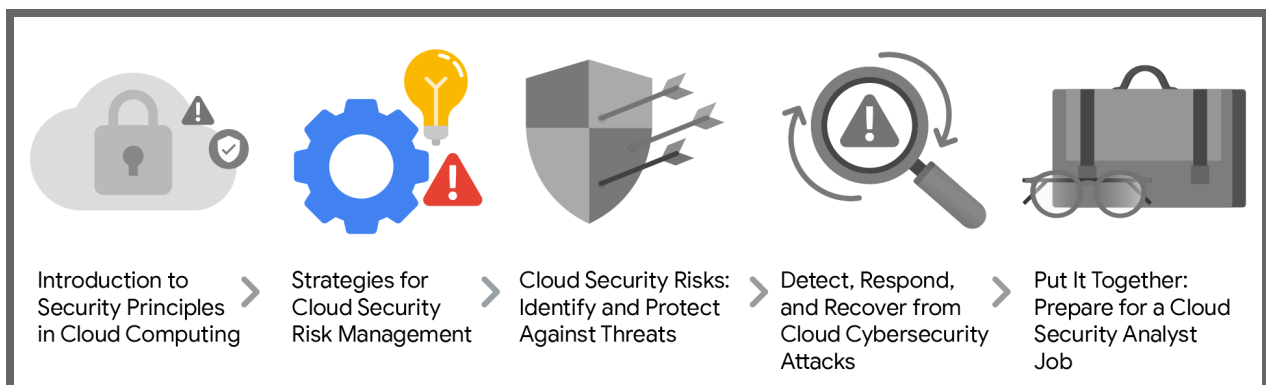


Hello and welcome to **Strategies for Cloud Security Risk Management**, the second course in the Google Cloud Cybersecurity Certificate!

In this course, you'll develop a greater understanding of the most widely used cloud risk management frameworks. You'll also explore security domains, the compliance lifecycle, and regulations and industry standards that cloud security analysts follow on the job. Then, you'll learn how to identify and reduce risks, evaluate compliance while managing data protection and privacy, and compare and adopt frameworks. You'll also learn about Google Cloud and multi-cloud tools for risk and compliance management.

## Certificate program progress

The Google Cloud Security Certificate program has five courses. **Strategies for Cloud Security Risk Management** is the second course.



| Introduction to Security Principles in Cloud Computing | Strategies for Cloud Security Risk Management | Cloud Security Risks: Identify and Protect Against Threats | Detect, Respond, and Recover from Cloud Cybersecurity Attacks | Put It Together: Prepare for a Cloud Security Analyst Job |

1.  Introduction to Security Principles in Cloud Computing — In this course, you'll explore the fundamentals of cloud computing, learn how security principles apply to cloud products and services, and investigate Google Cloud tools.

2. **Strategies for Cloud Security Risk Management** (current course) — In this course, you'll learn about risk management frameworks used to secure cloud resources. You'll also be introduced to tools, regulations, and industry standards that cloud security analysts follow on the job.

3. Cloud Security Risks: Identify and Protect Against Threats — In this course, you'll gain experience with tools and techniques used to protect cloud resources from threats. You'll also explore threat and vulnerability management, cloud native principles, and data protection.

4. Detect, Respond, and Recover from Cloud Cybersecurity Attacks — In this course, you'll learn how cloud security professionals use logging and monitoring systems to identify and mitigate attacks. You'll also explore techniques used to detect, respond to, and recover from a security incident.

5. Put It Together: Prepare for a Cloud Security Analyst Job — In this course, you'll add your new skills to your resume and explore job search tips. Then, you'll apply concepts like risk management, identifying vulnerabilities, incident management, and crisis communications in a capstone project.

## Course 2 content

Each course in this certificate program is broken into modules. You can complete courses at your own pace, but the module breakdowns are designed to help you finish the entire Google Cloud Cybersecurity Certificate in about 3-6 months if you complete about 1-2 modules per week.

What's to come? Here's a quick overview of the skills you'll learn in each module of this course.

### Module 1: Introduction to frameworks within security domains

In this module, you'll learn about security domains, compliance frameworks, data privacy fundamentals, risk, and security controls. You'll also explore the differences between security and compliance. Then you'll learn how to define and explain controls and frameworks, and the three areas of compliance: people, process and technology. You'll also explore risk and security controls, and how security controls are implemented.

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

In this module, you'll learn how traditional networking concepts translate to the cloud. Then, you'll learn about security controls used to secure cloud networks, and how controls can be combined to create defense in depth. Finally, you'll explore how cloud service providers and customers work together to secure cloud resources, including using identity and access management (IAM) policies.

### Module 3: The compliance lifecycle

In this module, you'll get a comprehensive overview of the compliance lifecycle. Then, you'll learn about controls and control mapping, assessments and auditing, regulatory requirements, negative organizational impacts of non-compliance, and Policy-as-Code (PaC) in Infrastructure-as-Code (IaC).

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

In this module, you'll explore Google and multi-cloud cloud security posture management tools. Then, you'll learn to use Security Command Center, Risk Manager, and Policy Analyzer to secure cloud resources. You'll also use risk protection programs and organizational policies for compliance and risk mitigation.

## What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
- **Activities** and **labs** give you practice in applying the skills you're learning and allow you to assess your own work by comparing it to a completed example.
- **Glossaries** provide a list of key terms for you to review to prepare for quizzes.
- **Practice quizzes** allow you to check your understanding of key concepts, and provide you with valuable feedback.
- **Graded quizzes** allow you to demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate. You can take a graded quiz multiple times to achieve a passing score.

**Note:** Some learning item types may not be included in every course.

## Tips for success

- It's strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.
- Participate in all learning opportunities to gain as much knowledge and experience as possible.
- If something is confusing, don't hesitate to replay a video, review a reading, or repeat an activity.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.