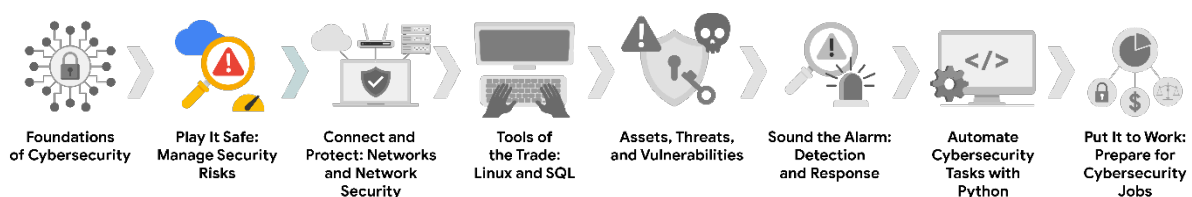# Get started on the next course

Congratulations on completing Course 2 of the Google Cybersecurity Certificate: **Play It Safe: Manage Security Risks**! In this part of the program, you learned about the focus of the eight Certified Information Systems Security Professional (CISSP) security domains. You also learned more about threats, risks, and vulnerabilities, as well as common security controls and frameworks. Additionally, you explored how to use the National Institute of Standards and Technology Risk Management Framework (NIST RMF), security information and event management (SIEM) technology, and playbooks to identify and help prevent security issues that can harm organizations and the people they serve.

The Google Cybersecurity Certificate has eight courses:

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.
2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. *(This is the course you just completed. Well done!)*
3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.
4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.
8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Now that you have completed this course, you're ready to move on to the next course: **Connect and Protect: Networks and Network Security**.

Keep up the great work!