Explore the CISSP security domains

- Explore the CISSP security domains, Part 1
- Explore the CISSP security domains, Part 2
- Security domains cybersecurity analysts need to know
- Ashley: My path to cybersecurity

Explore the CISSP security domains, Part 1

Welcome back! You might remember from course one that there are eight security domains, or categories, identified by CISSP. Security teams use them to organize daily tasks and identify gaps in security that could cause negative consequences for an organization, and to establish their security posture. Security posture refers to an organization's ability to manage its defense of critical assets and data and react to change.

In this video, we'll discuss the focus of the first four domains: security and risk management, asset security, security architecture and engineering, and communication and network security.

The first domain is security and risk management. There are several areas of focus for this domain: defining security goals and objectives, risk mitigation, compliance, business continuity, and legal regulations. Let's discuss each area of focus in more detail.

By defining security goals and objectives, organizations can reduce risks to critical assets and data like PII, or personally identifiable information. Risk mitigation means having the right procedures and rules in place to quickly reduce the impact of a risk like a breach. Compliance is the primary method used to develop an organization's internal security policies, regulatory requirements, and independent standards. Business continuity relates to an organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.

And finally, while laws related to security and risk management are different worldwide, the overall goals are similar. As a security professional, this means following rules and expectations for ethical behavior to minimize negligence, abuse, or fraud.

The next domain is asset security. The asset security domain is focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. This means that assets such as PII or SPII should be securely handled and protected, whether stored on a computer, transferred over a network like the internet, or even physically collected. Organizations also need to have policies and procedures that ensure data is properly stored, maintained, retained, and destroyed. Knowing what data you have and who has access to it is necessary for having a strong security posture that mitigates risk to critical assets and data.

Previously, we provided a few examples that touched on the disposal of data. For example, an organization might have you, as a security analyst, oversee the destruction of hard drives to make sure that they're properly disposed off. This ensures that private data stored on those drives can't be accessed by threat actors.

The third domain is security architecture and engineering. This domain is focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data. One of the core concepts of secure design architecture is shared responsibility. Shared responsibility means that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security. By having policies that encourage users to recognize and report security concerns, many issues can be handled quickly and effectively.

The fourth domain is communication and network security, which is mainly focused on managing and securing physical networks and wireless communications. Secure networks keep an organization's data and communications safe whether on-site, or in the cloud, or when connecting to services remotely.

For example, employees working remotely in public spaces need to be protected from vulnerabilities that can occur when they use insecure bluetooth connections or public wifi hotspots. By having security team members remove access to those types of communication channels at the organizational level, employees may be discouraged from practicing insecure behavior that could be exploited by threat actors.

Now that we've reviewed the focus of our first four domains, let's discuss the last four domains. (Required)
en

Explore the CISSP security domains, Part 2

In this video, we'll cover the last four domains: identity and access management, security assessment and testing, security operations, and software development security.

The fifth domain is identity and access management, or IAM. And it's focused on access and authorization to keep data secure by making sure users follow established policies to control and manage assets. As an entry-level analyst, it's essential to keep an organization's systems and data as secure as possible by ensuring user access is limited to what employees need. Basically, the goal of IAM is to reduce the overall risk to systems and data.

For example, if everyone at a company is using the same administrator login, there is no way to track who has access to what data. In the event of a breach, separating valid user activity from the threat actor would be impossible.

There are four main components to IAM. Identification is when a user verifies who they are by providing a user name, an access card, or biometric data such as a fingerprint. Authentication is the verification process to prove a person's identity, such as entering a password or PIN. Authorization takes place after a user's identity has been confirmed and relates to their level of access, which depends on the role in the organization. Accountability refers to monitoring and recording user actions, like login attempts, to prove systems and data are used properly.

The sixth security domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security control testing can help an organization identify new and better ways to mitigate threats, risks, and vulnerabilities. This involves examining organizational goals and objectives, and evaluating if the controls being used actually achieve those goals. Collecting and analyzing security data regularly also helps prevent threats and risks to the organization.

Analysts might use security control testing evaluations and security assessment reports to improve existing controls or implement new controls. An example of implementing a new control could be requiring the use of multi-factor authentication to better protect the organization from potential threats and risks.

Next, let's discuss security operations. The security operations domain is focused on conducting investigations and implementing preventative measures. Investigations begin once a security incident has been identified. This process requires a heightened sense of urgency in order to

minimize potential risks to the organization. If there is an active attack, mitigating the attack and preventing it from escalating further is essential for ensuring that private information is protected from threat actors.

Once the threat has been neutralized, the collection of digital and physical evidence to conduct a forensic investigation will begin. A digital forensic investigation must take place to identify when, how, and why the breach occurred. This helps security teams determine areas for improvement and preventative measures that can be taken to mitigate future attacks.

The eighth and final security domain is software development security. This domain focuses on using secure coding practices. As you may remember, secure coding practices are recommended guidelines that are used to create secure applications and services. The software development lifecycle is an efficient process used by teams to quickly build software products and features. In this process, security is an additional step. By ensuring that each phase of the software development lifecycle undergoes security reviews, security can be fully integrated into the software product.

For example, performing a secure design review during the design phase, secure code reviews during the development and testing phases, and penetration testing during the deployment and implementation phase ensures that security is embedded into the software product at every step. This keeps software secure and sensitive data protected, and mitigates unnecessary risk to an organization.

Being familiar with these domains can help you better understand how they're used to improve the overall security of an organization and the critical role security teams play. Next, we'll discuss security threats, risks, and vulnerabilities, including ransomware, and introduce you to the three layers of the web.

Security domains cybersecurity analysts need to know

As an analyst, you can explore various areas of cybersecurity that interest you. One way to explore those areas is by understanding different security domains and how they're used to organize the work of security professionals. In this reading you will learn more about CISSP's eight security domains and how they relate to the work you'll do as a security analyst.

Domain one: Security and risk management

All organizations must develop their security posture. Security posture is an organization's ability to manage its defense of critical assets and data and react to change. Elements of the security and risk management domain that impact an organization's security posture include:

- Security goals and objectives
- Risk mitigation processes
- Compliance
- Business continuity plans
- Legal regulations
- Professional and organizational ethics

Information security, or InfoSec, is also related to this domain and refers to a set of processes established to secure information. An organization may use playbooks and implement training as a part of their security and risk management program, based on their needs and perceived risk. There are many InfoSec design processes, such as:

- Incident response
- Vulnerability management
- Application security
- Cloud security
- Infrastructure security

As an example, a security team may need to alter how personally identifiable information (PII) is treated in order to adhere to the European Union's General Data Protection Regulation (GDPR).

Domain two: Asset security

Asset security involves managing the cybersecurity processes of organizational assets, including the storage, maintenance, retention, and destruction of physical and virtual data. Because the loss or theft of assets can expose an organization and increase the level of risk, keeping track of assets and the data they hold is essential. Conducting a security impact analysis, establishing a recovery plan, and managing data exposure will depend on the level of risk associated with each asset. Security analysts may need to store, maintain, and retain data by creating backups to ensure they are able to restore the environment if a security incident places the organization’s data at risk.

Domain three: Security architecture and engineering

This domain focuses on managing data security. Ensuring effective tools, systems, and processes are in place helps protect an organization’s assets and data. Security architects and engineers create these processes.

One important aspect of this domain is the concept of shared responsibility. Shared responsibility means all individuals involved take an active role in lowering risk during the design of a security system. Additional design principles related to this domain, which are discussed later in the program, include:

- Threat modeling
- Least privilege
- Defense in depth
- Fail securely
- Separation of duties
- Keep it simple
- Zero trust
- Trust but verify

An example of managing data is the use of a security information and event management (SIEM) tool to monitor for flags related to unusual login or user activity that could indicate a threat actor is attempting to access private data.

Domain four: Communication and network security

This domain focuses on managing and securing physical networks and wireless communications. This includes on-site, remote, and cloud communications.

Organizations with remote, hybrid, and on-site work environments must ensure data remains secure, but managing external connections to make certain that remote workers are securely accessing an organization’s networks is a challenge. Designing network security controls—such as restricted network access—can help protect users and ensure an organization’s network remains secure when employees travel or work outside of the main office.

Domain five: Identity and access management

The identity and access management (IAM) domain focuses on keeping data secure. It does this by ensuring user identities are trusted and authenticated and that access to physical and logical assets is authorized. This helps prevent unauthorized users, while allowing authorized users to perform their tasks.

Essentially, IAM uses what is referred to as the principle of least privilege, which is the concept of granting only the minimal access and authorization required to complete a task. As an example, a cybersecurity analyst might be asked to ensure that customer service representatives can only view the private data of a customer, such as their phone number, while working to resolve the customer's issue; then remove access when the customer's issue is resolved.

Domain six: Security assessment and testing

The security assessment and testing domain focuses on identifying and mitigating risks, threats, and vulnerabilities. Security assessments help organizations determine whether their internal systems are secure or at risk. Organizations might employ penetration testers, often referred to as “pen testers,” to find vulnerabilities that could be exploited by a threat actor.

This domain suggests that organizations conduct security control testing, as well as collect and analyze data. Additionally, it emphasizes the importance of conducting security audits to monitor for and reduce the probability of a data breach. To contribute to these types of tasks, cybersecurity professionals may be tasked with auditing user permissions to validate that users have the correct levels of access to internal systems.

Domain seven: Security operations

The security operations domain focuses on the investigation of a potential data breach and the implementation of preventative measures after a security incident has occurred. This includes using strategies, processes, and tools such as:

- Training and awareness
- Reporting and documentation
- Intrusion detection and prevention
- SIEM tools
- Log management
- Incident management
- Playbooks
- Post-breach forensics
- Reflecting on lessons learned

The cybersecurity professionals involved in this domain work as a team to manage, prevent, and investigate threats, risks, and vulnerabilities. These individuals are trained to handle active attacks, such as large amounts of data being accessed from an organization's internal network, outside of normal working hours. Once a threat is identified, the team works diligently to keep private data and information safe from threat actors.

Domain eight: Software development security

The software development security domain is focused on using secure programming practices and guidelines to create secure applications. Having secure applications helps deliver secure and reliable services, which helps protect organizations and their users.

Security must be incorporated into each element of the software development life cycle, from design and development to testing and release. To achieve security, the software development process must have security in mind at each step. Security cannot be an afterthought.

Performing application security tests can help ensure vulnerabilities are identified and mitigated accordingly. Having a system in place to test the programming conventions, software executables, and security measures embedded in the software is necessary. Having quality assurance and pen tester professionals ensure the software has met security and performance standards is also an essential part of the software development process. For example, an entry-level analyst working for a pharmaceutical company might be asked to make sure encryption is properly configured for a new medical device that will store private patient data.

Key takeaways

In this reading, you learned more about the focus areas of the eight CISSP security domains. In addition, you learned about InfoSec and the principle of least privilege. Being familiar with these security domains and related concepts will help you gain insight into the field of cybersecurity.

Ashley: My path to cybersecurity

My name is Ashley and my role at Google is CE Enablement Lead for SecOps sales. All that means is I help set up training for customer engineers that support our products. Grew up with a computer, loved the Internet. I have one of the earliest AOL screen names in history and I'm very proud of that. My dad is an engineer and I think there was always an interest in tech. But when I got out of high school, there wasn't a clear path to get there. It wasn't a linear path at all. I was a knucklehead growing up. I gave up in 10th grade and I just didn't care for a long time and I was getting in trouble a lot and I pretty much told myself if I don't join the military and get out of here, I will probably not be here in about 2-3 years if I continue down this path. I joined the army right out of high school, graduated in June, and four days later I was at bootcamp at Fort Jackson, South Carolina as a trumpet player, believe it or not, I come back and had to get a job and was not even tracking on tech jobs or anything like that. I was pulling in carts for a big hardware store, selling video games, retail, box slinger for a freight company. All of that stuff has happened before I even figured out that tech was an option. The military was kind enough to retrain me in IT, and that's kind of how I actually got the official first wave of schooling to be able to actually say, hey, I have the skills to at least be a PC technician. I went back to community college and I actually did find a cybersecurity associates degree program, worked on some certifications. I went to my first DEFCON, which is a big hacking conference, and that set off a light bulb, I think to actually get that clarity on what the path could look like. I landed my first security analyst job back in 2017 and I went to a Veterans Training Program at my last company that was free for vets and ended up getting hired out of the training. I was with that company for almost five years before I came to Google. If you're new and you're just coming in, you have to know how to work with a team. I think a lot of us learned that in customer service settings. Some of the skills I learned working in retail, dealing with hard customers, learning how to even talk to people or diffuse a situation if people are upset about things, just learning how to talk to people. In IT we need that. It's no longer just the tech skills we need, the more T-shaped which they're soft skills, there's people skills, and there's technical skills. You have to have good analysis skills, and again, it doesn't even have to be technical analysis, if you can read a book and pick apart the rhetorical devices of that story, you can do analysis work. I didn't have to be a software engineer to work in this field. For many of us, there's like a math fear, programming is a big hurdle, but we work with people, we work with processes, and you don't necessarily need to have that coding knowledge to understand people or processes. There's so many ways to break in, so do not get discouraged and don't be scared to think outside of the box to get your foot in the door.