The CISSP (Certified Information Systems Security Professional) certification validates your knowledge across a broad range of cybersecurity domains. Here's a breakdown of each domain to give you a good understanding of its role in information security:

1. **Security and Risk Management (16% of CISSP exam):** This domain focuses on the big picture of information security. It covers:
   - **Developing security policies:** Creating guidelines for how your organization handles information security.
   - **Risk identification and assessment:** Identifying potential threats and vulnerabilities to your systems and data.
   - **Risk mitigation strategies:** Implementing controls to reduce security risks.
   - **Business continuity and disaster recovery (BC/DR):** Having a plan to recover from security incidents or natural disasters.
2. **Asset Security (10% of CISSP exam):** This domain deals with protecting your valuable resources, including hardware, software, data, and facilities. It covers:
   - **Classification of assets:** Categorizing your assets based on their importance and sensitivity.
   - **Inventory management:** Keeping track of all your IT assets.
   - **Data security:** Protecting data at rest, in transit, and in use.
   - **Physical security:** Securing your physical infrastructure, like data centers and server rooms.
3. **Security Architecture and Engineering (13% of CISSP exam):** This domain focuses on designing and implementing secure systems. It covers:
   - **Security models:** Applying different security frameworks and models to your organization.
   - **Cryptography:** Using encryption to scramble sensitive data.
   - **Network security:** Securing your computer networks from unauthorized access.
   - **Secure system design principles:** Building security into systems from the ground up.
4. **Communication and Network Security (13% of CISSP exam):** This domain dives deeper into network security concepts. It covers:
   - **Network security protocols:** Understanding how protocols like firewalls and VPNs work.
   - **Wireless network security:** Securing Wi-Fi networks.
   - **Intrusion detection and prevention systems (IDS/IPS):** Deploying systems to detect and prevent network attacks.
   - **Secure communication channels:** Ensuring the confidentiality and integrity of data transmissions.
5. **Identity and Access Management (IAM) (13% of CISSP exam):** This domain focuses on controlling who has access to your systems and data. It covers:
   - **Authentication:** Verifying a user's identity before granting access.
   - **Authorization:** Granting users the specific permissions they need to perform their jobs.
   - **Access control models:** Implementing different access control methods like role-based access control (RBAC).
   - **Identity federation:** Allowing users to access multiple systems with a single set of credentials.
6. **Security Assessment and Testing (12% of CISSP exam):** This domain covers how to identify and assess vulnerabilities in your security posture. It includes:

   - **Vulnerability scanning:** Using tools to discover weaknesses in your systems.
   - **Penetration testing:** Simulating a cyberattack to identify exploitable vulnerabilities.
   - **Security audits:** Systematically reviewing your security controls to identify gaps.
   - **Risk assessments:** Evaluating the likelihood and impact of security threats.

7. **Security Operations (13% of CISSP exam):** This domain focuses on the day-to-day tasks of keeping your systems secure. It covers:
   - **Incident response:** Having a plan to identify, contain, and recover from security incidents.
   - **Security information and event management (SIEM):** Using tools to collect and analyze security data.
   - **Log management:** Monitoring and analyzing system logs for suspicious activity.
   - **Security awareness training:** Educating employees about cybersecurity best practices.
8. **Software Development Security (10% of CISSP exam):** This domain focuses on integrating security throughout the software development lifecycle. It covers:
   - **Secure coding practices:** Writing code that is resistant to vulnerabilities.
   - **Secure software development methodologies:** Using secure development practices like secure coding standards and code review.
   - **Application security testing:** Identifying and mitigating vulnerabilities in applications.
   - **Software supply chain security:** Securing the software development process from start to finish.