CISSP Syllabus

The CISSP domains are drawn from various information security topics within the (ISC)² CBK. The CISSP CBK consists of the following 8 domains:

- **Security and Risk Management** (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
    - Confidentiality, integrity, and availability concepts
    - Security governance principles
    - Compliance
    - Legal and regulatory issues
    - Professional ethic
    - Security policies, standards, procedures and guidelines
- **Asset Security** (Protecting Security of Assets)
    - Information and asset classification
    - Ownership (e.g. data owners, system owners)
    - Protect privacy
    - Appropriate retention
    - Data security controls
    - Handling requirements (e.g. markings, labels, storage)
- **Security Engineering** (Engineering and Management of Security)
    - Engineering processes using secure design principles
    - Security models fundamental concepts
    - Security evaluation models
    - Security capabilities of information systems
    - Security architectures, designs, and solution elements vulnerabilities
    - Web-based systems vulnerabilities
    - Mobile systems vulnerabilities
    - Embedded devices and cyber-physical systems vulnerabilities
    - Cryptography
    - Site and facility design secure principles
    - Physical security

- **Communication and Network Security** (Designing and Protecting Network Security)
    - Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
    - Secure network components
    - Secure communication channels
    - Network attacks

- **Identity and Access Management** (Controlling Access and Managing Identity)
    - Physical and logical assets control
    - Identification and authentication of people and devices
    - Identity as a service (e.g. cloud identity)
    - Third-party identity services (e.g. on-premise)
    - Access control attacks
    - Identity and access provisioning lifecycle (e.g. provisioning review)

- **Security Assessment and Testing** (Designing, Performing, and Analyzing Security Testing)
    - Assessment and test strategies
    - Security process data (e.g. management and operational controls)
    - Security control testing
    - Test outputs (e.g. automated, manual)
    - Security architectures vulnerabilities
- **Security Operations** (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
    - Investigations support and requirements
    - Logging and monitoring activities
    - Provisioning of resources
    - Foundational security operations concepts
    - Resource protection techniques
    - Incident management
    - Preventative measures
    - Patch and vulnerability management
    - Change management processes
    - Recovery strategies
    - Disaster recovery processes and plans
    - Business continuity planning and exercises
    - Physical security
    - Personnel safety concerns
- **Software Development Security** (Understanding, Applying, and Enforcing Software Security)
    - Security in the software development lifecycle
    - Development environment security controls
    - Software security effectiveness
    - Acquired software security impact