CCSP All-In-One

- Chapter 1
  - Why get Certified
  - How to get Certified
  - CCSP Domains
  - Introduction to IT Security

Why get Certified?

- $(ISC)^2$ is well respected
- Good for the career
- Good for all levels
  - Starting analyst to CISO
- Complements other certifications
- More $$$$

How to get Certified

- To qualify for the CCSP certification, you must have:
  - A minimum of five years cumulative, paid work experience in IT
  - Three of those years must be in information security
  - One year in one or more of the six domains of the CCSP Common Body of Knowledge (CBK)
  - CSA's CCSK certificate can be substituted for one year of experience
  - CISSP credential can be substituted for the entire CCSP experience requirement.

How to get Certified

- OR… go the Associate route
  - Pass the CCSP exam
  - Six years to earn your required work experience for the CCSP.
  - More Info - https://www.isc2.org/Certifications/Associate

CCSP Domains

Domains

1. Architectural Concepts & Design Requirements
2. Cloud Data Security
3. Cloud Platform & Infrastructure Security
4. Cloud Application Security
5. Operations
6. Legal and Compliance

Domain 1 – Architectural Concepts and Design Requirements

- Cloud computing concepts – Based on ISO/IEC 17788. Lays the foundation for the basics. Includes definitions, roles (customer and provider), characteristics such as on demand self-service, multi-tenancy, boraod network access, elasticity, and scalability and the building block technologies (virtualization, storage, networks, and underlying infrastructure)
- Cloud reference architecture – Based on ISO/IEC 17789. Introduces cloud computing activities, cloud service categories (SaaS, IaaS, PaaS), deployment models, cloud cross-cutting aspects such as portability, interoperability, reversibility, security, resiliency, privacy, and availability
- Security concepts related to cloud computing – Network security, access control, data and media sanitization, cryptography, and virtualization
- Secure design principles of cloud computing – Cloud SDLC, business continuity and disaster recovery planning in a cloud environment, cost benefit analysis (changes in operation, policy, configuration, and regulatory
- Instilling trust – i.e. How do you trust someone who is hosting your app. No hosting makes this important. certification are based on common means or criteria, system/subsystem product certification such as FIPS 140-2

Domain 2 – Cloud Data Security

- Cloud data storage is about design, principles, and best practices.
- Includes architecture and controls used for securing them like encryption, data masking, tokenization and data life cycle management (data discovery and classification)
- Encompasses all principles, concepts, standards and structures used for designing, implementing, monitoring and securing the networks, operating systems, equipment, applications, and controls that enforce confidentiality, integrity and availability in cloud.
- Data Rights Management (DRM) technology, and the deletion, retention and archiving
- Logging including what needs to be logged, the level and detail, and which sources need to be logged (app and/or system).

Domain 3 – Cloud Platform Infrastructure Security

- Covers virtual and physical security risks related to cloud infrastructure (virtualization and the hosts)
- Access to physical systems (BIOS and hardware layers) and the software running on the hosts.
- Identity and access management, authentication and authorization
- Business continuity
- Disaster Recovery

Domain 4 – Cloud Application Security

- Testing of systems and applications
- DAST (Dynamic Application Security Testing) software that acts like a hacker (black box)
- SAST (Static Application Security Testing) softweare that scans source code (white box)
- Pentesting – A real hacker (black/gray/white box)
- RASP (Runtime Application Self Protection – react to events/issues that are suspect
- Risk assessment models STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (D.o.S), Elevation of privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability)

Domain 5 – Operations

- Planning process of the Data Center Design
- Development and implementation of Physical infrastructure of Cloud
- Running and management of physical infrastructure for Cloud
- Building, running and managing logical infrastructure for cloud
- Complying with frameworks and regulations such as ISO/IEC 20000-1, ITIL.
- Carrying out physical and logical infrastructure risk assessment
- Understanding of collection and preservation of digital evidence
- Managing communication with concerned parties

Domain 6 – Legal and Compliance

- Unique risks and legal requirements of cloud environment
- Privacy issues, that also include jurisdictional variation
- Audit process and methodologies of cloud computing environment
- Enterprise Risk Management of cloud
- Cloud Contract Design and Outsourcing
- Vendor management

Introduction to IT Security

- Least Privilege
- Defense in Depth
- CIA (Confidentiality Integrity Availability)
- Cryptography
- Certificates
- Physical Security
- Risk Management
- Business Continuity and Disaster Recovery

Least Privilege

- Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to
- Only give access to the people who need it and only give them the permissions they need to accomplish their task

Defense in Depth

- any single defense may be flawed, and the most certain way to find the flaws is to be compromised by an attack — so a series of different defenses should each be used to cover the gaps in the others' protective capabilities. Firewalls, intrusion detection systems, malware scanners, integrity auditing procedures, and local storage encryption tools can each serve to protect your information technology resources in ways the others cannot
- Don’t have a single point of failure in your security controls

CIA (Confidentiality Integrity Availability)

- The security triad
- Confidentiality – ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them
- Integrity – ensures that information are in a format that is true and correct to its original purposes.
- Availability – ensures that information and resources are available to those who need them when they need them

Cryptography

- Make information unreadable for anyone not authorized
- Symmetric encryption - The same key for both encryption and decryption of your data or message.
- Asymmetric encryption - Uses not one key but a pair of keys: a private one and a public one

Certificates

- Certificates create an encrypted connection and establish trust
- Contains info on the user, organization, locality, and other info
- Issued by a CA (Certificate Authority)

Physical Security

- Security related to the facility where the servers are running
- Same defense in depth principle (fences, cameras, guards, alarms, locked doors, etc.
- An attacker who gains physical access to a server can own it.

Risk Management

- Determine risk through analysis and testing
- Includes weakness, vulnerabilities, data issues, and systems
- External includes physical, environmental, insider threats.
- Musy know risk to manage it

Business Continuity and Disaster Recovery

- Sudden, unexpected, and catastrophic loss of systems and/or data
- Resiliency is key. Systems and process should be redundant and scoped for capacity
- Recovery is key. Backups and testing required
- Failure of BCDR must also be planned for.

OWASP Links

- OWASP Cloud Security Project
  - https://www.owasp.org/index.php/OWASP_Cloud_Security_Project#tab=Main
- Cloud Top 10 Security Risks (Pre Alpha)
  - https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

Links

- (ISC)² CCSP Info
- https://www.isc2.org/Certifications/CCSP
- OWASP Cloud Project
- https://www.owasp.org/index.php/OWASP_Cloud_Security_Project
- OWASP Top 10 Cloud
- https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project
- (ISC)² Exam Outline
- https://www.isc2.org/CCSP-Exam-Outline