CompTIA Advanced Security Practitioner (CASP+)

1. **Enterprise Security**
    a. Identifying security concerns in scenarios
        1. Exploring cryptographic techniques
        2. Advanced PKI concepts
    b. Distinguishing between cryptographic concepts
        1. Entropy
        2. Confusion and diffusion
        3. Chain of trust
    c. Securing enterprise storage
        1. Examining storage types and protocols
        2. Secure storage management
    d. Analyzing network security architectures
        1. Designing secure networks
        2. Employing virtual networking solutions
    e. Troubleshooting security controls for hosts
        1. Host security: trusted OS, end-point, host hardening
        2. Vulnerabilities in co-mingling of hosts
    f. Differentiating application vulnerabilities
        1. Web application security
        2. Application security concerns
        3. Mitigating client-side vs. server-side processing
2. **Risk Management and Incident Response**
. Interpreting business and industry influences and risks
        1. Analyzing risk scenarios
        2. Identifying the impact of de-perimeterization
        a. Executing risk mitigation planning, strategies and control
        1. Assessing the CIA aggregate scores
        2. Making risk determination
        b. Privacy policies and procedures
        1. Developing policies to support business objectives
        2. Safeguarding Personally Identifiable Information (PII)
        c. Conduct incident response and recovery procedures
        1. Constructing a data inventory with e-discovery
        2. Minimizing the severity of data breaches
3. **Research, Analysis and Assessment**
. Determining industry trends impact to the enterprise
        1. Performing ongoing research to support best practices

2. Researching security requirement for contracts
a. Appropriate security document usage
1. Request for Information (RFI)
2. Request for Quote (RFQ)
3. Request for Proposal (RFP)
b. Evaluating scenarios to determine how to secure the enterprise
1. Conducting cost benefit and security solution analysis
2. Reviewing effectiveness of existing security controls
c. Conducting an assessment and analyzing the results
1. Determining appropriate tools for data gathering
2. Identifying methods to perform assessments

4. Integrating Computing, Communications and Business Disciplines

. Collaborating across diverse business units to achieve security goals
1. Communicating with stakeholders
2. Interpreting security requirements and providing guidance
3. Identifying secure communications goals
a. Selecting controls for secure communications
1. Utilizing unified collaboration tools
2. Mobile devices
3. Applying over the air technologies
b. Implementing security across technology life cycle
1. Selecting security controls
2. Developing Security Requirements Traceability Matrices

5. Technical Integration of Enterprise Components

. Integrate devices into a secure enterprise architecture
1. Securing data following existing security standards
2. Applying technical deployment models
3. Integrating storage and applications into the enterprise
a. Integrating advanced authentication and authorization technologies
1. Implementing certificate-based and SSO authentication
2. Applying federation solutions