SSCP exam outline, effective 1 October 2025

1 Security Concepts and Practices (16%)

- Codes of ethics
- Security concepts: CIA, least privilege, SoD
- Control types and functions
- Asset and change management
- Awareness and physical security

2 Access Controls (15%)

- Authentication, SSO, federation
- Trust architectures and the DMZ
- Identity management lifecycle
- Access control models

3 Risk Identification, Monitoring and Analysis (15%)

- Risk management and treatment
- Legal and regulatory concerns
- Assessments and vulnerability management
- Logs, SIEM, continuous monitoring
- Analyzing monitoring results

4 Incident Response and Recovery (14%)

- Incident response lifecycle
- Forensic investigations
- BCP and DRP: RTO, RPO, MTD
- Backups, redundancy, testing

5 Cryptography (9%)

- Reasons and requirements
- Hashing, salting, encryption
- Secure protocols
- PKI and key management

6 Network and Communications Security (16%)

- OSI and TCP/IP, ports and protocols
- Network attacks and countermeasures
- Network access control and segmentation
- Security appliances
- Wireless and IoT

7 Systems and Application Security (15%)

- Malicious code and activity
- Endpoint device security
- Mobile provisioning: COPE, BYOD, MDM
- Cloud security
- Secure virtual environments

Smart Admins Rarely Ignore Critical Network Signals

S Security Concepts and Practices **A** Access Controls **R** Risk Identification, Monitoring and Analysis
I Incident Response and Recovery **C** Cryptography **N** Network and Communications Security **S** Systems and Application Security

credentialpress.com/guides/sscp-mind-map · free to share and print with this line kept