EC-Council

ECSS™

EC-Council Certified Security Specialist

ECSS Exam Blueprint v1

S.No	Domain	Sub Domains	Weightage
1	**Information Security and Networking Fundamentals**	• Overview of Information Security Fundamentals • Understanding Information Security Laws and Regulations • Overview of Networking Fundamentals • Overview of OSI and TCP/IP Model • Understanding Basic Network Security Procedures and Policies • Overview of Secure Network Protocols	9%
2	**Information Security Threats and Attacks**	• Understanding Various Stages of Hacking Cycle • Understanding Internal Threats (Sniffing, ARP Spoofing, etc.) • Understanding External Threats (Malware Attacks, Password Cracking, DoS, Session Hijacking, etc.) • Overview of Different Social Engineering Techniques • Understanding Various Firewall and IDS Evasion Techniques • Understanding Various Wireless and VPN Threats • Understanding Various Web Applications and Network Threats • Understanding Email Crime	21%
3	**Information Security Controls**	• Overview of Identification, Authentication, and Authorization • Overview of Cryptography and Encryption Algorithms • Understanding Different Firewall Technologies • Overview of Intrusion Detection System (IDS) • Introduction to Data Backup • Securing Organization Against Various Information Security Attacks	23%
4	**Wireless Network, VPN, and Web Application Security**	• Overview of Wireless Networks and Topology • Understanding Different Types of Wireless Encryption • Securing Wireless Networks • Understanding VPN and Protocols Used to Secure VPN • Introduction to Web Applications and Securing Web Application Against Web Attacks	17%
5	**Ethical Hacking and Pen Testing**	• Introduction to Ethical Hacking • Introduction to Penetration Testing	1%
6	**Incident Response and Computer Forensics Fundamentals**	• Overview of Incident Handling and Response Process • Understand Different Computer Security Incidents and Computer Crimes • Overview of Computer Forensics Fundamentals • Understanding Computer Forensics Investigation Methodology	6%

7	**Digital Evidence and File Systems**	• Understanding Digital Evidence and Examination Process • Collecting Digital Evidence from Electronic Devices • Overview of Different File Systems (Windows, Linux, Mac OS X, and CD-ROM / DVD File Systems)	4%
8	**Windows and Network Forensics**	• Understanding Network Forensics Analysis Mechanism • Understanding Windows Forensics (Collecting Volatile and Non-volatile Information) • Collecting Metadata and Events Data • Introduction to Steganography • Understanding Different Types of Steganography based on Cover Medium	10%
9	**Logs and Email Crime Forensics**	• Examining Various Security Logs • Overview of Event Correlation • Overview of Email Technology • Investigating Email Crime and Violation	6%
10	**Investigation Report**	• Writing Computer Forensics Report • Understanding Best Practices for Writing Forensics Report	3%