Exam Certification Objectives & Outcome Statements

The topic areas for each exam part follow:

Access Control & Password Management
: The candidate will understand the fundamental theory of access control and the role of passwords in managing access control.

Contingency Plans
: The candidate will understand the critical aspect of contingency planning with a business continuity plan and disaster recovery plan

Critical Controls
: The candidate will understand the purpose, implementation, and background of the Critical Security Controls

Cryptography
: The candidate will have a basic understanding of the concepts of cryptography, including a high-level understanding of the major types of cryptosystems and steganography.

Cryptography Algorithms & Deployment
: The candidate will have a basic understand of the mathematical concepts that contribute to cryptography and identify commonly used symmetric, asymmetric, and hashing cryptosystems.

Cryptography Application
: The candidate will have a high-level understanding of the use, functionality, and operation of VPNs, GPG, and PKI

Defense in Depth
: The candidate will understand what defense in depth is and an identify the key areas of security and demonstrate the different strategies for implementing effective security within an organization.

Defensible Network Architecture
: The candidate will demonstrate how to architect a network to be monitored and controlled to resist intrusion.

Endpoint Security

The candidate will demonstrate a basic understanding of the function and uses of endpoint security devices, such as endpoint firewalls, HIDS, and HIPS

Enforcing Windows Security Policy

The candidate will have a high-level understanding of the features of Group Policy and working with INF security templates

Incident Handling & Response

The candidate will understand the concepts of incident handling and the processes pertaining to incident handling.

IT Risk Management

The candidate will understand the terminology and approaches to cyber security risk management including identification of the steps of the Threat Assessment process

Linux Security: Structure, Permissions and Access

The candidate will demonstrate understanding of a variety of Linux operating systems, including mobile systems, to better understand how to configure and secure Linux.

Linux Services: Hardening and Securing

The candidate will demonstrate an ability to gain visibility into a Linux system to be able to secure and harden the system.

Linux: Monitoring and Attack Detection

The candidate will demonstrate an understanding of the use of system baselines, log files, and other tools common to Linux operating systems in order to better monitor systems for signs of attack.

Linux: Security Utilities

The candidate will demonstrate an understanding of how to use key security utilities and tools that are available for Linux systems to enhance system security.

Log Management & SIEM

The candidate will demonstrate a high-level understanding of the importance of logging, the setup and configuration of logging, and log analysis with the assistance of SIEMs

Malicious Code & Exploit Mitigation

The candidate will understand important attack methods and basic defensive strategies to mitigate those threats.

Network Device Security

The candidate will have a basic understanding of the risks of network devices and how to secure them.

Network Security Devices

The candidate will demonstrate a basic understanding of the function and uses of network security devices, such as, firewalls, NIDS, and NIPS

Networking & Protocols

The candidate will demonstrate an understanding of the properties and functions of network protocols and network protocol stacks.

Securing Windows Network Services

The candidate will know how to take basic measures in securing Windows network services such as IPSec, IIS, and Remote Desktop Services

Security Policy

The candidate will understand the purpose and components of policy.

Virtualization and Cloud Security

The candidate will have a basic understanding of the risks of virtualization and cloud services and how to secure them.

Vulnerability Scanning and Penetration Testing

The candidate will demonstrate an understanding of the concepts and relationship behind reconnaissance, resource protection, risks, threats, and vulnerabilities including preliminary abilities to create network maps and perform penetration testing techniques

Web Communication Security

The candidate will demonstrate an understanding of web application security and common vulnerabilities including CGI, cookies, SSL and active content.

Windows Access Controls

The candidate will understand how permissions are applied in the Windows NT File System, Shared Folders, Printers, Registry Keys, and Active Directory, and how Privileges are applied

Windows as a Service

The candidate will understand how to manage updates for a network of Windows hosts.

Windows Automation, Auditing, and Forensics

The candidate will be introduced to the techniques and technologies used to audit Windows hosts.

Windows Security Infrastructure

The candidate will identify the differences between types of Windows OSes and how Windows manages groups and accounts, locally and with Active Directory and Group Policy

Wireless Network Security

The candidate will have a basic understanding of the misconceptions and risks of wireless networks and how to secure them.