**LEMUEL OKECHUKWU**

**VEPH/20B/CY082**

**TASK 38B**

**CYBERSECURITY CERTIFICATIONS TO UPSKILL ONES CAREER**

**TASK 38B:**

* Identify and explain five cybersecurity certification-based roles, highlighting the core responsibilities typically associated with professionals holding these certifications

[](https://www.edoxi.com/studyhub-detail/key-roles-and-responsibilities-of-cyber-security-professionals)

For cybersecurity professionals, obtaining certifications is a significant step towards enhancing their skills and advancing their careers.

**1. Certified Information Systems Security Professional (CISSP)**

The CISSP certification is one of the most recognised credentials in the cybersecurity field. Offered by ISC2 it validates your expertise in designing, implementing, and managing a best-in-class cybersecurity programme.

**Why Does CISSP Matter?**

CISSP demonstrates your ability to effectively manage security in a business environment. It covers eight domains, including Security and Risk Management, Asset Security, and Security Operations. This certification is highly valued by employers, often leading to higher-paying job opportunities.

**Who Should Pursue CISSP?**

This certification is ideal for experienced security practitioners, managers, and executives who want to prove their knowledge across a wide array of security practices and principles.

**How Do I Obtain CISSP?**

To qualify for the CISSP exam, you need at least five years of cumulative, paid work experience in two or more of the eight domains of the CISSP Common Body of Knowledge (CBK). A four-year college degree or an additional certification from the ISC2 [W(1] approved list can substitute for one year of experience.

**2. Certified Ethical Hacker (CEH)**

The CEH certification, offered by the EC-Council, focuses on identifying and addressing security weaknesses by thinking like a hacker.

**Why Does CEH Matter?**

CEH professionals are trained to understand and counteract hacking techniques. This certification covers topics such as footprinting and reconnaissance, scanning networks, and system hacking.

**Who Should Pursue CEH?**

CEH is suitable for security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

**How Do I Obtain CEH?**

To be eligible for the CEH exam, candidates must have at least two years of work experience in the information security field. Alternatively, they can attend an official EC-Council training.

**3. CompTIA Security+**

CompTIA Security+ is an entry-level certification that provides a global benchmark for best practices in IT security.

**Why Does CompTIA Security+ Matter?**

This certification is vendor-neutral, making it a versatile choice for professionals seeking foundational knowledge in cybersecurity. It covers essential principles for network security and risk management.

**Who Should Pursue CompTIA Security+?**

Ideal for beginners, this certification is a great starting point for those looking to enter the cybersecurity field. It's also valuable for IT professionals seeking to transition into a security role.

**How Do I Obtain CompTIA Security+?**

There are no formal prerequisites for the Security+ exam, but it is recommended that candidates have two years of work experience in IT with a security focus.

**4. Certified Information Security Manager (CISM)**

Offered by ISACA, the CISM certification is designed for managing IT professionals on the front lines.

**Why Does CISM Matter?**

CISM focuses on managing and governing an enterprise's information security programme. It covers domains such as Information Security Governance, Risk Management, and Incident Management.

**Who Should Pursue CISM?**

This certification is perfect for individuals who design and manage an enterprise's information security programme and want to demonstrate their expertise in information security management.

**How Do I Obtain CISM?**

Candidates need at least five years of information security management experience. Passing the CISM exam and adhering to ISACA's continuing education policy is required to maintain the certification.

**5. Certified Information Systems Auditor (CISA)**

CISA, another certification from ISACA, is geared towards audit control, assurance, and security professionals.

**Why Does CISA Matter?**

CISA signifies proficiency in assessing vulnerabilities, reporting on compliance, and instituting controls within an enterprise. It covers five domains, including Information System Auditing Process and Governance and Management of IT.

**Who Should Pursue CISA?**

Ideal for IT auditors, audit managers, consultants, and security professionals, CISA is highly regarded in the finance, accounting, and auditing sectors.

**How Do I Obtain CISA?**

Candidates must have at least five years of professional experience in information systems auditing, control, or security. Passing the CISA exam and adhering to ISACA's Code of Professional Ethics is required.

**Benefits of Earning a Cybersecurity Certification**

* **Improved job prospects**: Certificate holders are in high demand and often command higher salaries than their non-certified counterparts.
* **Increased credibility**: A cybersecurity certification demonstrates your commitment to your field and can help you stand out from the competition.
* **Enhanced knowledge and skills**: The process of studying for and taking a certification exam will help you deepen your understanding of cybersecurity concepts and practices. Certificate holders are in high demand.
* **Career advancement**: A cybersecurity certification can open doors to new career opportunities and promotions to you.

In the dynamic field of cybersecurity, certifications are a crucial way to validate your skills and stand out to potential employers. Whether you're just starting your career or looking to advance to the next level, earning one or more of these top certifications can greatly enhance your professional credibility and opportunities.