Cybersecurity and Auditing - All You Need to Know

Duration: 5 Days

Language: en

Course Code: PI1-120

Objective

Upon completion of this course, participants will be able to:

- Understand the importance of cybersecurity within an organisation.

- Investigate the advantages of effective cybersecurity and the consequences of poor cybersecurity.
- Review the technical specifications of cybersecurity.
- Implement information security management.
- Analyse network architecture and intrusion detection systems.
- Conduct risk appraisal and establish risk management plans.
- Identify methods of risk assessment.
- Be familiar with ISO 27001 and COBITS.
- Assess the approach for crisis management and disaster recovery.
- Account for local and regional laws and regulations associated with cybersecurity.
- Review IPv6 and IPv4 configurations and associated risks.

Audience

This course is designed for anyone responsible for cybersecurity and risk management within an organisation. It would be most beneficial for:

- Risk Managers
- Risk Auditors
- Project Managers
- IT Personnel
- System Analysts
- Technology Engineers
- System Engineers
- Communication Specialists

Training Methodology

This course uses a variety of adult learning styles to aid full understanding and comprehension. Participants will review genuine cybersecurity audit examples to highlight key details that make an audit effective.
Combined with presentations, discussions, and practical demonstrations, participants will develop a thorough understanding of the concepts, principles, and skills related to cybersecurity auditing and risk management. They will later be granted the opportunity to create their own audits in relation to their respective roles and supplied with the ideal equipment and programs to do so.

Summary

Within the modern world, technology is constantly advancing at a rapid rate. However, with new technology comes new risks. An organisation utilising technology to any degree should be aware of cybersecurity and have risk management plans in place to maintain system integrity.
Cybersecurity is the process of keeping organisational information safe and covering all digital factors, including finances and customer information. Cyber threats can be minor and, at most, an inconvenience. Still, major threats also exist and could completely disrupt business functions, causing a loss in assets, clients, and reputation. Maintaining effective risk management would reduce the probability of risks and allow the organisation to be better prepared if they do occur.
For cybersecurity to be efficient, cybersecurity audits must be conducted. These audits will detail the technologies themselves, potential threats, and preventative measures. Multiple frameworks can be used as guidelines for these audits to ensure all essential areas are accounted for.
Creating risk and crisis management plans from the information collected in cybersecurity audits is crucial for ensuring safe business functions. In preventing risks and scenarios where risk occurs, the plans should emphasize business continuity and methods for safely recovering losses.

Course Content & Outline

Section 1: IT Security Evolution

- Defining cybersecurity.
- Categorising physical and electronic risk within an organisation.
- Understanding the different communication technologies impacted by identified risks.
- Evaluating computer system designs and how cybersecurity fits within them.
- Reviewing laws and regulations that influence cybersecurity.
- Assess current threats and conduct trend analysis.

Section 2: Risk and Crisis Management

- IPv4 to IPv6 configurations in relation to risk.
- Domain Name System Security Extensions (DNSSEC).
- Identifying what must be involved in crisis and risk management.
- Methods of evaluating risk.
- Creating detailed risk and crisis management plans to be clearly understood by all necessary personnel.
- Forensic and Electronic Investigations.
- Focusing on business continuity.

Section 3: Cybersecurity Audit Preparation

- Utilising the NIST Cybersecurity Framework to prioritise risks.
- Establishing policy requirements for when cyber incidents occur.
- Understanding the elements of the COBIT 5 framework.
- Creating audit plans aligned with both NIST and COBIT 5 frameworks.

Section 4: Executing Cybersecurity Audits

- Reviewing the bowtie method.
- Using the bowtie for continuous risk management.
- Conducting cybersecurity audits using AuditXP software.
- Creating audit questionnaires in AuditXP aligned with NIST and COBIT 5 frameworks.
- Maintaining detailed records of completed audits.
- Integrating audit results with known information to update risk management plans.

Section 5: Cybersecurity Management

- Forming a team of competent individuals.
- Evaluating audits and utilising NIST to prioritise risks.
- Communicating with the team and delegating tasks effectively.
- Creating action plans detailing cybersecurity intentions.
- Implementing changes.
- Continuously monitoring cybersecurity and working for system improvement.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by the British Assessment Council (BAC) and The CPD Certification Service (CPD), and are certified under ISO 9001, ISO 21001, and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

AI, Data and Visualisation, IT & Computer Application, Technology, Finance, Accounting & Budgeting

Tags

Risk, technology, Auditing, security, banking, Cybersecurity, computer

Related Articles

Navigating Cyber Threats: A Full Guide to Risk Management

In the digital era, cybersecurity risk management is paramount. This blog post delves into the process of identifying, assessing, and mitigating cyber risks. Learn about AI-driven solutions, UK laws, and how to integrate risk management with your business objectives.

YouTube Video

https://www.youtube.com/embed/G-48k90DvaM?si=ASUXct8oU0j3Fufi