CISSP Exam Preparation Workshop

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

About CISSP

The CISSP training course provides delegates with a theory-based approach to learning the security process. The course is centered around teaching the fundamental domains of Information Security. These eight domains provide delegates with all the information they require to obtain a comprehensive understanding of Information Security and pass the CISSP exam. Despite being a theory-based course, the CISSP certification trains individuals to practically apply what they have learnt. This CISSP course gives delegates skills which are desirable in any company, and so this qualification can help individuals stand out in a competitive market.

This workshop is designed for this purpose, as well as to provide the insight into the importance of cybersecurity risk management framework covering 8 comprehensive security domains.

For additional information, please write to us at:
info@tlcpak.com

Workshop details:

Domain 1 –Security and Risk Management

1.1: Understand and apply concepts of confidentiality, integrity and availability.
1.2: Evaluate and apply security governance principles.
1.3: Determine compliance requirements.
1.4: Understand legal and regulatory issues that pertain to information security in a global context.
1.5: Understand, adhere to, and promote professional ethics.
1.6: Develop, document, and implement security policy, standards, procedures and guidelines.
1.7: Identify, analyze, and prioritize Business Continuity requirements
1.8: Contribute to and enforce personnel security policies and procedures.
1.9: Understand and apply risk management concept.
1.10: Understand and apply threat modeling concepts and methodologies.
1.11: Apply risk-based management concepts to the supply chain.
1.12: Establish and maintain a security awareness, education, and training program.

Domain 2 – Asset Security

2.1: Identify and classify information and assets.
2.2: Determine and maintain information & asset ownership.
2.3: Protect privacy.
2.4: Ensure appropriate asset retention.
2.5: Determine data security controls.
2.6: Establish information and asset handling requirements.

Domain 3 - Security Architecture and Engineering

3.1: Implement and manage engineering processes using secure design principles.
3.2: Understand the fundamental concepts of security models.
3.3: Select control based upon systems security requirements.
3.4: Understand the security capabilities of information systems.
3.5: Assess and mitigate the vulnerabilities of security architectures, design and solution elements.
3.6: Access and mitigate vulnerabilities in web-based systems.
3.7: Access and mitigate vulnerabilities in web-based systems.
3.8: Assess and mitigate vulnerabilities in mobile systems.
3.9: Assess and mitigate vulnerabilities in embedded devices.
3.10: Apply cryptography.
3.11: Apply security principles to site and facility design.
3.12: Implement site and facility security controls.

Domain 4 - Communication and Network Security

4.1: Implement secure design principles in network architecture.
4.2: Secure network components.
4.3: Implement secure communication channels according to design.

Domain 5 - Identity and Access Management (IAM)

5.1: Control physical and logical access to assets.
5.2: Manage identification and authentication of people, devices and services.
5.3: Integrate identity as a third-party service.
5.4: Implement and manage authorization mechanisms.
5.5: Manage the identity and access provisioning lifecycle.

Domain 6 - Security Assessment and Testing

6.1: Design and validate assessment, test and audit strategies.
6.2: Conduct security control testing.
6.3: Collect security process data.
6.4: Analyze test output and generate reports.
6.5: Conduct and facilitate security audits.

Domain 7 – Security Operations

7.1: Understand and support investigations.
7.2: Understand the requirements for different types of investigations.
7.3: Conduct logging and monitoring activities.
7.4: Securely provision resources.
7.5: Understand and apply foundational security operations concepts.
7.6: Apply resource protection techniques.

In a nutshell, cybersecurity is crucial for protecting sensitive information and systems from cyber threats like hacking, malware, and data breaches, ensuring the confidentiality, integrity, and availability of data. It's important for individuals and organizations to safeguard personal information, financial transactions, and intellectual property, as well as maintain business continuity and comply with regulations.

CISSP Exam Preparation Workshop

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

Target Audience

Business, application, audit, risk, compliance, infoSec and CyberSec Professionals, project managers, IT operations, Enterprise Architectures, and legal professionals with a familiarity of basic IT/IS concepts.

Within any organization, system security is crucial, and it is becoming clear that organizations require better means to combat malicious cyber-attacks, as they increasingly become more and more advanced and difficult to manage. As such, businesses require trained staff who have an up-to-date understanding of the latest threats to information system security.

Workshop Methodology

The training course flow will be a mix of lectures & classroom discussions and videos so that participants can have a detailed understanding of various components and technologies used to combat against cyber attacks.

To see the list of all of our Executive Leadership Series program, please visit: www.tlcpak.com/ELS.html

Domain 7 – Security Operations – Continued

7.7: Conduct incident management.
7.8: Operate and maintain detective and preventative measure.
7.9: Implement and support patch and vulnerability management.
7.10: Understand and participate in change management processes.
7.11: Implement recovery strategies.
7.12: Implement disaster recovery processes.
7.13: Test disaster recovery plans – DRP.
7.14: Participate in business continuity planning and exercises.
7.15: Implement and manage physical security.
7.16: Address personal safety and security concerns.

Domain 8 - Software Development Security

8.1: Understand and apply security in the software development lifecycle.
8.2: Enforce security controls in development environments.
8.3: Assess the effectiveness of software security.
8.4: Assess security impact of acquired software.
8.5: Define and apply secure coding guidelines and standards.

CISSP Certification – Knowledge and Skills

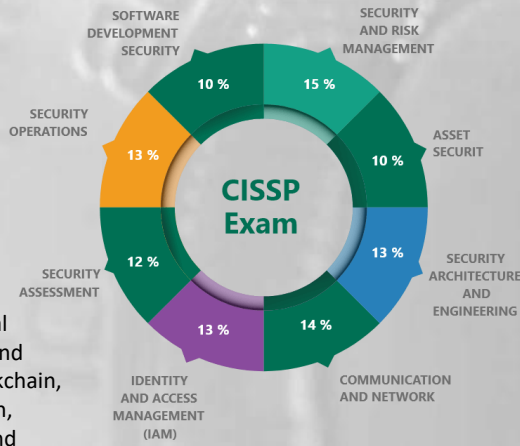
- **Comprehensive Knowledge:** CISSP validates expertise in key security domains, providing a broad understanding of information security principles.
- **Risk Management and Compliance:** The certification demonstrates the ability to manage security risks and ensure compliance with industry standards.
- **Staying Current:** CISSP requires ongoing professional development to maintain the certification, encouraging continuous learning.
- **Organizational Benefits:** Positive Reputation:
- Companies with CISSP-certified professionals demonstrate a strong commitment to security, building trust with stakeholders.
- **Access to Resources:** Certified professionals gain access to exclusive (ISC)² resources, educational materials, and tools.
- **Compliance and Risk Mitigation:** CISSP helps organizations meet compliance requirements and mitigate potential risks.

Career Advancement and Recognition:

Global Recognition: CISSP is globally recognized, making it valuable for professionals seeking opportunities in various locations.
Increased Earning Potential: CISSP-certified individuals often command higher salaries due to their demonstrated expertise.
Career Progression: It can open doors to leadership roles like Security Manager, Director, or even Chief Information Security Officer.
Credibility and Trust: The certification enhances credibility with employers and clients, showcasing a commitment to security excellence.

About the instructor

Training will be delivered by an experienced trainer with 30+ years of career experience imparting education and training services both locally and internationally and have served international enterprise technology vendors including IBM, Fujitsu, and ICL (an England based organization).



Our instructor holds various industry professional certifications in the space of enterprise servers and storage technologies, Information Security, Blockchain, Enterprise Architecture, ITIL, Cloud, Virtualization, Green IT, and a co-author of 10 IBM Redbooks and have designed and developed 75 courseware's based on stack of storage, information security, cybersecurity, enterprise architecture and digital technologies.

Detail Information

Course Code : TN229
Course Duration : 5 Day - Face- to-Face Workshop
Course Location : TLC and Customer On-site.
Terms & Conditions :100% payment in advance.
Course Deliverable : Comprehensive Student Guide and Course Certificate

For additional information, please write to us at:
info@tlcpak.com

Opportunities are made, not found