Cybersecurity Risk Management Framework

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

TLC Education & Training Services

About this workshop

In the era of digital transformation, the importance for having substantial knowledge on cybersecurity is becoming essential skills to acquire for every technology professional today. The reason behind is the protection of information which is considered as one of the critical function for all enterprises. Cybersecurity is a growing and rapidly changing field and it is vital that the principal concepts that frame and define this increasingly pervasive field are clearly understood by technology professionals who are involved and concerned with the security implications of information Technologies.

This workshop is designed for this purpose, as well as to provide the insight into the importance of cybersecurity risk management framework, and the integral role of cybersecurity professionals.

After completing this workshop, you will be able to:

- Understand basic cybersecurity concepts and definitions
- Recognize malware analysis concepts and methodology
- Distinguish system and application security threats and vulnerabilities
- Classify types of incidents (categories, responses and timelines of response)
- Outline disaster recovery and business recovery and business continuity planning
- Comprehend incident response and handling methodologies
- Understand security event correction tools and how different file types can be used for analytical behavior
- Be aware of the basic concepts, practices, tools, tactics, techniques and procedure for processing digital forensic data
- Recognize new and emerging information technology and information security technologies.

Workshop details:

Unit 1 –Cybersecurity Overview

- A world without cybersecurity.
- Top Security Concerns for the Executive Management.
- Understanding Cybersecurity and Cyberspace.
- Differences between Information Security & Cybersecurity.
- Protection layers offered by Cybersecurity.
- Difference types of cybersecurity threats.
- Understanding attack Vector, Attack Surface and Malicious Actors, Malware detection and their types.
- What are the key objectives of Cybersecurity?
- Adoption of Cybersecurity best practices.
- 10 key steps to Cybersecurity.
- Questions you should ask your Security Services Provider.
- What is Zero Trust Security
- What you need to remember – Cybersecurity.
- Unit Assessment.

Unit 2 – Understanding the Role of Risk Management

- Understand Fault Tolerance and Fault Resilience.
- Why data protection is important
- Examining the Cost of a Data Breach.
- Leaders must avoid common myths to avoid threats.
- Understand Incidents, Breaches, Risk & Vulnerability.
- Describe fundamental security principles to help guide you.
- Differentiate between incident, breach, risk & vulnerability.
- Threats and security challenges faced today.
- Threat Management Model and key elements and layers.
- Performing a Threat Modeling exercise.
- Security threats and their channels – A route to your Asset.
- Identify and describe types of risk categories.
- Know your risks & the role of Risk Management.
- Essential practices required to effectively manage risks.
- Defense Planning – Risk Analysis and Assessments.
- Risk Management Approach, key objectives and benefits.
- A small backdrop on ISO 27001 and essential safeguards.
- Understand ISO 27002 and it's essential components.
- Major steps to ISMS implementation.
- Issues/criteria that needs attention from storage security POV.
- Discuss technologies to ensure data storage security.
- Types of comprehensive vulnerability assessments.
- Performing Qualitative Risk Assessments.
- Elements of Risks.
- Top recommendations for closing the security gaps.
- Unit 2 Assessment.

Unit 3 – Principle Guidelines and Cybersecurity Framework

- Understand Cybersecurity Principles and Cybersecurity Laws.
- Describe Strategy and Strategic Planning?
- Steps for creating a Cybersecurity Risk Management Strategy.
- Cybersecurity framework – Things that you cannot ignore.
- Goals and Principles of Cybersecurity.

Cybersecurity Risk Management Framework

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

TLC Education & Training Services

Target Audience

- CIO/CTO, IT Directors, Senior IT Managers, Business leaders, Application, Audit, Risk and Compliance, InfoSec & CyberSec professionals, IT Operations, Project Managers, Network Security Engineers, and Enterprise Architects.
- This workshop is equally recommended for IT Consultants, Systems Integrators, Technology Consultants, Sales and Technical Sales resources who want to refresh their know in the field of Cybersecurity.
- Fresh university graduates who want to embark in the field of 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 available courses , please visit: www.tlcpak.com/educ.html

- Know industry top four security frameworks.
- Understand NIST Cybersecurity Framework.
- Cybersecurity Framework implementation approach.
- Development of the Framework, Framework Components and Framework Profiles.
- CIST Cybersecurity Framework Implementation Tiers.
- Implementing the NIST Cybersecurity Framework using COBIT.
- Implementation alignment of NIST and COBIT.
- Framework key attributes & Examples of Framework Industry Resources.
- Essential publications and general information.
- Center of Internet Security Guidelines: Top 20 Cybersecurity Controls.
- ISO/IEC 27032:2012 – Guidelines for Cybersecurity.
- Unit 3 Assessment.

Unit 4 – Fundamentals of Security Operations Center

- Understand 9 Layers of IT Infrastructure Foundation from overall Security perspective.
- Security Operations Center Defined.
- How to make you SOC responsive?
- Understand what actually a Security Operations Center do?
- Prerequisites to establishing a SOC.
- Understand Cyber Incident Recovery Tool and its importance.
- SOC objectives and questions that you should know to ask.
- Data Collection and Analysis and types of supported SOC Data Sources.
- Prerequisites to establishing a successful SOC.
- SOC Feature Services – Monitor and Manage.
- Requirements for Effective SOC – Resource Availability & Non Availability Matrix.
- Measuring Capability and Maturity levels in Security Operations Centers.
- SOC Capability Maturity Assessment Model.
- Log Management/Analytics – One of the most critical aspect of your SOC.
- SOC Team Structure.
- SOC Design Criteria and Flow.
- Build SOC Approach.
- Common Cybersecurity Mistakes that should be avoided.
- Five key considerations when developing a Security Operations Center.
- Generic SOC Framework.
- Preparation testing should be a part of managing you SOC.
- Describe and understand Penetration Testing and its key stages.
- Zero-day and your Security Strategy.
- The critical issue with Zero-day vulnerability.
- Suggestions for Mitigating the effects of a Zero-day attack.
- Outside threat protection – The Big Picture.
- Unit 4 Assessment.

About the instructor

Training will be delivered by an experienced trainer with 25+ 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, Enterprise Architecture, ITIL, Cloud, Virtualization, Green IT, and a co-author of 10 IBM Redbooks and have designed and developed 30 plus courseware's based on complete of stack of storage, information security, cybersecurity, enterprise architecture and digital technologies.

Detail Information

Course Code	: TN227
Course Duration	: 1 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