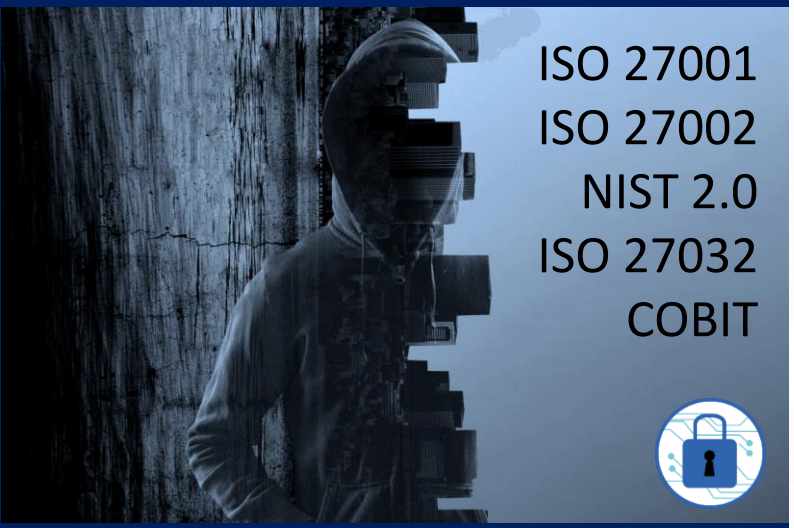
Cybersecurity Risk Management Framework – CSF 2.0

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

TLC Education & Training Services

About this workshop:

The risks that come with cybersecurity can be overwhelming to many organizations. Building a robust **cybersecurity program** is often complicated to conceptualize for any organization, regardless of size. Yet, the cyber security benefits of baselining to an industry-standard guide are worth the restructuring that might be involved. Frameworks are not a new concept to cybersecurity professionals, and the benefits are immense – nor do they need to be complicated to be effective. In this two-day workshop, we will dive into the benefits of the **NIST Cybersecurity Framework (CSF)** and why it should be a cornerstone for your cybersecurity solution.



This workshop is designed based on the purpose to provide the insight into the importance of developing Cybersecurity Risk Management Framework mapping NIST CSF 2.0, ISO 27001, and COBIT frameworks followed by understanding the key role of ISO/IEC 27032:2012, a guidelines for Cybersecurity.

Opportunities are made, not found

After completing this workshop, you will be able to:

- Focus on applying the NIST CSF 2.0 framework in practical scenarios, integrating it with an organization's broader risk management strategy.
- Understand the role of Enterprise Risk Management Framework.
- Distinguish system and application security threats and vulnerabilities.
- Know your risks and the role of Enterprise Risk Management and Controls.
- Demystifying Storage, Data Classification and subsequent Categories and develop Information Security Lifecycle Management strategy.
- ISO/IEC 27032:2012 – Guidelines for Cybersecurity.
- Perform Qualitative Assessments using Simple and DREAD techniques.
- Practice performing actual risk assessments within a specific scope (e.g., a small business network or a specific system) using the CSF's six functions: Govern, Identify, Protect, Detect, Respond, and Recover.
- Develop and integrate using ISO 27001, NIST 2.0 and COBIT frameworks.
- Create "Current Profiles" (an organization's existing cybersecurity posture) and "Target Profiles" (the desired state). The next step involves performing a gap analysis and creating a prioritized action plan to bridge those gaps..

Workshop details:

Unit 1 – Risk Assessment, Mitigation and Response Planning

- Differences between Information Security and Cybersecurity.
- Multiple layers of protection offered by Cybersecurity.
- What are the Key Objectives and Goals of Cybersecurity?
- Foundational steps to Implement Cybersecurity.
- Threat Categories – Network-based, Host-based, & Application-based Threats.
- OSI Layers and Attacks types.
- Understanding Risk and its impact on Cybersecurity.
- Key Steps in Identifying Critical Assets – Example of Critical Assets.
- Risk Sources and Threat Actors – Changing Attacker Profiles.
- Knowing security threats and their channels.
- Attack Progression Model used by Cybercriminals – An Illustration.
- Maintaining a Cybersecurity Asset Inventories.
- A layered Cyber Defense Approach – The bigger picture.
- The importance of Risk Assessment in Cybersecurity.
- Vulnerability Assessment (vulnerability Analysis).
- Types of Comprehensive Vulnerability Assessments.
- Qualitative and Quantitative Risk Assessment.
- How to perform a Qualitative Risk Analysis using DREAD Model – Activity.
- Elements of Risks – The Big Picture.
- Understand Risk Register – A Four Step Process.
- What Data and Information should go into a Risk Register?
- Risk Scoring – Business Impact.
- Risk Mitigation and Response Planning.
- Developing and Implementing Cybersecurity Controls.
- Understand Incident Response Planning.
- Seven Key Phases of an Incident Response Plan.
- Cyber Management Process and Cyber Incident Management Framework.
- Cybersecurity Controls and Compliance Mapping.
- The Challenge of Control Mapping and Control Mapping Process.
- Risk Monitoring, Reporting and Governance.
- Unit 1 Assessment.

Unit 2 – Understanding the Role of Enterprise Risk Management

- Enterprise Risk Management Defined.
- Why Data Protection is important.
- To address security threats, leaders must avoid common myths.
- Three categories of Risks – Business Resilience and Cyber Resilience.
- The Three Lines of Defense Model for Risk Management.
- Understanding Risk Management Framework, Role and Workflow.
- Risk Management: Know your risks and the role of Enterprise Risk Management.
- Know your Storage Risks and than Plan.
- Essential practices required to effectively manage risks.
- Defense Planning – Risk Analysis and Assessments.
- Risk Management Approach, key objectives and benefits.
- 10 essential practices required to effectively manage risk.
- Risk Management Approach, Key Objectives and Risk Management Plan template.
- About ISO 27001 and Key changes in the ISO 27001 2022 revision.
- What are the key objectives of using standard?
- Updated attribute categories for security controls.
- Risk Treatment Plan – An essential part of Risk Assessment Program.
- Key steps to an Effective Risk Assessment using ISO 27001.
- Major steps to ISMS Implementation.
- Automating the Enterprise Risk Management Process.
- General issues that needs attention from Storage Security POV.
- Criteria can help determine the effectiveness of a storage security.
- Key recommendations for developing an Enterprise Risk Management strategy and framework targeting cybersecurity.
- Vulnerability Assessment and vulnerabilities that organizations cannot ignore.
- Performing Qualitative Risk Assessment using Simple and DREAD techniques.
- Top 10 recommendations for closing the security gap.
- Unit 2 Assessment .

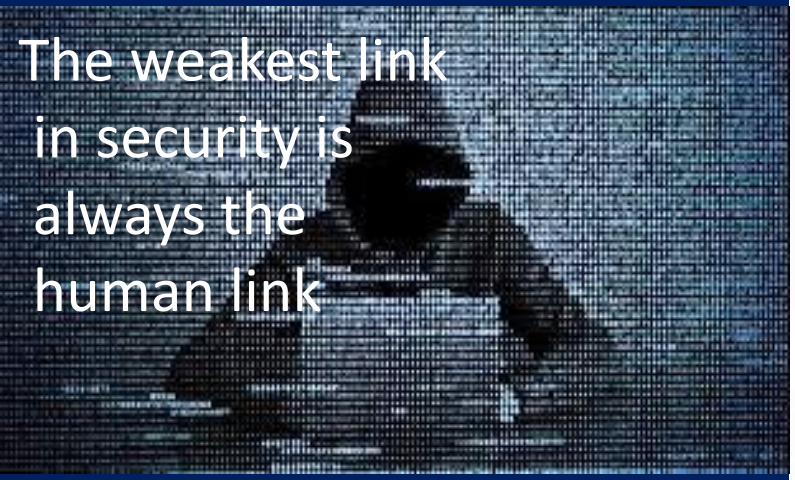
Cybersecurity Risk Management Framework – CSF 2.0

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

TLC Education & Training Services

Target Audience

- CISO, CIO, CTO, IT Directors, VP/IT Directors , IT, Senior IT and IS Managers, Business leaders, CSOC Managers and Threat Hunters, Application Testers, Risk and Compliance, Cybersecurity and Information Security professionals, SOC Teams, Project Managers, Network Security Engineers, Enterprise Architects, Solution Architects, and Technical Writers.
- This workshop is equally recommended for IT Consultants, Systems Integrators, Technology Consultants, Sales and Technical Sales resources who want to upskill their present set of knowledge field of Cybersecurity.
- Fresh university graduates who want to embark in the field of cybersecurity and information 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

Unit 3 – Information Security Lifecycle Management Strategy

- What is Strategy and Strategic Planning?
- Generalize Security Framework – Traditional to Enterprise Security in a View.
- Top 10 Cybersecurity Trends to Watch in 2026.
- Common Storage silos – The Bigger Challenge.
- Understanding why Data Management is important?
- Why do we build Operational Security Controls & Capabilities?
- The Data-driven Enterprise and its Challenges.
- Questions that you should ask as a part of Data Collection & Analysis exercise.
- Five ways to Optimize Data Strategy.
- 14 important information about Data Storage Management.
- Understand Life Cycle Management and Information Security?
- The Information Security Lifecycle Management Program.
- Information Security Lifecycle Model.
- Understanding Data Lifecycle Management – DLM.
- Storage Vs Data Classification.
- Information Lifecycle Management – ILM.
- Exploiting types of ILM Data Storage Strategies.
- Understanding the difference between ILM and DLM.
- Information Lifecycle Management Example.
- Difference between ILM and DLM – Summary.
- Consequences for not following security management lifecycle.
- Unit Assessment 3.

Unit 4 – Principal Guidelines for developing Cybersecurity Risk Management Framework

- Understand Cybersecurity Principles and Cybersecurity Laws.
- Specific business goals for implementing cybersecurity.
- Steps for creating a Cybersecurity Risk Management Strategy.
- Principal Guidelines for Developing Cybersecurity Risk Management Framework.
- Principles of Cybersecurity Laws and Advanced Cybersecurity Solutions.
- Understand Cybersecurity Framework – NIST 1.1 Vs. NIST 2.0.
- Cybersecurity Framework implementation approach.
- Recommended Steps for the Implementation of CRMF.
- Key Roles of NIST 2.0 Core Functions.
- Framework Development, Framework Components and Framework Profiles.
- CIST Cybersecurity Framework Implementation Tiers – Framework Structure.
- Integrating NIST 2.0, ISMS 27001 and COBIT.
- Mapping of an Enterprise Risk Management (ERM) framework to NIST Cybersecurity Framework (CSF) 2.0.
- Considerations for Cybersecurity Risk Management.
- Essential Cybersecurity Templates.
- ISO/IEC 27032:2012 – Guidelines for Cybersecurity.
- Unit 4 Assessment.

Why this workshop is important to attend?

Almost every organization today is undergoing some form of digital transformation. Each new technology and step in this journey can expand the attack surface and expose more assets to the Internet, leaving them vulnerable to threat actors. The explosion of machine identities, cloud entitlements, and remote access pathways have created a fertile environment for attackers.

In this two-day session, we will cover how to develop and integrate Cybersecurity NIST 2.0, ISO 27001-2022 and COBIT frameworks. Also, you will learn how organizations enables identity-centric security to confidently pursue their cybersecurity risk management framework initiatives at planetary scale using framework key attributes along with examples of framework industry resources followed by using Simple and DREAD Qualitative Vulnerability Assessment tools.

In a nutshell, 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 functions 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.

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.

Our instructor holds various industry professional certifications in the space of enterprise servers and storage technologies, Information Security, Enterprise Architecture, Blockchain, ITIL, Cloud, Virtualization, Green IT, and a co-author of 10 IBM Redbooks and have designed and developed 70 plus courseware's based on storage, information security, cybersecurity, enterprise architecture and digital technologies stacks.

Detailed Information

Course Code	: TN227
Course Duration	: 2 Day Face-To-Face Workshop
Course Location	: TLC, Customer On-site, and Online.
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