itSM Solutions®
IT Experience. Practical Solutions.

NISTCSF Foundation Training
Course Description & Outline

The NIST CSF Foundations Course outlines current security challenges and explains how organizations who implement a Cybersecurity Program based on the NIST CSF can mitigate these risks

IS THIS COURSE RIGHT FOR YOU OR YOUR STAFF?	WHO SHOULD ATTEND?	WHAT'S COVERED IN THE COURSE?
Do you want to: ▪ Understand how improved security leads to risk mitigation ▪ Build your knowledge of the NIST Cybersecurity Framework ▪ Learn how implementing security tools/ technologies and establishing effective operational and management practices can reduce cybersecurity risk **WHAT'S IN IT FOR YOU?** **What is covered:** The NIST CSF Foundations training course outlines the challenges surrounding critical infrastructure sector security and explains how implementing a security program based on the NIST Cybersecurity Framework can help organizations mitigate these issues. Key areas of discussion include: ▪ Control costs and gain real-world insights on best practices ▪ Understand the NIST Cybersecurity Framework and related technical and business controls. ▪ Drive security controls and best practices across your business environment **COURSE DELIVERY** Course content is delivered as: ▪ Self-paced eLearning course ▪ Hosted one-day, on-site instructor-led training for an organization's employees or clients You will earn five (5) Continuing Professional Education (CPE) hours for the eLearning course and six (6) for the instructor-led option. There is no exam or qualification associated with this course.	Geared to a broad audience including executives, managers, as well as staff who are responsible for or affected by cybersecurity and risk management requirements, this course is for anyone interested in learning more about the NIST Cybersecurity Framework, with a focus on those individuals working for organizations that are directly or indirectly responsible for building or complying with the organizations cybersecurity or risk management program. Perquisites - None Typical job titles include: ▪ IT Audit Manager ▪ IT Audit Specialist ▪ Business Analyst ▪ Compliance Officer ▪ Finance Manager ▪ IS Manager ▪ IT Specialist ▪ Project/Program Manager ▪ Risk Manager ▪ Risk Analyst ▪ Security Manager ▪ Security Analyst ▪ Senior Developer ▪ Software Engineer ▪ System Administrator ▪ Web Master	This course helps improve security, reduce the risk of data loss / compromise, and improve security controls for an organization: ▪ High-level overview of NIST Cybersecurity Framework and the key deliverables including core functions, implementation tiers, and security profiles ▪ Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk ▪ Framework Core Functions include a set of cybersecurity activities, desired outcomes, categories, subcategories, and applicable references that are common across critical infrastructure sectors ▪ Framework Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. ▪ The Profile is characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. ▪ Understand the Controls Factory Model that organizations can use to better understand how the NIST Cybersecurity framework can be used to implement technical and business controls. ▪ Understand the key components of the Controls factory including the Engineering Office, Technology Center and Business Center. Upon completion of the course, you will be able to: ▪ Understand the key elements of risk including threats, vulnerabilities, controls and assets / identities ▪ Understand the NIST Cybersecurity Framework capabilities ▪ Understand the Controls Factory Model and deliverables ▪ Understand the key technical and business elements of a Cybersecurity Program and a Risk Management Program