

COURSE DESCRIPTION:

Cybersecurity Risk Management Framework Strategy for Defense Platform Systems



The Cybersecurity Risk Management Framework Strategy for Defense Platform Systems course prepares command leadership to implement the National Institute of Standards and Technology's (NIST) cybersecurity Risk Management Framework (RMF) from a Platform Information Technology (PIT) perspective.

This one-day workshop reviews the five functions of cybersecurity (identify, protect, detect, respond, recover) that leadership must consider when making decisions about program resources and requirements. Leaders will learn how to apply the risk management framework – from identifying cyber threats and how they impact operation, to assigning control strategies and analyzing the cost and benefits of secure designs.

Technical innovations offer capability and efficiency advantages but also introduce risks to data confidentiality and integrity, and system availability. To help leaders define and mitigate cyber risks, attendees in this class will review case studies of successful cybersecurity programs. This is followed by practicing a process for creating a strategic action plan to implement the risk management framework in their environment.

Learn How to:

- List the five functions of cybersecurity
- Identify cyber threats and impact on operation
- Assign control strategies to mitigate threats
- Analyze cost and benefits of secure designs
- Create strategic action plan to implement RMF

What Our Students Are Saying:

"Learning activities kept the course energized and interactive. Facilitator practiced what she taught; very relevant."

*- Training Specialist,
US Marine Corps*

"Truly amazed how [LCE] picked up on our requests for tying in our info into the curriculum. Very professional SME's on the material and delivery."

*- Kathleen Gebhard,
SPAWAR*

Who Should Attend:

Individuals and teams responsible for the application of Risk Management Framework (NIST SP800-37) and cybersecurity of special purpose systems within the DoD. This includes those with funding authority and responsibility for security for infrastructure, software, systems, communication and IT personnel.

- DoD Program Managers
- Technical Managers
- Technical Directors
- Requirements Officers
- IT Managers

Course Information:

Each course includes a comprehensive active learning manual, morning and afternoon refreshments and lunch. This is a one-day class. All students completing a class at the Life Cycle Institute will receive a certificate of completion awarding .8 CEU's.

Life Cycle Institute:

Life Cycle Institute is a recognized and respected leader in Learning, Leadership and Change Management solutions. Be prepared to be an active learner. When you invest in training with the Life Cycle Institute, you will gain knowledge and learn skills that you will be able to apply immediately. Our courses are designed to teach by doing. Your training with the Life Cycle Institute is different because we offer:

- Facilitators who practice what they teach and teach what they practice
- Course content that is constantly updated with the latest proven tools and methods
- Adult learning methods that minimize lecture and emphasize learning by doing
- Classrooms that are specifically designed to facilitate learning

Registration:

Download our class schedule for the latest class dates and course costs or contact the Life Cycle Institute at: 800-556-9589 • education@LCE.com • www.LCE.com

Private Classes:

Your training needs are unique. Unique needs may require customized, on-site training. Learn from practicing reliability professionals – on your site – at a time convenient for you – tailored for your environment. For more information please contact education at: 800-556-9589 • education@LCE.com • www.LCE.com