LDR419: **Performing A Cybersecurity Risk Assessment™**

2 Day Course | 12 CPEs | Laptop Required

You Will Be Able To

- Construct a risk management program
- Create a cybersecurity program charter
- Choose appropriate cybersecurity safeguards
- Perform third-party risk assessments
- Perform a cybersecurity risk assessment
- Evaluate cybersecurity documentation
- Examine the implementation of cybersecurity safeguards
- Thoroughly report risk to business stakeholders
- Effectively report risk to technical stakeholders
- Productively respond to risks identified during an assessment

Who Should Attend

- Risk management professionals
- Governance, risk, compliance professionals
- IT auditors
- Directors of security compliance
- Information assurance management
- System administrators/engineers

NICE Framework Work Roles:

- Risk Management (RSK) SP-RSK-001
- Risk Management (RSK) SP-RSK-002
- Test and Evaluation (TST) SP-TST-001

Business Takeaways

- Establish the business case for a cyber security risk assessment
- Prepare for a risk assessment that matters to the business
- Meet and exceed regulatory requirements
- Effectively export the results of a risk assessment to key stakeholders
- Create a strategy for how to respond to identified cybersecurity risks

Every organization should be performing risk assessments as a part of their cybersecurity program. Regular risk assessments allow organizations to create practical strategies for defense and evaluate where there are weaknesses in their cybersecurity program that could keep them from achieving their goals. Most cybersecurity risk courses are theoretical and academic, often leaving students unsure how to do the actual assessment work. This cyber security risk assessment training teaches students the practical, hands-on skills they need to perform risk assessments.

The course uses the Cyber42 leadership simulation game to put students into real-world scenarios that spur discussion and critical thinking of situations that they will encounter at work. Throughout the class students will participate in multiple Cyber42 activities to help them practice what they learn and ensure that they will be able to take these skills immediately back to the office.

Author Statement

"Every organization needs to be performing risk assessments on a regular basis, no matter what kind of organization it is. We do risk assessments for two main reasons. First, we do risk assessments to figure out what defenses our organizations need to make sure our technology supports our business objectives. Second, we do risk assessments to identify where our organization is not doing the things, we should be doing to defend ourselves and ensure stakeholders understand those gaps.

"I wrote this class to give students a practical understanding of how to perform risk assessments of all types. This course starts by teaching students the foundational context of risk and then quickly pivots to cover a specific, step-by-step approach for performing a cyber security risk assessment. Students will leave this class with the knowledge, tools, and templates they need to return to their offices and perform a risk assessment, communicate the results to business stakeholders, and productively respond to identified risks. I hope students will take what they learn and use it to make a difference in their organizations."

—James Tarala

Section Descriptions

SECTION 1: Preparing for A Cybersecurity Risk Assessment

To effectively perform a risk assessment, cybersecurity professionals need to understand the business context for cybersecurity risk. Ultimately, risk assessments are not performed in a vacuum—they can only exist in the context of technology and business objectives. Understanding risk requires students to understand a framework for cybersecurity governance and how risk fits into that framework. In other words, before someone can perform a risk assessment, they need to understand how to prepare themselves for a risk assessment and why they are performing a risk assessment. In this section of the course, students will learn the practical, foundational skills necessary to prepare for and plan for performing a risk assessment.

TOPICS: The Business Context for Risk Assessment; An Architecture for Governance and Risk; The Risk Management Lifecycle; Selecting Cybersecurity Safeguards; Scoping Internal vs. Third-Party Risk Assessments

SECTION 2: Performing A Cybersecurity Risk Assessment

In this section of the course, students will learn the step-by-step practical skills to perform a cybersecurity risk assessment. Students will be provided templates, tools, and checklists for performing a cybersecurity risk assessment and taught the skills necessary to use those resources effectively. Through the extensive use of real-world case studies, students will have the opportunity to practice the skills they learn and be able to put them into practice under the guidance of an experienced instructor-mentor. To close the class, students will learn what to do with the results of their assessment and their role in encouraging an organization's stakeholders to take appropriate steps to respond to the risks identified throughout the process.

TOPICS: Risk Assessment Quality; Evaluating Cybersecurity Documentation; Evaluating Cybersecurity Safeguards; Presenting Risk to Stakeholders; Risk Remediation and Response