



## Cyber Resilience (CRLE 2000)

**Track:** Cyber Resilience

**Course Title:** Cyber Resilience

**Course ID:** CRLE 2000

**Relevant Certifications (requires additional step):** ACRP, CCRP

**Duration:** 4 Days (4 full days of instruction 8:30 a.m. – 5:00 p.m.; Examination online at your leisure)  
32 Continuing Education Activity Points (CEAPs) may be awarded towards recertification.

**Examination:** Cyber Resilience Examination

The cost of this course includes both the course and the exam.

**Cost:** \$2,850.00

### Description

Cyberattacks are a constant threat, causing substantial financial losses and disrupting critical business operations. A robust cyber resilience practice is essential to mitigate these risks and ensure a swift recovery. This CRLE 2000 Cyber Resilience course provides a comprehensive four-day experience, equipping you with the knowledge and skills to build a holistic organizational defense against cyber threats.

This course delves into the critical integration of business continuity, cybersecurity, and mission-critical functions within your organization. You'll explore the six core phases of the NIST Cybersecurity Framework 2.0, which closely align with the DRI International's Professional Practices for Business Continuity. Collectively, these concepts and the resulting action plans, aligned with DRI best practices, will help you develop a strategy to effectively respond to unforeseen events and get your organization back up and running as quickly as possible.

Collaboration is essential for a prompt, effective, and efficient response, and with this course, you'll learn how to make that happen in your organization. Doing so will result in well-coordinated preparation, response, and recovery to cyberattacks and data breaches. As a cyber resilience professional, you'll not only be giving your organization an advantage against cyberattacks, but you'll also be giving yourself the professional advantage, bringing the most current information and skillsets to the table.

### Objective

1. Provide students with detailed instruction, case studies, examples, frameworks, and guidance for implementing the concepts essential to combining cyber security and business continuity into an effective Cyber Resilience program.
2. Prepare students with, activities, exercises, and actionable recommendations to represent an appropriate "value proposition" to an organization's executive management that will help to ensure any investment necessary to step up to a strong Cyber Resilience program.



For more information, visit [drii.org](https://drii.org).



3. Have students engage in cyber, response, and recovery exercises to help understand the issues that they will face.
4. Share experiences with other professionals.
5. Prepare to pass the Cyber Resilience Examination, so students can take the next steps toward being certified as a DRI International Certified Cyber Resilience Professional.

## Outline

### **DAY 1**

- Stepping up from cybersecurity into cyber resilience
- Types of recent cyber threats and cyberattacks
- The cause-and-effect relationship and how cybersecurity affects business continuity
- NIST 2.0, the cybersecurity framework
- The CIA triad and cyber resilience
- The problem, the challenge, and the approach

### **DAY 2**

- The value of cyber resilience
- Achieving cyber resilience with cultural change
- Cyber resilience minimum requirements
- The powerful business impact analysis aligned with cybersecurity
- Integrating cybersecurity and business continuity
- Cyber insurance
- Cybersecurity framework and regulations

### **DAY 3**

- Cyber resilience planning
- Adapting the cybersecurity framework
- Creating effective
  - Preparation and identification plans
  - Protection and detection plans
  - Response and recovery plans
- Effective collaboration between cyber incident response and business recovery of operations



For more information, visit [drii.org](https://drii.org).



#### DAY 4

- Describe the importance of regular cyber awareness training
- Understand how cybersecurity and business continuity both work with reputation management
- Creating and maintaining your plans
- Creating effective crisis communication plans for cyber incidents
- Discuss how training and awareness initiatives should be employed to embed cyber resilience within the entire organization and ensure that personnel are ready to respond and recover
- Cyberattack tabletop

#### For in-person courses:

This course will be held in-person, and the exam will be online, at-leisure. A computer is required for this course in order for you to take the exam. The system requirements will be sent to you via email together with information about how to access the course materials prior to the start of the course.

#### For courses held online:

All online courses are held via Zoom and a computer is required for this course. The system requirements will be sent to you via email together with information about how to access the course materials prior to the start of the course. You will also be provided with instructions for how to take the exam online, at-leisure following the course.

#### For international courses:

This course is being hosted by a DRI International partner. To register, you will be asked to provide your contact information and we will put you in touch with the local team for details.

#### For courses held pre-conference:

This course is being held in-person prior to the DRI Annual Conference at or near the conference venue. You can attend the conference immediately following the course with additional registration (separate fee applies).

#### Career Track:

Educate. Certify. Connect.



##### Cyber Resilience

Master the elements of cyber resilience by  
Integrating business continuity and cyber security.

Cyber Resilience (CRLE 2000)  
Cyber Resilience Review (CRP 501)

ACRP  
CCRP



For more information, visit [drii.org](https://drii.org).