# Cyber Resilience Course (CRLE 2000)

**Course ID:** CRLE 2000
**Language:** English
**Relevant Certifications (requires additional step):** ACRP, CCRP
**Duration:** 4 Days (4 full days of instruction; Examination online at your leisure)
**Examination:** Cyber Resilience Examination
**Cost: 2.600,00 Euro + VAT (if applicable)** The cost of this course includes the course and the exam

**Description**

Cyberattacks are causing increased losses and significant delays in the recovery of mission-critical business functions. A cyber resilience practice can enhance overall resilience and mitigate losses caused by such attacks. That's why this course is an absolute must. Cyber Resilience is an information-packed, four-day experience that will provide a holistic perspective and understanding of how the entire organization should prepare for, respond to, and recover from cyberattacks.

Through this course, you'll discover how business continuity, cybersecurity, and mission-critical functions must integrate within every organization, using the five elements of cyber resilience: prepare/identify, protect, detect, respond, and recover. Collectively, these concepts and the resulting action plans 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.
3. Have students engage in cyber, response, and recovery exercises to help understand the issues t they will face.
4. Share experiences with other professionals.

5. Prepare to pass the Cyber Resilience Examination, so students can take 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, 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

**DAY 4**

- Describe the importance of regular cyber awareness training
- Understand how cybersecurity and business continuity both work with reputation management
- 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

## Course delivery modes

### Public courses

These courses are open to all, and are delivered online or in person: check the calendar of courses available in Italy at www.dri-italy.it

### Private courses

Companies, Associations, and Public Bodies wishing to train several employees, partners or collaborators may request from segreteria@dri-italy.it a quotation for a private course, which will be delivered at the purchaser's preferred times and locations.

## Certifications

The course enables students to take the certification examination and - in the event of success - subsequently purchase the required certificate (ACRP, CCRP) directly on the DRI International website www.drii.org

All certifications require payment of a one-off fee NOT included in the course fee, payable by credit card at www.drii.org - The certification costs in 2025 are as follows:

- ACRP: 200 USD
- CCRP: 400 USD

ACRP certification (Associate Cyber Resilience Professional)

ACRP certification has no requirements other than passing the final examination.

CCRP (Certified Cyber Resilience Professional)
Applicants with more than two years of Cyber/BCM/DR experience may apply for a higher level of certification

## Contacts

Email segreteria@dri-italy.it for additional information