DESIGN QUALITY SERVICES
DRIVEN TO SUPPORT INNOVATORS

CYBERSECURITY RISK MANAGEMENT (CRM)

COURSE OVERVIEW

Cybersecurity Risk Management (CRM) for medical devices is the systematic process of identifying, analyzing, evaluating, and controlling risks associated with cyberattacks, data breaches, and unauthorized access to medical device systems. This course was developed by practitioners, for practitioners, to address global cybersecurity regulatory requirements, support product submissions, and build more secure medical devices.

COURSE CURRICULUM

- Cybersecurity Regulations & Guidance
- Cybersecurity & Product Development
- Secure Product Development Framework (SPDF)
- Threat Modeling
- Network Diagrams & Security Architecture
- Cybersecurity Evaluations & Testing
- Software Bill of Materials (SBOM)
- CIA Triad & Safety Risk Management
- Cybersecurity Risk Management Process
- Common Vulnerability Scoring System (CVSS)
- Cybersecurity Risk Control Measures
- Evidence Capture & Trusted Input
- Vulnerability Disclosure & Collaboration
- Post-Market Cybersecurity & Device Updates

COURSE AT A GLANCE

Price: $1,500
Lessons: 359
Video Content: 3 hours
Quizzes: 14
Final Exam: 1
Time Limit: 60 days
Certificate: Yes, upon passing
Format: Self-paced

LIVE EXPERT SESSIONS

Each student receives two live virtual sessions with a DQS expert:

Before Class: 30-minute orientation session

After Class: 60-minute Q&A and implementation support

90 minutes of personalized expert guidance included!

DOWNLOADABLE FILES

- Complete course slides
- Sample CRM procedure, comprehensive Cybersecurity Risk Analysis template, and CVSS example
- Practice device exercises and a list of additional resources

LEARNING OBJECTIVES

- Analyze and apply regulatory requirements for cybersecurity in medical devices across US, EU, and global jurisdictions
- Implement a Secure Product Development Framework (SPDF) integrating cybersecurity throughout design controls
- Conduct comprehensive threat modeling to systematically identify security vulnerabilities, threats, and assets
- Execute cybersecurity risk assessments using the CIA triad and standardized scoring approaches like CVSS
- Design layered security architectures with authentication, authorization, encryption, and evidence capture systems
- Develop cybersecurity evaluation strategies, including penetration testing, vulnerability assessments, and fuzz testing
- Create and maintain Software Bills of Materials (SBOMs) for supply chain transparency and vulnerability management
- Integrate cybersecurity into Software Development Life Cycle (SDLC) processes with proper configuration management
- Establish postmarket cybersecurity management, including coordinated vulnerability disclosure and secure updates
- Anticipate auditor expectations and demonstrate systematic cybersecurity risk management to regulatory bodies