

# SOEBIT Cybersecurity Quantum Computing Foundation (SCQCF)



## 1 day edition Course Overview

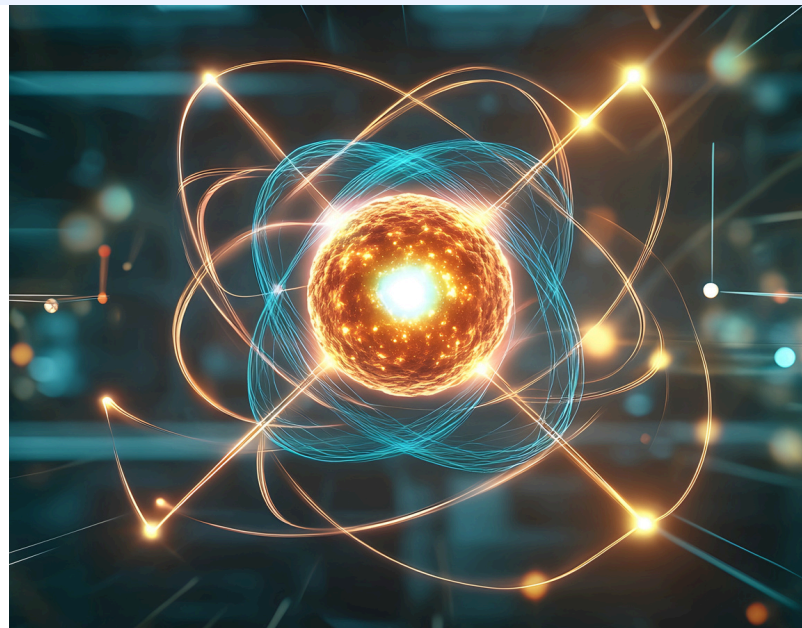
The Quantum Computing Foundation (SCQCF) training course delivers a comprehensive and practical introduction to the principles, models, and real-world implications of quantum computing technologies. This course explains how quantum systems differ from classical computing and covers foundational concepts such as qubits, superposition, entanglement, interference, and quantum measurement. It also introduces key quantum computing architectures, quantum algorithms, and the emerging quantum technology ecosystem.

Participants develop a strong conceptual foundation in how quantum computing works, where it provides advantages over classical systems, and how it is expected to impact fields such as cybersecurity, optimization, artificial intelligence, and scientific research. The course also addresses current limitations, risks, and readiness challenges associated with real-world quantum adoption.

By the end of this program, learners gain the knowledge required to evaluate quantum computing claims, participate in informed technical and strategic discussions, and assess organizational preparedness for future quantum developments.

## Course agenda

- Introduction to Quantum Computing
- Classical vs Quantum Computing Models
- Qubits, Superposition, and Entanglement
- Quantum Gates, Circuits, and Algorithms
- Quantum Computing Architectures and Ecosystem
- Impact of Quantum Computing on Cybersecurity
- Quantum Readiness, Risks, and Adoption Challenges
- Practical Quantum Readiness Assessment Scenarios



## Prerequisites

- No prior quantum computing, advanced mathematics, or physics experience is required.
- This course is designed for beginners and professionals from diverse backgrounds.

## Why should you attend?

As quantum computing advances from research labs toward early commercial and enterprise use, understanding its fundamental principles has become increasingly important for both technical professionals and decision-makers. Quantum technologies introduce new computational capabilities, but also significant challenges, including security implications, skills gaps, and uncertainty around timelines and practical deployment.

Many organizations struggle to separate realistic quantum opportunities from hype, leading to misaligned investments or unpreparedness for long-term risks such as cryptographic disruption. This course enables participants to clearly understand how quantum computing operates, what it can and cannot do today, and how organizations can approach quantum readiness in a structured and informed manner.

## Who should attend?

This course is ideal for professionals across technical and non-technical roles, including:

- Students, beginners, and early-career professionals building foundational knowledge of emerging technologies
- Managers and decision-makers responsible for technology strategy, innovation, or long-term risk planning
- Engineers, architects, and researchers interested in quantum computing concepts and applications
- Information security and cryptography professionals preparing for future quantum-related risks
- Professionals involved in R&D, innovation programs, or advanced computing initiatives
- Anyone responsible for understanding the business, security, or strategic implications of quantum technologies

## What You Will Learn

By completing this course, you will be able to:

- Understand the fundamental concepts and principles of quantum computing
- Explain how qubits, superposition, entanglement, and interference enable quantum computation
- Describe common quantum computing models, hardware approaches, and algorithm categories
- Identify potential applications and limitations of quantum technologies across industries
- Recognize the impact of quantum computing on cybersecurity and encryption systems
- Assess organizational quantum readiness and emerging adoption challenges

## Key Skills Gained

- Quantum computing conceptual literacy
- Technology and risk awareness for emerging computing models
- Understanding of quantum algorithms and architectures
- Cybersecurity impact analysis from quantum advancements
- Strategic thinking for quantum readiness and innovation planning
- Informed evaluation of quantum technology claims and use cases

## Career Benefits

After completing this course, you will be better prepared to:

- Participate confidently in quantum computing discussions and initiatives
- Support informed technology and innovation decisions
- Assess future cybersecurity risks related to quantum advancements
- Contribute to organizational quantum readiness planning
- Navigate emerging opportunities and limitations of quantum technologies

