Enhancing Cybersecurity Through Capacity Building and Accreditation

One-Day Awareness Programme on Accreditation Scheme for IT/ICS Training Bodies (TBs) & Consultancy Organisations (COs)

Key Takeaways

- Accreditation Insights: Gain a clear understanding of the Accreditation Scheme for TBs and COs, ensuring dependable training and consultancy services.
- Capacity Building: Explore how accredited TBs and COs equip CSEs with the expertise required to implement and sustain robust cybersecurity measures.
- Framework Overview: Learn about the Conformity Assessment Framework (CAF) and its alignment with national and international standards.
- Comprehensive Lifecycle Support: Understand the role of accredited COs in assisting CSEs during preparatory and implementation phases of cybersecurity management.

Who Should Attend?

- IT/ICS Training Bodies (TBs) aspiring for accreditation.
- IT/ICS Consultancy Organisations (COs) seeking accreditation.
- Professionals from Critical Sector Entities (CSEs).
- Cybersecurity practitioners and consultants.
- Government and industry stakeholders.
- Academic and training institutions.
- Applicable to all sectors.

Why Attend?

- Build Capacity: Gain actionable insights to improve cybersecurity skills and organizational resilience.
- Ensure Quality: Understand the accreditation criteria that ensure credible training and consultancy services.
- Strengthen Resilience: Learn how to implement effective cybersecurity measures aligned with global best practices.
- Support CSEs: Equip your organization to handle evolving cyber threats with the right knowledge and support.

REGISTER NOW

About the Programme

The digital age has made cyberspace a cornerstone of modern life, but it also presents significant risks to Critical Sector Entities (CSEs). To safeguard Critical Information Infrastructure (CII) and build resilience, it is essential to enhance professional capacity and implement robust cybersecurity measures.

The Quality Council of India (QCI), in collaboration with the National Critical Information Infrastructure Protection Centre (NCIIPC), has developed the Accreditation Scheme for IT/ICS Training Bodies (TBs) & Consultancy Organisations (COs) under the Conformity Assessment Framework (CAF). This one-day training programme provides an in-depth understanding of these schemes and their role in advancing cybersecurity through competent professionals and accredited organizations.

CONTACT US padd_trg@qcin.org

Strengthening Cyber Resilience in Critical Sectors

One-Day Awareness Programme on Scheme for Cyber Security Management System (CSMS) & Inspection of Critical Sector Entities (CSEs)

Key Takeaways

- CSMS Framework: Understand the three-tiered architecture of Cyber Security Management Systems:
  - Level 1: Basic Technical Criteria (BTC) – Common cybersecurity requirements across critical sectors.
  - Level 2: Supplementary Technical Criteria (STC) – Sector-specific cybersecurity controls for power sector.
  - Level 3: Additional Technical Criteria (ATC) – Advanced controls for specific systems within power sector.
- Inspection Scheme: Learn how inspections validate the implementation and effectiveness of safeguards and configurations in IT/ICS systems.
- Defense-in-Depth Approach: Explore a multi-layered security strategy to strengthen resilience against cyber threats.
- Sector-Specific Controls: Dive into enhanced controls designed for critical sectors like power and Industrial Control Systems (ICS).
- Practical Insights: Address key challenges like availability, risk management, vendor dependency, legacy systems, and resource constraints in control system environments.

Who Should Attend?

- Professionals and decision-makers from Critical Sector Entities (CSEs)
- IT/ICS Cybersecurity Practitioners and Inspectors
- Consultants and Trainers involved in cybersecurity implementation
- Government and regulatory stakeholders
- Industry associations and academic institutions

Why Attend?

- Enhance Knowledge: Deepen your understanding of cybersecurity measures specific to CII protection.
- Stay Compliant: Learn how CSMS and Inspection complement each other to ensure compliance with national and international standards.
- Sector-Specific Focus: Explore tailored cybersecurity controls for critical sectors like power, banking, telecommunications, health, and transportation.
- Actionable Insights: Equip your organization with tools to identify, manage, and mitigate cyber risks effectively.

REGISTER NOW

About the Programme

Cyber threats pose significant risks to Critical Sector Entities (CSEs), impacting national security, economy, public health, and safety. To address these challenges, a robust framework for Cyber Security Management Systems (CSMS) and Inspection has been developed to safeguard Critical Information Infrastructure (CII) and ensure resilience against latest cybersecurity threats.

This training programme, developed by the Quality Council of India (QCI) in collaboration with the National Critical Information Infrastructure Protection Centre (NCIIPC), offers comprehensive insights into the Scheme for CSMS & Inspection. Participants will gain a deeper understanding of how to implement effective cybersecurity measures and inspection protocols tailored for CSEs.

CONTACT US padd_trg@qcin.org

भारतीय गुणवत्ता परिषद्
QUALITY COUNCIL OF INDIA
Creating an Ecosystem for Quality

PADD

Empowering Cybersecurity Experts Through Certification

One-Day Awareness Programme on Personnel Certification Scheme for IT/ICS Cyber Security Professionals

Key Takeaways

- Understanding the Scheme: Learn about the framework for attesting and certifying the competence of cybersecurity professionals in IT/ICS domains.
- Competency Profiles: Explore the defined competency criteria for various job roles, enabling organizations to map activities and tasks to required expertise levels.
- Career Advancement: Discover how certification can enhance employment opportunities and career progression for cybersecurity professionals and aspirants.
- Guidance for Stakeholders: Learn how organizations, training bodies, and consultancy firms can leverage the Scheme to build cybersecurity capacity.
- Third-Party Attestation: Understand the role of Certification Bodies for Persons (PrCBs) in assessing and certifying cybersecurity competencies.

Who Should Attend?

- Cybersecurity professionals and aspirants aiming for certification and career growth.
- Critical Sector Entities (CSEs) building certified cybersecurity teams.
- IT/ICS System Owners defining cybersecurity job roles and competencies.
- Training Bodies (TBs) and Consultancy Organizations (COs) enhancing their services with certified professionals.
- Applicable to all critical sectors.

Why Attend?

- Gain insights into the certification process and its relevance to IT/ICS cybersecurity.
- Enhance your professional credentials and align with current industry requirements.
- Build a pathway for career growth and recognition in the cybersecurity domain.
- Learn how to design training programs and develop organizational competencies in cybersecurity

REGISTER NOW

About the Programme

In the evolving digital landscape, Critical Sector Entities (CSEs) face growing cybersecurity threats that demand skilled professionals to safeguard Critical Information Infrastructure (CII). To address this need, the Personnel Certification Scheme for IT/ICS Cyber Security Professionals has been developed to create a pool of certified professionals with proven competencies to manage cybersecurity risks in IT/ICS systems effectively.

This one-day training programme, organized by the Quality Council of India (QCI) in collaboration with the National Critical Information Infrastructure Protection Centre (NCIIPC), provides insights into the certification process, competency criteria, and expertise levels defined for cybersecurity professionals.

CONTACT US padd_trg@qcin.org