Certified Incident Manager (CIM)™

Certified Incident Manager (CIM) - Certification Overview

The Certified Incident Manager (CIM)™ is a professional credential offered by the Global Association for Quality Management (GAQM) that validates an individual's expertise in incident management within organizational and IT environments. Although GAQM's official site does not currently have a specific named CIM page, the certification typically emphasizes structured processes for identifying, reporting, assessing, responding to, and resolving incidents that impact business operations or IT services — helping minimize disruption and restore normal service operations as swiftly and efficiently as possible. GAQM certifications are globally recognized credentials designed to demonstrate competency in professional practices and quality management domains, and they follow a published body of knowledge and online proctored examination format.

The CIM certification equips professionals with skills and knowledge in incident handling techniques, incident lifecycle methodologies, communication and coordination during incident response, escalation procedures, and post-incident review and reporting. It supports career growth by validating ability to manage incidents in structured frameworks, improving operational resilience, and strengthening organizational readiness against disruptions. Many organizations view certified incident practitioners as valuable assets because they help maintain service continuity, support risk mitigation efforts, and improve stakeholder confidence through standardized incident workflows. GAQM's certifications are intended to be accessible to a broad set of candidates with optional e-book and exam scheduling flexibility.

Target Audience

The Certified Incident Manager (CIM)™ certification is suitable for professionals responsible for or aspiring to roles that involve incident coordination, response, recovery, and communication. Ideal candidates include:

- IT Support Managers and Service Desk Leads
- Incident Response Coordinators and Team Leads
- IT Operations and Systems Administrators
- Risk and Compliance Officers
- Security Analysts and Incident Handlers
- Network Operations Center (NOC) Staff
- Project and Service Delivery Managers
- Professionals transitioning into incident management or IT service roles

What Modules are covered?

Module 1 - Incident Management Fundamentals

Covers the basics of incident management, including definitions, objectives, lifecycle phases (detection → response → recovery → closure), key terminology, and the role of an incident manager n modern business and IT environments.
- Introduction to Incident Management
- Types of Incidents (IT service, security, operational)
- Incident Lifecycle & Prioritization
- Roles & Responsibilities in Incident Teams

Module 2 - Detection, Reporting & Triage

Focuses on how incidents are identified, logged, classified, and prioritized. Covers alerting mechanisms, stakeholder communication protocols, and initial response criteria.
- Monitoring & Detection Tools
- Incident Logging Best Practices
- Triage and Severity Assessment
- Communication Channels for Reporting

Module 3 - Incident Response Planning & Coordination

Teaches planning, coordination, and execution of response activities — establishing response teams, creating playbooks, escalation paths, and coordination with relevant internal and external teams.
- Incident Response Plans & Playbooks
- Escalation Procedures
- Internal & External Communications
- Resource Coordination

Module 4 - Incident Containment, Mitigation & Recovery

Looks at how to effectively contain an incident to limit impact, mitigate harm, and restore systems or services back to normal operation.
- Containment Strategies
- Mitigation Approaches
- Service/Process Recovery Steps
- Testing Post-Recovery Stability

Module 5 - Post-Incident Analysis & Reporting

Focuses on reviewing resolved incidents, extracting lessons, improving processes, and reporting to leadership.
- Post Mortem & Root Cause Analysis (RCA)
- Lessons Learned Implementation
- Performance Metrics & KPIs
- Incident Reporting and Documentation

Module 6 - Governance, Compliance & Continuous Improvement

Covers compliance requirements, legal/regulatory reporting, internal governance standards, and how to keep improving the incident management function.
- Regulatory & Legal Incident Reporting
- Risk & Compliance Interactions
- Policy Development & Governance
- Continuous Improvement Framework