JOB DESCRIPTION - CYBER SECURITY ANALYST -REQUIREMENTS CONSULTANT

About HackIT

HackIT Technology and Advisory Services is an IT/Cyber Security company, operating since 2009. HackIT is an Indian Computer Emergency Response Team, CERT-IN (www.cert-in.org.in) empaneled provider for IT Security Audit Services. HackIT provides a broad range of security consulting and advisory services to a diverse group of clients, including government organizations, corporations, Military establishments, financial institutions and start-up, to name few. Our work spans multiple sectors and industries, including Telecommunications, Defense and Military, ITeS, Financial Services, Aviation, Hospitality, Healthcare and Research. We work end-to-end—from diagnosis to delivery of lasting impact — together generating tangible results that are improving the security posture of organizations worldwide.

Job Title	• Cyber Security Analyst - Requirements Consultant
Location	• Chennai
Duration	• 6 to 12 Months

Job Overview

We are seeking a detail-oriented Cyber Security Analyst – Requirements Consultant to support our Cybersecurity team. The role involves analyzing global cybersecurity regulations, extracting and interpreting technical requirements, and aligning them with existing product and service security controls. The ideal candidate will play a critical role in ensuring compliance with international cybersecurity standards and regulatory frameworks, while strengthening the organization's overall security posture.

Job Responsibilities

- Analyze and interpret global cybersecurity regulations and legislative frameworks (e.g., NIS2 and similar directives).
- Extract and segregate technical cybersecurity requirements from regulatory and legal documents.
- Categorize requirements based on priority (e.g., mandatory, optional, recommended).
- Map regulatory requirements to existing product and service security controls.
- Perform gap analysis between regulatory expectations and current cybersecurity practices.
- Prepare clear, structured, and comprehensive reports on requirement analysis and compliance status.
- Collaborate with internal stakeholders, including cybersecurity, product, and compliance teams.
- Participate in knowledge transfer sessions, project discussions, and review meetings.
- Provide regular updates on task progress in weekly status meetings.
- Ensure adherence to organizational standards, templates, and documentation practices.

- Support continuous improvement of cybersecurity compliance and governance processes.
- Use tools and platforms (e.g., MS Teams, email) for effective communication and collaboration.

Technical Skillsets (Mandatory)

- Strong understanding of cybersecurity regulations and legislative frameworks (e.g., NIS2).
- Experience in requirement analysis and regulatory mapping.
- Knowledge of Operational Technology (OT) cybersecurity.
- Ability to interpret legal and technical documents into actionable security requirements.
- Strong analytical, documentation, and reporting skills.

Technical Skillsets (Preferred)

- Experience working with global compliance standards and frameworks.
- Familiarity with product and service security architecture.
- Exposure to risk assessment and cybersecurity governance.
- Experience working in cross-functional and distributed teams.
- Knowledge of tools used for requirement tracking and documentation.

Education & Certifications

- Bachelor's degree in Engineering, Cybersecurity, Information Security, or related field.
- IEC 62443 Certification (or relevant certification in IEC 62443 series) – Mandatory.

Experience

5-8 years' experience

Send your updated profiles to **careers@hackit.co**