NOVARTIS

Associate Director, DDIT ISC Cyber Defense

Job ID
REQ-10092338
Nov 10, 2026
LOC_CZ

About the Role

#LI-Hybrid
Location: Prague

Key Responsibilities:

- Drive implementation and ongoing compliance with country-specific cybersecurity, privacy, AI, and critical infrastructure regulations.
- Act as a trusted ISC advisor, guiding business and DDIT stakeholders on security policies, controls, and secure practices.
- Support cybersecurity audits, regulatory inspections, and certifications, including evidence preparation and remediation.
- Manage country-level security risks, issues, and incidents, collaborating with SOC, threat detection, incident response, and cyber defense teams.
- Design and deliver impactful security awareness and training programs, including phishing simulations, targeted training, and campaigns.
- Use security behavior data and insights to identify risks and develop targeted awareness interventions.
- Partner across ISC, DDIT, and business functions to coordinate regulatory, security, and country-specific initiatives.
- Leverage AI, automation, low-code/no-code, and AI-assisted development to streamline compliance, reporting, awareness, and security processes.
- Assess AI-related security risks, including data exposure, access controls, prompt injection, insecure integrations, third-party risks, and misuse.
- Monitor KPIs, emerging cyber threats, regulations, and technology trends, translating insights into improved controls, SOC detection capabilities, and security services.

Essential Requirement:

- 8+ years of experience in information security, with strong experience in security governance, cybersecurity regulatory compliance, security risk management, information security advisory, or related areas.
- Demonstrated experience implementing cybersecurity or technology regulatory requirements in a multinational environment, ideally including NIS2 or comparable national cybersecurity and critical infrastructure regulations.
- Strong knowledge of established information security frameworks and standards, such as ISO/IEC 27001, NIST Cybersecurity Framework and related security control frameworks.
- Experience translating information security and regulatory requirements into practical solutions within complex business and technology environments. Experience supporting security risk management, audits, regulatory assessments, inspections or compliance programs.
- Strong stakeholder management, communication and influencing skills, with the ability to explain complex cybersecurity topics to technical and non-technical audiences.
- Hands-on experience using generative AI and AI coding assistants for rapid prototyping or vibe coding, with the ability to build practical automations, integrations, workflows or lightweight applications. Experience may include tools such

as GitHub Copilot, Microsoft Copilot, Power Platform, or comparable technologies.
- Good understanding of AI security risks and controls, including secure AI adoption, data protection, identity and access management, third-party or model risk, prompt injection, sensitive-data leakage, human oversight, monitoring and responsible use.
- Working knowledge of SOC operating processes, including security monitoring, alert triage, incident escalation, threat-informed detection engineering, detection-rule lifecycle management, testing and tuning. Ability to collaborate with SOC teams to establish new detection use cases and rules based on country, regulatory or threat requirements.

Desirable Requirement :

- Recognized information security certification such as CISSP, CISM, CRISC, CISA, CCSP, or ISO 27001 Lead Implementer/Lead Auditor. Experience designing or delivering security awareness and behavior-change programs, including phishing simulations, targeted awareness campaigns, or security training.
- Experience with security automation, SIEM or security analytics platforms, and development collaboration practices such as version control, testing and documentation. Experience with Microsoft Sentinel, Microsoft Defender XDR, Kusto Query Language (KQL), or comparable technologies are advantageous. Experience working within a large, global, and highly regulated organization, preferably within the pharmaceutical, healthcare or life sciences industry.

Expected Annual Base Salary Range for role: 1,120,210.00 - 2,080,390.00 CZK

The base salary offered is determined based on gender-neutral objectives, such as relevant skills, competencies and experience in accordance with the Novartis pay setting policy and upon joining Novartis will be reviewed periodically.

In addition to your base salary, you may be eligible for a performance-based bonus depending on certain performance parameters.

The rewards of being part of our team go far beyond base pay and incentives. We also offer a variety of competitive benefits in kind to help you thrive personally and professionally, such as insurance plans, retirement plans, wellbeing resources and global recognition programs. In addition, we provide flexible and hybrid working options, where possible, and minimum 14 weeks paid parental leave.

Pay equity is a fundamental principle of our employment policy and reflects our commitment to create a diverse, equitable and inclusive environment that treats all employees with dignity and respect, as outlined in our Code of Ethics.

Read our brochure to learn more about our global total rewards offering:
https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf

Note: Benefits and compensation may vary by country and are subject to local legal requirements, including provisions of collective bargaining agreements where applicable. A full overview of your compensation package, including any relevant collective bargaining agreement details applicable to your role based on your employment location and Novartis employer entity, will be communicated separately to you during the application process.

Commitment to Diversity & Inclusion:

Novartis is committed to building an outstanding, inclusive work environment and diverse teams representative of the patients and communities we serve.

Accessibility and accommodation:

Novartis is committed to working with and providing reasonable accommodation to all individuals. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to receive more detailed information about the essential functions of a position, please send an email to di.cz@novartis.com and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

Role Requirements

Primary location salary range
Kč1,120,210.00 - Kč2,080,390.00
Division
DIV_TO
Business Unit
Information Technology
Location
LOC_CZ
Site
Prague
Company / Legal Entity
CZ02 (FCRS = CZ002) Novartis s.r.o.
Functional Area
FCT_IT
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10092338

Associate Director, DDIT ISC Cyber Defense

Apply to Job

Source URL: *https://jobapi.novartis.com/req-10092338-associate-director-ddit-isc-cyber-defense*

List of links present in page

1. https://jobapi.novartis.com/req-10092338-associate-director-ddit-isc-cyber-defense
2. https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf
3. mailto:di.cz@novartis.com
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Associate-Director--DDIT-ISC-Cyber-Defense_REQ-10092338
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Associate-Director--DDIT-ISC-Cyber-Defense_REQ-10092338