Sr. Specialist, DDIT ISC Third Party Risk

Job ID
REQ-10014937
Aug 20, 2024
India

Summary

The Third-Party Cyber Security Risk team within Information Security and Compliance (ISC) function is responsible for managing the cyber security risk arising out of engaging third party information technology and / or data services, this includes evaluating, assessing and monitoring of third-party security programs and ensuring protections for all aspects of third-party security landscape for the scope of services. The role will conduct information security assessments of vendors providing services to Novartis, analyze and review independent security audit reports, analyze threat data, security incidents (if any) of the vendor and / or service(s) / solutions by reviewing security risks holistically and ensure mitigations actions are recommended.

About the Role

Major accountabilities:

- Collaborate with business to understand threats and ensure Novartis most critical business processes and data is protected.
- Highly motivated and possess strong, hands-on, technical knowledge of a wide range of information security topics / controls used for evaluating their design and effectiveness in the third-party landscape
- Ensure implementation of the Third-party controls framework to safeguard the integrity, confidentiality and availability of information owned, controlled or processed by Novartis.
- Assess security risks around third parties and deliver services to reduce exposure -
- Proficient in reviewing independent audit reports like SOC reports (all types), Hi-Trust etc.,
- Ability to make judgements / decisions basis the risk appetite and considering alternative controls.
- Recommend additional security clauses into contracts when deemed necessary basis the residual risk and findings of cyber security posture evaluation.
- Perform assessments and verification of achieved quality levels and risks in respect to external legislative and regulatory requirements, as well as internal policies -
- Establish close collaboration with stakeholders to facilitate alignment with policies, risks as well as internal and external audits.
- Previous information technology/security audit/assessment experience preferred.
- Ensure the security process is governed by organizational policies and practices that are consistently applied.
- Ability to leverage attention to detail and analytical skills,
- Ability to multi-task and work both independently as well as part of an assessment team.
- Ability to plan, execute and document assessment activities following established processes and procedures
- Ability to identify information security gaps of third-party environment and articulate the risk arising out of it.

- Ability to Summarize and draft the assessment outcomes via a report

Key performance indicators:

- Effectiveness of oversight and leadership around information security risk and compliance activities.
- Transparency level of risks across the enterprise.
- Governance elements and principles established and enforced with high efficiency and effectiveness.
- Levels of collaboration/working relationship achieved with enterprise senior management.

Minimum Requirements:
Work Experience:

- 6-10 years of Third-party cyber security risk management
- Influencing without authority.
- Relationship Management.
- Accountability.
- Experience working cross-functionally and trans-nationally.
- Interactions with business stakeholders and vendor partners.
- Collaborating across boundaries.

Information and Cyber Security Skills

- Information Security Areas and controls (Infrastructure Security, IAM / Access Management, Physical Security, Vulnerability Management, Security Operations, End point Security, Network Security, Application Security, Cloud Security, OT Security, Generative AI etc.)
- IT Compliance, Data Privacy / GDPR Compliance and SOX Compliance
- Very good understanding of NIST, ISO 27001, CIS Benchmarks, SDLC, COBIT standards etc.,
- Enterprise Risk Management. Ability to articulate clearly the risk arising out of the gaps / issues identified.
- CISSP, CISM and/or CISA certifications are preferred

Why Novartis? Our purpose is to reimagine medicine to improve and extend people's lives and our vision is to become the most valued and trusted medicines company in the world. How can we achieve this? With our people. It is our associates that drive us each day to reach our ambitions. Be a part of this mission and join us! Learn more here: https://www.novartis.com/about/strategy/people-and-culture

You'll receive: You can find everything you need to know about our benefits and rewards in the Novartis Life Handbook. https://www.novartis.com/careers/benefits-rewards

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

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to hear more about Novartis and our career opportunities, join the Novartis Network here:

https://talentnetwork.novartis.com/network

Why Novartis: Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together? https://www.novartis.com/about/strategy/people-and-culture

Join our Novartis Network: Not the right Novartis role for you? Sign up to our talent community to stay connected and learn about suitable career opportunities as soon as they come up: https://talentnetwork.novartis.com/network

Benefits and Rewards: Read our handbook to learn about all the ways we'll help you thrive personally and professionally: https://www.novartis.com/careers/benefits-rewards

Division
Operations
Business Unit
CTS
Location
India
Site
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10014937

Sr. Specialist, DDIT ISC Third Party Risk

Apply to Job

Source URL: *https://prod1.id.novartis.com/careers/career-search/job/details/req-10014937-sr-specialist-ddit-isc-third-party-risk*

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://talentnetwork.novartis.com/network
3. https://www.novartis.com/careers/benefits-rewards
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Sr-Specialist--DDIT-ISC-Third-Party-Risk_REQ-10014937
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Sr-Specialist--DDIT-ISC-Third-Party-Risk_REQ-10014937