AFRIKA KOMMT! 2022-2024

An Initiative of German Industry for Future Leaders from Africa

Candidate Profile: Information Protection & Security Officer

Company:	**Boehringer Ingelheim**	Boehringer Ingelheim

Education:	The candidate should hold a degree in computer science / business informatics. Security certification (e.g. CISSP, CISM) or similar experience.
Professional Experience:	Technical knowledge of and experience with Information Security architecture and systems including best practices for Information Security (e.g., access control, identity access management, encryption, endpoint security. Working experience in global, multicultural teams. Used to work in a virtual team throughout different time zones. Communicate information security-related concepts to a broad range of technical and non-technical staff. Excellent leadership skills, strong customer focus, strategic thinking, communications, relationship management, negotiation skills. Ability to build consensus and influence decisions. The candidate must be familiar with regulatory requirements relevant to security and data protection / privacy.
Additional Qualifications:	• Fluency in English is a must • Project management training and / or experience, especially experience in agile project methodologies is an addon • Experience in risk management methodology, conducting maturity assessments including proposal of mitigation measures • Good presentation style. Ability to conduct training for different audiences
Division / Department, Place:	Within IT the position is in the Governance, Quality & Compliance area. Specifically in Information Protection & Security (Cybersecurity Governance)
Assignment / Area of Activity:	The candidate's responsibility is to consult and guide all Information Protection & Security relevant topics. Contribute to the creation of global Security strategy and facilitate a consistent and effective implementation. Ensure alignment with IT Security specifications and architectural standards. Consults and advises business and functional areas to understand and establish acceptable levels of risk. Review of new technical solutions and IT systems including cloud initiatives, identifying security risks, and proposing mitigation measures. Drive IP & Security awareness, activities and behavior through regional representation and trainings in proximity to the business partners.
Remarks:	n/a

Preferred Nationality:	No preferences