Information Security Team Lead Customer Compliance

JOB DESCRIPTION:

- Drive the creation and implementation of information security policies, standards, and programs consistent with local, regional, and global strategy
- Develop, maintain, evaluate and implement standards and procedures as well as enforce policies in line with both business requirements and national and international legislative changes related to information security
- Maintain an understanding of global security regulations and compliance controls, and mentor direct reports in detailed understanding of requirements
- Lead engagements and serve as primary point of contact for external auditors and assessors during customer audits and examinations over global Diebold Nixdorf facilities, external and internal business solutions, customer solutions and environments
- Drive the development, maturation and maintenance of the security customer compliance program
- Serve as primary internal point of contact and subject matter expert for customer security related questions, concerns, and issues
- Coordinate the fulfillment of security related customer requests by other team members, including questionnaire completion, requests for documentation, phone based risk assessments, and onsite audits to ensure that all requests receive an appropriate answer. Serve as the primary point of contact for security related customer escalations
- Analyze customer request metrics, trends, issues, and remediation activities and use this information to provide input and advice to leadership
- Lead security risk assessments over business areas, their environments, and vendors to determine and remediate security gaps to security, regulatory and contractual requirements
- Evaluate, identify and remediate any security gaps in our products or solutions related customer and contractual requirements
- Perform other duties as assigned

QUALIFICATION REQUIREMENTS:

Must have:

- Knowledge of multiple security frameworks such as ISO 27001/27002, PCI DSS, COBIT, NIST, and SSAE16
- Knowledge of security and privacy regulations (SOX, PCI, GLBA, GDPR)
- Knowledge of risk management concepts and risk assessment best practices
- Bachelor’s degree in IT, Cyber Security, or other relevant subject area or equivalent experience

- Ability to communicate fluently in English (speak, read, write)
- 4+ years of experience in Information Security, Audit, or other relevant subject area
- Experience managing at least one direct report
- Experience leading security assessments/audits
- Proficiency in PowerPoint, MS Word and MS Excel
- High degree of initiative, dependability and ability to work with little supervision
- Self - motivated person demonstrating good communication skills and ability to work effectively in team environment
- Ability to work in a multicultural and virtual team environment
- High degree of organization and ability to work on multiple tasks/requests simultaneously
- Flexibility to travel domestically and internationally

Nice to have:

- CISA, CRISC, ITIL or similar certification
- Experience dealing directly with customers and maintaining the highest degree of professionalism and patience
- Experience managing multiple direct reports
- Master’s degree in IT, Cyber Security, or other relevant subject area

APPLY NOW

Minimum basic wage component (gross): 1 600 EUR/month