

Information Security Officer

Event Store is a rapidly expanding Open Source Software Database company with offices across the world, embarking on an exciting growth journey to revolutionize how modern distributed systems are built.

The users of Event Store products and services are software architects, senior developers, and operators who strive to build and maintain world-class software applications. Event Store is poised to become a leading database technology for modern distributed applications and these architects, developers, and operators require a high performing database to leverage for their applications.

We are looking for a strong Information Security Officer to deliver a robust information security compliance and certification programme. This location for this role is remote or could be at Event Store's Austin Texas U.S.A, Bath U.K., or The Hague Netherlands office.

Responsibilities

- To assess and implement all IT security procedures and policies
- Management of Information Security compliance to ISO27001 / SOC2
- Carrying out regular internal auditing in line with the internal audit schedule and raising any non-conformances for review
- Work with the delivery team to ensure that information security risks are addressed in every project
- Deliver security awareness training
- Follow and contribute to business continuity/disaster recovery procedures
- Vulnerability management using available tools
- Patch management monitoring ensuring that systems are adequately updated in a timely manner
- Be part of the incident response team
- Suggesting and planning any risk mitigation work
- Maintain the company information security risk assessments and treatment plans

Experience

- Experience in an information security role that focuses on Governance, Risk & Compliance
- Strong analytical skills to analyse security requirements
- Proven expedience & ability to successfully deliver results in accordance to specific deadlines
- Clear ability to engage with technical and non technical audiences at various levels
- Familiarity with relevant UK, US, EU & international security & privacy regulation & legislation would be advantageous.
- Proven track record of being able to assess and prioritise business imperatives to ensure the team supports both the IT and the firms strategic and functional goals

- Experience of implementing, managing or working with risk management methodologies or common information security management frameworks and standards, such as ISO27001, SOC2, ISO 31000, CIS, ITIL, COBIT, PCI-DSS or NIST within a regulated environment, performing risk assessments and business impact analysis would be beneficial

Qualifications

- A valid Information Security related certification such as CompTIA Security+, CISM, CISA or equivalent
- Excellent communication and organizational skills, and the ability to stay focused on completing tasks and meeting goals within a busy workspace