Job Description | Information Security Assurance and Compliance Specialist

Department: Information Security and Risk

Location: Glasgow

Role: Information Security Assurance and Compliance Specialist

The Role

The mission of the firm's Information Security and Risk team is to establish a risk-managed environment that enables the firm to adequately and reasonably protect the confidentiality, integrity and availability of information used by the business and on behalf of clients. The successful candidate will be primarily supporting the team's mission by focusing on internal and Client related security governance, compliance, audit, due diligence and management of risk. The role will require the candidate to work as part of the team that manages overall information security assurance and compliance, maintaining an information security management system (ISMS), responding to client driven information security questions, due diligence and audit requests in a timely manner, represents the firm in external audit and carries out internal audit and controls assurance. The role requires a broad working knowledge of information security standards, best practices, good organisational and writing skills and attention to detail. The role must be sensitive to the nature of Client communication and interactions, and the business context to the requests made of the team. The individual must be self-motivated and feel comfortable working across departments and with other members of the IT team to deliver these services in a timely manner and with a high degree of quality.

Key Responsibilities

- Review proposed Client engagement contracts, SLAs and complete client due diligence questionnaires, audit requests and competitive bids, working to Client orientated deadlines.
- Maintain repository of standard information security responses and design effectiveness evidence for external audit, client assessments, client RFPs, etc
- Maintain and uphold the firm's certifications and Information Security Management System in line with the standard, facilitate such internal and external audit exercises plus ensure timely remediation for any identified non-conformance as is necessary to keep compliance with the ISO27001 certification.
- Assess and recommend information security, governance, risk management, and compliance services and working practices that reflect emerging Client expectations and best meet, develop and improve the firm's current and future information security environment. Assist the Information Security, IT and other departments with the identification and measurement of security risks and help identify appropriate controls. Carry out periodic assurance of controls to ascertain design effectiveness and maturity.
- Assist members of the team to carry out other workloads relating to the operation of the Information Security department during periods of higher demand, or where additional resources are required.

- Facilitate continual improvement by investigating and utilising latest technologies such as Artificial Intelligence/Machine Learning and other process methodologies to help transform the delivery of the services with a focus on greater efficiency and accuracy.
- Identify emerging Client implications and requirements for consideration into the firm's information security frameworks, strategy, roadmap, policies and into IT initiatives roadmap.
- Stay abreast of technical, industry, regulatory and company changes and/or trends as they relate to cyber security, the legal industry, information management, InfoSec, technological standards/trends and IT efficiencies.
- Facilitate/establish and report on monthly metrics and Key Performance/Risk Indicators relating to Client due diligence work.
- Provide education and insight to members of IT and other relevant areas, relating to the requirements and expectations of Clients.
- Build and maintain relationship with the team and relevant members of the Risk and Client Operations departments share best practice and ensure that due diligence activities are coordinated and executed efficiently.

Essential Skills and Experience

- Proven experience of working in an Information Security and IT Risk Management role within a fast-paced environment. Experience within the legal industry is ideal, but not essential.
- Operational knowledge of one or more international information security standards, risk management and control frameworks/practices e.g. ISF SOGP, ISO27001/2, ISO31000, IRAM2, NIST 800-53 and cybersecurity framework. COBIT, CPS-234 etc.
- Strong organisational skills and the ability to handle multiple conflicting priorities.
- Able to work to very tight deadlines under pressure and to assimilate information quickly.
- Strong interpersonal skills including confidence, positivity, diplomacy, the ability to influence and persuade, maintain an open viewpoint, and to gain credibility quickly across the Firm and with Clients.
- Excellent verbal and written communication skills, with the ability to simplify technical points where required, and to present effectively to senior stakeholders and managers.
- Demonstrates attention to detail with a high level of accuracy.
- Positive and tenacious with the ability to pro-actively drive initiatives forward and motivate resources within and outside their team. Work with external teams where it is required, to comply with certification and due diligence requirements, exercising diligence and due consideration to their prevailing workloads.

Business Services Competencies

Clyde & Co is committed to providing extensive, personal, and professional development opportunities for our people enabling them to be highly effective in their current role as well as assisting them to fulfil their career aspirations.

The competencies are used to inform all aspects of Business Services career development. They vary across levels and different business areas and fall under the following areas:

- Technical Excellence
- People and Team
- Client/Stakeholder Relationships
- Service Delivery and Commercial Awareness
- Personal Effectiveness