

IT SECURITY & COMPLIANCE SUPERVISOR

DESCRIPTION

The IT Security & Compliance Supervisor is responsible for assisting in the management of all technology-related compliance issues across the organization including information security, privacy, business continuity, identity management, user access and data integrity. This includes providing objective risk assessments of the company's compliance with regulatory, organizational, and client requirements governing the organization's information technology systems. The IT compliance manager will also assist with the development and implementation of policies, procedures and controls to ensure that the organization's practices remain observant to all pertinent local, state/province/county and federal laws and industry standards. In this role, the IT compliance manager will work closely with the firm's Legal and Compliance department, as well as other various business units within the organization.

RESPONSIBILITIES

- Maintain an inventory of all regulatory, client, and organizational technology compliance requirements.
- Ensure current IT compliance policies and controls meet the desired level of compliance maturity reflected in a given standard or framework.
- Oversee, manage, and mature the firm's existing IT risk assessment program, business continuity plan, and user access and entitlement review process.
- Maintain and keep current AEW's existing catalog of documentation.
- Identify any gaps between the desired level of compliance and the current level of maturity.
- Conduct necessary IT compliance control monitoring and testing activities to determine the effectiveness of the controls and ensure ongoing adherence to established policy.
- Maintain an IT compliance issue management tracking and resolution process that will address known issues, according to severity and potential impact to the organization.
- Coordinate audit-related tasks such as ensuring the readiness of IT managers and their organizations for audit testing and facilitating the timely resolution of any audit findings.
- Provide technological advice and insight on compliance requirements to both IT and non-IT senior management.
- Assist business and IT managers with the acquisition of tools and expertise to assist with IT compliance-related projects and initiatives.
- Work with corporate legal and compliance representatives to identify all related IT compliance requirements (i.e., security, user access, privacy, data integrity, etc.) associated with the laws and regulations within all relevant jurisdictions.
- Ensure all related IT compliance policies are updated, based on any relevant regulatory changes or new laws.
- Assist the Legal and Compliance Department with eDiscovery requests.
- Work with IT and business representatives to identify the goals and objectives of the organization and translate them into IT compliance requirements such as IT security and user access policies and controls.
- Evaluate any related external frameworks or standards (i.e., NIST, ITIL, COBIT, etc.) or internal standards (e.g., code of conduct and use) to determine the relevant IT compliance requirements and controls.
- Develop and maintain a data classification framework that can be applied across the firm's various systems.
- Assist with the review and response to due diligence requests from clients.

REQUIRED QUALIFICATIONS

- A four-year college degree or equivalent industry training and certifications.
- At least three years of relevant work experience in the financial services industry.
- Demonstrated experience implementing and/or enforcing security and compliance frameworks such as NIST, ITIL, COBIT, ISO, etc.
- Strong familiarity with regulatory bodies, specifically the Securities and Exchange Commission, Monetary Authority of Singapore, Financial Conduct Authority (FCA), etc.
- Direct experience and knowledge of national, state, provincial and local information technology laws and regulations, including GDPR, CCPA, and 201 CMR 17.00.
- Proven ability to translate understanding of the organization's goals and objectives into compliance requirements.
- Experience with developing and implementing effective controls that are consistent with the needs and current level of risk within an organization.
- Exceptionally self-motivated, directed and detail-oriented.
- Superior analytical, evaluative and problem-solving abilities.
- Proven experience developing and submitting IT audit and compliance reports to governing bodies, legal entities and/or external authorities.
- Experience in planning, organizing, and developing information technology policies, procedures and practices.
- Strong communication skills (written and oral), particularly with government/legal agencies and external/internal auditors.
- Demonstrated ability to apply IT-related knowledge and experience in solving compliance issues.
- Excellent knowledge of technology environments, including information security, encryption methods and privacy-based solutions.

SKILLS & TECHNOLOGIES

- Working knowledge of Proofpoint Enterprise Archive
- Experience with Microsoft's O365 Security and Compliance Center

EDUCATION & EXPERIENCE:

- B.S. or B.A. degree
- 5+ years of related experience