Job Description

Job Title: Information Technology Risk Analyst (Associate)
Date: ASAP
Reporting to: IT Manager
Location: Hybrid

Overview

Prioclen LTD is a fast-growing Nigerian based management consulting firm with its head-quarters in Abuja Nigeria. We have a forte in providing strategic consultancy and advisory services to organizations- private, governmental and individual firms, by creating and integrating information technology solutions to enhance their service delivery and ensure sustainable growth and development in niche-based brands to these individuals/ organizations.

Job Purpose

We are looking to recruit an Information Risk Analyst (Associate) who will provide leading threat/ risk analysis, and data science initiatives that help to protect the firm and clients from information and cyber security risks. It also involves managing key tasks and projects, including performing IT risk assessments, IT advisory reviews, IT project assessments, 3rd party IT testing, and other project reviews as identified across all aspects of the firm's information technology structure while coordinating and facilitating awareness and training for information technology risk program elements to ensure that risk responsibilities are understood and carried out throughout the department.

As IT risk analysts, you are also responsible for application development, cyber security, enterprise architecture, business continuity, and disaster recovery. Your, duty also entails assessing the current adequacy of the firm's security strategy and threats to systems, and then calculating the impact of potential adverse events and change management adhering to the IT risk program standards, utilizing industry best practice frameworks such as COBIT, ITIL, SANS, NIST, Basel, GLBA, SOX, PCI-DSS, FFIEC, etc., and ensure employee compliance with security controls and deficiencies.

Responsibilities

- Correlates threat data from various sources to complete a comprehensive picture of potential cyber-attacks and decipher attack motivations and techniques.

- Works closely with other technical, incident management, and forensic personnel to develop a fuller understanding of the intent, objectives, and activities of cyber threat actors and enables a world-class cyber defense program.
- Responsible for conducting research and evaluating technical and all-source cyber intelligence to develop in-depth assessments of threats to the organization's networks, systems, users, and data.
- Serves as liaison and point of contact for new issues and vetting.
- Conducts complex cyber intelligence analysis and awareness through collaboration with other internal experts and trusted outside organizations.
- Performs threat analysis utilizing a combination of standard intelligence methods and business processes to uncover advanced threat actors.
- Designs an innovative threat and security incident management solution.
- Creates technical assessments and cyber threat profiles of current events on the basis of inventive collection and research using classified and open information sources to enables advanced threat intelligence.
- Develops and maintains analytical procedures to meet changing requirements and enable more strategic detections.
- Utilizes threat messaging, models, analyses, presentations, or recommendations to convey complicated technical or behavioral analysis to senior management.
- Participates in a coverage model to prevent and remediate security threats against the organization.
- Stays abreast of innovative business and technology trends in IT security, risk, and controls.
- Advices leadership on technology initiatives that support latest trends in IT security, risk and controls.
- Ensures effective execution of the risk management framework by managing relationships with key stakeholders within strategic business groups and technology.
- Responsible for conducting deep dives on IT security-related processes and systems.
- Verifies that IT risks are appropriately mitigated and leads multiple stakeholders in agreement on appropriate solutions/controls.
- Responsible for identifying applicable regulatory risks from changes or additions to regulatory guidance and requirements.
- Provides expertise for resolution and risk mitigation.
- Develops, tracks, and reports on Key Risk Indicators (KRIs) for information technology.
- Monitors, tracks, and reports mitigation and resolution of IT risks
- Performs process-level walkthroughs, control testing, etc. for the identification and assessment of IT risks and controls.

- Effectively communicate key risks, findings, and recommendations for improvement with key stakeholders.

Requirements

Essential:

- A minimum of Bachelor's degree in Computer Science, Cyber Security, Information Technology, or a similar technical degree with at least 2 years' experience in a similar role ideally within the not-for-profit sector

Certification:

- Analysts may be required to be Certified Information Systems Security Professional (CISSP), Certified Information Security Manager, (CISM), Certified Information Systems Auditor (CISA), or Certified in Risk and Information Systems Control (CRISC), depending on the preference of the organization
- Self-motivation and initiative;
- Ability to work both independently and as part of a team;

Knowledge:

- They require an understanding of key technology concepts such as access control, confidential data, encryption, business continuity, info-sec scans, and vendor apps.
- They also require strong knowledge of IT organization business processes and systems including (IT Security, data management, architectural and planning, technology life cycle management, regulatory concerns).
- They may also be required to possess solid understanding of risk management functions, including IT audit, cyber security, and/or IT compliance. Experience or knowledge of 3rd party/vendor management lifecycle may also be required.

Skills:

- They require strong oral and written communication skills to work effectively with employees at all levels of the organization.
- It is also essential that they are comfortable driving conversations with teams with varied backgrounds and purpose, such as conversing with Risk Team/Info-Sec/Technology Teams/Vendors/ Vendor Managers, etc.

It is also important that they can be receptive to guidance from manager and able to effectively.

Summary Terms and Conditions

Contract: 12-month fixed term contract
Salary: Very Competitive
Annual leave: 22 days holidays per annum pro rata excluding public holidays
Pension: Minimum 10% Employer contribution with minimum 8% Employee contribution
Healthcare: Company scheme subject to terms and conditions.
Life assurance: Company life assurance scheme.
Location: Abuja Nigeria
Notes: This post will be subject to background checks. A full statement of the main terms
and conditions of employment will be supplied with any formal offer of employment. This job description does not form part of your contract of employment.

How to apply

To apply for this job opportunity, please send a CV and covering letter to recruitment@prioclen.com
Unfortunately, because of the volume of applications we are likely to receive we regret that we are unable to respond to every unsuccessful applicant. If we have not made contact with you within 2 weeks of the closing date you have not been selected for interview on this occasion.