CAREER OPPORTUNITIES

Job Description:

GRC & Audit Lead (UK)

WELCOME TO PCI PAL

PCI Pal is a leading provider of SaaS solutions that empower companies to take payments securely, adhere to strict industry governance, and remove their business from the significant risks posed by non-compliance and data loss. We are integrated and resold by some of the world's leading business communications vendors, as well as major payment service providers.

We are currently looking for a GRC & Audit Lead to join our UK team.

THE OPPORTUNITY:

PCI Pal's Information Security team requires a dynamic and proactive individual to lead all Governance, Risk and Compliance (GRC), audit requirements for our team and the company. We are an agile and innovative team and are responsible for ensuring that the confidentiality, integrity and availability (CIA) of our internal, external environments, and client solutions are always maintained. The Lead GRC & Audit function will be focused on ownership of all Information Security GRC, Audit and project initiatives, including proactive cross-functional collaboration with other variety of business stakeholders. The role will ultimately encompass all facets from ensuring that GRC and audit requirements are suitably managed, maintained and matured.

YOU WILL BE RESPONSIBLE FOR:

- Managing, maintaining, and maturing the already established audit lifecycles for the following frameworks:
  - PCI DSS v4.0
  - ISO 27001:2022
  - ISO 9001:2015
  - ISO 14001:2015
  - Cyber Essentials
  - Cyber Essentials Plus
  - SOC2 Type 1 – 3
  - HIPAA
- Working in close collaboration with other team members, with peers, and across the business to ensure that mandatory and audit defined GRC requirements are effectively managed, maintained and suitably matured.
- Bring a highly progressive and pragmatic approach to implementing and maturing innovative GRC and Data Privacy solutions processes and procedures.
- Assist in defining the technical requirements for both the tactical, to strategic, Information Security roadmap.
- Function as a subject matter expert, both within the team, and with peers for all matters relating to GRC, and audit management.
- Managing, maintaining and maturing our third-party vendor risk management programme.
- Work in close collaborative partnership with the Legal and People teams.
- Ensuring that all procedural, process, and policy documentation pertaining to GRC and audit requirements remains up-to-date and relevant.
- Provide assistance, as and where required, to complete GRC / Audit requirements for client derived security self-assessment (SSA) questionnaires.
- Managing PCI Pal's outsourced Data Privacy programme and ensuring compliance to global data privacy regulations is always adhered to.
- Assist and maintaining our commitments and requirements to managing a security, education, training and awareness (SETA) programme.

WE WANT TO HEAR FROM YOU IF YOU:

- Possess extensive and comprehensive knowledge of Information/Cyber Security processes and methodologies as they relate to maintaining compliant PCI DSS and ISO certified environments.
- Have exceptional knowledge of steering and strategically managing GRC and audit roadmaps and associated strategy as it relates to an overarching Information Security strategy.
- Be a subject matter expert level knowledge of all the Information Security frameworks (as listed within the *You Will be Responsible For* section), e.g. PCI DSS, ISO 27001:2022, SOC2 etc.
- Possess a good, and demonstrable, understanding of EU/UK GDPR and the Data Protection Act 2018 etc.
- Have led and managed audit programmes from inception to completion for PCI DSS and ISO 27001:2022.
    - Experience in managing SOC2 audit requirements is highly desirable.
    - Any experience of working with CSA CCM v4.0 and associated cloud security frameworks is highly desirable.
- Have excellent knowledge of the principles of risk management, associated processes, and their relevance to maintaining a GRC programme.
- Are a strong and proactive collaborator with a positive professional, pragmatic work ethic.
- Possess a thorough understanding of applicable cyber security assurance methodologies and frameworks, e.g. NIST & CIS etc.
- Have a rudimentary understanding of AI GRC requirements that can be used to develop and mature AI GRC and assurance requirements.
- Have excellent written skills and be highly proficient in writing, reviewing and maturing GRC and Data Privacy governance documentation.
- Have extensive experience in with managing working relationships with managed security service providers (MSSPs) and external audit service providers.
- Possess an excellent, structured, and methodical working ethos that aligns to project management principles and requirements.
- Be adept in communicating GRC and audit requirements and processes to all levels of seniority.
- Be equally comfortable utilising and working with cloud GRC and Data Privacy services and traditional tooling.
- Being tenacious about delivering high quality results for our both the team and the business.
- Have completed, or having a desire to complete, a combination of the following certifications,
    - Certified Information Systems Auditor (CISA)
    - ISO 27001 Lead Implementer
    - GRC Professional (GRCP)
    - PCI SSC Payment Card Industry Professional (PCIP)
    - CISPP
    - CISM

IN RETURN WE OFFER:

- 25 days holiday, rising to 28 days per annum with length of service.
- Medical, dental, and optical insurance cover
- Option to either work in our Ipswich office, or from home (or both!)
- An exciting and flexible working environment surrounded by friendly and committed co-workers.
- Electric Vehicle Scheme incentive
- “Work from anywhere” 2 weeks per year policy
- Reward, benefits and wellbeing hub (offering support, discounts, cashback, and savings)

TALK TO US:
If you have any questions or want to find out more, we’d love to hear from you.

Please contact the Recruitment Team recruitment@pcipal.com