CAREER OPPORTUNITIES

Job Description:
Information Security GRC Analyst - 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 worlds' leading business communications vendors, as well as major payment service providers.

We are currently looking for an Information Security GRC Analyst to join our UK team.

THE OPPORTUNITY:

The GRC Analyst strengthens PCI Pal's central Information Security function by providing structured governance, risk and compliance analysis across audit, assurance, control management and strategic change. The role turns requirements, evidence, risks and delivery updates into accurate, traceable information that supports timely decisions by the GRC Lead and CISO.
The role works in close partnership with the Information Security Project Manager to track ongoing and strategic initiatives, maintain clear ownership and delivery visibility, and provide concise, evidence-based updates. It remains a GRC role: the Analyst provides assurance, analysis and tracking, while the Project Manager retains responsibility for project governance, planning and delivery coordination.

YOU WILL BE RESPONSIBLE FOR:

3.1 Governance, Risk & Compliance

- Support the CISO, GRC Lead and wider Information Security team with risk, compliance and control analysis.
- Maintain governance artefacts including policies, standards, control mappings, risk registers, Statements of Applicability and supporting records.
- Review security policies, procedures, control narratives and evidence for accuracy, completeness, consistency and alignment with applicable frameworks.
- Identify control gaps, emerging risks and compliance issues, and provide practical recommendations with clear owners and target dates.
- Monitor relevant regulatory and industry developments, assess potential business impact and support the controlled update of affected requirements and documentation.

3.2 Audit & Assurance

- Support internal and external audits, certification activity and customer assurance reviews, including evidence coordination, quality review and follow-up.
- Conduct control assessments, testing and evidence reviews, with clear findings and conclusions reported to the GRC Lead.
- Maintain audit plans, evidence requests, findings and remediation actions so that progress and closure are fully traceable.
- Challenge incomplete or unsupported evidence and work with control owners to resolve quality, scope and timing issues.
- Produce clear assurance reporting for the GRC Lead, CISO and relevant governance forums.

3.3 Program Tracking & Strategic Initiatives

- Work in close partnership with the Information Security Project Manager to track ongoing, planned and strategic departmental initiatives against agreed milestones, dependencies, risks, actions and outcomes.
- Maintain accurate initiative trackers, action logs and reporting inputs, ensuring updates are supported by evidence and reflect the position agreed with accountable owners.
- Obtain and consolidate progress updates from Information Security and cross-functional stakeholders, highlighting overdue actions, delivery risks, control impacts and decisions required.

3.4 Risk, Findings & Remediation Management

- Maintain clear linkage between identified risks, control deficiencies, audit findings, remediation work and closure evidence.
- Coordinate with Information Security Architecture & Engineering, Information Security Operations, Engineering and Product to obtain appropriate technical input rather than independently interpreting technical risk without subject-matter validation.
- Track remediation progress against risk-based priorities and agreed timescales, escalating blockers, slippage and residual risk to the GRC Lead and Information Security Project Manager as appropriate.
- Verify that closure evidence addresses the underlying requirement and that accepted risks are documented and approved through the established governance process.

3.5 AI Governance & Emerging Risk

- Support the maintenance of PCI Pal's AI Management System and associated AI governance, risk and assurance activities.
- Validate AI-assisted or AI-generated GRC outputs, including security questionnaire responses, control mappings and draft analysis, to identify inaccuracies, omissions or misclassification before use.
- Support AI system and supplier assessments, ensuring conclusions are evidence-based and referred to technical specialists where validation is required.

3.6 Collaboration & Continuous Improvement

- Build effective working relationships with control owners and stakeholders across PCI Pal while maintaining appropriate independence and challenge.
- Improve GRC processes, templates, evidence standards, automation and reporting so that assurance activity becomes more consistent, efficient and audit-ready.
- Contribute to the Information Security Target Operating Model and departmental roadmap, providing GRC progress and risk information to the Information Security Project Manager and CISO.

WE WANT TO HEAR FROM YOU IF YOU:

Essential

- Relevant experience in GRC, information security compliance, risk management, internal audit or assurance.
- Working knowledge of at least one major framework, such as PCI DSS, ISO/IEC 27001, SOC 2 or NIST CSF, with the ability to apply requirements in practice.
- Experience reviewing policies, audit reports, control narratives and evidence, and translating findings into clear actions.
- Strong organisation and tracking skills, including the ability to maintain plans, actions, risks, dependencies and status reporting across multiple concurrent initiatives.
- Strong written and verbal communication skills, with the ability to produce concise, accurate updates for operational and senior stakeholders.
- A collaborative working style and the confidence to challenge incomplete evidence, unclear ownership or unsupported status updates.

- High attention to detail, sound analytical judgement and the ability to manage priorities with limited supervision.

Desirable

- Experience operating within a PCI DSS Level 1 service provider, regulated technology or cloud services environment.
- Familiarity with ISO/IEC 42001, ISO 9001, HIPAA/HITECH, Cyber Essentials or related assurance frameworks.
- Experience using GRC, audit, project tracking or evidence automation platforms, such as Drata, Jira, ServiceNow GRC, Archer or OneTrust.
- Experience supporting programme governance, PMO reporting or strategic transformation initiatives in partnership with a Project Manager.
- Experience reviewing AI-generated content, data annotation, quality assurance or AI governance workflows.
- Relevant qualification or certification in information security, risk, audit, compliance or project delivery.

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)
- Training and development opportunities
- Ad-hoc team events, incentives and competitions

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