



## Information Security Analyst

### About Carbonplace

An exciting opportunity to rapidly scale and shape a fintech committed to driving climate action at scale. Expected to launch later this year, Carbonplace is a global carbon credit transaction network that will enable the simple, secure, and transparent transfer of certified carbon credits. Developed by nine of the world's foremost financial institutions, Carbonplace's modern infrastructure will enable the trust, transparency, and accessibility required to open the carbon markets to the world and accelerate global climate action. In joining this innovative venture, you will engage with teams that have a start-up mindset focused in launching a product to market and building the foundations of a company.

### About This Role:

Carbonplace are seeking a highly motivated and experienced Information Security Analyst to join our team and help build the market infrastructure to open the carbon markets to the world and accelerate global climate action. We are looking for individuals that are able to establish, maintain, and improve policies, procedures and controls, to ensure information security and data management across the organization. As an Information Security Analyst, you will be self-directed and responsible to deliver industry standards and best practices for the organization.

### Responsibilities:

- Assist in ensuring that security concerns for the business, corporate systems, application, and infrastructure are addressed and mitigated.
- Identify and assess areas of concern, validate policy compliance, scope and plan engagements, automate test procedures and collection of evidence, influence action plans,
- Partner with leadership, audit departments and team members to complete and improve assessment processes, share of best practices, and key learning across the organization.
- Assess and implement requirements to be compliant with GDPR and requirements from banks and corporate customers regarding data privacy, data retention and data management.
- Establishing and maintaining an ISMS, support and lead efforts for ISO 27001 certification, including resource allocation, engagement with third parties and stakeholders (consulting firms, auditors, management, etc.).
- Evaluate the information security controls and assist the development and use of repeatable processes and procedures.
- Monitor and report on open risks to stakeholders with the appropriate level across the organisation and help assignees to define remediation plans to resolution.
- Develop and execute strategy to educate about Information Security concerns and good practices.

### Location and Commitments:

We offer hybrid working, with a minimum of 2 days a week in the City of London office.

### Candidate Requirements:

- 3+ years of experience working in financial services, delivering against compliance and regulatory requirements.



- Experience with Azure public cloud architecture, including Regions, AZ, High Availability, DR, Monitoring, etc.
- Experience using Azure public cloud services (API Gateway, AKS, Event Hub, Azure AD, Azure Storage, API Developer Portal, Azure Container, Azure Monitor, Data Factory, etc.).
- Experience in scripting and automation using Python, Powershell, Java and/or others.
- Knowledge in infrastructure-as-code, CI/CD and DevOps practices,
- Experience working with information security management frameworks and standards such as ISO 27001, NIST and SOC
- Experience in Data Loss Prevention, data management and regulation (e.g. GDPR).
- Demonstrated ability to work independently, take initiative and self-manage.
- Candidate must demonstrate incredible attention to detail.
- Collaborative, interpersonal and communication skills. Ability to convey complex ideas in a manner that resulted in a definitive direction and result.
- Ability to manage multiple priorities successfully and ability to make effective/informed decisions under pressure.

### **Remuneration & Benefits:**

Salary according to experience

