A logo with white text

Description automatically generated

**Job Description – Beauparc Leadership Role**

|  |  |
| --- | --- |
| **Job Title** | Governance Risk and Compliance (GRC) Administrator |
| **Reports to** | Head of Cyber Security and Risk |
| **Business/Function** | IT |
| **Location** | UK/Ireland |

|  |
| --- |
| **Purpose:**  The GRC Administrator plays a vital role in enhancing the organisation’s security posture by ensuring compliance with industry standards, managing risk, and supporting effective incident response. This role is responsible for assisting the Head of Cyber Security and Risk with implementing and maintaining security policies, conducting assessments, and collaborating with stakeholders to strengthen security controls. By proactively identifying vulnerabilities, optimising security tools, and fostering a culture of cyber awareness, the GRC Administrator will contribute and develop the organisation’s resilience against evolving threats while ensuring alignment with frameworks such as ISO 27001, NIST, and NIS2. |

|  |
| --- |
| **Scope of accountability:**  The GRC Administrator is accountable for:   * Supporting and enhancing the organisation’s security, risk, and compliance framework. * Maintaining the Cyber Security Risk Register. * Completing regular internal and external audits ensuring alignment to agreed frameworks.   Additionally, the GRC Administrator is accountable for:   * Managing vulnerability assessments and remediation plans to address security gaps. * Delivering security awareness initiatives to enhance the organisation’s security culture. * Supporting internal and external audits, ensuring regulatory and compliance obligations are met.   This role requires a proactive approach to risk management, stakeholder engagement, and continuous improvement, ensuring the organisation remains resilient to evolving security threats |

|  |
| --- |
| **Areas of responsibility:**   * Conduct regular Business Impact and Security assessments and audits to evaluate and improve the organisation’s security posture. * Conduct regular supplier audits * Develop, update, and maintain security policies, standards, and procedures in alignment with security frameworks such as ISO 27001, NIST or NIS2 frameworks. * Assist teams in monitoring security incidents, analysing impact, and responding effectively to mitigate risks. * Collaborate with IT teams to ensure security best practices are embedded across systems, infrastructure, and processes. * Deliver clear and actionable reports to stakeholders, detailing security assessments, identified vulnerabilities, and incident response outcomes. * Assist with delivering engaging security awareness initiatives, including phishing simulations and tailored staff training, fostering a culture of cybersecurity awareness. * Assist with external and internal audits to ensure successful outcomes. |

|  |
| --- |
| **Qualifications, Skills and Knowledge:**  **Essential**   * Proven IT background * ISO Auditor qualifications or similar * Understanding of relevant regulatory and compliance frameworks (e.g. ISO, NIST, NIS, GDPR) * Knowledge of Vulnerability Management * Strong analytical problem-solving skills * Ability to work independently and collaboratively in a team environment * Strong communication and interpersonal skills, with the ability to explain complex security concepts to all stakeholders. * Detail-oriented approach to policy development and documentation.   **Desirable**   * Certified in Risk and Information Systems Control (CRISC) (Desirable) * Knowledge of Incident Management (Desirable) |