Challenge Group

Job Title	Senior GRC Specialist

Organisation	CAS
Location	Malta
Reports to	CISO
Position Code	CAS74
Job Purpose	As a GRC (Governance, Risk & Compliance) Specialist, you will play a key role in strengthening the organization's information security and compliance framework. • You will be responsible for developing, implementing, and maintaining governance, risk management, and compliance programs in alignment with international standards (ISO 27001, GDPR, NIST, etc.). • This role requires strong analytical and organizational skills, cross-functional collaboration, and the ability to translate security and compliance requirements into actionable business processes. • This role serves as the single point of accountability for Information Security Governance, Risk, and Compliance across the entire Challenge Group. • The GRC Specialist independently owns and coordinates all information security compliance activities across subsidiaries, jurisdictions, and regulatory frameworks, report directly to the CISO and senior stakeholders.
Responsibilities	Own, develop, and maintain the organization's Information Security Governance framework, policies, and procedures. • Independently conduct and own risk assessments across systems, processes, vendors, and group entities; manage mitigation plans and follow up. • Own and monitor compliance with applicable regulations, standards, and contractual requirements across the group (ISO 27001, GDPR, PARTIS, NIS2, etc.). • Act as the end-to-end owner of the ISO 27001 ISMS, including scope definition, risk assessment, Statement of Applicability, internal audits, management reviews, and certification readiness. • Coordinate ISO 27001 implementation and ongoing compliance across all relevant subsidiaries and business units. • Ensure alignment with aviation and EU regulatory requirements, including EASA Part-IS, NIS2, GDPR, and applicable aviation authority expectations. • Own and manage vendor risk management and third-party due diligence processes across the group. • Act as the primary point of contact for regulators, auditors, and external assessors on information security and compliance matters, in coordination with the CISO. • Support and prepare for internal and external audits, including evidence collection and remediation tracking. • Collaborate with IT, Legal, HR, and business units to ensure security and compliance requirements are embedded in daily operations. • Maintain the group risk register and report risk levels, trends, and KPIs to management and the CISO. • Assist in security awareness and compliance training programs.

	• Own post-incident compliance reviews and contribute to incident response documentation. • Support the implementation of GRC tools and dashboards for centralized risk and compliance management.

Job Requirements

Education	Bachelor's degree in information systems, Computer Science, Industrial Engineering, or equivalent experience
Experience, Skills, and Personal Attributes	• 5+ years of experience in Governance, Risk & Compliance, Information Security, or Audit, including independent ownership of compliance activities. • Certificate holder – CISA, CRISC, CISSP – Advantage • Hands-on experience leading or owning compliance activities for ISO 27001, GDPR, Part-IS, SOC 2, or similar frameworks. • Experience working in a regulated environment (aviation, logistics, or finance)– Advantage. • Proven ability to work directly with regulators, auditors, and external stakeholders in compliance and audit contexts. • Experience with risk management methodologies and GRC platforms (ServiceNow GRC, One Trust, Archer, etc.) – Advantage. • Strong analytical and communication skills; ability to present complex information clearly. • Excellent English – written and spoken. • Highly independent, proactive, and organized, with strong attention to detail

Job Description – xxx