Regulatory & Compliance Manager

Prepared by:
Department Name: People Operations
Email:
peopleoperations@cirrusconnects.com

Public

TABLE OF CONTENTS

JOB DESCRIPTION

Reports to: Chief Operating Officer (COO) with dotted line to Chief Financial Officer (CFO)
Direct Reports: None (matrix leadership across functions)
Location: Remote with visits to Head Office as required

1 ROLE PURPOSE

To manage Cirrus' governance across compliance, data protection, supplier assurance, certification, and ethical/ESG obligations. This role is hands-on management of the organisation's regulatory, contractual, operational and security integrity, ensuring that Cirrus operates with a robust control environment that supports sustainable growth, operational resilience, and customer trust.

This role supports business growth by enabling teams to meet objectives in a compliant, secure and customer-trusted way. The role holder acts as a regulatory advisor, embedding risk-aware decision making and simplifying governance into scalable, pragmatic processes, whilst remaining conscious of operating as a lean organisation.

2 KEY RESPONSIBILITIES

Enterprise Risk Management

- Maintain the business Risk Register on behalf of CFO, ensuring risks are accurately described, scored, tracked, and escalated.
- Prepare risk register for CFO and Audit & Risk Committee (ARC) including trends, mitigations, and assurance evidence.
- Facilitate strategic risk reviews between CFO with Finance, Technology, Product, Commercial and Operations leaders.
- Manage cross-functionally (e.g., ISO owners, BCP leads) to embed compliance into daily operations.

Audit & Certification Management

- Lead planning, readiness, evidence collection and close out activities for:
    - ISO 27001, ISO 42001,ISO 9001/14001

- Cyber Essentials/Cyber Essentials Plus
- AI governance/ISO 42001 readiness

- Manage internal audit programmes.
- Maintain all policies, manuals, procedures and mandatory documentation.

Data Protection & Privacy Leadership

- Act as the organisation's senior authority on GDPR compliance and privacy by design.
- Lead all Data Protection Impact Assessments (DPIAs), Record of Processing Activities (ROPAs), data mapping, retention reviews, risk assessments and privacy impact escalations.
- Own post contract data deletion workflows and issue customer deletion confirmations.
- Interpret and advise on controller/processor roles for contracts and services.

Supplier Assurance & Third/Fourth Party Risk

- Manage supplier due diligence, contractual reviews (DPA, NDA, SLA alignment), and periodic assurance.
- Maintain the supplier assurance framework including onboarding, reapproval cycles, incident handling and contract term verification.
- Review supplier security practices, risk scores and exception requests.

Operational Compliance & Change Controls

- Define, document and enforce governance gates for high-risk operational changes.
- Ensure processes include approval workflows, documented evidence, audit trails and customer declarations where applicable.
- Review and approve compliance-centric Help Centre and customer-facing knowledge articles.

Regulatory & Framework Compliance

- Provide compliance input into submissions, tender responses and commercial/go-to-market activities.
- Support legal and commercial teams with regulatory obligations and contract clauses.
- Monitor and prepare the organisation for emerging regulatory frameworks (e.g., EU AI Act).

ESG, Ethical Conduct & Mandatory Training

- Own the organisation's Modern Slavery, Ethics, Harassment & Bullying and similar mandatory policies.
- Oversee and track mandatory training completion (e.g., data protection, security awareness, harassment & bullying).
- Contribute governance and risk data to ESG assessments, Board reviews, and external reporting.
- Own the compliance elements of Cirrus' sustainability and DEI objectives.

Policy Framework & Awareness

- Maintain the enterprise-wide policy suite (AI Usage, Cloud Services, HR linked conduct policies, security, data protection).
- Lead annual reviews, approval cycles and organisation-wide communications.
- Ensure policy decisions are embedded through training, guidance and operational workflows.

3 SKILLS, EXPERIENCE & QUALIFICATIONS

Essential

- Proven experience leading audit or compliance functions in a technology/SaaS or regulated environment.
- Deep experience with ISO 27001, 42001, 9001, 14001 operations, audits and management systems.
- Strong GDPR and privacy expertise including DPIAs and data lifecycle governance.
- Demonstrated ability to design compliance processes and operational controls.
- Experienced in supplier assurance, and data protection review.
- Excellent written communication skills for SLT level reporting and policy authorship.
- Ability to translate complex compliance requirements into practical operational steps.

Desirable

- ISO 27001/9001/14001 Lead Auditor/Lead Implementer
- GDPR Practitioner/Professional Certificate

- Experience with ISO 42001 or AI governance frameworks
- Background in public-sector procurement frameworks (e.g., G Cloud)
- Familiarity with ESG reporting frameworks
- Understanding of AI risk frameworks

4 KEY COMPETENCIES

- Hands-on delivery of regulatory and compliance activities
- High degree of autonomy; ability to manage without direct reports
- Influencing and cross-functional management
- Analytical skills and attention to detail
- Strong ethical judgement and confidentiality
- Process design, documentation and continuous improvement mindset

5 KPIs

- Risk register completeness, freshness and action closure rate
- Audit outcomes: number of non-conformities, closure cycle time
- Policy compliance: % policies within review cycle, acknowledgment rates
- DPIA completion lead time; privacy request turnaround
- Supplier assurance coverage (% onboarded, DPA/NDA compliance)
- Mandatory training completion rates
- G Cloud and ESG submission accuracy and timeliness
- % of tenders supported with accurate compliance input
- Time-to-response for commercial input (RFIs, due diligence, DPA reviews)

6 SECURITY PROTOCOL

- As part of this role, you may be required to go through enhanced background checks. It will be essential for you to cooperate fully with the application process to obtain future DBS and BPSS, or other enhanced background checks as required.
- The Company is required by law and other regulations to comply with data protection and confidentiality and best practice information security governance.
- It is therefore your responsibility to maintain Company and client confidentiality at all times. You must not disclose any secrets or other information of a confidential nature relating to the Company or its business, or in respect of any obligation of confidence which the company owes to any third party, during or after your employment expect in the proper course of employment or as required by law.
- It is your responsibility to understand our Information Security Policy in full and to implement any further developments as required.

It is your responsibility to observe and be compliant with all additional regulations in the Employee Handbook