

Position Description – Head of Risk & Compliance

DIVISION & TEAM	Commercial Legal & Risk	REPORTS TO	Chief Commercial Officer (CCO) (or any other position as determined and advised by JSCL)
BAND	I		
FUNCTIONAL RELATIONSHIPS	<p><i>INTERNAL</i></p> <ul style="list-style-type: none"> • ELT • FINANCE AND COMMERCIAL BUSINESS UNIT • BUSINESS UNITS • PEOPLE & CAPABILITY FUNCTION • BOARD AUDIT, RISK & MANAGEMENT COMMITTEE (ARMCO) 	<p><i>EXTERNAL</i></p> <ul style="list-style-type: none"> • SKIPTON GROUP RISK FUNCTION • SKIPTON GROUP INTERNAL AUDIT • EXTERNAL CERTIFICATION BODIES (ISO, SOC2, CYBER ESSENTIALS) • EXTERNAL AUDIT & ASSURANCE PROVIDERS 	
DOES THIS ROLE HAVE DELEGATED AUTHORITY?	YES	IF YES, DELEGATED AUTHORITY AMOUNT	AS PER JADE DFA LEVEL DOCUMENT

1. ROLE PURPOSE

The Head of Risk & Compliance is responsible for strengthening and embedding Jade's enterprise-wide risk and compliance framework in alignment with Skipton Group requirements, while ensuring Jade maintains and enhances its external certifications and assurance posture.

This role provides hybrid operational and second-line risk leadership, overseeing certification management (ISO 27001, Cyber Essentials, SOC 2), coordinating internal audit engagements, and leading the implementation and embedding of the Group Risk Management Framework (GRMF) within Jade.

In addition, the role ensures Jade's risk and compliance practices are positioned as a commercial strength – building customer trust, supporting enterprise sales, and reinforcing Jade's reputation as a dependable, secure and robust SaaS and Managed Services partner.

The role ensures Jade's risk practices are proportionate, commercially aligned, and scalable to support a growing global business, while delivering appropriate oversight, reporting, and assurance to the CCO, ELT, ARMCO, and customers.

2. KEY ACCOUNTABILITIES & EXPECTATIONS

Enterprise Risk & GRMF Implementation

- Lead the rollout, implementation and embedding of the Skipton Group Risk Management Framework (GRMF) within Jade, ensuring it is proportionate to Jade's size, complexity, and operating model.
- Translate Group requirements into practical, scalable processes that work within a product-led SaaS and Managed Services environment.
- Enhance and mature Jade's existing risk register to meet Group standards, ensuring:
 - Clear ownership of material risks
 - Defined controls and control effectiveness assessments
 - Alignment to Risk Appetite statements
 - Regular review and refresh cycles
- Drive risk awareness across the organisation, ensuring risk identification and management is embedded into business planning, product development, operational processes, and strategic initiatives.
- Ensure Jade's risk framework can be clearly articulated externally to customers and partners as evidence of disciplined and mature risk management practices
- Develop and deliver risk reporting to ELT and ARMCO that provides meaningful insight, trend analysis, and clear articulation of emerging and material risks.
- Support the CCO in preparing Board-level and ARMCO reporting and periodically present risk updates as required.

Customer Assurance & Commercial Enablement

- Act as Jade's subject matter lead for customer-facing risk and compliance enquiries, including due diligence reviews, and assurance discussions.
- Partner with Sales, Commercial, and Security teams to respond to customer security and compliance requirements in a timely, consistent, and commercially balanced manner.
- Support enterprise sales opportunities by articulating Jade's risk framework, control environment, and certifications in a clear and confidence-inspiring way.
- Proactively identify opportunities to leverage Jade's risk and certification posture as a competitive differentiator in target markets and sectors.
- Ensure customer-driven compliance requirements are assessed for proportionality, commercial impact, and alignment with Jade's operating model before acceptance.
- Develop and maintain a structured repository of risk and compliance artefacts to support efficient customer due diligence processes.
- Provide oversight where customers require specific security or assurance commitments to ensure they are operationally deliverable and sustainable.

Certification & Assurance Management

- Own and coordinate Jade's external certification programme, including ISO 27001, SoC2, and Cyber Essentials.
- Partner with the Head of Security and Security team to ensure control frameworks remain effective, audit-ready, and aligned to certification standards.
- Lead certification renewals, scope extensions, surveillance audits, and remediation activities.
- Ensure audit findings are tracked, addressed, and closed in a timely and structured manner.
- Assess opportunities to rationalise, uplift, or enhance Jade's assurance posture in alignment with commercial growth and customer expectations.
- Ensure certification strategy supports sales enablement, customer trust, and market expansion.

Internal Audit & Assurance

- Act as primary liaison for Skipton Group Internal Audit engagements affecting Jade.
- Coordinate audit planning, information gathering, and stakeholder engagement across the business.
- Ensure management responses are robust, commercially balanced, and aligned to Group expectations.
- Track and monitor remediation actions to completion, ensuring sustainable control improvements.
- Work collaboratively with first-line leaders to avoid duplication of effort and maintain a pragmatic, value-add assurance approach.

Risk Reporting & Governance

- Establish and maintain a clear and effective risk reporting cadence to CCO, ELT, ARMCO, and Skipton Group (as required)
- Ensure reporting provides forward-looking insight, not just compliance updates.
- Support development of risk appetite metrics and tolerance thresholds appropriate to Jade's operating model.
- Ensure appropriate documentation of policies, frameworks, and governance artefacts in alignment with Group expectations.

Commercially Aligned Risk Leadership

- Balance regulatory and certification requirements with Jade's commercial objectives, ensuring risk management enables rather than restricts growth.
- Provide pragmatic challenge and advice to business leaders on new initiatives, product developments, acquisitions, and market expansion activities.
- Support risk assessments for strategic projects, integrations, and new customer propositions.
- Support customer contract negotiations where specific risk, compliance, or assurance obligations are being considered.
- Advise on the risk implications of customer-imposed security requirements to ensure sustainable and scalable commitments.
- Ensure Managed Services expansion and product growth are supported by appropriate control design and risk oversight.

Continuous Improvement

- Identify opportunities to streamline, automate, and improve risk and compliance processes.
 - Leverage data and insights to improve control effectiveness and reduce operational friction.
 - Stay informed on emerging regulatory, cybersecurity, and SaaS industry risk trends relevant to Jade's business model.
 - Maintain strong working relationships with Skipton Group Risk to ensure alignment and constructive partnership.
-

Leadership

- Provide strong matrix leadership across the organisation without direct line management.
- Influence and engage senior leaders to take ownership of risks within their domains.
- Act as a trusted advisor to the CCO and ELT on enterprise risk and assurance matters.
- Build risk capability across the business through education, coaching, and practical guidance.
- Demonstrate balanced judgement, independence of thought, and strong stakeholder management.

Jade Values and Culture

- You know our values, what they mean to us and behave in line with them.
- Feedback regarding your behaviour in line with the values from your stakeholders is positive and you seek feedback on areas where you might feel challenged.
- You keep up to date with our vision and purpose, strategies, and priorities. You ask questions if you don't understand and challenge when you have different ideas.
- You behave in line with our policies, procedures and legislative obligations.

Personal Development

- You have an established training and development plan, in consultation with your People Leader and you commit to delivering against it each year.
- You engage in regular development conversations with your People Leader and actively work on areas of your development.

Safety & Wellness

- You actively participate in and support safety and wellness initiatives.
- You understand and comply with our safety and wellness policies and procedures including emergency procedures.
- Report all accidents and incidents, including discomfort and near misses promptly.
- You keep your work area tidy and clear of clutter and hazards.

Other duties as may be reasonably required from time to time.

3. PERSON SPECIFICATION

	ESSENTIAL	PREFERRED/DESIRABLE
Education/Training	<ul style="list-style-type: none"> • Bachelor's degree in Commerce, Law, Risk, IT, Business or related field. 	<ul style="list-style-type: none"> • Professional certification in Risk, Audit, Compliance, or Information Security (e.g. IRM, CISA, CRISC, ISO Lead Auditor or equivalent).
Experience/Knowledge/Skills	<ul style="list-style-type: none"> • Minimum 5 years in Senior risk role and 8+ years in total experience. • Demonstrated experience implementing or enhancing an enterprise risk management framework. • Experience managing ISO 27001 certification and audit cycles. • Experience coordinating internal and/or external audit engagements. • Strong understanding of risk identification, assessment, control design, and reporting. • Experience operating in a hybrid first- and second-line risk role within a growing organisation. • Ability to translate complex risk and regulatory requirements into pragmatic business processes. • Strong stakeholder management and influencing capability across senior leaders. • Experience preparing risk reporting suitable for Board or Committee level. • Commercially pragmatic mindset with ability to balance risk, compliance and growth objectives. 	<ul style="list-style-type: none"> • Experience in SaaS, technology, digital services, or managed services environments. • Experience expanding ISO certification scope across business units or products. • Experience working within a Group or matrixed environment with parent-company oversight. • Familiarity with SOC 2 frameworks. • Experience supporting post-acquisition integration risk activities.