SCAN FOR THE TEMPLATE

JOB DESCRIPTION TEMPLATE

Chief AI Risk Officer (CAIRO)

The organization's senior authority on AI risk governance, owning enterprise AI risk across the full model lifecycle.

Department	Enterprise Risk Management / AI Governance / Executive Leadership
Reports to	CEO, Chief Risk Officer, or Board Risk Committee
Location	Remote, Hybrid, or On-site
Employment type	Full-time
Experience	12 to 15+ years

Free, ready-to-post template from GRC Careers · AGJ, the AI governance job board
Download or post this role at **ai-governance-jobs.com/templates/chief-ai-risk-officer**

POSITION OVERVIEW

The Chief AI Risk Officer (CAIRO) provides executive leadership for the organization's enterprise AI risk management program. This role is responsible for identifying, assessing, mitigating, monitoring, and reporting risks associated with artificial intelligence systems throughout their lifecycle.

The CAIRO partners closely with executive leadership, legal, compliance, cybersecurity, privacy, data governance, technology, internal audit, and business leaders to ensure AI technologies are deployed responsibly, ethically, securely, and in alignment with organizational objectives and regulatory requirements. As AI becomes increasingly integrated into business operations, the CAIRO serves as the organization's senior authority on AI risk governance and helps build a culture of responsible innovation.

KEY RESPONSIBILITIES

ENTERPRISE AI RISK STRATEGY

- Develop and execute the enterprise AI Risk Management Framework.
- Establish organizational AI risk appetite and tolerance levels.
- Integrate AI risk into Enterprise Risk Management (ERM).
- Present AI risk updates to executive leadership and the Board.
- Develop AI governance policies and enterprise standards, and build a long-term roadmap for AI risk maturity.

AI RISK ASSESSMENTS

Lead enterprise assessments involving generative AI, machine learning models, autonomous systems, third-party AI vendors, foundation models, LLMs, AI agents, and decision automation systems. Evaluate bias and discrimination, hallucinations, model drift, data quality, privacy, intellectual property, security, regulatory compliance, operational resilience, reputational impact, third-party risk, and human oversight.

GOVERNANCE

- Chair or co-chair the AI Governance Committee.
- Establish AI approval and review processes; oversee AI system inventories.
- Define AI risk classifications and ensure AI projects undergo appropriate governance before deployment.
- Maintain executive dashboards and reporting.

REGULATORY COMPLIANCE

Monitor and implement requirements related to the EU AI Act, NIST AI Risk Management Framework, ISO/IEC 42001, ISO 31000, ISO 27001, OECD AI Principles, state AI legislation, and emerging global AI regulations.

CROSS-FUNCTIONAL LEADERSHIP

Partner with Information Security, Privacy, Legal, Compliance, Internal Audit, Enterprise Risk, Technology, Procurement, Data Governance, Human Resources, and business unit leaders.

THIRD-PARTY AI RISK

Evaluate AI vendors, review contractual AI provisions, assess vendor governance maturity, monitor concentration risk, review AI service providers, and develop AI due diligence procedures.

MONITORING AND REPORTING

Develop enterprise reporting covering Key Risk Indicators (KRIs), AI incidents, model performance, emerging threats, regulatory developments, executive dashboards, Board reporting, audit findings, and corrective action tracking.

INCIDENT RESPONSE

Lead response efforts involving AI failures, unauthorized AI usage, model compromise, data leakage, ethical concerns, high-risk AI incidents, and regulatory inquiries.

PROGRAM DEVELOPMENT

Build and maintain the AI Risk Register, AI Controls Library, AI Risk Taxonomy, AI Governance Framework, risk assessment methodology, risk scoring models, AI approval workflow, AI risk metrics, and AI policy library.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Risk Management, Information Systems, Computer Science, Data Science, Cybersecurity, Business, Law, or a related discipline. Master's degree preferred.
- 12 to 15+ years of progressive experience in enterprise risk management, technology risk, cybersecurity, model risk management, compliance, or governance.
- 5+ years leading enterprise risk or governance programs.
- Experience briefing executive leadership and Boards of Directors.
- Strong understanding of AI technologies and machine learning concepts.
- Experience implementing governance frameworks within complex organizations.

PREFERRED CERTIFICATIONS

One or more of: CRISC, CISSP, CISM, CIA, CISA, PMP, CDPSE, AIGP, ISO/IEC 42001 Lead Implementer or Lead Auditor, PRM, FRM.

TECHNICAL KNOWLEDGE

AI governance, enterprise risk management, AI risk assessments, model risk management, responsible AI, AI security, AI privacy, data governance, LLM governance, AI agent governance, model lifecycle management, vendor risk management, regulatory compliance, AI controls testing, risk quantification, and GRC platforms.

ESSENTIAL COMPETENCIES

Strategic leadership, executive communication, Board presentation skills, risk-based decision making, critical thinking, ethical judgment, collaboration, change leadership, program management, regulatory interpretation, analytical problem solving, and negotiation and influence.

SUCCESS MEASURES: FIRST 12 MONTHS

- Establish an enterprise AI risk governance program; implement an AI Risk Register and assessment methodology.
- Develop executive AI risk dashboards; launch AI governance committees and reporting processes.
- Complete baseline AI risk assessments across business units; integrate AI risk into Enterprise Risk Management.
- Develop AI policies, standards, and procedures; improve organizational AI governance maturity.

This is a free, editable template. Replace bracketed fields with your specifics before posting.
Post this role, or find more executive templates, at **ai-governance-jobs.com/templates/chief-ai-risk-officer** · A resource from **GRC Careers**