



MARTIN AGGREY-MILLS

INFORMATION SECURITY MANAGER, CISA, CISM, CISSP

Profile

Strategic Information Security Leader with experience across all three lines of defense first line (operational management), second line (risk and compliance functions), and third line (internal audit) transforming cybersecurity into a business enabler rather than a roadblock. Expert in building Trust Architecture and aligning security programs with organizational growth, from early-stage operations to enterprise scale.

Proven ability to embed security into business strategy, manage risk, ensure regulatory compliance (NIS2, DORA, KRITIS, GDPR, ISO 27001, PCI DSS, NIST CSF, NIST 800-Series), and foster a risk-aware culture. Trusted advisor to executives, driving resilience, stakeholder confidence, and sustainable organizational trust.

Experienced in Enterprise AI Security Management, designing and implementing secure frameworks to maximize AI adoption while mitigating associated cyber and compliance risks.

Employment History

Information Security Manager, OC Payment GmbH – Cologne, Germany (Rewe Group Company), Germany

MAY 2025 – PRESENT

- Building a comprehensive cybersecurity control framework aligned with organizational objectives and regulatory requirements.
- Conducting maturity assessments to evaluate the current security posture and prioritize strategic initiatives.
- Designing and implementing a P2PE readiness program to secure transaction data and strengthen operational resilience.
- Developing and enhancing security capabilities across the 1st, 2nd, and 3rd lines of defense to improve coordinated risk management and assurance.
- Leading Enterprise AI Security Management, establishing governance, controls, and risk frameworks for secure AI adoption across the company.
- Driving DORA and NIS2 regulatory readiness, ensuring alignment with emerging EU mandates.
- Managing the ISO 27001 audit process to maintain compliance with global security standards.
- Developing business continuity plan (BCP) to increase operational resilience and ensure service availability during disruptions.
- Creating strategic security plans for products to align cybersecurity initiatives with business objectives.
- Developing and enforcing security policies, standards, and governance frameworks that support NIS2, DORA, KRITIS, ISO 27001, NIST, GDPR, and PCI-DSS compliance.
- Driving third-party and vendor risk management, identifying and mitigating supply chain risks.
- Leading IAM governance, ensuring RBAC, identity lifecycle management, and privileged access oversight.
- Advising senior management on strategic security priorities, regulatory readiness, and emerging cyber threats.
- Delivering cybersecurity awareness programs to foster a risk-aware organizational culture.

Details

Roonstrasse 8 50674

Cologne

Germany

+4915252683620

millsaggrey@gmail.com

Links

[LinkedIn](#)

www.martinaggreymills.com

Skills

Governance Domain

Identify Domain

Detect Domain

Protect Domain

Respond Domain

Recover Domain

Information Security Specialist , Aioi Nissay Dowa SE. (Toyota Insurance Services), Germany

NOV 2022 – MAY 2025

- Conducted enterprise wide protection needs and control framework while strengthening cybersecurity governance across the organization.
- Lead the design and implementation of security controls aligned with DORA & ISO 27001 to ensure ongoing EU regulatory compliance.
- Drove enterprise risk management, conducted gap assessments, and coordinated remediation with cross-functional teams.
- Conducted continuous monitoring and control assurance to track security posture and compliance maturity.
- Lead Third Party Risk Management (TPRM) and operated scalable vendor risk methodologies through OneTrust.
- Advised IT leadership on IAM governance, access lifecycle management, and role-based access control.
- Governed Data Loss Prevention (DLP) policies to continuously optimise detection rules.
- Delivered enterprise cyber awareness programs, strengthened security culture and reduced human factor risk.
- Advised senior stakeholders on risk ownership, policy adoption, and strategic security priorities.

Senior Information Security Analyst, Milden Systems , Laurel, MD, USA

SEPT 2018 – NOV 2022

- Led internal and external audit readiness for ISO 27001, NIST 800-171, SOX, TISAX, and HIPAA, strengthening enterprise compliance posture.
- Directed enterprise risk assessments, defined remediation strategies, and provided recommendations to executive leadership.
- Designed and executed control mapping across GDPR, NIST, ISO 27001, PCI-DSS, and SOC frameworks.
- Guided incident response and threat analysis, supporting leadership in containment, recovery, and long-term mitigation.
- Established vulnerability management processes, including risk scoring, prioritization, and structured reporting.
- Produced executive-level audit reports, risk dashboards, and compliance metrics for senior management and board stakeholders.
- Contributed to long-term security roadmaps to improve confidentiality, integrity, and availability across business units.

Information Security Specialist , E&P Services Ltd, Accra, Ghana

JAN 2016 – SEPT 2018

- Aligned security operations and controls with SOC 2, NIST, ISO 27001, and GDPR frameworks.
- Enhanced vendor risk processes, including onboarding, performance monitoring, and risk classification.
- Facilitated risk identification, documentation, and development of corrective action plans.
- Led security awareness training programs to improve organizational readiness.
- Developed documentation, procedures, and compliance guidelines to support audits and regulatory requirements.

Education

B.Sc. Computer Science, Central University, Accra, Ghana, Ghana

CISSP

CISM

CISA

CompTIA Security+