West Midlands Combined Authority

Job Description

Job Title:	Information Security & Integrity Manager
Directorate/Team:	Technology & Insight Directorate
Location:	16 Summer Lane or other site/location
Responsible to:	Business Management Unit Lead (Technology & Insight)
Responsible for:	No direct line management
Key working relationships: (internal)	CTIO; BMU Lead; Enterprise Architect; Head of Corporate IT (and Cyber Security Manager); Heads of Product/Data/Technology Systems & Infrastructure; Data Protection Officer/Information Governance; Audit; Legal; Procurement
Key working relationships: (external)	Auditors, assurance bodies, suppliers; sector-wide information-sharing forums

Purpose of the Post

The Information Security & Integrity Manager will own, mature, and continuously improve WMCA's Information Security Management System (ISMS) and broader security governance framework. The role ensures the organisation has clear, evidence-based assurance over its information assets — including what data the organisation holds, where it resides, its sensitivity, how it is used, and whether it remains relevant, high-quality and well-governed.

The postholder will define and maintain security policies, Minimum Security Baselines, risk frameworks, lifecycle controls, and supplier security requirements, ensuring alignment with ISO 27001/27701/22301, UK GDPR and NCSC guidance. They will work closely with the Cyber Security Manager to align governance with technical safeguards, and with Data Engineering, Information Governance and technology teams to ensure data architecture, data processes and storage platforms (including Microsoft Purview and SharePoint) enforce appropriate controls, automate compliance, and support defensible decision-making. Owns security certification programmes (e.g., CE+, PCI) and DPIA/Privacy-by-Design security input, partnering with DPO/IG, and aligns the Information Security Risk Register with the Corporate Strategic Risk Register.

The role will provide independent assurance to leadership on information security, data integrity and the controlled operation of business services, ensuring security is embedded into cadence, change and documentation. It will also lead the organisation's security awareness and culture uplift, promoting disciplined, evidenced-driven continuous improvement across WMCA.

Accountabilities

- Maintain the ISMS and demonstrate continuous improvement towards ISO 27001/27701/22301 alignment.
- Define security policies, MSBs, and risk appetite; maintain the Information Security risk register and risk exception process.
- Lead incident governance (classification, reporting, lessons learned); coordinate with Cyber Security Manager on technical response and evidence.
- Own security awareness programme and culture uplift.
- Maintain the Information Security Risk Register and ensure explicit alignment with the Corporate Strategic Risk Register, providing routine updates through BMU to Executive, ARAC and Internal Audit.

- Own and programme-manage WMCA's external security certifications and audits (e.g., Cyber Essentials Plus, PCI DSS); maintain annual compliance plan, evidence packs and remediation governance with Corporate IT and suppliers.
- Oversee third-party security expectations and due diligence; align contracts to standards.
- Provide assurance reporting to the Technology & Insight Directorate's Business Management Unit / Leadership and WMCA Audit & Assurance teams and coordinate audit responses.
- Maintain oversight of organisational datasets, ensuring clear visibility of what data exists, where it resides, how it is protected, and how it is used across business services.
- Define and maintain protocols for data classification, retention, minimisation and lifecycle management, aligned with WMCA governance, UK GDPR and NCSC guidance.
- Lead Privacy by Design and security input to DPIAs in partnership with the DPO/IG, ensuring security controls, data minimisation, retention and lifecycle requirements are designed-in and evidenced.
- Establish governance mechanisms using Microsoft Purview to monitor data estates, automate policy enforcement, and support audit readiness for structured and unstructured data.
- Provide assurance over the alignment of SharePoint site structures and permissions to security, integrity and lifecycle requirements.
- Partner with Data Engineering and Data Governance to ensure the organisation's data is accurate, relevant, high-quality and backed by controlled change and governance processes and relevant operational metrics and records.

Responsibilities

Strategic

- Translate regulatory and sector guidance (NCSC, ICO) into practical policy sets and control objectives.
- Advise on risk appetite and prioritisation; support governance boards.
- Establish and maintain the organisation's Cyber and Resilience Strategy so as to support and enable overall organisational strategy and objectives
- Translate organisational needs into a coherent data security and lifecycle governance model, ensuring datasets are well-understood, purposeful, and appropriately governed.
- Set minimum security requirements in the procurement lifecycle (pre-proc, tender, contract, in-life), including due-diligence, data-protection/security clauses, right-to-audit, and supplier assurance reporting; coordinate with Legal/Procurement and service owners.
- Define security requirements for Business Continuity and Disaster Recovery (BCP/DR) and assure exercises; *(Cyber Security Manager leads technical DR runbooks and tests)*.
- Advise leadership on data-related risks, including data sprawl, quality deficits, legacy datasets, and shadow data repositories.

People

- Act as a coordinator for WMCA's formal liaison with national and regional authorities and communities of practice (e.g., NCSC, ICO, CPNI, ROCU, CiSP, WARP) and with certification bodies, the WMCA is engaged appropriately, relevant information and intelligence is flowing and threat intelligence, guidance and findings are translated into policies and controls.
- Build strong working relationships across T&I service areas, Corporate PMO, Service Desk, suppliers and operational teams and technical teams across the WMCA.
- Work with data owners and engineering teams to embed a culture of data literacy, responsible data stewardship and quality-driven practices.
- Coach teams on Purview-enabled governance, including classification, retention labels, DLP policies and data mapping.
- Promote a culture of disciplined, evidence-driven continuous improvement.
- Lead the awareness and training plan; coach control owners on compliance.
- Influence without line authority; build strong relationships across RUN/CHANGE.
- Work collaboratively with all colleagues and stakeholders to further common goals.
- Promote agile and Lean working practices across the directorate, including team ceremonies, retrospectives and continuous improvement cycles.
- Support capability-building by identifying skill gaps, utilisation patterns and upskilling needs.

- Create a culture of safety around the organisation's Information Security eco-system where blameless lessons learnt are rapidly embedded into continuous improvement cycles.

Operational

- Ensure CAB/change includes security readiness criteria and artefacts.
- Collaborate to ensure non-functional requirements for services/products/projects have sufficient clarity to enable security by design.
- Develop the Information Security environment in such a way as to enable effective operation of DevOps across the organisation / Directorate.
- Maintain evidence packs and ISO/QMS artefacts with the Business Management Unit.
- Use Microsoft Purview to monitor, classify and provide assurance reporting on data holdings, sensitivity labels, data access patterns and lifecycle controls.
- Support automation of data processes in SharePoint, including template governance, retention schedules, approval workflows and controlled information architecture.
- Implement data quality assurance checkpoints in collaboration with Data Engineering (e.g., schema validation, metadata standards, freshness/recency monitoring, quality thresholds).
- Maintain visibility of organisational data assets through evidence-based mapping, ensuring datasets have appropriate owners, controls, and justifiable business purposes.

Financial

- No direct budget responsibility, but input to security/compliance budgets; optimising spend across controls vs risk.

Other

- Operate effective matrix working between the Directorate and WMCA Corporate PMO to ensure effective project delivery, portfolio oversight, and financial monitoring.
- Ensure adherence to WMCA governance, HR, procurement and financial protocols.
- Support the BMU Lead in maintaining a high-quality operational environment, predictable workflows, and disciplined scheduling practices.
- Drive continuous improvement in operational processes, tools, and ways of working.
- Represent the WMCA in a professional manner.
- Undertake such tasks as may reasonably be expected commensurate with the scope and level of the role.

Person Specification

Candidates/post holders will be expected to demonstrate the following:	Essential / Desirable		How Evidenced?		
Experience	**E**	**D**	**A***	**I***	**T***
• Running an ISMS and aligning to ISO 27001 in complex, multi-supplier environments.	x		x	x	
• Establishing policies, MSBs, risk registers, DPIAs, and supplier security.	x		x	x	
• Leading incident governance and audit responses; delivering organisation-wide training.	x		x	x	
• Experience working with operational, service, delivery or technology-related data.	x		x	x	
• Experience producing dashboards, reports or analytics for senior stakeholders.	x		x	x	
• Experience supporting continuous improvement or lessons-learned processes.	x		x	x	
• Experience of working in Agile, Lean or DevOps-aligned delivery practices (e.g., Kanban, flow metrics, sprint planning, CI/CD awareness).	x		x	x	
• Experience of working with CABs, release cycles or readiness reviews.	x		x	x	

• Experience collaborating with Data Engineering, Data Governance or analytics teams to implement data controls, metadata standards and data quality checkpoints.	x		x	x	
• Experience assuring or governing data pipelines, data flows, integrations or data processing environments (rather than building them).	x		x	x	
• Experience implementing or overseeing data lifecycle governance, including classification, retention, minimisation and defensible deletion.	x		x	x	
• Experience working with Microsoft Purview, M365 compliance tooling or equivalent enterprise governance platforms.	x		x	x	
• Experience providing assurance over SharePoint information architecture, permissions, retention schedules and automated workflows.	x		x	x	
• Experience assessing the relevancy, quality and business purpose of organisational datasets, and advising on remediation of legacy or low-quality data.	x		x	x	
• Experience producing data-driven insights or assurance reporting on data use, data volumes, sensitivity, access patterns or compliance posture	x		x	x	
• Experience working in or alongside portfolio-led environments with multiple concurrent projects or product teams.		x	x	x	
Skills / Knowledge	**E**	**D**	**A***	**I***	**T***
• Strong analytical ability, attention to detail and record-keeping discipline and ability to interpret operational data.	x		x	x	
• Understanding of enterprise architecture, service management, or technology asset management.	x		x	x	
• Deep knowledge of UK GDPR/DPA 2018, ISO 27001, NCSC guidance.	x		x	x	
• Understanding of **data engineering concepts**, including data lineage, metadata management, schema validation, data quality dimensions and ETL/ELT patterns — sufficient to provide assurance and governance input.	x		x	x	
• Knowledge of **Microsoft Purview** features (e.g., Data Map, Data Catalog, sensitivity labels, DLP, retention) and how they support automated policy enforcement.	x		x	x	
• Knowledge of **SharePoint information architecture**, including site templates, permission models, retention policies and workflow governance.	x		x	x	
• Understanding of **data lifecycle management**, including classification, retention, minimisation, defensible disposal and archival processes.	x		x	x	
• Ability to translate business and regulatory needs into **data governance requirements**, control sets and assurance measures.	x		x	x	
• Strong ability to interpret data-driven indicators (freshness, completeness, lineage gaps, anomalous access patterns) to identify assurance concerns.	x		x	x	
• Familiarity with **metadata standards** (e.g., business glossary, controlled vocabularies, structural metadata, data definitions) and their role in data integrity.	x		x	x	
• Knowledge of **data-related risks**, including data sprawl, shadow repositories, uncontrolled copies, unstructured data growth and quality deficits.	x		x	x	
• Understanding of how **DevOps**, CI/CD and data-pipeline automation create data integrity and security assurance considerations.	x		x	x	
• Strong risk and assurance capability; documentation, excellent collaborative and diplomatic communication and influencing skills.	x		x	x	
• Ability to work with technical teams to gather and validate information.	x		x	x	
• Understanding of digital and technology delivery environments: software engineering, data pipelines, corporate IT operations, OT/public-realm systems.		x	x	x	
• Highly organised; strong attention to detail; excellent communication skills; strong problem-solving ability.		x	x	x	
• Familiarity with DevOps toolchains (e.g., Azure DevOps, Jira, GitHub boards, CI/CD pipelines).		x	x	x	
• Proactive, organised, and comfortable managing multiple priorities.	x		x	x	

• Committed to continuous improvement and high standards of delivery.	x		x	x	
• Able to build trust and credibility with senior leaders and technical experts.	x		x	x	
Qualification / Education / Training	**E**	**D**	**A***	**I***	**T***
Evidence of relevant continuous professional development.	x		x		
CISSP/CISM or ISO 27001 Lead Implementer/Lead Auditor (or equivalent)	x		x		
Training or certification in data governance, data quality management, or metadata management (e.g., DCAM, CDMP, DAMA DMBoK-aligned training).	x		x		
Privacy certifications (e.g., CIPM/CIPP/E), ITIL Foundation, SharePoint administration		x	x		
Qualifications in data analysis, data literacy, data lifecycle management, service management, Agile/Lean, or continuous improvement (e.g., basic Lean/Six Sigma).		x	x		

***Key: A** = Application, **I** = Interview, **T** = Testing/Assessment

Core Expectations

Health, Safety & Wellbeing	All employees have a duty to take reasonable care for the health, safety, and wellbeing of themselves and of other persons who may be affected by their acts or omissions at work; and co-operate with their employer so far as is necessary to enable it to successfully discharge its own responsibilities in relation to health, safety, and wellbeing.
Equality & Diversity	Promote and champion equality and diversity in all aspects of the role.
Learning & Development	Participate in and take responsibility of any learning and development required to carry out this role effectively.
Performance Management	Actively engage in the performance management process and take responsibility for managing performance outcomes.
GDPR	Ensure the reasonable and proportionate protection, processing, sharing, and storing of WMCA information in accordance with the relevant legislation, corporate policies, and in the best interests of the data subjects (Data Protection/GDPR), the WMCA, our partners, and the West Midlands, in all aspects of the role.
Adherence to Policies	Be aware of and comply with all organisation policies.
Other	There may be a requirement to work outside normal office hours on occasion, including a requirement to work within stakeholder and partner offices within the WMCA constituent area on a regular basis.

Values

Our culture is underpinned by what we do and how we do it. Our behaviours outline the ways we need to work to deliver success, become truly inclusive, and make the organisation somewhere where everyone can give their best contribution.

Value	Competency	Behaviour
Collaborative	Team Focussed	Works as part of team, managing and leading.
	Service Driven	Customer, resident, and partner focussed.
Driven	Empowered & Accountable	Takes ownership and leads when needed.
	Performance Focused	Ambitious and going the extra mile.
Inclusive	'One Organisation' Mindset	Believe in each other's expertise.
	Open & Honest	We do what we say we are going to do.
Innovative	Forward Thinking	Embrace change and open to new possibilities.
	Problem Solving	Go for clear and simple whenever possible.

Additional Post Requirements

Essential Car User		Politically Restricted Post		Disclosure and Barring Service (DBS)				Vetting	
Yes ☐	No ☐	Yes ☐	No ☐	Basic ☐	Standard ☐	Enhanced ☐	None ☐	Yes ☐	No ☐

Job Evaluation Details			
Date Evaluation Agreed	**JEP Reference**	**Grade**	**Job Family**