

**Manchester City Council
Role Profile**

**Cyber Operations Platform Manager - Grade 10
ICT Service, Corporate Core Directorate
Reports to: Cyber Security and Configuration Manager
Job Family: Technical**

Key Role Descriptors:

The role holder will have lead accountability across children and adults social care management and education systems for the delivery of a range of major technical initiatives and work packages.

As a subject matter expert, the role holder will oversee the design, development and implementation of innovative frameworks which enable the operation of effective technical services and support their contribution to the achievement of strategic and operational objectives.

Key Role Accountabilities:

Provide a lead technical consultancy function for the assigned service area, ensuring that complex and innovative technical solutions are delivered in line with customer and legislative requirements. Dependent on the service area, this may include software / information technology support, engineering, surveying, curating, or other specialist functions.

Drive the effective delivery of work packages to ensure service objectives are achieved, to support the effective decision-making processes of the Council and to enable it to meet its legal obligations and strategic objectives.

Play a key role in the review and development of organisational strategies, ensuring that key performance indicators are met. Provide effective operational and strategic support to the authority's corporate approach to external regulatory / inspection and internal governance processes.

Foster successful relationships and secure stakeholder commitment through strong and effective negotiation to ensure work packages are delivered effectively and to customer requirements and agreed objectives.

Effectively commission work packages both within the assigned service area and from other service areas / organisations to provide a holistic approach to advice and ensure that all factors are accounted for in the decision-making processes of the organisation, including consideration of Public Service Reform principles.

Coordinate the implementation of new platform developments and new releases, including liaison with the operational services, Finance, Corporate Procurement and Third-Party suppliers.

To undertake testing of new systems and new releases as part of a managed installation and hand-over process, in collaboration with all key stakeholders.

Ensure that all processes and procedures are appropriately documented and provide an appropriate level of internal control.

Develop and support the delivery of associated training and awareness for all relevant service users within the Council linked to the respective subject matter.

A strong and clear advocate for the organisation's *m people* approach.

Roles at this level may be required to manage a range of assigned resources, which may be human, financial or other, to ensure continuous improvement in service delivery. Staff management duties may be either through direct line management of a team (including appraisals, performance management and other duties) or through matrix management of a virtual team of officers.

Dependent on the service area, the role holder may be required to work on a rota basis including out of hours as required to meet customer demand.

Demonstrate a personal commitment to continuous self-development and service improvement.

Through personal example, open commitment and clear action, ensure diversity is positively valued, resulting in equal access and treatment in employment, service delivery and communications.

Where the role holder is disabled, every effort will be made to supply all necessary aids, adaptations or equipment to allow them to carry out all the duties of the role. If, however, a certain task proves to be unachievable, job redesign will be fully considered.

Role Portfolio:

Manchester City Council

Manchester City Council (MCC) supports a resident population of approx. 575,000 people and employs over 7300 staff & supports various external partnerships. The *Our Manchester Strategy - Forward to 2025* sets out how MCC will create a sustainable, equal and inclusive city. At the heart of these ambitions is the desire to achieve equality for all Manchester communities, recognising that for some communities this will mean more support is needed to reduce inequalities and improve outcomes.

The Council is split into Directorates: Adults' Services; Chief Executive's; Children's Services; Corporate Services; Growth and Development; Neighbourhoods; Population, Health, and Wellbeing.

ICT & Digital Department

The vision of the ICT & Digital department is "a relentless drive towards digitally empowering better outcomes for the Council and its communities using inclusive, secure & connected technologies to underpin exemplary ICT & Digital service delivery."

The ICT & Digital department support Manchester City Council by providing technology, infrastructure, and digital services. These range from public facing websites to network operations and cloud services. ICT Portfolio and core functions include:

- **Digital Delivery & Business Partnering:** Lead and direct ICT for each of the Council directorates, ensuring the ICT Strategy is aligned to the delivery of the City's strategic priorities and enables services to deliver effectively. The Heads of Digital Delivery & Business Partnering are responsible and accountable for all new ICT & Digital related demand within the specific directorates for which they are responsible utilising teams of programme, project, and product managers to support the continuous delivery of transformational change.
- **Portfolio & Departmental Management Office (PDMO):** Ensures alignment of all ICT & Digital activity with strategic objectives, outcomes, and capacity to deliver, to enable benefit realisation and support continual service improvement. Provides governance standards across all ICT & Digital areas to allow proactive selection, prioritisation, and control of the complete portfolio of activity. Has overarching responsibility for all financial management, contracts and licensing that underpin effective transition and sustainable ICT & Digital service delivery.
- **ICT Operations:** Provides the core operational function of the ICT & Digital department. It is responsible for the following IT Infrastructure Library (ITIL) functions: Service Desk, IT Operation Management, Technical Management, Platform Management and Application Support Management. ICT Operations is at the forefront of ICT service delivery and is one of the most important elements that keeps the organisation running.

- **Cyber Security & Compliance:** Provides the operational security controls, security guidance, security assurance, cyber risk management, and compliance activities that support all products and platforms within the Council. Protects networks, devices, and data from unauthorised access or criminal use by the practice of ensuring confidentiality, integrity, and availability of information.
- **Enterprise Architecture (EA):** Provides a well-defined practice for conducting enterprise analysis, design, planning, and implementation for the successful development and execution of strategy. Enterprise Architecture reduces redundancy, complexity and information silos and business risks associated with ICT investments.

A high-level summary is provided below to add scale and context to the wide variety of services provided by the Council's ICT & Digital service that is also supported by an investment plan to deliver Digital Transformation across:

- 212 Office locations inc. 27 libraries
- Circa 8000 ICT users and 96 elected Councillors
- 200+ Line of Business Applications
- 1000+ Virtual Servers hosted across resilient Cloud and On-Prem Data Centres
- 10,000+ Laptops, PC's, and associated End User Devices
- 300 printers

Cyber Security and Compliance Team

The wider Cyber Security and Compliance Team provide the operational security controls, security guidance, security assurance and compliance activities that support all products and platforms within the Councils. Protecting networks, devices, and data from unauthorised access or criminal use by the practice of ensuring confidentiality, integrity, and availability of information. These services underpin all operational IT and digital services for the whole organisation that are consumed by our internal staff, external partners along with the customers, residents, and visitors of Manchester.

Cyber Operations

The Cyber Operations team provide pro-active threat hunting capabilities along with security governance, assurance, and compliance activities, create and manage policies and processes to ensure that all technology remains secure and compliant. Through continuous vulnerability scanning the Cyber team test all security layers are safe, secure, and compliant against both our Internal Security Standards and Statutory Obligations whilst ensuring that all supporting hardware and software is current, capacity managed, and professionally documented and administered; either internally or by 3rd parties.

Typical security platforms / applications managed by the Cyber Operations team include (but not limited to):

- Firewalls
- DMZ
- Web Filtering
- Email Filtering
- Ransomware Protection
- Endpoint Detection and Response
- Security Incident and Event Monitoring (SIEM)
- Vulnerability Identification and Management
- OS and Application Security Patching

The role and experience of the Cyber Operations Platform Manager should include:

- A minimum of 5 year's experience working in an IT Security Operations team with detailed knowledge of managing network, server, applications, and end user computing in a complex environment.
- Demonstrable familiarity with the concepts and operation of common security applications and tooling.
- Detailed knowledge of Security and Cloud architecture principles
- Strong experience of managing security monitoring, alerting and service recovery in a pressurised and complex environment.
- Recent experience as a senior or lead member of a multi-disciplinary team managing operational cyber security functions (eg. firewall / filtering / DMZ / Pen Testing / Vulnerability Management) and potential 3rd party teams.
- Role holder must hold relevant professional accreditation to a recognised Cyber Security standard eg. CISSP, CISM, CCP, CCSP. The successful candidate must maintain the associated professional accreditation and be willing continually develop within this evolving service area.
- Recent experience of providing high quality management reports; supported by transparent and factual data analysis; with the aim of demonstrating problems, opportunities for risk reduction and improvement across the service.
- Ability to perform Investigations and Forensics, provide Security Representation on Projects, to perform Threat Management and Vulnerability Assessments.
- Knowledge and understanding of PSN Code of Connection compliance requirements, and experience of coordinating penetration testing and remediation activities to support the submission process.
- Experience of supplier and vendor management in a complex enterprise environment.
- A strong understanding of Prince2 (or equivalent project management methodology) and how projects should be transitioned into production and the rules and standards that govern this transition, specifically in relation to security and compliance requirements.

- Recent experience of Security Service report writing and other required reports; supported by transparent and factual data analysis; with the aim of demonstrating problems, opportunities / options with / for the service.
- Significant experience of IT Service Operations, and how an IT installation works across 7 *24.
- Significant knowledge of the relevant legislative framework and professional standards both within the ICT industry and in particular to a local authority.
- To work flexibly including out of hours and bank holidays as required to meet customer demand and customer requirements and potential incidents up-to a Major Incident.

Key Behaviours, Skills and Technical Requirements

Our Manchester Behaviours

- We are proud and passionate about Manchester
- We take time to listen and understand
- We 'own it' and we're not afraid to try new things
- We work together and trust each other
- We show that we value our differences and treat people fairly

Generic Skills

- **Communication Skills:** Understanding the dynamics of conflict and how to achieve mutual agreement. Demonstrating the ethics of good practice, including respect for all parties, tolerance of different people and perspectives, confidentiality, and the importance of honesty. Listening actively to others and working to formulate options and solutions.
- **Analytical Skills:** Skills to analyse a wide range of data and other sources of information to break them down into component parts, patterns, and relationships; probes for further understanding of problems and risks and makes rational judgements from the available information and analysis demonstrating and understanding of how one issue may be part of a much larger system/issue.
- **Planning and Organising:** Sets clearly defined objectives, plans activities and projects well in advance and takes account of risks and changing circumstances; identifies and organises resources and manages time effectively monitoring performance against milestones and deadlines.
- **Project Management:** Ability to influence, monitor and control the risk environment, both strategic and operational, through effective allocation of roles and responsibilities. Has ability to manage risk effectively in the context of projects and programmes.
- **Problem Solving and Decision Making:** Ability to react to immediate problems of a highly complex nature with associated risk factors and deliver pragmatic solutions sometimes under extreme pressure.
- **ICT Skills:** Skills to coordinate ICT resources to meet business objectives and create value for the stakeholders by improving the performance of ICT functions, whilst maintaining professional standards and clarity of purpose.
- **Financial Management:** Excellent financial planning skills to develop short-, medium- and long-term financial plans with an ability to budget proactively with large, high-risk, or volatile elements being identified and cross-referenced to operational activity.
- **People Management:** Ability to exert positive influence over the performance of others, promoting others' self-esteem, inspiring trust, and fostering confidence in others' ability to achieve high standards, thereby enhancing a performance orientated culture which supports the delivery of high-quality services to the community.

Technical Requirements (Role Specific)

- Qualified to ITIL, with a strong practical understanding of how the core ITIL functions (CM / IM / PM / RM and Configuration Management) interface and interact to collectively support IT and the Business.
- Professional accreditation to a recognised Cyber Security standard eg. CISSP, CISM, CCP, CCSP
- A strong understanding of Prince2 (or equivalent project management methodology) and how projects should be transitioned into production and the rules and standards that govern this transition.
- Significant experience of IT Service Operations, and how an IT installation works across 24x7.
- Significant knowledge of the relevant legislative framework and professional standards both within the ICT industry and in particular to a local authority.
- Experience of managing team(s) to provide effective Cyber Security defences.
- To work flexibly including out of hours and bank holidays as required to meet customer demand, service requirements and potential incidents up-to a Major Incident.