Principal Security Consultant (Risk Management)

This is a fantastic opportunity to join a highly skilled Security Consultancy Team who specialise across the full range of cyber security disciplines. We are a fast growing Small to Medium-Sized Enterprise (SME) who offer a varied workload day-to-day, with long term careers through multiple progression paths, and a culture that promotes both a social working environment and an accommodating work life balance.

“Working at Logiq has been an amazing move for myself. Not only is it a great overall business, but being able to nip out here and there to do the school run has taken a huge level of stress off myself and my partner’s life” …

About Logiq

Logiq Consulting are Cyber Security and Information Assurance experts. Specialising in delivering leading edge consultancy to clients with high-risk business operations, along with a range of security services and products relied upon throughout the Private and Public Sector.

Our existing programmes of work are expanding rapidly, and we have urgent requirements for a Principal Consultant, to enable us to continue to deliver at an accelerated rate. Ideally you will have current or recent experience working in a government security advisory role, either within Defence or Security organisations.

About You

We are seeking a highly capable Principal Security Consultant to join the Security Risk Management team within the company’s primary Cyber Security Practice.

The successful candidate will be a Full Member of the Chartered Institute of Information Security (CIISec) and should hold a certification such as Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) (or equivalent). It would also be desirable for them to hold professional registration with the Cyber Security Council in the Risk Management specialism.

Logiq Consulting are a leading player in MOD’s cyber security transformation to Secure by Design (SbD). We are looking for team members and leaders who share our vision that cyber risk management is driven by business requirements and a holistic view of security that can guide clients to optimal risk management decisions, and delivery of capabilities which are inherently secure.

Ideally you will have worked across the system lifecycle, undertaking the security risk management activities required to support each phase, from initial threat and risks assessments and specification of security requirements, through to overseeing implementation and testing of socio-technical security architectures. You will also have experience of defining and implementing risk management strategies and plans and coordinating the continuous security assurance and risk management processes which underpin delivery and operation of secure capabilities.

The ideal candidate will be both experienced and invested in ensuring that our clients' solutions are Secure by Design and will have the inter-personal skills needed to do this, e.g. ability to lead

workshops, engage with business leaders, and interact with a diverse range of project teams and stakeholders. With your defence experience you will be comfortable operating in a 'customer friend' type role, supporting clients understand, mitigate, and manage their security risks appropriately, and ensuring secure capabilities are delivered to meet operational requirements. Our Principal Consultants are engaged across Security Engineering, Risk Management and Assurance tasks, working on parallel projects and workstreams, and take lead roles on client projects.

You will also be comfortable enhancing customer relationships and identifying opportunities for growth and will have experience developing proposals and tender submissions in pursuit of new business opportunities.

Experience and Knowledge :

Demonstrable experience of:

- Coordination and leadership of risk management and assurance workstreams for projects delivering secure systems and services within a government context.
- Undertaking and producing socio-technical security risk assessments, ideally including technical threat modelling (e.g. using STRIDE).
- Development and implementation of risk management strategies and plans.
- Specification, development and technical assurance of security policies and procedures.
- Specification and definition of system security and control requirements.
- Leadership of security risk management events and workshops.
- Specification and coordination of security verification, validation, and assurance testing.
- Specification, development and technical assurance of security risk management and assurance artefacts and evidence.
- Development of proposals and tender submission artefacts.

Knowledge and understanding of core cyber security risk management areas, including but not limited to:

- Security governance and risk management approaches, tools, and techniques.
- Threat modelling (e.g. STRIDE) and socio-technical risk assessment (e.g. NIST 800-30) methodologies.
- Attack classification and characterisation frameworks (e.g. MITRE ATT&CK)
- Computer, Network and Cloud Security architectures and controls, System Hardening, Secure Boundary Protection architectures and controls, Cryptographic controls (Data at Rest, Data in Transit, Public Key Infrastructure (PKI)), Security Monitoring and System Security Audit.
- National and international security standards including the International Standards Organisation (ISO) 27000 series, NIST Cyber Security Framework, Risk Management Framework, and Special Publication 800 Series, NCSC Cyber Assessment Framework, and other industry frameworks.
- Familiarity with NCSC and industry best practice guidance.
- Experience in MOD security policy, processes, and practices (inc Joint Service Publications 604, 440, 902, DEFCON 659a).

Essential Qualifications:

- Full Membership of the Chartered Institute of Information Security (CIISec).
- Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM), or another industry recognised cyber security certification.
- Desirable Qualifications:
- Chartered or Principal status via the UK Cyber Security Council for Risk Management.
- NCSC Certified Cyber Professional in Risk Management.
- IEng or CEng registered with UK Engineering body.
- Chartership through the British Computer Society.

Company benefits include:

- Discretionary 10% bonus
- Discretionary annual training fund per employee
- Car allowance
- Very competitive pension scheme
- Death in Service Benefit