Lead Risk Advisor

Closing Date: Tuesday 15th June 2021

Location: London, Birmingham, Sheffield, Nottingham & Glasgow
Salary Range: London £36,798 National £30,989
Interviews: w/c 5th July 2021

The Role
We're recruiting for a Lead Risk Advisor here at MoJ Digital & Technology, to be part of our warm and collaborative Security, Privacy and Live Services team.

As part of the cyber assistance team, you will take responsibility for ensuring cyber security risks are well-understood and well-managed for the systems used to deliver the services of the MoJ in your allocated part(s) of the organisation. You work with stakeholders at all levels in various business areas to understand, analyse and raise the key risks to services, systems and processes.You will identify and manage risks within your area in a transparent and open way, escalating when needed. You will create awareness of key risks to help those responsible for services to solve cyber security problems as systems are procured, designed and built.

You bring experience of analysis and will thrive in various complex organisational and technical environments. You are open to new approaches, advising on pragmatic risk management measures to enable technical teams and operational areas to deliver solutions. You find creative new ways to reduce the risk to the business in the services that Digital and Technology provides, whether internally or through third party suppliers.

The vast majority of your work will be about working on initiatives to ensure that risks are identified, appropriately mitigated, well-managed, and that we can accurately understand our cyber security position as an organisation. Your guidance and advice will help shape investment priorities. You may also be responsible, as part of the risk management process, for supervising the work of commercial suppliers.

You also work with our Security Operations team to understand the ongoing cyber risks to systems, and then communicate this to the relevant parts of the business - helping them to understand the actual risks and potential impacts to their services, what their responsibilities are, and guiding their thinking about appropriate and proportionate risk controls. This role will give significant opportunities for you to learn from other parts of the organisation and develop professionally.

You also collaborate internally, building your profile and being an advocate for a positive security culture within the MoJ and across Government, engaging with security colleagues in other departments and the Government Security Profession, representing the MoJ and helping to lead and influence the discussion.

To help picture your life at MoJ D&T please take a look at our blog and our Digital & Technology strategy.

Key Responsibilities:

- Take responsibility for risk management activities within a given area of the MoJ, usually within established security and risk management governance structures.
- Lead the analysis and derivation of business-supporting security needs, undertake Cyber Security related risk assessments, conduct tailored threat assessment and other risk management activities, and ensure activities are consistent with applicable regulations and legislation.
- Provide tailored advice to a range of stakeholders on how to remedy identified risks by proportionately applying security capabilities, using published guidance, standards, and drawing on a range of experts as well as personal expertise.
- Provide expert security advice that highlights Cyber Security related risks, so risk or service owners can make well-informed, cost-effective and auditable decisions.
- Develop and maintain a good understanding of the data and information systems in use in your assigned business areas, and the overarching threats to these, being able to articulate this to others in the cyber security team.
- Proactively manage cyber security risks to your assigned area's technology estate, being able to quickly articulate the biggest areas of concern, and what is being done to address them. Collate residual risks, summarise them in business terms and report to your business partners and senior management.
- Review risk submissions and risk registers provided by suppliers, making sure these are being kept up to date. Keep internal risk registers up to date, both manually and using risk management tools.
- You will be involved, from a security perspective, in activities relating to contract and commercial management such as supply chain management and contract/ review, tender evaluations, procurement and DPIA reviews. You will help to standardise processes where needed.
- Work closely with Digital and Technology's teams that are supporting your assigned area of the business, such as to advise on where investment is needed to reduce risks.
- Review the outputs of IT Health Check reports both for internal and externally supplied systems and provide guidance and advice to system and service owners on the appropriate treatment of the report findings.

If this feels like an exciting challenge, something you are enthusiastic about, and want to join our team please read on and apply!

This is a **MoJ Band B** role with a salary of **London £36,798 National £30,989** plus great benefits:

- 37 hours per week and flexible working options including working from home, working part-time, job sharing, or working compressed hours.
- We are committed to nurturing our staff and provide lots of training and development opportunities with learning platforms such as: Linux Academy, O'Reilly, Pluralsight, Microsoft Learning, Civil Service Learning, GDS Academy, etc.

- 10% dedicated time to learning and development with a budget of £1000 a year per person
- Generous civil service pension based on defined benefit scheme, with employer contributions of 26-30% depending on salary.
- 25 days leave (plus bank holidays) and 1 privilege day usually taken around the Queens' birthday. 5 additional days of leave once you have reached 5 years of service.
- Compassionate maternity, adoption, and shared parental leave policies, with up to 26 weeks leave at full pay, 13 weeks with partial pay, and 13 weeks further leave. And maternity support/paternity leave at full pay for 2 weeks, too!
- Wellbeing support including access to the Calm app.
- Nurturing professional and interpersonal networks including those for Careers & Childcare, Gender Equality, PROUD and SPIRIT
- Bike loans up to £2500 and secure bike parking (subject to availability and location)
- Season ticket loans, childcare vouchers and eye-care vouchers.
- 5 days volunteering paid leave.
- Free membership to BCS, the Chartered Institute for IT.
- Some offices may have a subsidised onsite Gym.

Person Specification

Essential

- Able to apply an analytical approach to real problems and consider all relevant information. Applies appropriate rigour to ensure a full solution is designed and achieves the business outcome.
- Able to effectively translate and accurately communicate risk implications across technical and non-technical stakeholders, and able to respond to challenges. Able to manage stakeholders' expectations and be flexible, adapting to stakeholders' reactions to reach consensus.
- Enabling and informing risk based decisions - works with risk owners and business stakeholders to build understanding, advise and give feedback. Able to explain real-world implications of risks in a balanced and pragmatic way to enable business decisions to be made effectively.
- Understands the context of their business area and diverse views and perspectives of their stakeholders and is able to bring these views together.
- Take ownership of regular risk register and ad-hoc risk submission reviews in collaboration with suppliers and internal stakeholders, and ensure risks are managed to closure.
- Adaptable, willing to learn and collaborative in your approach both within your team and across the wider organisation.

Desirable:

- Understands different risk methodologies and how these are applied, as well as the proportionality of risk.
- Understanding security implications of transformation - Can interpret and apply understanding of policy and process, business architecture, and legal and political implications in order to assist the understanding of cyber security risks.
- Ability to supervise audit of suppliers' and business partners' cyber security and information management practices.
- Communicating security effectively between the technical and non-technical roles.
- Use expert knowledge of systems and the associated risks to set priority of cyber security work, and to advise on the investment priorities for Digital and Technology.
- Knowledge of relevant regulations, legal requirements, HMG policies and guidance, and industry good practice.

We welcome the unique contribution diverse applicants bring and do not discriminate on the basis of culture, ethnicity, race, nationality or national origin, age, sex, gender identity or expression, religion or belief, disability status, sexual orientation, educational or social background or any other factor.

Our values are Purpose, Humanity Openness and Together. Find out more here about how we celebrate diversity and an inclusive culture in our workplace.

How to Apply

Candidates must submit **a CV and a statement of suitability (of no more than 500 words)** which describes how you meet the requirements set out in the Person Specification above.

In D&T, we recruit using a combination of the **Digital, Data and Technology Capability** and **Success Profiles** Frameworks. We will assess your Experience, Technical Skills and the following Behaviours during the assessment process:

- Making effective decisions
- Working together
- Seeing the big picture
- Managing a quality service
- Communicating and Influencing

Your application will be reviewed and sifted against the Person Specification above by a diverse panel.

Successful candidates who meet the required standard will then be invited to a 1-hour panel interview held via video conference.

Should we receive a high volume of applications, a pre-sift based on your experience will be conducted prior to the sift.

Further Information

Please review the following Terms & Conditions which set out the way we recruit and provide further information related to the role.

If you have any questions please feel free to contact recruitment@digital.justice.gov.uk