Introduction

These are exciting times at MOJ Digital and Technology. We have a clear vision - to develop a digitally-enabled justice system that works more simply for users - and we're looking for talented people to help us achieve it.

We're making things better by building adaptable, effective services and making systems that are simple to use for staff and citizens. It can be challenging but it's also important and rewarding.

As well as doing great work, we're creating a place that's great to do work in. We offer tip-top kit, brilliant training opportunities and support from expert colleagues. On top of that, you'll find flexible working, an inclusive culture and a place where your opinion is valued.

The Role

You are responsible for ensuring cyber security risks are well-understood and well-managed for the systems supporting particular business areas of the MOJ. You work with stakeholders at all levels in those business areas to understand what really matters to them in terms of the information they're responsible for, and the environments they operate in, and use this knowledge to prioritise which products and projects get attention by Cyber Security Consultants as systems are designed and built. 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 their actual risks, and what their responsibilities are.

The vast majority of your work will be about ensuring that risks are identified, appropriately mitigated, risks remain well-managed, and that we can accurately understand our cyber security position as an organisation. Your expert guidance and advice will help shape investment priorities, and find new creative approaches to reducing the risk to the business in the services that Digital and Technology provides. You may also be responsible, as part of the risk management process, for supervising the audit of commercial suppliers personnel, premises, services and certifications.
One of the main aspects of the role is the importance of building and maintaining effective relationships with the key stakeholders, and that the job holder should anticipate travelling to meet these stakeholders regularly.

MAIN RESPONSIBILITIES

- Working closely with SIROs, IAOs, and other interested stakeholders in your assigned parts of the MOJ to build a rich picture of the business risks they care about and the implications for Digital and Technology-provided systems.

- Developing and maintaining a good understanding of the data and information systems in use in your assigned business area, and the overarching threats to these, being able to articulate this to others in the cyber security team.
- Using your understanding of the technology products and projects in-use and in-planning in your assigned area, and the potential impact a cyber security issue would cause for the data in-use, advising on the prioritisation of cyber security advisor support.
- Coordinating cyber security advisor work across your assigned area, and collating the resulting risks, summarising them in business terms to your business partners.
- Actively managing 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.
- Working 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.

CAPABILITIES

The essential skills and experience required are:

- Communicating security effectively between the technical and non-technical roles. Able to effectively translate and accurately communicate security and risk implications across technical and non-technical stakeholders, and able to respond to challenge. 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 different risk methodologies and how these are applied, as well as the proportionality of risk.
- 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.

Desirable:

Analysis - Able to apply the approach to real problems and consider all relevant information. Applies appropriate rigour to ensure a full solution is designed and achieves the business outcome.

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.

Essential:

- Making effective decisions
- Collaborating and partnering
- Seeing the big picture

Desirable:

- Delivering value for money
- Changing and improving
- Managing a quality service
- Leading and communicating
- Building capacity for all
- Delivering at pace

Throughout the process we will assess your technical specialist skills and experience on the above requirements.

We are an equal opportunity employer and value diversity at our company. We do not discriminate on the basis of race, religion, colour, national origin, gender, sexual orientation, age, marital status or disability status.

Salary and working arrangements
If successful, the salary we offer you will be within the advertised range and will depend on the skills and experience you demonstrate at the interview.
Therefore in your cover letter it would be helpful to the hiring teams if you can indicate your salary expectations and if possible your notice period.

You'll also get:

- Flexible working options such as working from home or remotely, working part-time, job sharing, or working compressed hours, we have people doing it and are happy to discuss further
- Lots of training and development opportunities
- A civil service pension with an average employer contribution of 22%
- 25 days annual leave (plus bank holidays), and an extra day off for the Queen's birthday. No promises you'll be invited to her party, though
- Great maternity, adoption, and shared parental leave, 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!

- Bike loans and secure bike parking (subject to availability and location)
- Season ticket loans, childcare vouchers, and eye-care vouchers.

Selection process details
Candidates must submit:

- a current and relevant CV;
- a Cover letter (1 page max) setting out why you are interested in the role and how you meet the essential skills and experience required.

The job advert lists the essential, specialist skills and experience as well as key Civil Service competencies required for the role.

At the CV review/sift stage we will use the technical/specialist skills and experience to determine your suitability for the role. At the interview we ask you questions based on the specialist/technical skills and experience in the job advert. If invited to an interview we will send you a detailed Job description to help you prepare for your interviews.

We conduct competency based interviews which means the interviewers will ask open-ended questions to which they are seeking answers/evidence of essential, previous experience in order to guide their hiring decision. Some roles may also require us to use assessments as part of the interview process.

Please note that due to the volume of applications we receive we are unable to provide feedback after the CV review (sift) stage.

Things you need to know

Security and Immigration checks
Successful candidates must pass a disclosure and barring security check.
Successful candidates must meet the security requirements before they can be appointed. The level of security needed is security check.
Candidates will be subject to UK immigration requirements as well as Civil Service nationality rules.

If you're applying for a role requiring security clearance please be aware that foreign or dual nationality is not an automatic bar. However certain posts may have restrictions which could affect those who do not have sole British nationality or who have personal connections with certain countries outside the UK.

Nationality requirements
Open to UK, Commonwealth and European Economic Area (EEA) and certain non EEA nationals. Further information on whether you are able to apply is available here.

Eligibility
Candidates in their probationary period are not eligible to apply for vacancies within this department.

Working for the Civil Service

The Civil Service Code sets out the standards of behaviour expected of civil servants.

We recruit by merit on the basis of fair and open competition, as outlined in the Civil Service Commission's recruitment principles.
The Civil Service embraces diversity and promotes equality of opportunity. There is a guaranteed interview scheme (GIS) for candidates with disabilities who meet the minimum selection criteria.

Contact point for applicants
For further information regarding this role please contact MoJ D&T Recruitment.

Further information

All Civil Servants will adhere to the 'Civil Service code', which outlines the Civil Service's core values, and the standards of behaviour expected of all civil servants in upholding these values.

Note for Civil Servants only: If successful, the salary offered would normally be determined by applying the MoJ salary progression rules. If the appointment is on level transfer your substantive salary (excluding any allowances) will remain unchanged, unless it exceeds the maximum stated within the MoJ pay band, and unless your current salary is below the relevant MoJ grade minimum. If the appointment is on temporary or substantive promotion the salary will be increased by the appropriate promotion percentage or moved to the minimum of the relevant MoJ grade minimum, whichever is the greater.

Note for all Applicants: This post is open to UK Nationals, Commonwealth Citizens, EEA Nationals of other member states and certain non-EEA family members. There must be no employment restrictions or time limit on your permitted stay in the UK. You should normally have been resident in the United Kingdom for at least 3 years and in some cases 5 or even 10 years preceding your application due to the requirement to have a checkable history for security vetting purposes. If you answer 'No' to the questions regarding nationality then it is unlikely your application will be pursued. If you are unsure as to your eligibility on any of these points, please contact the recruitment team for clarification or advice.