National Audit Office

CHANGE YOUR WORLD

National Audit Office

Head of Information Security Assurance

CHANGE YOUR WORLD

1. Introduction

Thank you for your interest in joining the National Audit Office as Head of Information Security Assurance. This pack will give you a better idea of who we are, what you'll do when you join us, and what we offer. It also gives more details about the application process.

Our position is unique, and our work is extraordinarily influential. Totally and distinctively independent, we scrutinise public spending for Parliament. This means we work for, and for the good of, everyone in the country. Our financial audit and value for money work, and everything else we do, helps society work better – supporting and enabling improvements in the way services are delivered right across the public sector. The recommendations from our work result in financial savings and positive changes in government to improve services and ensure value for money for the taxpayer. The NAO is also a world leading audit institution and has a role to play on the international stage.

More about the NAO is available on our website nao.org.uk

2. The Role

Main purpose of the role

The NAO is granted extensive access to privileged government and personal information and must in addition to its own data preserve both the confidentiality and safety of that resource. The Information Security Team's objective is to provide timely and robust assurance to the C&AG and Senior Information Risk Officer that our Information Security Management System is robust and successful in meeting both external and insider threats, whilst alerting them to any emerging or residual risks which require mitigating.

To support this the post holder will:

- Design and report upon progress of our Information Security Plan.
- Ensure the NAO designs and operates a best of breed Information Security Management System compliant with IS27001.
- Stress tests the NAO's Digital Plan and IT architecture to identify potential weaknesses and threats to defending the information assets we hold.
- Engage with technology projects and provide timely input and advice.
- Design and implement a communications strategy so that all staff fully understand and comply with our policies and procedures to protect our information assets, including the appropriate security classification of information, use of applications and hardware, and the protection of paper and other non-IT information assets.
- Lead on incident response plans and conduct investigations into actual breaches or near misses to ensure lessons are learned and remedial actions are implemented in a timely manner.
- Contribute to the design and maintenance of an information disaster recovery strategy, ensuring it is regularly tested and reviewed in the light of lessons learned.
- Keep the Departmental Security Officer (DSO) and Chief Information Security Officer (CISO) informed of emerging threats or unmitigated risks to the effective design and operation of our IT and other

Information procedures and policies.

- Be visible and the first point of contact for advice by Information asset owners across the NAO.
- Work with audit clients and third-party suppliers to the NAO to ensure that data is transferred appropriately and retained/destroyed in line with NAO requirements and legal requirements.
- Monitor compliance with our legal obligations and act as our nominated Data Protection Officer.

Relationships

Reporting to: Departmental Security Officer (DSO)

Relationships:

Internal: Critical relationships with Heads of Departments and Information Asset owners.

Strong internal relationships with NAO staff at all levels to ensure that everyone is mindful of the role they must play in preserving the security of our information assets through strong customer service focus. Infrastructure Analysts, Deputy & Infrastructure Team Leader.

External: Suppliers, vendors, and peers in similar organisations and the financial services sector. Relationships with a number of support organisations such as Cabinet Office, National Cyber security Centre and Centre for the Protection of National Infrastructure.

Resources Managed: As per project requirements and responsibility for team's staff and cash budget

Main responsibilities

Key tasks include:

- Overseeing and coordinating security efforts across the Office including the implementation of the Digital Assurance components of the NAO Digital Plan.
- Identifying and establishing security initiatives and standards throughout the Office
- Planning, directing and coordinating the Office's information security policies, setting procedures and guidelines to ensure all information

systems are functional, secure, and safeguarded. Ensure compliance with privacy, client and information security laws and regulations applicable to HMG and other defined benchmarks we chose to adopt.

- Providing technical and administrative support for the development of Disaster recovery and administrative support and development.
- Providing advice and support relating to accreditation, risk management and security architecture for the NAO
- Providing technical security advice in areas such as the development of new methods to providing digital services, new business cases for change projects with an information asset dimension and for the risk assessment of existing and planned information systems.
- Aligning our approach to information security within an approved Digital Plan including where cloud solutions drawing on the technical standards / principles produced by HMG.
- Monitoring access to all systems and conducting deep dive reviews of access control profiles and segregation of duties.
- Identifying and recommending actions to mitigate information security risks within our stated appetite.
- Providing consultancy advice on the security of the NAO's technical infrastructure including risk management, mitigation activities and tools.
- Ensuring that IT projects, policies and procedures comply with the HMG's Security Policy Framework (SPF).
- Ensuring that IT Health Checks (PenTests) are undertaken at a predetermined frequency either by external and /or internal resources and any resulting action to address vulnerabilities are identified and implemented within an agreed action plan.
- Keeping up to date with the key requirements of standards including ISO27001, Cyber Essentials plus, and HMG guidance.
- Acting as the NAO lead liaison point with the technical security agencies.

3. The person we are looking for

Skills, experience, attributes and qualifications

Behavioural skills

- Effective communicator and change agent, linking strategic view with pragmatic, operational execution and excellence.
- Proven track record for driving new initiatives such as Network Behaviour Analysis, Cyber Security, Compliance, Risk Management, Endpoint protection through deploying effective change management techniques.
- Transformational leadership style to deliver the optimum performance from the team.
- Strong analytical and problem-solving skills with an attention to detail.
- Good team player who can facilitate knowledge sharing and collaborative working in multi-disciplinary teams with professional audit and ICT staff.
- Self-starter, with energy and enthusiasm for driving continuous improvement and organisational learning from project experiences and analysis of business operations.

Security Experience

- Skilled in the strategy, planning, delivery, implementation, operations and compliance reviews of:

  -Cyber and Network Security | Cloud Security (Azure) | Data Analytics | Regulatory Compliance | Data Protection 1998 Act | General Data Protection Regulations - GDPR 2018 | ISO 27001 & ISO 9000 | IT General Controls | IT Forensics | IT Target Operating Models - TOM | IT Systems Disaster Recovery | Business Continuity and Resilience |Security Operations - SOC | Security Incident and Event Management - SIEM | Third Party Vendor Compliance and Security Assessments (incl. SLAs)

- Substantial experience of an information security role gained in a similar sector or financial services organisation.

- Working towards or holding an appropriate certification level such as Certified Information System Manager (CISM)
- Successful applicants will be required to achieve SC Security Clearance
- Advanced knowledge of;
    - Government Information Assurance Policies
    - Current IT security issues, in particular those affecting government and or highly sensitive organisations.
    - Windows operating systems and networking
    - TCP/IP network theory and practice

Technical Experience

Extensive knowledge of:

- Information security assessment and auditing procedures from both a technical and business perspective
- Vulnerability scanning and auditing tools
- Enterprise scale network and host-based IDS architectures
- Enterprise scale firewall architectures
- Ecommerce application security
- Computer investigation and forensic methods and technologies
- Secure messaging architectures
- Regulatory framework

Strengths in:

- Project management skills and leadership
- Business continuity planning and auditing
- Effective communication and securing buy in from all colleagues.
- Positively supporting effective change management within a safe operating environment and meeting business need.

4. What we offer

- A very competitive salary: £69,141 up to c£85,000
- 35 days leave per year (including public holidays)
- Membership of an excellent civil service pension scheme. The Alpha pension scheme which is a defined benefit, career average scheme
- Along with work that just means more, you'll benefit from a sociable, collaborative working culture, working with other highly professional people committed to making a real difference as part of a high performing organisation
- We provide excellent learning and development opportunities combining: formal training on a wide range of analytical methods, as well as management and leadership skills; learning through our work; and learning from other colleagues
- Our annual LearnFest week combines presentations, workshops and seminars on a whole host of topics (you could also deliver one if you wish).
- Looking further ahead we run talent programmes which identify, support and develop those with the potential to reach our most senior levels.
- Modern open plan offices, centrally located in London and Newcastle and equipped with a range of excellent on-site facilities
- On-site gym at our London Office and subsidised gym membership in Newcastle
- Access to a wide variety of social activities, from quizzes to sporting events, coordinated by the NAO Sports and Social Association.
- Free Employee Assistance Program for confidential, wellbeing support and advice

5. How to apply

To apply candidates should provide an up to date CV and covering letter setting out briefly why you are suitable for this role. Please apply through our NAO website here

The closing date for applications is 11.55 on Sunday 17 November.

The selection process will involve both a panel interview and a presentation. We expect interviews to take place as soon as possible following the closing date.