Job description

Service Area:	People and Corporate Services
Job Title:	**Head of Security & Information Governance (Deputy SIRO)**
Band:	8d
Location:	Stella House, Newburn Riverside, Newcastle Upon Tyne – with regular travel nationally and across all sites.

Job purpose

Reporting to the Executive Director of People and Corporate Services, the Head of Security & Information Governance is a broad, cross-organisational role responsible for the strategic oversight and vision and leading the direction of the following wide-ranging professional, high-quality services:

- Information Security & Assurance including security risk management, incident management, internal audits, and compliance with our statuary and mandatory obligations
- Information Governance including compliance with Data Protection legislation and records retention
- Business Continuity Management ensuring the business has robust plans, impact assessments and regular testing programme
- Inquiry preparation team ensuring the retention of documents to support our evidence and providing support and training to the Leadership Team.

The role will be responsible for leading the strategic development of these areas and overseeing the creation and delivery of solutions to deliver these strategies. The post holder will have credibility at Board level, acting as the expert advisor to the CEO, Leadership Team, SIRO and Board, with responsibly for the transformation and organisational change in these key areas.

The post holder will be forward-thinking and commercially minded, implementing and developing strategies and solutions which are aligned with the business strategy requirements now and into the future in order to ensure that the business meets its objectives and strategic goals. They will lead on the development and implementation of all relevant strategies, policies, information systems and procedures that are based on a wide-ranging

legal and mandatory requirements and best practice and which fit the requirements of the NHSBSA by keeping abreast of all corporate and strategic issues ensuring they are pro-active in style and support the strategic business and direction of the NHSBSA.

The Head of Security & IG will also:

- Provide excellent leadership, training and coaching to the Security & IG team, Leadership Team, Board and wider governance groups across the NHSBSA.
- Ensure the Security & IG function has the right structure, staff and skills to deliver against the NHSBSA's business objectives.
- Deliver the Security & IG strategy, ensuring there is an effective planning and prioritisation process in place including insight development and evaluation.
- Build and maintain effective relationships with system partners to ensure effective delivery of Security & IG across the wider health and care system
- Manage and ensure delivery against the Security & IG business plan, being accountable for financial performance and demonstrating value for money
- Manage the NHSBSA business continuity plans and lead the operational response in a crisis; and
- Ensure the Security & IG team delivers high quality, professional advice to the business, operating within the framework set out in the NHSBSAs Security & IG strategy.

In this role, you are accountable for

Information Security, Information Governance & Business Continuity

- As part of the People and Corporate Services Senior Management Team, developing and interpreting the Security & IG Strategy, leading on producing appropriate short- and long-term action plans through pro-active research, interpreting of legislation and consultation with external bodies, to ensure they reflect up- to-date law, best practice and overseeing their implementation to achieve the business aims, inputting into budgets planning and spending plans as appropriate.

- Ensuring the NHSBSA meets it statutory obligations in respect to the full range data protection legislation, in additional to mandatory requirements for security across the whole organisation.

- To have responsibility for and provide effective leadership, management, development, performance and motivation to accountable staff working with them supportively to provide cohesive and efficient service delivery of individual and team objectives. This includes providing support and coaching to the Security & IG teams to support their professional development and develop their capability.

- Ensuring that robust processes are in place to withstand scrutiny of compliance with our statuary and mandatory obligations by the ICO, National Audit Office and other relevant audit or inspection bodies

- To provide strategic direction to the NHSBSA on all Information Security, Information Governance & Business Continuity activities including the implementation of an Information Security Management System (ISMS) and robust business continuity arrangements

- Responsible for the management and development of the corporate wide Information Security Management System, Business Continuity Management System, and information assets systems (both physical and non-physical assets) including overseeing the design and implementation of information systems which meet the requirement of frameworks and national standards.

- To act as the NHSBSA's strategic lead on all Information Security, Information Governance and Business Continuity related activities including contributing to the design of national security policy and interpreting all related NHS & National Cyber Security Centre (NCSC) policy and strategy ensuring NHSBSA policies are aligned in order to establish the goals, policies, and standards.

- Responsible for interpreting and managing risk around highly complex emerging legislation, government standards, best practice, and wider trends relevant to security, IG, BC and cyber threat landscape, interpreting the impact of these across all services of the NHSBSA by providing professional knowledge and advising on the legal significance for the business.

- As a highly visible leader on the security strategy, act as a strategic partner to the Leadership Team to shape local security and data strategies to meet business and service needs, working with the security leads across physical and cyber security, ensure cross functional working, and that we operate as a collective.

- To analyse and interpret highly complex information produced by the DHSC, NHSD, National Cyber Security Centre (NCSC) and other organisations and produce recommendations for implementation across the Authority.

- Working in partnership with the Head of Communications and Marketing to lead the design of a robust internal and external communications and engagement strategy across the security, IG and BC agendas, which is sponsored by both internal and external stakeholders, to ensure the delivery of the strategies, increasing colleague engagement and raising the profile of the Security & IG team and wider NHSBSA through external promotion with a wide range of stakeholders

- Leading on communications to the Leadership Team, ARC, Board and stakeholder groups to report on relevant strategies and their progress, producing detailed and highly complex and nationally sensitive cyber security threat reports as well as developing and presenting papers and providing comprehensive training as necessary to the ARC, Board and Leadership Team, addressing legislative, changes in cyber threat profile, policy changes, security incidents, new initiatives and projects.

- Leading on the development of a corporate wide communication solution to be used in an emergency response to a business continuity incident.

- Oversee the procurement and contract management of the NHSBSA business continuity software, secure collaboration platforms and FOI portal, ensuring the appropriate support are in place and that value for money metrics are adhered to.

- Undertaking highly specialist and complex project work as necessary for example on the Covid19 public inquiry preparations.

- Leading on the identification and creation of a range of metrics for security, IG and business continuity to support the scoreboard for the Leadership Team and Board and to provide a robust baseline to measure and benchmark performance.

- Managing relationships and partnership work with key stakeholders on the Covid19 Public Inquiry and wider security agenda including working with leads from the Department of Health and Social Care, NHS England, Arms Length Bodies, Solicitors and Barristers.

- Building our brand by being an ambassador for the NHSBSA through networking, speaking at external events and partner relationships with national and regional security and IG organsiations, groups, forums as a subject matter expert, raising the external profile of the NHSBSA in these fields, and sharing best practice with other organisations.

- Ensuring the Security & IG budgets of over £1.1m are maintained and value for money metrics adhered to, along with the compilation benchmarking data and return on investment metrics relevant to the function as a whole

- Responsible for budget setting and management of multiple services including covid19 public inquiry preparations and ensuring ongoing budget is available for legal support and team growth.

- To assist the Executive Director of People and Corporate Services where necessary, in the development of a shared vision for the NHSBSA, and ti promote a culture where all staff understand and are involved and working together towards achievement of Directorate and Authority objectives.

- To be aware of own development requirements and actively seek development opportunities.

- Acts as the subject matter expert for all aspects of assurance, security, Information Governance and Business Continuity.

- Accountability for the security assurance framework covering all NHSBSA systems and information assets (both physical and nonphysical) ensuring that the effort is proportionate and justified and meets the requirement of frameworks and national standards. Influences Information Asset Owners (IAOs), board members and other stakeholders to support accreditation and assurance processes. Builds constructive relationships with clients and suppliers, ensuring risk management and accreditation is an integral on-going part of business and project plans. Where accreditation is due, ensures the IAO has the relevant information to determine how effectively the identified risks are being managed. Provides necessary, proportionate and appropriately tailored communications to facilitate SIRO and managerial oversight.

- To implement the requirements of and maintain compliance with relevant frameworks and standards e.g., Government Security Policy Framework (SPF), ISO27001:2013, IG Toolkit

- To actively participate in BSA Management meetings and strategic decisions and to take the strategic lead on all Information Security related activities.

- Maintain an appropriate and effective training and induction programme for relevant aspects of IS, IG and BC and ensure the delivery and monitoring to ensure an understanding and observance of all necessary information security policies, procedures and standards.

- Ensure legal compliance of the NHSBSA with all information security legislation, directives and standards whilst tailoring to business requirements

- Ensure the delivery and monitoring of adequate training for NHSBSA staff training to ensure an understanding and observance of all necessary information security policies, procedures, and standards.

Deputy SIRO responsibilities

- Accountability for the security and risk acceptance for all NHSBSA systems and information (both physical and non-physical assets) the overall responsibility for the systems lies with the Executive Director.

- Contribute to the development and implementation of the NHSBSA's strategic direction, supporting the SIRO through effective influential communication with key stakeholders to ensure that Information Security is embedded in the organisation.

- Oversee the development of an Information Risk Policy. This should include a Strategy for implementing the policy within the existing Information Governance Assurance Framework and be compliant with NHS IG policy, standards and methods

- Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the Statement of Internal Control.

- Ensure that the Board and the Accountable Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners

- Review and agree actions in respect of identified information risks.

- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements

- Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures

- Advise the Board on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising etc

In addition to the above accountabilities, as post holder you are expected to

1. Undertake additional duties and responsibilities in line with the overall purpose of your role and as agreed by your line manager.
2. Demonstrate NHSBSA values and core capabilities in all aspects of your work.
3. Foster an environment where your own and colleagues' safety and well-being is promoted.
4. Contribute to a culture which values diversity and inclusion.
5. Comply with NHSBSA policies, procedures and protocols as they apply to your role.

Working relationships

Responsible to	Executive Director of People & Corporate Services and Senior Information Risk Owner (SIRO)

Responsible for

Security & Information Governance team and accountable for the following functions including:

- Information Security Risk
- Information Security Assurance
- Information Governance
- Business Continuity
- Inquiry preparations

Key relationships and connections

- Chief Executive and Leadership Team
- Chair and Non-Executive Board members
- Head of Technology Operations
- Caldicott Guardian
- Data Protection Officer
- Peers and senior colleagues within DHSC and other healthcare organisations
- Members of the public and outside agencies
- Internal and External Customers & Stakeholders

Person specification

Service area	People & Corporate Services
Job title	**Head of Security & Information Governance (Deputy SIRO)**

Personal Qualities, Knowledge and Skills

Essential criteria

- Ability to work at a strategic level, clear vision of both security and business objectives to influence and engage with wider colleagues and stakeholders
- Extensive specialist knowledge of current and developing threats in security, Information Governance, business continuity, mandatory requirements, best practice and Data Protection law and legislation. .
- Analytical skills and ability to understand and interpret complex information
- Excellent leadership skills
- Budgetary management
- Highly developed communication and interpersonal skills in order to engage with leaders, managers, colleagues and external stakeholders
- Innovative thinker able to use initiative, prioritise and work well under pressure, ensuring delivery to deadlines
- Highly developed analytical and problem-solving skills
- Committed to continuing personal/professional development.

- High level of report writing and presentation skills
- High level of training and communicating to large audiences.
- Ability to work at a strategic level developing new Security & IG solutions and policies to meet business need
- Strong people management skills, gained through managing and developing teams
- Excellent communication skills, including the ability to communicate effectively with individuals and groups about complex matters.

Desirable criteria

- In depth knowledge of NHS and government security strategy and policy agendas.
- Understanding of the NHS and relevant policies.
- Proven track record of understanding complex measurement metrics including the implementation of a robust data management approach.
- Facilitation skills
- Able to frequently travel to other national locations
- Excellent knowledge of Information Security & Business Continuity Management Systems
- Training, coaching and mentoring skills
- In depth understanding of NHS and government Cyber Security strategy and policy agenda

Demonstrated by

- Approval Body certification
- Interview

Experience

Essential criteria

- Significant experience working at a senior level in a large, complex organisation including input to development of Security strategy and intelligent use of threat notifications and changing cyber landscape to inform strategic and operational decisions
- Extensive experience in a senior security and IG role within a large complex organisation advising on relevant policy, law and best practice across all areas of the organisation.
- Experience of facilitating, managing change and chairing and leading large forums / networks of people

- Extensive experience of staff and budget management
- Experience in project management wih proven ability to deliver projects on budget and on time with benefits realised.
- Significant experience of advising and training senior leaders and board members on security.

Experience of developing and implementing corporate policies, strategies and action plans.

- Significant experience of analysing and reporting on Cyber Security risk within an industry recognised control and audit framework - ISO27001

Desirable criteria

- Strategic planning
- Experience of managing teams
- Experience of contract management or working with Procurement teams
- Budgetary management
- Experience in managing an Information Security Management system (ISMS)
- A thorough understanding of the implementation of the Government Security Policy Framework, NHS Data Security & protection Toolkit
- Experience of developing positive working relationships with a wide range of individuals.

Demonstrated by

1. Application Form/Interview/References

Qualifications

Essential criteria

- Degree calibre with relevant in-depth knowledge of the subject matter across one or more specialised areas.

OR

- Relevant direct specialist experience in information security and Information Governance
- Evidence of on-going Continuing Professional Development
- Industry recognised qualifications in specialised field e.g Certified Information Security Manager (CISM), ISO27001 Lead Implementor, HMG

Information Standards, ISO standards, ITIL. Information Accreditation

Desirable criteria

- Educated to Masters level or equivalent in relevant discipline
- Membership (or equivalent professional membership)

Demonstrated by

- Approval Body Certification
- Application Form

Core capability (minimum level) – Level 5

- ***Communicating with Influence and Impact –*** Is highly articulate and credible at the most senior levels inside and outside the NHSBSA (*Level 5)*
- ***Improving and Innovating*** - Drives a culture that emphasises continuous improvement, efficiency, and value for money (*Level 5*)
- ***Working Together*** - Drives a diverse and collaborative working culture which challenges insular thinking and encourages transparency and open communication (*Level 5)*
- ***Enabling Performance and Potential*** - Builds a strong culture of continuous learning and knowledge sharing, where everyone, including under-represented groups, can benefit from development opportunities (*Level 5*)
- ***Making and Owning Decision*** - Maintains a clear focus on maximising resource efficiency, continually questioning the value of activities against strategic priorities (*Level 5*)
- ***Understanding the Bigger Picture*** - Fully engages with and utilises Non-Executive Directors' wider experience and knowledge to support strategic decision making *(Level 5)*

Relevant Professional Framework – ISACA (Information Systems and Audit Control Association)