change
Language
121
BQsDAAAABgoHY2xvc2luZwAAAApzZWFyY2h
1224
yes
1770479551-e564c62a9080746957e083683

Cyber Security Supply Chain Risk Manager

Government Digital Service

Apply before 11:55 pm on Sunday 22nd February 2026

Government
Digital Service

Reference number

447705

Salary

£55,403 - £72,466

£56,070 - £64,040 (National) / £61,740 - £72,466 (London) Based on capability. The base salary of this grade is £61,005 for London and £55,403 for other locations. Offers made above this will be made up with a specialist pay allowance.

Job grade

Grade 7

Contract type

Permanent

Business area

GDS - Technology & Security

Type of role

Digital
Information Technology
Security

Working pattern

Flexible working, Full-time, Job share, Part-time, Compressed hours

Number of jobs available

1

Contents

Location

Bristol, London, Manchester

About the job

Job summary

The Government Digital Service (GDS) is the digital centre of the government. We are responsible for setting, leading and delivering the vision of a digital modern government.

Our priorities are to drive a modern digital government, by:

1. joining up public sector services
2. harnessing the power of AI for the public good
3. strengthening and extending our digital and data public infrastructure
4. elevating leadership and investing in talent
5. funding for outcomes and procuring for growth and innovation
6. committing to transparency and driving accountability

We are home to the Incubator for Artificial Intelligence (I.AI), the world-leading GOV.UK and at the forefront of coordinating the UK s geospatial strategy and activity. We lead the Government Digital and Data function and champion the work of digital teams across government.

We re part of the Department for Science, Innovation and Technology (DSIT) and employ more than 1,000 people all over the UK, with hubs in Manchester, London and Bristol.

The Government Digital Service is where talent translates into impact. From your first day, you ll be working with some of the world s most highly-skilled digital professionals, all contributing their knowledge to make change on a national scale.

Join us for rewarding work that makes a difference across the UK. You'll solve some of the nation s highest-priority digital challenges, helping millions of people access services they need

The Cyber Security Supply Chain Risk Manager is responsible for ensuring the security, integrity, and resilience of the organisation's supply chain in relation to cybersecurity risks. This role involves identifying and assessing cybersecurity risks within the supply chain, identifying suitable tender/contract security requirements/obligations to mitigate these risks, managing third-party vendor compliance with GDS specified security terms, and ensuring compliance/alignment with regulatory requirements and industry standards respectively. The Cyber Security Supply Chain Risk Manager will work cross-functionally with procurement, commercial, IT, risk management, engineering operations and legal departments to ensure that cybersecurity risks in the supply chain are understood and effectively managed throughout the supply chain lifecycle.

Job description

What you ll do:

- **Cybersecurity Risk Assessment**: conduct and manage comprehensive risk assessments of suppliers, vendors, and partners to identify and mitigate cybersecurity threats in the supply chain
- **Service Team Collaboration**: support and assist Service Teams with the security aspects of their procurement needs, ensuring that appropriate information and cyber security requirements are included in tender documents, specifications and contracts Liaise with Commercial and Legal functions to ensure the requirements are included in tender and contract documentation
- **Vendor Due Diligence**: collaborate with procurement and legal teams to assess vendor security practices during onboarding and throughout the vendor lifecycle ensure third-party vendors comply with the organisation s cybersecurity policies and standards
- **Supply Chain Risk Management (SCRM)**: develop and maintain a robust cybersecurity supply chain risk management (SCRM) program, including standardised supply chain risk logging, continuous monitoring, auditing, and evaluating third-party risk exposure individually, by category and in aggregate
- **Compliance and Standards**: ensure supply chain activities comply with relevant cybersecurity frameworks and regulations (e.g., NCSC Cyber Assessment Framework, GovS007, ISO 27001, GDPR/DPA18) Implement best practices from industry standards to secure supply chain operations
- **Third-Party Contract Management**: work with the legal and commercial teams to ensure cybersecurity clauses are included in supplier contracts Define key performance indicators (KPIs) and service level agreements

- (SLAs) around vendor cybersecurity responsibilities Periodically audit contracts for security terms, in order to understand any gaps in live contracts
- **Incident Response**: support the development of processes and protocols for managing third-party cybersecurity incidents, including coordinating with vendors during a breach, ensuring timely communication, and mitigating the impact on the organisation
- **Vendor Cybersecurity Audits**: lead or co-ordinate periodic cybersecurity audits of vendors and third parties to ensure they maintain high security standards Identify gaps and work with vendors to implement remediation plans
- **Training and Awareness**: provide training and support to internal stakeholders on supply chain cybersecurity risks and vendor management best practices Increase awareness of supply chain threats and trends within the organisation
- **Collaboration and Communication**: work closely with IT, risk, and procurement teams to communicate findings and recommended mitigations Ensure transparency and alignment between teams on cybersecurity risks and strategies
- **Intelligent customer supply chain management**: contribute to the working relationship and management of inter-government supply chain, for example, internal services provided by another government department
- **Supply Chain Resilience**: develop strategies to ensure supply chain resilience in the face of cybersecurity threats, including supply chain mapping and diversification to mitigate risk
- **Monitoring and Reporting**: continuously monitor the security posture of the supply chain and provide regular reports to leadership on third-party risk exposure, incidents, and mitigation efforts

Person specification

We re interested in people who have:

- significant demonstrable experience in cybersecurity, supply chain management, and vendor/third-party risk management, including supply chain risk assessments and audits
- experience working with cybersecurity frameworks, risk management methodologies, and compliance requirements (e.g., NCSC CAF, ISO

27001, SOC 2), with strong information and cyber security risk knowledge and experience

experience in managing cybersecurity for complex supply chains in sectors such as technology, healthcare, finance, or critical infrastructure, with the ability to identify and assess potential cybersecurity risks across the supply chain

in-depth knowledge of cybersecurity principles and how they apply to supply chain and third-party risk management, including familiarity with emerging threats such as cyber-physical risks, counterfeit hardware/ software, and compromised components

strong understanding of supply chain operations, global supply chain regulations, and their intersection with cybersecurity policies, including integration of cybersecurity practices into procurement processes and supplier lifecycle/third-party vendor risk management

knowledge of cloud service providers, managed service providers (MSPs), and other third-party IT service ecosystems, and experience working with vendor management systems, supply chain management tools, and cybersecurity risk platforms

excellent communication and negotiation skills, with the ability to manage complex relationships with suppliers and vendors, and strong analytical skills to translate complex cybersecurity issues into actionable business term

indicative professional qualifications / accreditations:
a degree in Information Security, Information Technology, Business, or a related discipline (or equivalent professional experience), complemented by preferred professional certifications such as CISSP, CISM, CTPRP, or CSCP, with ISO 27001 Lead Auditor or Implementer qualifications considered advantageous

Benefits

There are many benefits of working at GDS, including:

flexible hybrid working with flexi-time and the option to work part-time or condensed hours

a Civil Service Pension with an average employer contribution of 28.97%

- 25 days of annual leave, increasing by a day each year up to a maximum of 30 days
- an extra day off for the King s birthday
- an in-year bonus scheme to recognise high performance
- career progression and coaching, including a training budget for personal development
- a focus on wellbeing with access to an employee assistance programme
- job satisfaction from making government services easier to use and more inclusive for people across the UK
- advances on pay, including for travel season tickets
- death in service benefits
- cycle to work scheme and facilities
- access to an employee discounts scheme
- 10 learning days per year
- volunteering opportunities (5 special leave days per year)
- access to a suite of learning activities through Civil Service learning
- access to children's holiday play schemes across different locations in central London

Any move to Government Digital Service from another employer will mean you can no longer access childcare vouchers. This includes moves between government departments. You may however be eligible for other government schemes, including Tax Free Childcare. Determine your eligibility at https://www.childcarechoices.gov.uk

Office attendance

The Department operates a discretionary hybrid working policy, which provides for a combination of working hours from your place of work and from your home in the UK. The current expectation for staff is to attend the office or non-home based location for 40-60% of the time over the accounting period.
DSIT does not normally offer full home working (i.e. working at home); but we

do offer a variety of flexible working options (including occasionally working from home).

Things you need to know

Artificial intelligence

Artificial intelligence can be a useful tool to support your application, however, all examples and statements provided must be truthful, factually accurate and taken directly from your own experience. Where plagiarism has been identified (presenting the ideas and experiences of others, or generated by artificial intelligence, as your own) applications may be withdrawn and internal candidates may be subject to disciplinary action. Please see our candidate guidance (opens in a new window) for more information on appropriate and inappropriate use.

Selection process details

The standard selection process for roles at GDS consists of:

a simple application screening process - we only ask for a CV and responses to 2 knockout questions and a security check question
Important tip - please ensure that your responses include how you meet the skills and experience listed in the person specification section above

a 60 minute video interview

Depending on how many applications we get, there might also be an extra stage before the video interview, for example a phone interview or a technical exercise.

In the event we receive a high volume of applications, we will conduct the initial sift against the lead criteria which is:

significant demonstrable experience in cybersecurity, supply chain management, and vendor/third-party risk management, including supply chain risk assessments and audits

In the Civil Service, we use Success Profiles to evaluate your skills and ability. This gives us the best possible chance of finding the right person for the job, increases performance and improves diversity and inclusivity. We ll be assessing your technical abilities, skills, experience and behaviours that are relevant to this role.

For this role we ll be assessing you against the following Civil Service Behaviours:

- working together
- managing a quality service
- communicating and influencing

We ll also be assessing your experience and specialist technical skills against the following skills defined in the Government Security Profession Career Framework (see pages 124-125 inclusive) for the Cyber Security Risk Manager role:

- information risk assessment & risk management
- applied security capability
- protective security
- threat understanding

Want to know more about who Government Digital and Data are? Click Here

Recruitment Timeline

Sift completion: 28th February 2026

Panel interviews: w/c 2nd March 2026

Candidates that do not pass the interview but have demonstrated an acceptable standard may be considered for similar roles at a lower grade.

A reserve list will be held for a period of 12 months, from which further appointments can be made.

The Civil Service is committed to attract, retain and invest in talent wherever it is found. To learn more please see the Civil Service People Plan and the Civil Service D&I Strategy.

Please note that this role requires SC clearance, which would normally need 5 years UK residency in the past 5 years. This is not an absolute

requirement, but supplementary checks may be needed where individuals have not lived in the UK for that period. This may mean your security clearance (and therefore your appointment) will take longer or, in some cases, not be possible.

For meaningful checks to be carried out, you will need to have lived in the UK for a sufficient period of time, to enable appropriate checks to be carried out and produce a result which provides the required level of assurance. Whilst a lack of UK residency in itself is not necessarily a bar to a security clearance, and expectation of UK residency may range from 3 to 5 years. Failure to meet the residency requirements needed for the role may result in the withdrawal of provisional jobs offers.

Sponsorship

DSIT cannot offer Visa sponsorship to candidates through this campaign. DSIT holds a Visa sponsorship licence but this can only be used for certain roles and this campaign does not qualify.

Feedback will only be provided if you attend an interview or assessment.

Security

Successful candidates must undergo a criminal record check.

Successful candidates must meet the security requirements before they can be appointed. The level of security needed is security check (opens in a new window).

See our vetting charter (opens in a new window).

People working with government assets must complete baseline personnel security standard (opens in new window) checks.

Nationality requirements

This job is broadly open to the following groups:

- UK nationals

nationals of the Republic of Ireland

nationals of Commonwealth countries who have the right to work in the UK

nationals of the EU, Switzerland, Norway, Iceland or Liechtenstein and family members of those nationalities with settled or pre-settled status under the European Union Settlement Scheme (EUSS) (opens in a new window)

nationals of the EU, Switzerland, Norway, Iceland or Liechtenstein and family members of those nationalities who have made a valid application for settled or pre-settled status under the European Union Settlement Scheme (EUSS)

individuals with limited leave to remain or indefinite leave to remain who were eligible to apply for EUSS on or before 31 December 2020

Turkish nationals, and certain family members of Turkish nationals, who have accrued the right to work in the Civil Service

Further information on nationality requirements (opens in a new window)

Working for the Civil Service

The Civil Service Code (opens in a new window) 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 (opens in a new window).

The Civil Service embraces diversity and promotes equal opportunities. As such, we run a Disability Confident Scheme (DCS) for candidates with disabilities who meet the minimum selection criteria.

Diversity and Inclusion

The Civil Service is committed to attract, retain and invest in talent wherever it is found. To learn more please see the Civil Service People Plan (opens in a new window) and the Civil Service Diversity and Inclusion Strategy (opens in a new window).

Apply and further information

This vacancy is part of the Great Place to Work for Veterans (opens in a new window) initiative.

The Civil Service welcomes applications from people who have recently left prison or have an unspent conviction. Read more about prison leaver recruitment (opens in new window).

Once this job has closed, the job advert will no longer be available. You may want to save a copy for your records.

Contact point for applicants

Job contact :

Name :	gdsrecruitment@dsit.gov.uk
Email :	gdsrecruitment@dsit.gov.uk

Recruitment team

Email :	gdsrecruitment@dsit.gov.uk

Further information

If you feel your application has not been treated in accordance with the Recruitment Principles and you wish to make a complaint, you should contact gds-complaints@dsit.gov.uk in the first instance.

If you are not satisfied with the response you receive you can contact the Civil Service Commission by email: info@csc.gov.uk Or in writing: Civil Service Commission, Room G/8 1 Horse Guards Road, London, SW1A 2HQ.

Civil Service Commission

disability confident EMPLOYER