

Buyer Needs

RM3764iii Cyber Services 3

Dynamic Purchasing System Agreement



**Contents**

[**1.** **Introduction** 3](#_Toc24719481)

[**1.1**  **Buyer Needs Statement** 3](#_Toc24719482)

[**1.2**  **The Opportunity** 3](#_Toc24719483)

[**1.3**  **The current situation** 6](#_Toc24719484)

[**2.** **Specification (DPS Schedule 1 (Specification)**……………………………………... 6](#_Toc24719485)

[**2.1.** **Our priorities**……………………………………………………………………………. 6](#_Toc24719486)

[**2.2.** **Scope**…………………………………………………………………………………….. 6](#_Toc24719487)

[**2.3.** **Service Types**…………………………………………………………………………... 7](#_Toc24719488)

[**2.4.** **Accreditations and Standards**………………………………………………………. 8](#_Toc24719489)

[**2.5.** **Sectors/ Experience:**………………………………………………………………….. 9](#_Toc24719490)

[**2.6.** **What is outside of the scope of the DPS Contract?**........................................ 9](#_Toc24719491)

[**3.** **Mandatory Requirements:**…………………………………………………………….. 10](#_Toc24719492)

# **Introduction**

## **1.1 Buyer Needs Statement**

Crown Commercial Service (CCS) is seeking to establish a Dynamic Purchasing Agreement (DPS) for the provision of Cyber Services for all UK central government departments, wider public sector organisations and charities as listed in the OJEU Contract Notice for RM3764iii – Cyber Services 3 DPS.

This DPS Agreement will be managed by CCS and any contract(s) awarded under this DPS Agreement will be managed by individual Buyers.

The intended duration period of the RM3764iii DPS Agreement was for 3 years (36 months). We have since undergone a 2 year extension increasing the total duration to 5 years (60 months). In the event that the RM3764iii DPS Agreement is terminated without fault, CCS shall give the Supplier no less than thirty (30) days written notice. CCS acknowledges that RM3764iii DPS Agreement will not be terminated within the initial first three (3) months from the commencement date.

CCS may extend the duration of this DPS Agreement for any period or periods from the expiry of the Initial RM3764iii DPS Agreement period by giving the Supplier no less than three (3) Months' written notice. Any such extensions will be notified to the wider market using the appropriate specified route.

The flexibility of the contracting period allows the buyer to determine appropriate contracting timelines required in order that the supplier can meet the needs of the buyer for large and complex projects.

## **1.2 The Opportunity**

The RM3764iii – Cyber Services 3 DPS Agreement will provide central government and wider public sector buyers with the opportunity to procure an extensive range of Cyber Security services from a range of suppliers.

Upon application to join the DPS Agreement, bidders are required to indicate which categories and services they are able to bid for. It is therefore essential that bidders select the exact elements relevant to their service offering in order to be invited to the relevant competitions.

Buyers will use the product and service element filters as detailed in Attachment 1 – Cyber Services 3 Product and Services Matrix, to short list appointed suppliers offering their service requirements and invite to competition.

**What is a Dynamic Purchasing System (DPS)?**

A DPS is a public sector sourcing tool for common goods and services under regulation 34 (Dynamic Purchasing Systems) of the [PCR 2015](http://www.legislation.gov.uk/uksi/2015/102/contents/made). Bidders can apply to join at any point and don’t require any special IT equipment as a DPS eliminates unnecessary activity for the bidder, up front:

**CCS Dynamic Purchasing System (DPS)**

Cyber Services 3 Compliance achieved

Multiple Suppliers

Suppliers can apply to join DPS at any point

DPS Agreement Terms & Conditions accepted

Multiple Buyers

Buyers Competition through the DPS

Suppliers accepted to the DPS – DPS Agreement executed

Suppliers Request to Participate (RtP) in the DPS

DPS Selection criteria satisfied

Supplier(s) Awarded a Contract

Publish Call for Competition

Capable DPS Suppliers respond

Buyers evaluate Supplier responses

**How will the services within the DPS for RM3764iii – Cyber Services 3 be organised?**

The RM3764iii DPS will be organised into distinct categories so:

* Bidders can indicate all elements relevant to their service offering, and
* Buyers can filter the elements to produce a shortlist of appointed suppliers to invite to a competition.

The six (6) distinct categories comprise of:

* Consultancy and Advice
* Penetration testing and IT Health Check
* Incident Management
* Data destruction and sanitation services
* Encryption Services
* Managed Security Services

Full details of the six (6) distinct categories and the sub-categories can be found at Attachment 1 – Cyber Services 3 Product and Services Matrix.

**Who are the Buyers of the RM3764iii – Cyber Services 3** **DPS Agreement?**

The RM3764iii – Cyber Services 3 DPS Agreement will be available to all central government and wider public sector buyers as listed in the OJEU notice, including but not limited to the following:

Central Government:

* Environment
* Defence
* Other Central Government

Wider Public Sector:

* Education
* Fire and Rescue
* Health
* Local Government
* Not for Profit (Charitable)
* Police
* Housing Associations

Other Wider Public Sector

The RM3764iii DPS Agreement is expected to be used by buyers who use an existing public sector agreement offering Cyber Services and also new buyers who choose to purchase Cyber Services via this DPS route.

**What are the benefits of the RM3764iii – Cyber Services 3 DPS Agreement?**

|  |
| --- |
| * Simpler, quicker process – accessible for both SMEs and other suppliers seeking opportunities to provide services to the public sector. * Automated, electronic process – streamlined electronic process. * Flexible - new bidders can apply to join at any point. * Choice - increased scope/scale of service offerings and access to public sector business. * Filtering of supplier offering - ensures suppliers receive notifications of competitions that are relevant to their service offering. * Dynamic – Buyers can create bespoke specifications, competitions and contracts. * Supports localism and Social Value - enabling appointed suppliers to bid for business either locally, regionally or nationally. * Savings – drives savings through the ‘Call for Competition’ procedure. * Efficiencies – reduces Buyers costs and process cycle time |

**What is the estimated value of the RM3764iii – Cyber Services 3 DPS Agreement?**

## The estimated value for this agreement is £255 million excluding VAT which is detailed in the contract notice. This will comprise of multiple contracts with multiple suppliers, however there is no guarantee of work or spend under this RM3764iii DPS Agreement.

## **1.3 The current situation**

This DPS Agreement is a replacement for the Cyber Services 2 Framework Agreement.

G-Cloud no longer offers a route to market for NCSC assured suppliers. CCS frameworks for Digital Outcomes and Solutions (DOS) and Technology Services 2 both offer cyber security services as part of a larger requirement (for example, from a supplier contracted to complete an IT transformation project). These routes are not available for standalone cyber security services which will only be offered through this DPS Agreement.

# **Specification (DPS Schedule 1 (Specification))**

# **Our priorities**

Crown Commercial Service (CCS) has key priorities:

* To maximise commercial benefits;
* To focus on the Customer (Buyer)
* To help strengthen the UK economy through effective policy delivery.

The DPS for Cyber Security Services will support these priorities. It offers a route to quality Services provided by suppliers who can offer a range of experience and industry standards.

The DPS is a dynamic commercial model, which suppliers can join via a straightforward selection process. Buyers will be able to access a wider market of suppliers, obtain more choice and achieve better value.

The range of services available via this DPS will help Buyers to protect public assets and comply with regulatory requirements for protecting citizens’ data.

# **Scope**

This section sets out what CCS and our Buyers want.

The Supplier must only provide the Deliverables for the Filter Categories to which they have been appointed.

For all Filter Categories and/or Deliverables, the Supplier must help Buyers comply with any specific applicable Standards of the Buyer.

There are four Filter Categories available on the DPS:

* Assured NCSC Services / Non-assured NCSC Services
* Service Types
* Accreditations and Standards available (in addition to NCSC)
* Sectors / Experience

The Supplier must only select NCSC Assured for the services that they have been certified to provide, which include Cyber Security Consultancies, Certified Training, CHECK, Assured Services (CAS), Cyber Incident Response (CIR) and Certification.

If the Supplier has specialists that are members of the Cyber Certified Professionals (CCP) scheme they **will not** be able to deliver services under the NCSC Assured route unless they are certified as a consultancy. For more information on registering as a consultancy please see <https://www.ncsc.gov.uk/information/ncsc-certified-cyber-security-consultancy>.

***Suppliers should ensure they only select ‘NCSC Assured' if they CAN provide NCSC Assured services. In the event suppliers select this option in error, this may result in a supplier missing out on an opportunity, and will be deemed a supplier fault NOT CCS.***

# **Service Types**

The Supplier has demonstrated that they can supply Services within at least one of the following Service Types as documented in the DPS Appointment Form associated with their DPS Contract

|  |  |  |
| --- | --- | --- |
| **Category/ Service type** | | **Service Description/ Example** |
| Consultancy and Advice | GovAssure | Independent assurance review of a government organisations self-assessed return against the Cyber Assessment Framework (CAF) by a provider that meets the minimum security clearance and assurance requirements (detailed below) |
| Risk Management | Documenting risks to help Buyers identify and tackle relevant security risks. |
| Risk Assessment | Recommending how to manage cyber security risks. |
| Audit and Review (including evaluation and testing). | Identifying, testing and evaluating risks. Reporting outcomes to show compliance with internal and external policies and procedures. |
| Security Architecture | Designing and developing security architectures that take account of business outcomes |
| Certification. e.g. Cyber Essentials | Assessing compliance with regulatory and industry compliance standards |
| BCDR | Providing advice and strategies to help organisations build resilience and respond to disasters, including research, impact assessment, testing and training. |
| Training | Providing training covering different aspects of cyber security. |
| Cyber Programme Delivery | Delivering a wide range of activities such as planning, implementing and managing initiatives aimed at improving cyber security within an organisation |
| Policy Development | Providing advice and review of IT security policies. |
| Security Specialists | Supplying Cyber Security Specialists to provide resources to augment capability. |
| Security Supply Chain Analysis | Identifying and analysing cyber risks within the supply chain and building assurance activities into supply chain management. |
| Security Strategy | Developing and implementing security strategy to help organisations meet the highest quality standards, quantify risk, improve security, inform policy, build resilience and create a cyber security culture. |
| Cyber Transformation | Planning, developing and implementing a cyber transformation programme to align people, processes and technology with strategic goals and help organisations enhance security function, understand evolving threats, rapidly reduce risk, adopt new digital technologies, invest in cyber security and create a cyber security culture. |
| Penetration test / Health check | Penetration Testing/Pen test | Testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures. |
| Red Teaming | Red teaming is an exercise used to test capabilities and is when an authorised individual/ team simulate an attack on your estate utilising physical, technical and social engineering methods. |
| Check | Penetration testing offered by NCSC approved suppliers who use an approved methodology and provide reports to a specific standard. |
| IT Health Check | Checking of IT systems to identify vulnerabilities and recommend remedial action. |
| Incident Management | Incident Response | Fast action response to cyberattacks, providing recommendations to deal with the compromise and mitigate risks. |
| Cyber Incident Response Level 1 | NCSC assured service providing cyber incident response to the UK Central Government, Critical National Infrastructure or operate in the regulated sector |
| Cyber Incident Response Level 2 | NCSC assured service providing cyber incident response to local government bodies, large, medium and small businesses, and charity organisations within the UK |
| Cyber Exercising | NCSC assured service providing table-top or live play incident exercising for UK Central and Regional Government, and medium and large organisations |
| Disaster Recovery | Providing advice and producing disaster recovery plans. |
| Threat Intelligence | Providing advice on cyber threats drawing upon intelligence from appropriate sources. |
| BCDR | Providing range of advice and support covering business continuity and disaster recovery planning and responses. |
| Data Destruction | Secure data removal and IT sanitisation services. | Secure data erasure and disposal of IT media and assets using audited destruction procedures. |
| Encryption Services | IP Crypto | NCSC assured service, supplier must be approved on the **Crypt Key Company Standard Register** and continue to meet the requirements of the Standard. |
| Managed Security Service | CREST Accredited Security Operations Centre (SOC) | Security Operations Centre (SOC) provided by a CREST accredited supplier who has met the necessary discipline requirements. |
| Security Operations Centre (SOC) | Providing a Security Operations Centre (SOC) which can include activities such as monitoring, detecting, analysing and investigating cyber threats. |
| Managed Detection and Response (MDR) | Providing a proactive managed security service which can include threat intelligence, threat hunting, security monitoring, incident analysis and incident response capabilities. |

**2.3.1 GovAssure**

GovAssure is the new cybersecurity assurance regime for government, adopting NCSC’s Cyber Assessment Framework (CAF) as its central framework.

Departments will complete a self-assessment against the relevant government CAF profile (baseline / enhanced) for the selected systems in scope. This will involve assessing whether they are meeting the security outcomes defined under CAF, and providing some supplemental information.

Following the department’s self-assessment against the CAF, via WebCaf (online submission platform) they will procure the services of an appropriately accredited reviewer to verify the department’s return.

**Obligations**

All suppliers providing a GovAssure service must fulfil the below obligations:

* There must be a **named authority** who is responsible for signing-off the audit on behalf of the organisation carrying out the audit.
* The **named authority** is the equivalent of a Head Consultant for Risk Management or Audit & Review
* The **named authority** must have oversight throughout the audit
* The **named authority** must participate in the bespoke training provided by the NCSC or other training providing, and must agree to use and comply with the audit methodology specified by Government Security Group. The **named authority** should disseminate the key elements of the training to other GovAssure team members, if they are not able to directly attend a training session.
* In the interests of transparency, the bidding authority and supplier must declare any potential conflicts of interest when it comes to providing assurance on a specific government system e.g. they may have been involved in the design of the system or CHECK pen testing previously, or involved in architectural design reviews. This won’t necessarily preclude that company from bidding for the work, but failure to declare any interests could preclude them from bidding for future GovAssure work.
* Team members must be willing to participate in lessons learned throughout first year (and any top-up training)
* If NCSC GovAssure - General T&Cs of your contract with NCSC for Assured Consultancy and CHECK also apply to this agreement.
* It is the responsibility of the **named authority** to ensure that the composition of the GovAssure review team reflects the skills needed (e.g. cyber technical, risk & audit) to carry out a successful review.
* **All members of the GovAssure Review Team must be SC cleared and the named authority must have experience of working with HMG organisations.**

The minimum standards for each GovAssure package are detailed below (suppliers must only apply the relevant GovAssure filter if they are able to meet these requirements, ***In the event suppliers select these options in error, this may result in a supplier missing out on an opportunity, and will be deemed a supplier fault NOT CCS***).

**NCSC GovAssure**

To be eligible to select ‘GovAssure’ through the NCSC Assured Route, organisations

must already be active participants in 2 NCSC schemes as laid out below:

|  |  |  |
| --- | --- | --- |
| Assured Consultancy Risk Management  **OR**  Assured Consultancy Audit & Review | **AND** | Assured Consultancy Security  Architecture  **OR**  CHECK Penetration Testing |

**Non-NCSC Assured GovAssure**

To be eligible to select ‘GovAssure’ through the Non-NCSC Assured Route, organisations must meet the below criteria:

|  |  |
| --- | --- |
| **Overview requirements for a company to be on GovAssure** | * Professional indemnity insurance * Management of the use of contractors * Staff vetting - minimum SC cleared for the review team members * Complaint handling * Data management & security * Cyber Essentials plus certification and information security policies and processes to handle HMG information for the system on which all information relating to GovAssure work is held * Willingness to use HMG IT equipment |
| **Cyber audit and risk management** | **One of**:   * ISO27001 Lead auditor * ISACA - Certified Information Security Auditor (CISA) |
| **Technical Cyber Security Expert** | * CREST Certified Penetration Tester * CREST Certified Infrastructure Tester * CREST Certified Web Applications Tester * CERT Certified Simulated Attack Specialist * CREST Certified Simulated Attack Manager * CREST Certified Intrusion Analyst * Cyber Scheme Team Leader (CSTL) * TigerScheme CHECK Team Leader (CTL / SST) |
| **Industrial Control Systems / Operational Technology Experts** | Optional if a department requires Operational Technology Experts |

# **Accreditations and Standards**

Buyers may also apply the following Filters as part of their Order Procedure. Suppliers must be able to demonstrate the relevant accreditation, standards, compliance or experience to satisfy the requirements of the relevant Filter.

**Suppliers should only select accreditation, standards or experience that they CAN provide. *In the event suppliers select these options in error, this may result in a supplier missing out on an opportunity, and will be deemed a supplier fault NOT CCS.***

|  |
| --- |
| Cyber Essentials Plus |
| Crest/ Tiger/ Cyber/ Other |
| PCI Assessor |
| Project Management – APM Qualified |
| Project Management – PRINCE Qualified |
| Clearance: Counter Terrorist Check |
| Clearance: Security Check |
| Clearance: Developed Vetting |
| NPPV (Non-Police Personnel Vetting) |
| Defence Assurance Risk Tool (DART) |
| ISO 27001 |

# **Sectors/ Experience:**

|  |
| --- |
| **Experience:** |
| Networks |
| Database |
| Internet |
| Cloud |
| Premises |
| Endpoint / applications |
| GDPR |
| Electronic Warfare (EW) |
| India |
| Indo Pacific |
| Africa |
| Middle East/ North Africa (MENA) |
| Cyber Capability Building |
| Other |
| **Sector:** |
| Chemicals |
| Civil Nuclear Communications |
| Defence |
| Energy |
| Finance |
| Food |
| Government |
| Health |
| Space |
| Transport |
| Water |
| Critical National Infrastructure |
| Other |
| **CNI Emergency Services:**  Police  Ambulance  Fire Services  Coast guard |
| Other |

# **What is outside of the scope of the DPS Contract?**

Products and services out of scope of this DPS include but are not limited to:

* Any/all hardware & infrastructure NOT specifically required to deliver the Cyber Security Services in Filter Categories covered by this Contract.
* Hosting
* Software or software licensing NOT specifically required to deliver the Cyber Security Services in service categories
* Networks or connectivity services.

# **Mandatory Requirements:**

1. **Quality Standards**

Suppliers shall use a documented quality management system, as part of delivering services under this DPS. The Supplier may be required by a Buyer to comply with specific quality standards set by industry bodies or Government codes of practice.

1. **Security Requirements**

The Supplier shall at all times during the DPS Contract Period and during the term of any Order Contract comply with the Buyer’s contracted security requirements. The Supplier will ensure controls and measures are in place to protect data handled, processed or stored as part of delivering the Services in accordance with Clause 14 of the Core Terms.

The Supplier shall comply with the applicable requirements set out in the Cabinet Office’s Security Policy Framework. Information about the framework can be found at: <https://www.gov.uk/government/publications/security-policy-framework>

The Supplier shall ensure that staff has security clearance to a minimum level: Baseline Personnel Security standard (BPSS). Should a Buyer require a higher level of security clearance this will be made clear in the Order Procedure.

1. **Environmental Standards**

Where applicable, the Supplier shall ensure that all Electric and Electronic Equipment (EEE) used or disposed of as part of delivery of the Services, complies with Restriction of Hazardous Substances (RoHs), WEEE regulations, or equivalent. Full details can be found via the following links: <http://www.hse.gov.uk/waste/waste-electrical.htm>

1. **Complying with future government requirements and standards**

The Supplier shall comply with relevant future Government requirements and standards in accordance with any Government guidance issued during the DPS Contract Period and as developed and updated, from time to time.

1. **Staff and Contractors**

Where appropriate the Supplier shall ensure that appropriate roles and grades of staff will be assigned to the Services in accordance with NCSC - defined experience levels, Skills Framework for the Information Age (SFIA), or other equivalent grading structures used by the cyber security industry for personnel providing the Services offered under this DPS.

1. **Social Value**

The Supplier shall identify Social Value options which are appropriate to Buyers at Order Contract award stage in accordance with the Buyer’s requirements communicated as part of their Order Procedure.

The Supplier shall complete annual Corporate Social Responsibility (CSR) assessments upon request from Buyers where specified as part of their Order Contract Obligations.

For more information on Social Value please see the following link:

<https://www.gov.uk/government/publications/social-value-act-introductory-guide>