

Direct Award Order Form Template

CALL-OFF REFERENCE: RM3808-0419

THE BUYER: Secretary of State for the Environment, Food & Rural Affairs

BUYER ADDRESS: Nobel House, 17 Smith Square, London, SW1P 3JR

SUPPLIER REFERENCE RM3808-L13-VodafoneLtd-#008– Vodafone Storm Special

THE SUPPLIER: Vodafone Limited

SUPPLIER ADDRESS: Vodafone House, The Connection, Newbury, Berkshire RG14 2FN

REGISTRATION NUMBER: 01471587

DUNS NUMBER: 226488435

SID4GOV ID: Not Applicable

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated the date of Buyer signature

It's issued under the Framework Contract with the reference number RM3808 for the provision of Network Services.

CALL-OFF LOT(S):

Lot 13 Contact Centre Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM3808

3. The following Schedules in equal order of precedence:

Joint Schedules for framework reference number RM3808-0419

- Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 6 (Key Subcontractors)
 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
- Call-Off Schedules for RM3808-0419
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 2 (Staff Transfer)
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedule 6 (ICT Services)
 - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
 - Call-Off Schedule 9 (Security)
 - Call-Off Schedule 10 (Exit Management)
 - Call-Off Schedule 11 (Installation Works)
 - Call-Off Schedule 12 (Clustering)
 - Call-Off Schedule 14 (Service Levels)
 - Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.5)

5. Joint Schedule 5 (Corporate Social Responsibility)

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

CALL-OFF START DATE 1 February 2021

CALL-OFF EXPIRY DATE 31 March 2022

CALL-OFF INITIAL PERIOD As set out above.

CALL-OFF OPTIONAL EXTENSION PERIOD Twelve (12) months

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION

The Buyer may terminate this Call-Off Contract at any time by giving the Supplier not less than 30 days' prior written notice. If the Buyer terminates this Call-Off Contract prior to the expiry of the Call-Off Initial Period, or any applicable Extension Period, the Buyer shall pay the Supplier the early termination charges as set out in the Supplier's Service Offer.

CATALOGUE SERVICE OFFER REFERENCE: RM3808-L13-SO#008

CALL-OFF DELIVERABLES

As set out in Annex 1 and Annex 2 of Call-Off Schedule 20 (Call-Off Specification)

For the avoidance of doubt, as at the Call-Off Start Date, the Buyer intends only to purchase those elements of the Service Offer listed in Call-Off Schedule 5 (Pricing Details) (but retains its option to purchase additional services within the Service Offer) ("Purchased Services"). Unless agreed otherwise, any provisions of the Service Offer which do not relate to the Purchased Services shall not apply to this Call-Off Contract and the Buyer shall not be bound by them.

Exit Management

The Parties agree that the following paragraphs of Call-Off Schedule 10 (Exit Management) are not being called-off by the Buyer and will not form part of the Exit Services to be provided by the Buyer:

2.1;
2.2.1;
2.3;
4.3.3;
4.3.4;
4.3.6;
6.1.6;

7.2.1;
7.2.2;
8.1.1;
8.1.2;
8.2 to 8.9 inclusive; and
10

In respect of Termination Assistance under paragraphs 5 and 6 of Call-Off Schedule 10 (Exit Management), the Supplier shall not be required to provide such Termination Assistance following the expiration of the Call-Off Contract Period.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is

[REDACTED]

CALL-OFF CHARGES

As set out in Call-Off Schedule 5 (Pricing Details).

REIMBURSABLE EXPENSES

As set out in Call-Off Schedule 5 (Pricing Details).

PAYMENT METHOD

BACS

BUYER'S INVOICE ADDRESS:

SSCL, Detra Accounts Payable, PO Box 790, Newport, Gwent, NP10 8FZ

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]

Suite DUnex House
Bourges Boulevard
Peterborough
PE1 1NG

BUYER'S ENVIRONMENTAL POLICY

Not Applicable

ADDITIONAL INSURANCES

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

GUARANTEE

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

SOCIAL VALUE COMMITMENT

Not applicable.

STAFF TRANSFER

The following parts of Call-Off Schedule 2 (Staff Transfer) shall apply:

Part C (No Staff Transfer On Start Date)

Part E (Staff Transfer on Exit) will apply to every Contract.

QUALITY PLAN

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

MAINTENANCE OF ICT ENVIRONMENT

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

BUSINESS CONTINUITY AND DISASTER RECOVERY

In accordance with Call-Off Schedule 8 (Business Continuity and Disaster Recovery) Part A, the Supplier's BCDR Plan at Annex 1 will apply.

SECURITY REQUIREMENTS

In accordance with Call-Off Schedule 9, Part A (Short Form Security Requirements) to apply

The following shall be incorporated into the Call-Off Contract and apply to the Deliverables, supplementing the provisions of Call-Off Schedule 9 (Security):

- the current version of the Supplier's Security Management Plan attached at Part A of Annex A of this Call-Off Order Form;
- the Supplier's current Core Security Statement attached at Part B of Annex A of this Call-Off Order Form; and
- the Key Subcontractor's current Storm Security overview document attached at Part C of Annex A of this Call-Off Order Form.

BUYER'S SECURITY POLICY

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Not Applicable

CLUSTERING

The Services will be provided to the Buyer and Cluster Members. The Cluster Members are as set out in Annex A to Call-Off Schedule 12 (Clustering) and comprise:

- The Rural Payments Agency (RPA);
- The Environment Agency (EA); and
- The Animal and Plant Health Agency (APHA).

Notwithstanding anything to the contrary in Schedule 12, the Parties have agreed that:

- the Buyer will act on behalf of the Cluster Members in relation to the governance and exercising of rights and obligations of the Buyer and Cluster Members under this Call-Off Contract;
- Invoices will be addressed to each Cluster Member and sent to the Buyer;
- Service related reports generated pursuant to Schedule 14 will be compiled on an aggregated basis, broken down by Cluster Member, and sent to the Buyer.

The Parties acknowledge that certain other Defra related entities may receive the benefit of the Services (“**Service Recipients**”). A list of entities who may be Service Recipients can be found at the following link:

<https://www.gov.uk/government/organisations#department-for-environment-food-rural-affairs>. With the exception of those Service Recipients listed in Annex A to Call-Off Schedule 12 (Clustering), Service Recipients shall not be Cluster Members for the purposes of this Call-Off Contract.

SERVICE LEVELS AND SERVICE CREDITS

Service Credits will accrue in accordance with Call-Off Schedule 14 Part B (Long Form Service Levels and Service Credits).

The required Service Maintenance Level is Level 1.

The Service Credit Cap is in accordance with Call-Off Schedule 14 (Service Levels).

The Service Period is one (1) Month.

In addition to the Service Maintenance Level set out in this Order Form, the Supplier shall on a reasonable endeavours basis seek (but is not contractually obliged) to achieve the service level targets set out in the Service Offer included at Annex 2 of Call-Off Schedule 20 (Call-Off Specification).

SUPPLIER’S AUTHORISED REPRESENTATIVE

[Redacted]

HQ, The Connection, Newbury, Berkshire, RG14
2FN

SUPPLIER’S CONTRACT MANAGER

[Redacted]

Vodafone House
The Connection
Newbury
RG14 2FN

PROGRESS REPORT FREQUENCY

Not Applicable

PROGRESS MEETING FREQUENCY

Not Applicable

OPERATIONAL BOARD

Not applicable when the Call-Off Contract is awarded through a direct award procedure.

KEY STAFF

Not Applicable

KEY SUBCONTRACTOR(S)

See list of Key Subcontractors set out in the Service Offer

COMMERCIALLY SENSITIVE INFORMATION

Supplier’s Commercially Sensitive Information

For and on behalf of:	
Signature:	[Redacted]
Name:	
Role:	
Date:	

ANNEX A: SECURITY

PART A: SUPPLIER’S CURRENT SECURITY MANAGEMENT PLAN

Vodafone Network Service Framework 2 (RM3803)

Security Management Plan

Introduction:

We have come a long way since making the first ever mobile call in the UK on 1 January 1985. Today, Vodafone has more than 500 million customers around the world. In 30 years, a small mobile operator in Newbury has grown into a global business operating in 26 countries and partner with networks in over 45 more.

In an increasingly connected world, it is no longer just about a domestic customer being able to talk and text. Our global network allows Customers to share images and videos securely around the World as soon as they're captured. And because we now do more than just mobile, more customers look to Vodafone for great value in their fixed and converged solutions. Some of our larger Enterprise Customers operate in multiple countries so we need to ensure these services are delivered securely.

Detailed below is information of how Vodafone's meets the requirements of Call-Off Schedule 9 (Security), detailing specifically the relevant clauses of Call-Off Schedule 9 and how Vodafone meets the requirements.

Security Posture:

Vodafone are committed to providing world-class security. We deliver some of the most secure telecommunications services in the world and have a proven record for delivering trusted mission-critical services to a wide range of customers, including government, utility, finance, and retail sectors. Our dedicated Security teams in both Group and UK work tirelessly together to ensure our customers are protected from security threats and can continue to operate in an event of a disaster.

Vodafone operates an Information Security Management System (ISMS) based on and, certified complaint with ISO27001:2013, including risk management, business continuity, incident management, physical security, security awareness training and much more. This document supports Network Service Framework 2 (RM3808) setting out how Vodafone manages security against Call of Schedule 9 Security clauses, this should be referenced alongside our ISO27001:2013 certificate and accompanying Statement of Applicability (SoA).

How we Manage Security in accordance with Schedule 9:

2. Complying with security requirements and updates to them

- 2.2 The Supplier shall comply with the Security Policy and the requirements in this Schedule including the Security Management Plan and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

Vodafone offer secure services that are independently audited by external accreditation bodies against ISO27001:2013

- 2.3 The Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

Vodafone welcome every opportunity to work with our customers and ensure the security and quality of our service exceed customer expectations.

- 2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

Vodafone welcome every opportunity to work with our customers and ensure the security and quality of our service exceed customer expectations.

- 2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

Vodafone welcome every opportunity to work with our customers and ensure the security and quality of our service exceed customer expectations.

3. Security Standards

- 3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

Vodafone is committed to providing world class services. We go to great lengths to ensure our products and services meet the highest levels of confidentiality, integrity and availability and demonstrate this through successfully gaining and maintain ISO27001:2013 certification.

Further more we have successfully gained CESG Assured Services – Telecoms (CAS(T)) certification for our core fixed connectivity services.

- 3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

- 3.2.1 is in accordance with the Law and this Contract;

Vodafone fully complies with all legislation and regulations for all local markets in which we operate.

- 3.2.2 as a minimum demonstrates Good Industry Practice;

Vodafone successfully gained and maintains certification against ISO9001, ISO20000, ISO22301, ISO27001

- 3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

Vodafone successfully gained and maintains certification against CESG Assured Service – Telecoms (CAS(T))

- 3.2.4 complies with the Security Policy and the ICT Policy.

Vodafone are confident we met the requirements of the Security Policy

and ICT Policy as evidenced by our commitment to maintaining ISO27001:2013 and CAS(T) certification

- 3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

Vodafone is committed to maintaining legislative and regulatory compliance, and continuing to maintain our certifications and adherence to good practice

- 3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

Vodafone continually monitor our network and services and will take immediate action to address any incidents that may impact those services. In the event an incident has an impact upon a customer(s), our Incident Management processes will trigger notification of affected customers.

4. Security Management Plan

4.1 Introduction

- 4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

Vodafone management of our ISMS and security policies is overseen by the Security Governance Board, which meets bi-monthly, and includes senior representatives from across the company.

4.2 Content of the Security Management Plan

- 4.2.1 The Security Management Plan shall:

- (a) comply with the principles of security set out in Paragraph 3. and any other provisions of this Contract relevant to security;

Vodafone are committed to maintaining our ISO27001:2013 and CAS(T) certificates.

- (b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

Vodafone are committed to providing world-class security. We deliver some of the most secure telecommunications services in the world and have a proven record for delivering trusted mission-critical services to a wide range of customers, including government, utility, finance, and retail sectors. Our

dedicated Security teams in both Group and UK work tirelessly together to ensure our customers are protected from security threats and can continue to operate in an event of a disaster.

Vodafone Group Corporate Security set over arching information security policy and directly support Vodafone Group Business Customers.

Vodafone Global Cyber Security implement and monitor technical security controls and respond to security incidents at a Global / Group level.

Vodafone Corporate Security UK set information security policy for the UK, manage information security and business continuity, external certifications, fraud, disclosures and security investigations.

Vodafone Cyber Security UK implement and monitor technical security controls and respond to security incidents for the UK

- (c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

Vodafone requires our suppliers to sign up to comply with Vodafone policies including Information Security, Business Continuity, and Code of Ethics.

- (d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

Vodafone is a Global company and has a Global Information Security policy owned jointly by the Global Cyber Security Director & Group Corporate Security Director, approved by the Group Chief Technology Officer. This sets out the minimum requirements for Vodafone Group and Local Markets to comply with.

The UK Information Security policy builds upon the Vodafone Group policy and overlays UK Legislation and Regulation obligations is owned by the Head of Cyber Security UK and is approved by Chief Technology Officer.

- (e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

Vodafone management of our ISMS and security policies is overseen by the Security Governance Board, which meets bi-monthly, and includes senior representatives from across the company.

Compliance and performance against our ISMS is monitored and tested by our security teams:

Corporate Security, manage security and business continuity certificates across the company.

Cyber Security, manage technology security risks and implementation of security controls across the company.

- (f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and the Security Policy; and

Vodafone management of our ISMS and security policies is overseen by the Security Governance Board, which meets bi-monthly, and includes senior representatives from across the company.

Changes to policy and security plans will be governed under Change Control via the Security Governance Board.

- (g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only



Vodafone Security Plan

reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 Development of the Security Management Plan

- 4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

Vodafone has held ISO27001 certification since 2005 and our Information Security Management System has been assessed by independent accreditation bodies annually.

4.4 Amendment of the Security Management Plan

- 4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
- (a) emerging changes in Good Industry Practice;
 - (b) any change or proposed change to the Deliverables and/or associated processes;
 - (c) any change to the Security Policy;
 - (d) any new perceived or changed security threats; and
 - (e) any reasonable change in requirements requested by the Buyer.

Vodafone policies are reviewed at least annually or on significant change within Vodafone or the landscape we operate in to ensure they are accurate, up to date and effective.

- 4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
- (a) suggested improvements to the effectiveness of the Security Management Plan;
 - (b) updates to the risk assessments; and
 - (c) suggested improvements in measuring the effectiveness of controls.

Vodafone are committed to maintaining our ISO27001:2013 and CAS(T) certificates. Our independent accreditation partners audit our compliance annually and we publish our certificates on our website.

- 4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the



Vodafone Security Plan

Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure. Vodafone management of our ISMS and security policies is overseen by the Security Governance Board, which meets bi-monthly, and includes senior representatives from across the company.

Changes to policy and security plans will be governed under Change Control via the Security Governance Board.

- 4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

- 5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

Vodafone will agree lines of communications for incidents and security incidents. Vodafone Network Management and Incident Management teams are available and can be contacted 24x7

- 5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

- 5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- (a) minimise the extent of actual or potential harm caused by any Breach of Security;

Defined processes exist to prioritise incidents based on the impact to Vodafone customers and business. Security teams have visibility of incidents and may declare an incident a security incident and escalate the priority accordingly.

- (b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

Defined processes exist to prioritise incidents based on the impact to Vodafone customers and business. Security teams have visibility of incidents and may declare an incident a security incident and escalate the priority accordingly.



Vodafone Security Plan

- (c) prevent an equivalent breach in the future exploiting the same cause failure; and

Vodafone perform post incident reviews on all incidents prioritised as medium or above to learn lessons and implement mitigations to prevent further occurrence of the incident.

- (d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

Vodafone will agree lines of communications for incidents and security incidents. Vodafone Network Management and Incident Management teams are available and can be contacted 24x7

- 5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security policy or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

ANNEX A: SECURITY
PART B: SUPPLIER'S CURRENT CORE SECURITY STATEMENT



Core Security Statement

Sep 2020



Vodafone are committed to providing world-class security. We deliver some of the **most secure** telecommunications services in the world and have a proven record for delivering trusted **mission-critical** services to a wide range of customers, including government, utility, finance, and retail sectors.





How we manage security

Vodafone operates an Information Security Management System (ISMS) based on the recommendations of ISO27001:2013, including risk management, business continuity, incident management, physical security, security awareness training and much more.

The Vodafone ISMS ensures that Security Governance is in place at the core of the organisation. Information Security Senior Management Reviews and Security Steering Committees meet on a bi-monthly basis to monitor performance; these meetings include senior stakeholders from across Cyber Security, Corporate Security, Enterprise Operations, Service Operations and relevant business owners and help to ensure that a wide security strategy is sustained so that business exposure to threats and risks is reduced.

Vodafone have designed the external certifications that we maintain so that customer services are covered from end to end, either with a dedicated assessment or as part of a wider management system; full coverage is generally achieved using a combination of Group, Local Market and Partner certification scopes.

Vodafone Business Security Group aims to protect Vodafone Business, its people, customers and critical assets in order to build a secure digital future. The business unit comprises Corporate Security, Customer Security Services, Customer Technical Assurance, Security Pre-Sales and Security Support and Delivery functions and includes a front desk that handles all Customer security related requests internally and from Vodafone Business Customers.

Data protection and privacy

Vodafone has in place a set of detailed rules and processes to protect Vodafone's and our customers' privacy; these are designed to ensure full compliance with all relevant laws. We approach privacy at a global level and all Vodafone companies are required to adhere to Vodafone's privacy policy.

Information about Vodafone's comprehensive privacy programme can be found online at:

<https://www.vodafone.com/about/privacy-centre>

Protecting our customers' privacy has always been critical to us, so ensuring we are compliant with the GDPR has been an evolution of what we already did.

The obligation to retain the confidentiality and security of personal information is fundamental to the Vodafone Code of Conduct that is binding on all employees worldwide. All Vodafone employees are required to complete online training covering the requirements of the Code of Conduct, as well as separate online training materials covering information security and data protection awareness to reinforce this obligation.

Vodafone's code of conduct is publicly available here:

<https://www.vodafone.com/about/operating-responsibly/code-of-conduct>



Information classification

All information is classified and protected to keep it safe. Our classification scheme uses “C1” to “C4” identification and rules of how to handle and manage information at each level is enforced through our Information Security Classification and Protection Global Policy and the implementation of a data loss prevention tool. Additional Vodafone Security Policies detail what controls we implement to manage both Vodafone and Customer data, including data retention and disposal.

Risk management

Our robust enterprise risk management process is subject to regular reviews and continuous improvement. This ensures that risks, including Customer specific operational risks, are identified, recorded, managed and mitigated as appropriate throughout our business. Major risks are reported and escalated to the board.

Our risk management process methodically addresses risks that may pose a threat to Vodafone, its infrastructure and services (both internal and external), its customers, staff, brand and assets. The risk management strategy provides a framework for the proactive management of risks to eliminate or minimize any impact.

Vodafone Group and local markets operate security risk governance programs and processes that ensure that security risks are captured, assessed and addressed by appropriate risk owners. Each program escalates its top significant risks into Vodafone Group, where "Top Tier" risks are reported and managed using Riskconnect.

Physical security

Vodafone ensures that we provide a secure environment for all of our colleagues and customers. We use live site monitoring and electronic protection systems to safeguard the integrity and security of Vodafone’s assets and our customer’s infrastructure, applications and data.

A 24x7 physical security control centre provide this live monitoring as well as management of all site access, management of third party access, travel security briefs and much more.



Screening/vetting

All Vodafone colleagues and contractors are subject to a process of pre-employment screening which meets good commercial practice.

Employee checks and vetting vary across the different countries in which we operate. The following table details some examples of country specific vetting | security clearance:

Country	Vetting Clearance Body	Type of Clearance Vetting
United Kingdom	Security Watch Dog Home Office FCO MoD Metropolitan Police Ministry of Defence (MoD)	Basic Personnel Security Standard (BPSS) Security Check (SC) Non Police Personnel Vetting (NPPV) Developed Vetting (DV)
Germany	Security Watch Dog Security authorities National Safety Authorities (G10-Act)	Standard (includes Criminal check) Pre - Security Clearance (SC) checks Security Clearance (SC)
USA	Background profiles	Standard US Background Check

As standard, these checks will look to verify some or all of the following:

- Identity Checks.
- Where applicable: Right to Work in the Country.
- Satisfactory business references from the previous three years of employment. Any gaps in employment history fully explained within the applicant's CV or Resume, and Confirmation checks on claimed academic and professional qualifications.
- Criminal history.
- Where applicable: Credit check
- Where applicable: Social Security trace for the US

Suppliers and third parties

We effectively manage cyber security risks associated with Vodafone suppliers by assessing and improving their security controls to safeguard Vodafone's customer data, systems and other assets.

We continually evaluate our suppliers using a series of assessments throughout the supplier lifecycle, starting from the initial stages of supplier on boarding through to in-life and service termination. We embed appropriate security requirements in supplier contracts in line with our internal policies and global regulations. Additionally, we require our suppliers to complete our detailed security risk and control assessment process to evaluate the effectiveness of their security controls and confirm that they meet Vodafone security policies and requirements. To further validate the security controls of our suppliers, we require independent assurance certifications and reports (e.g. ISO27001, SOC2), and we also use an independent security rating service to scan our critical suppliers' internet facing systems, address identified issues and obtain a real-time insight into the supplier risk posture.



Through our supplier risk and control assessments, we identify and scrutinise critical and high-risk suppliers who are then scheduled for more detailed reviews. We re-assess suppliers regularly to identify whether their services, security control effectiveness and any associated risks have changed.

Building on all assessments, we continually work with all our suppliers to improve their security controls, safeguard our customer data and reduce the cyber security risk.

Vodafone cloud and security

Building on more than two decades of collaboration between the two companies, IBM and Vodafone entered into a strategic commercial agreement in early 2019. The venture provides clients with the open, flexible technologies they need to integrate multiple clouds and prepare for the next wave of digital transformation enabled by AI, 5G, edge and Software Defined Networking (SDN).

With more than 70 percent of organisations today using up to 15 cloud environments as they strive to access powerful new digital solutions and services¹, the interconnectivity of clouds and the vulnerability of data have become global issues. Together, IBM and Vodafone Business will help companies remove the complexity and barriers from their technology choices and ensure that data and applications flow freely and securely across their organizations.

Under the venture, Vodafone Business customers have access to the full portfolio of IBM's cloud offerings, underpinned by IBM's deep industry expertise and open technologies.

As part of the agreement, IBM provide managed services to Vodafone Business' cloud and hosting unit. Customers can benefit from IBM's optimisation, automation and cognitive capabilities that help them to run their business effectively in a cloud environment.

The venture includes the co-development of new digital solutions, combining the strengths of Vodafone's leadership in IoT, 5G and edge computing with IBM's multi-cloud, industry expertise and professional services capabilities.

¹ IBM Institute of Business Value: Assembling Your Cloud Orchestra: <https://www-935.ibm.com/services/us/qbs/thoughtleadership/cloudlibrary.html>



Our certifications

The following security relevant standards and certifications are in place to help protect Vodafone and our customers. Copies of certificates are included  for Vodafone Group, Vodafone Germany and Vodafone UK where appropriate. Certificates for other markets are available on demand by contacting vbsecuritydesk@vodafone.com.

Vodafone Group/Vodafone Business

ISO/IEC 27001:2013 - GROUP SERVICES

Certification Body:	LR
Accreditation Body:	UKAS
Certificate Number:	10198292
Certificate Valid Until:	31 December 2020
Version:	ISO/IEC 27001:2013
Scope:	The Provision, Maintenance and Operations for Cyber Defence, Data Centres, Network, Infrastructure and Application services for Local Markets and Vodafone Business; Office IT services, Shared Service Centres and relevant Business Processes. Vodafone Business services includes International Network Connectivity, Unified Communications, Internet of Things, Cloud & Hosting and Customer Service Desks.
Frequency of audits:	6 Monthly Surveillance audits and Recertification audit every 3 years
Market Applicability:	International IT, network services and shared service centres



CAS(T) - VODAFONE ONE NET ENTERPRISE CLOUD (VONE-C) & VODAFONE CONTACT CENTRE CLOUD (VCCC) – VODAFONE GROUP ²

Certification Body:	KPMG
Accreditation Body:	NCSC
Certificate Number:	NCSC-264868406-1542
Certificate Valid Until:	22 July 2021
Version:	1.1
Scope:	The information security management system (ISMS) supporting the Vodafone NGN (Next Generation) MPLS Network and its customers, providing: Internet, voice and data products and services. Customer access connections and all other transmission systems are excluded from the scope. (This certification permits Vodafone Fixed Line Services to carry UK HM Government traffic at the classification of 'OFFICIAL'.
Frequency of audits:	Annual Surveillance audits and Recertification audit every 3 years



² NCSC have stated: "it is intended that the new Telecoms Security Requirements (TSRs) that were announced following the DCMS Supply Chain Review, will provide clarity to industry and customers on what is expected in terms of network security. The NCSC have no plans to launch a new scheme at this time."

Discussions regarding the content and regulation of the TSR are ongoing within Vodafone. Whilst we are committed to providing secure network and services for our customers, we cannot confirm at this stage that we will be implementing TSR. However, our CAS(T) certificate is retained and will run until its expiry in October 2021.

In addition following consultation with NCSC, KPMG (our auditor) and the CAS(T) forum we are incorporating elements of CAS(T) into our ISO27001 audits to continue assurance of our services.



PCI(DSS) – MULTIPLE SERVICES – VODAFONE GROUP

Certification Body:	NCC Services
Accreditation Body:	PCI Security Standards Council
Certificate Number:	Various
Certificate Valid Until:	Various
Version:	3.2
Scope:	Vodafone Group is compliant for multiple agreed PCI scopes and holds a number of Merchant Attestations of Compliance and Service Provider Attestations of Compliance. These attestations may be viewed during on-site assessments under controlled conditions where they are directly relevant to the services provided.
Frequency of audits:	Annual Assessment



Vodafone UK

ISO/IEC 27001:2013 - UK FIXED, MOBILE, CLOUD AND HOSTING, UNIFIED COMMUNICATIONS (UC)

Certification Body:	KPMG
Accreditation Body:	UKAS
Certificate Number:	749
Certificate Valid Until:	03 September 2023
Version:	ISO/IEC 27001:2013
Scope:	The Information Security Management System covers Vodafone UK Mobile & fixed network infrastructure, architectural design, management systems, processes & resources that support Unified Communications (Avaya Technologies) Mobile Voice Services & WifiCalling Data and Connected Services SMS and Voicemail Services Radio Access Network Operations Roaming and International Support Services Billing and Intelligent Network Services Fixed network IPVPN (including SD-WAN underlay) Ethernet VPN Ethernet Wireline Dedicated Ethernet -Optical and Dedicated Ethernet E-Line
Frequency of audits:	6 Monthly Surveillance audits and Recertification audit every 3 years





Vodafone | Core Security Statement | C1 Public

CAS(T) – UK CORE MPLS NETWORK ¹

Certification Body:	NCSC
Accreditation Body:	NCSC
Certificate Number:	NCSC-264868406-1849
Certificate Valid Until:	19 October 2021
Version:	1.1
Scope:	<p>The Information Security Management System covers systems, processes & resources that support end-to-end the Vodafone Business services listed below and certifies the Vodafone Fined Line network to carry UK HM Government traffic at the classification of 'OFFICIAL':</p> <ul style="list-style-type: none"> • Managed MPLS Services • IPVPN • Ethernet VPN • Ethernet Wireline • Dedicated Ethernet – Optical • Dedicated Ethernet – E-Line • PSN Connect
Frequency of audits:	Annual Surveillance audits and Recertification audit every 3 years



CYBER ESSENTIALS PLUS – UK OFFICE AND INTERNET PERIMETER

Certification Body:	NCC Group
Accreditation Body:	KPMG
Certificate Number:	0518597495425094
Certificate Valid Until:	28 January 2021
Version:	N/A
Scope:	<p>Vodafone Limited office environments and its Internet perimeter. (Vodafone UK was the first large company and the first telecommunications company to achieve the government certification called Cyber Essentials Plus in July 2014. The controls are based on ISO27001 and have a strong focus on cyber security Cyber Essentials certification is mandatory for central government contracts which involve handling personal information and providing certain ICT products and services.)</p>
Frequency of audits:	Annual recertification



PCI(DSS) – MULTIPLE SERVICES – VODAFONE UK

Certification Body:	NCC Services
Accreditation Body:	PCI Security Standards Council
Certificate Number:	Various
Certificate Valid Until:	Various
Version:	3.2
Scope:	<p>Vodafone UK is compliant for multiple agreed PCI scopes and holds a number of Merchant Attestations of Compliance and Service Provider Attestations of Compliance. These attestations may be viewed during on-site assessments under controlled conditions where they are directly relevant to the services provided.</p>
Frequency of audits:	Annual Assessment





Vodafone | Core Security Statement | C1 Public

PSN COMPLIANCE (MULTIPLE SERVICES) - UK

Certification Body: Government Digital Services (GDS)
 Accreditation Body: Cabinet Office
 Certificate Number: Various – please see scope below
 Certificate Valid Until: Various
 Version: N/A
 Scope: Vodafone provide numerous PSN Compliant services including overarching DNSP and GCNSP connectivity and DNS. The full list of services can be found at <https://www.gov.uk/government/publications/public-services-network-psn-service-compliance>.
 Frequency of audits: Annual recertification



CERTIFIED CYBER SECURITY CONSULTANCY – SECURITY ARCHITECTURE - UK

Certification Body: NCSC
 Accreditation Body: NCSC
 Certificate Number: 63147746 CCSC Security Architecture
 Certificate Valid Until: N/A – please see <https://www.ncsc.gov.uk/professional-service/cyber-security-consultancy-vodafone>
 Version: 1.1
 Scope: Vodafone Business Security Group has been awarded NCSC Cyber Security Professional Consultancy Status in the category of Security Architecture. This was achieved through demonstration to NCSC that the team has a proven track record of delivering defined cyber security consultancy services, a level of cyber security expertise supported by professional requirements defined by NCSC and the relevant NCSC Certified Cyber Professional (CCP) qualifications. The team was also able to demonstrate that they manage consultancy engagements in accordance with industry good practice and meet the stringent NCSC requirements for certified professional cyber services companies.
 Frequency of audits: Annual Recertification



ISO/IEC 22301:2012 - UK

Certification Body: LR
 Accreditation Body: UKAS
 Certificate Number: 10031084
 Certificate Valid Until: 18 October 2020
 Version: ISO/IEC 22301:2012
 Scope: Voice data services provided by Vodafone UK for its global telecommunications services.
 Frequency of audits: Annual Surveillance audits and Recertification audit every 3 years



001



Other local markets

ISO/IEC 27001:2013 - ALBANIA

Certification Body: LR
 Accreditation Body: UKAS
 Certificate Number: 10054353
 Certificate Valid Until: 03 February 2021
 Version: ISO/IEC 27001:2013
 Scope: Provision and Delivery of Telecommunication and IT services (voice and data), Commercial trade of mobile/fixed communications and internet equipment.
 Frequency of audits: 6 Monthly Surveillance audits and Recertification audit every 3 years



001

ISO/IEC 27001:2013 - ARMENIA

Certification Body: Bureau Veritas
 Accreditation Body: UKAS
 Certificate Number: IND18.0452/U
 Certificate Valid Until: 11 January 2021
 Version: ISO/IEC 27001:2013
 Scope: The Information Security Management System for telecommunication service as well as planning, design, construction, operation and maintenance of network facilities related to provision of such service.,
 Frequency of audits: 6 Monthly Surveillance audits and Recertification audit every 3 years



001

ISO/IEC 27001:2013 - CROATIA

Certification Body: SGS
 Accreditation Body: UKAS
 Certificate Number: HR19/2376
 Certificate Valid Until: 23 July 2022
 Version: ISO/IEC 27001:2013
 Scope: Process of defining and providing support, operations and maintenance, to external or internal companies, for hosting and colocation services, systems and equipment
 Frequency of audits: Annual Recertification audit
 Market Applicability: Croatia



001

ISO/IEC 27001:2013 - FRANCE

Certification Body: AFNOR Certification
 Accreditation Body: COFRAC
 Certificate Number: 2017/74269.4
 Certificate Valid Until: 19 February 2023
 Version: ISO/IEC 27001:2013
 Scope: Managed services of the Service Operations Center (CES), Security Operational Center (COS), Cloud Computing (Cloud v3), and colocation services in the datacenters
 Frequency of audits: 6 Monthly Surveillance audits and Recertification audit every 3 years



001



ISO27001:2013 – GERMANY MOBILE NETWORK SERVICES

Certification Body:	TÜV Rheinland
Accreditation Body:	DAkKS
Certificate Number:	01 153 1501451
Certificate Valid Until:	23 March 2023
Version:	ISO 27001:2013
Scope:	Operation of mobile network services including voice, data and SMS and operation of fixed network services including telephony, Internet and TV.
Frequency of audits:	6 Monthly Surveillance audits and Recertification audit every 3 years



ISO27001:2013 – GERMANY Vodafone Cloud and Security

Certification Body:	ISO27k GmbH
Accreditation Body:	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
Certificate Number:	BSI-IGZ-0422-2020
Certificate Valid Until:	20 July 2023
Version:	BSI-Standard 200-2: IT-Grundschutz-Methodik
Scope:	The information network comprises the basic reference architecture of Vodafone Cloud & Security in Germany (VC&S DE), which is required for the provision of Vodafone cloud services (private cloud, managed hosting, fusion cloud) and in the two German data centers of the Vodafone Group in Frankfurt on the Main and Rüsselsheim is installed in the same way. The reference architecture is based on the specifications of the National Institutes of Standard and Technology (NIST), taking into account the findings from the best practices for the provision of cloud services.
Frequency of audits:	Annual Surveillance audits and Recertification audit every 3 years



ISO27017:2015 – GERMANY VCHS

Certification Body:	LR
Accreditation Body:	UKAS
Certificate Number:	KLN00000426
Certificate Valid Until:	02 November 2020
Version:	ISO 27017:2015
Scope:	The management, operations and security of the Vodafone Cloud and Hosting Services based in the Frankfurt a. M. and Ruesselsheim a. M. data centres in Germany.
Frequency of audits:	6 Monthly Surveillance audits and Recertification audit every 3 years



ISO27018:2014 – GERMANY VCHS

Certification Body:	LR
Accreditation Body:	UKAS
Certificate Number:	KLN00000426
Certificate Valid Until:	02 November 2020
Version:	ISO 27018:2014
Scope:	The management, operations and security of the Vodafone Cloud and Hosting Services based in the Frankfurt a. M. and Ruesselsheim a. M. data centres in Germany.
Frequency of audits:	6 Monthly Surveillance audits and Recertification audit every 3 years





ISO/IEC 27001:2013 - GROUP SERVICES



Current issue date: 6 December 2019
Expiry date: 31 December 2020
Certificate identity number: 10237720
Original approval(s): ISO/IEC 27001 - 13 March 2001

Certificate of Approval

This is to certify that the Management System of:
Vodafone Group Services Limited

Vodafone House, The Connection, Newbury, RG14 2FN, United Kingdom

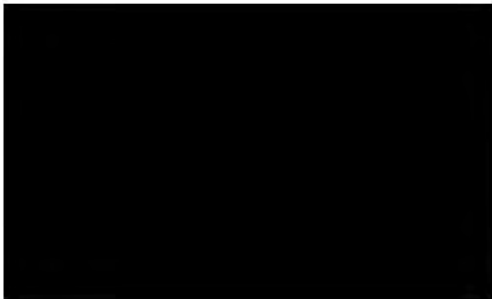
has been approved by Lloyd's Register to the following standards:

ISO/IEC 27001:2013

Approval number(s): ISO/IEC 27001 – 0044028

This certificate is valid only in association with the certificate schedule bearing the same number on which the locations applicable to this approval are listed.

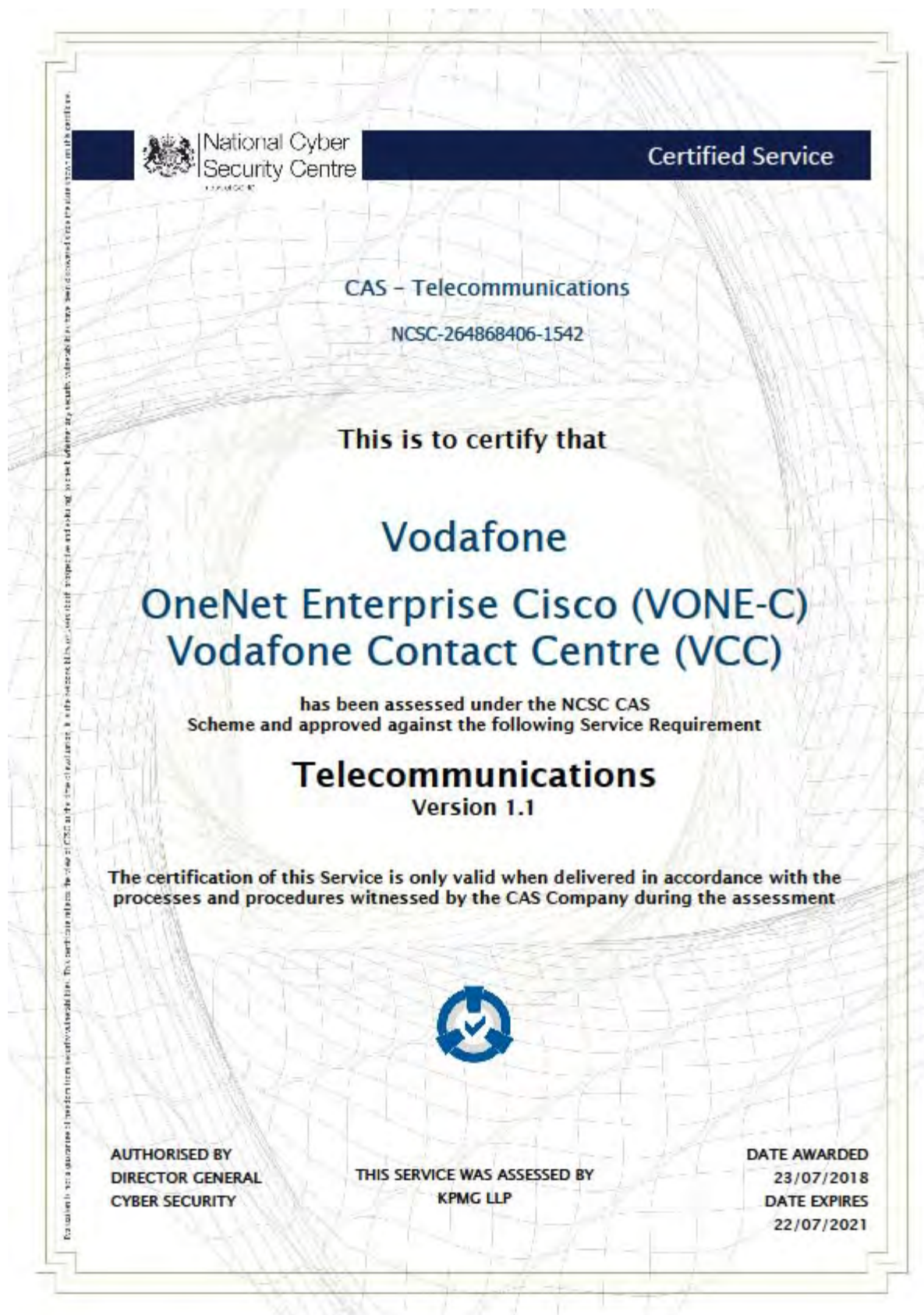
The scope of this approval is applicable to:
Information Security Management System of Vodafone Group functions covering: The Provision, Maintenance and Operations for Cyber Defence, Data Centres, Network, Infrastructure and Application services for Local Markets and Vodafone Business; Office IT services, Shared Service Centres and relevant Business Processes. Vodafone Business services includes International Network Connectivity, Unified Communications & Connectivity, Internet of Things, Cloud & Hosting and Customer Service Desks. This is in accordance with Statement of Applicability version 18.n



Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom



CAS(T) - VODAFONE ONE NET ENTERPRISE CLOUD (VONE-C) & VODAFONE CONTACT CENTRE CLOUD (VCCC) –
VODAFONE GROUP





ISO/IEC 27001:2013 - UK MOBILE & FIXED NETWORK INFRASTRUCTURE, ARCHITECTURAL DESIGN, MANAGEMENT SYSTEMS, PROCESSES & RESOURCES



ISO/IEC 27001:2013
Information Security Management

Certificate of Compliance

Certificate Number: 749

Awarded to	Vodafone UK Limited
The scope of approval	<p>The Information Security Management System covers Vodafone UK Mobile & fixed network infrastructure, architectural design, management systems, processes & resources that support</p> <p>Unified Communications (Avaya Technologies)</p> <p>Mobile Voice Services & Wifi Calling Data and Connected Services SMS and Voicemail Services Radio Access Network Operations Roaming and International Support Services Billing and Intelligent Network Services</p> <p>Fixed network IPVPN (including SD-WAN underlay) Ethernet VPN Ethernet Wireline Dedicated Ethernet - Optical and Dedicated Ethernet E-Line</p> <p>In accordance with Vodafone's Design, Build and Run model following SoA version 6.2</p>
Statement of applicability	Version 6.2

www.kpmg.co.uk

N.B. This certificate relates to the Information Security Management System and not to the products or services of the certified organisation.

This certificate remains the property of KPMG Audit Plc

Validity of this certificate can be verified by contacting kpmgcertificationservices@kpmg.co.uk with your query.

© 2020 KPMG Audit plc, a UK public limited company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks of KPMG International.

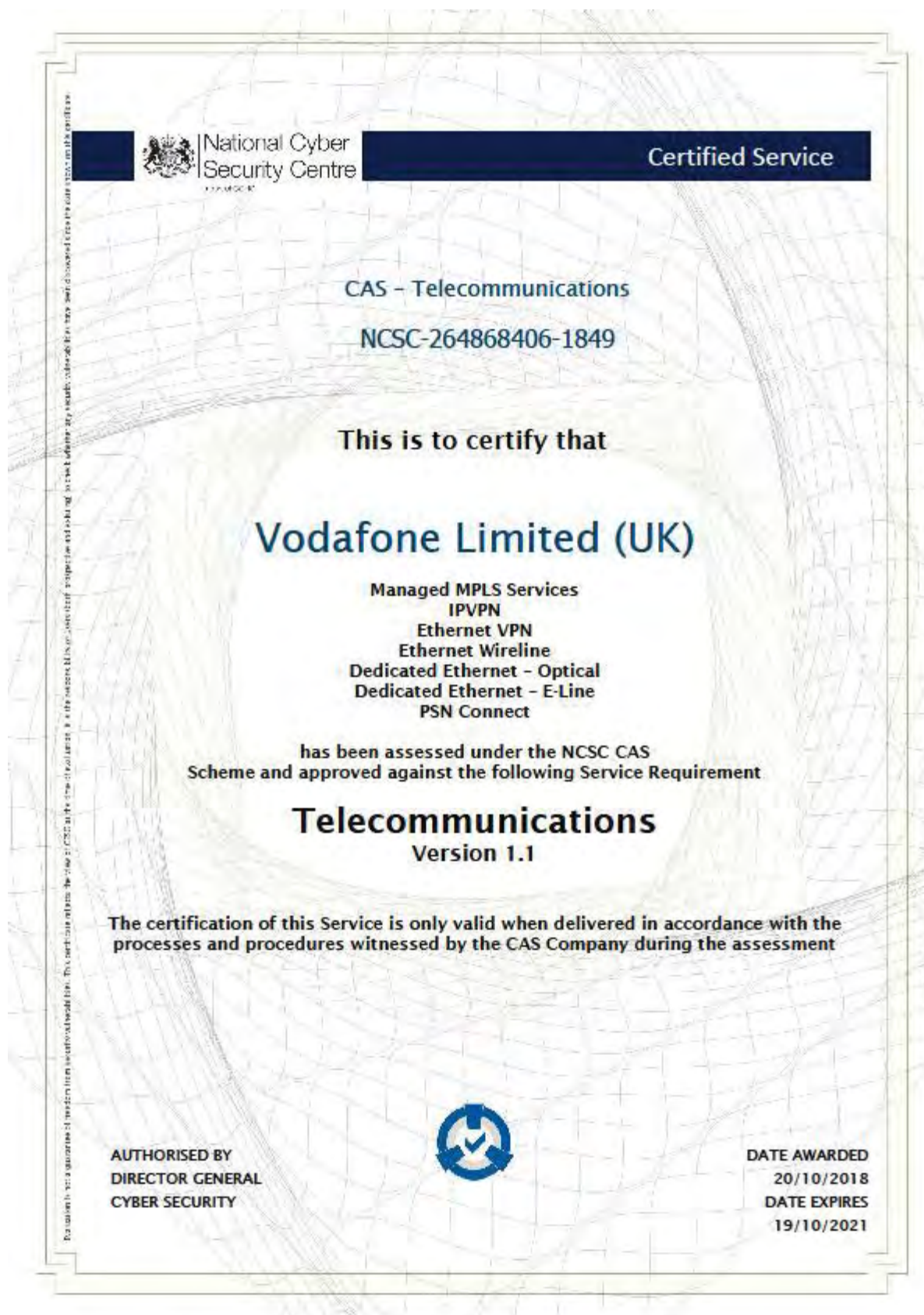
This certificate provides confirmation of compliance with ISO/IEC 27001:2013. It does not constitute an assurance opinion delivered in accordance with IAASB Assurance Standards

Registered office: 15 Canada Square, London, E14 5GL.

UKAS accredited office: One Snowhill, Snow Hill Queensway, Birmingham, B4 6GH



CAS(T) – UK CORE MPLS NETWORK



CYBER ESSENTIALS PLUS – UK OFFICE AND INTERNET PERIMETER





ISO/IEC 22301:2012 – UK



Certificate of Approval

This is to certify that the Management System of:

Vodafone Ltd

Vodafone House, The Connection, Newbury, RG14 2FN, United Kingdom

has been approved by LRQA to the following standards:

ISO 22301:2012



Current Issue Date: 19 October 2017
Expiry Date: 18 October 2020
Certificate Identity Number: 10031084

Original Approvals:
ISO 22301 – 24 February 2014

Approval Number(s): ISO 22301 – 0008735

The scope of this approval is applicable to:
Voice data services provided by Vodafone UK for its global telecommunications services.



001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued By: Lloyd's Register Quality Assurance Ltd, 1 Trinity Park, Sickenhill Lane, Birmingham B37 7YS, United Kingdom

Page 1 of 1



ISO/IEC 27001:2013 – ALBANIA



Certificate of Approval

This is to certify that the Management System of:

Vodafone Albania Sh.A

Kashar, Autostrata Tirane-Durres Rr. Nr. 61, Pavaresia, 1001 Tirana, Albania

has been approved by LRQA to the following standards:

ISO/IEC 27001:2013



issued by: Hellenic Lloyd's S.A.

for and on behalf of: Lloyd's Register Quality Assurance Limited

Current Issue Date: 4 February 2018

Expiry Date: 3 February 2021

Certificate Identity Number: 10054353

Original Approvals:

ISO/IEC 27001 – 4 February 2018

Approval Number(s): ISO/IEC 27001 – 0064420

The scope of this approval is applicable to:

Provision and Delivery of Telecommunication and IT services (Voice and Data). Commercial trade of mobile/fixed communication and Internet equipment
Statement of applicability (SoA) (May, 2017)





001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued By: Hellenic Lloyd's S.A., 87 Ald Moadul 18226 Pireas Greece for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7YS, United Kingdom

Page 1 of 1



ISO/IEC 27001:2013 – ARMENIA

	
MTS ARMENIA CJSC	
Argishti str., 4/1, Yerevan, 0015, Republic of Armenia.	
This is a multi-site certificate, additional site(s) are listed on the next page(s)	
<i>Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below</i>	
ISO/IEC 27001:2013	
<i>Scope of certification</i>	
Information Security Management System for telecommunication service as well as planning, design, construction, operation and maintenance of network facilities related to provision of such service.	
Statement of Applicability, version 1.5, dated 21.12.2017	
Original cycle start date:	12 January 2015
Expiry date of previous cycle:	11 January 2018
Recertification Audit date:	21 December 2017
Recertification cycle start date:	11 January 2018
Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: 11 January 2021	
Certificate No.	IND18-0452/U
Version: No.	1
Revision date:	11 January 2018
	
Local office: Floors 2&3, 30. Marshala Proshiyakova St., "Zenith-Plaza", Moscow, Russia, 123458	
	
Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation To check this certificate validity please call: +7 (495) 2287848	

1 / 2

SGS

Certificate #R'62376

The management system of
A1
A1 HRVATSKA d.o.o.
Varoš 1, 10000 Zagreb, Croatia

has been assessed and certified as meeting the requirements of
ISO/IEC 27001:2013
For the following activities:
Process of defining and providing support and maintenance, to external or internal companies, for hosting services, colocation services and IaaS, systems and equipment according Statement of applicability dated 06.03.2019.

This certificate is valid from 24 July 2019 until 23 July 2022 and remains valid subject to satisfactory surveillance audits. Recertification audit due a minimum of 90 days before the expiration date.
Issue #1. Certified since July 2007

Authorized by

SGS's Business Unit is located at: Office - Ljubljana, Slovenia
T +386 (0)151 362-6266 F +386 (0)161 563-1800 www.sgs.com

HC SGS 27001 2013 0111

Page 1 of 1

UKAS
MANAGEMENT
SYSTEMS
0005

This document is issued solely for your company and it is intended for internal use only. It is not to be used for advertising purposes. The responsibility of the customer who has received this document is to ensure its confidentiality. Any unauthorized disclosure of this document is prohibited and may result in legal action being taken against the responsible person. This document is issued under the terms of the contract between the customer and SGS. The customer agrees to indemnify and hold SGS harmless from all claims, damages, costs and expenses, including reasonable attorneys' fees, arising from the use of this document. This document is issued under the terms of the contract between the customer and SGS. The customer agrees to indemnify and hold SGS harmless from all claims, damages, costs and expenses, including reasonable attorneys' fees, arising from the use of this document.



ISO/IEC 27001:2013 – FRANCE



Certificat

Certificate

N° 2017/74269.4

Page 1 / 2

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

SFR

sous la marque commerciale/under the tradename
SFR BUSINESS

pour les activités suivantes :
for the following activities:

**PRESTATIONS DE SERVICES MANAGES DU CENTRE D'EXPLOITATION SERVICES (CES),
DU CENTRE OPERATIONNEL DE LA SECURITE (COS), DU CLOUD COMPUTING (CLOUD V3),
ET PRESTATIONS D'HEBERGEMENT DE COLOCATION AU SEIN DES DATACENTERS.
DECLARATION D'APPLICABILITE du 10/01/2020**

**MANAGED SERVICES OF THE SERVICE OPERATIONS CENTER (CES),
SECURITY OPERATIONAL CENTER (COS), CLOUD COMPUTING (CLOUD V3),
AND COLOCATION SERVICES IN THE DATACENTERS.
STATEMENT OF APPLICABILITY: January 10th, 2020**

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of:

ISO/IEC 27001 : 2013

et est déployé sur les sites suivants :
and is developed on the following locations:

ALTICE CAMPUS : 16 RUE DU GENERAL ALAIN DE BOISSIEU FR-75015 PARIS

Liste des sites certifiés en annexe / List of certified locations on appendix

Ce certificat est valable à compter du (année/mois/jour)
This certificate is valid from (year/month/day)

2020-02-20

Jusqu'au
Until

2023-02-19

Flashez ce QR Code pour
vérifier la validité du
certificat

11 rue Francis de Pressensac - 92571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
4000 rue reginald de 10-117 0204 - 479 076 002 RCS Bobigny - www.afnor.org

afnor
CERTIFICATION



ISO27001:2013 – GERMANY MOBILE NETWORK SERVICES

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2013**
Zertifikat-Registrier-Nr. **01 153 1501451**

Unternehmen:



Vodafone GmbH
Ferdinand-Braun-Platz 1
40549 Düsseldorf
Deutschland

mit den Standorten gemäß Anlage

Geltungsbereich:

Betrieb von mobilen Netzdiensten inkl. Sprache,
Daten und SMS und Betrieb von Festnetzdiensten
inkl. Telefonie, Internet und TV
SoA V3.2, 28.01.2020

Durch ein Audit wurde der Nachweis erbracht, dass die
Forderungen der ISO/IEC 27001:2013 erfüllt sind.

Gültigkeit:

Dieses Zertifikat ist gültig vom 24.03.2020 bis 23.03.2023.
Erstzertifizierung 2014

18.03.2020

© TÜV, TÜV und TÜV sind eingetragene Marken. Eine Nutzung und Verwertung bedarf der vorherigen Zustimmung.

www.tuv.com





ISO27001:2013 - GERMANY VODAFONE CLOUD AND SECURITY



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches



IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0422-2020

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Vodafone Cloud & Security in Deutschland - VC&S DE

der Vodafone Group Services GmbH

gültig bis: 20. Juli 2023*



Der Informationsverbund umfasst die grundlegende Referenzarchitektur der Vodafone Cloud & Security in Deutschland (VC&S DE), die für die Bereitstellung der Vodafone Cloud-Dienste (Private Cloud, Managed Hosting, Fusion Cloud) erforderlich ist und in den beiden deutschen Rechenzentren der Vodafone Group in Frankfurt am Main und Rüsselsheim in gleicher Weise installiert ist. Die Referenzarchitektur orientiert sich an den Vorgaben des National Institutes of Standard and Technology (NIST) unter Berücksichtigung der Erkenntnisse aus den Best Practices für die Bereitstellung von Cloud-Diensten.

Der oben aufgeführte Untersuchungsgegenstand wurde von Karsten Emmert, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodik) umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002. Dieses Zertifikat ist keine generelle Empfehlung des Untersuchungsgegenstandes durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Untersuchungsgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, den 21. Juli 2020



* Unter der Bedingung, dass die ab 21. Juli 2020 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, D-53175 Bonn · Postfach 20 03 63, D-53113 Bonn

Tel.: +49 (0)228 9582-0 · Fax: +49 (0)228 3582-5477 · Infoline: +49 (0)228 9582-311 · Internet: www.bsi.bund.de



ISO27017:2015 – GERMANY VCHS



RECORD OF VERIFICATION/ASSURANCE

This is to confirm that LRQA has undertaken a review and assessment including process sampling to verify that

Vodafone Cloud & Hosting Service (VCHS)

Eschborner Landstr 100, 60489 Frankfurt, Germany

has implemented the applicable requirements provided in

ISO27017:2015

The management, operations and security of the Vodafone Cloud and Hosting services based in the Frankfurt a. M. and Ruesselsheim a. M. data centres in Germany.

In accordance to the ISO27001 Statement of Applicability v17.n

Original Issue date: 03 November 2017

Record No: KLN00000426



Improving performance, reducing risk

Lloyd's Register Quality Assurance Limited is a limited company registered in England and Wales. Registered number: 1679970. Registered office: 71 Fenchurch Street, London, EC3M 4BS, UK. A member of the Lloyd's Register group, Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.



ISO27018:2014 – GERMANY VCHS



RECORD OF VERIFICATION/ASSURANCE

This is to confirm that LRQA has undertaken a review and assessment including process sampling to verify that

Vodafone Cloud & Hosting Service (VCHS)

Eschborner Landstr 100, 60489 Frankfurt, Germany

has implemented the applicable requirements provided in

ISO27018:2014

The management, operations and security of the Vodafone Cloud and Hosting services based in the Frankfurt a. M. and Ruesselsheim a. M. data centres in Germany.

In accordance to the ISO27001 Statement of Applicability v17.n

Original Issue date: 03 November 2017

Record No: KLN00000426



Improving performance, reducing risk

Lloyd's Register Quality Assurance Limited is a limited company registered in England and Wales. Registered number: 1676370. Registered office: 71 Fenchurch Street, London, EC3M 4BS, UK. A member of the Lloyd's Register group. Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this release as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has agreed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.



ISO/IEC 27001:2013 – QATAR

	BUREAU VERITAS Certification
	VODAFONE QSC Head Office: Qatar Science Technology Park Tech 2, Level 2, Al-Garaffa P. O. Box: 27727, Doha STATE OF QATAR
This is a multi-site certificate, additional site(s) are listed on the next page(s) <i>Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below</i>	
ISO/IEC 27001:2013 <i>Scope of certification</i>	
THE SCOPE OF ISMS COVERS THE CORE FUNCTIONS OF CUSTOMER SERVICES & CUSTOMER CARE, VENDOR GOVERNANCE, TECHNOLOGY SECURITY STRATEGY & PLANNING, LEGAL & REGULATORY AND SUPPORT FUNCTIONS INCLUDING ADMINISTRATION, HR, FINANCE, COMMERCIAL, EXTERNAL AFFAIRS, CORPORATE SECURITY, OFFICE IT SERVICES, SERVICE MANAGEMENT AND SOFTWARE PROJECT MANAGEMENT AT HEAD OFFICE, CALL CENTER, SALES OFFICE, RETAIL AND FRANCHISEE STORES INCLUDED IN THE SCOPE.	
This is in accordance with the Statement of Applicability version 2.0 dated 28/09/2017.	
Original cycle start date:	17 th November 2014
Expiry date of previous cycle:	16 th November 2017
Re-certification audit date:	6 th November 2017
Re-certification cycle start date:	16 th November 2017
Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: 16th November 2020	
Certificate No: IND 17 0034/11	Version 1, Revision date: 15 th November 2017
[Redacted] Holding SAS – UK Branch 5 th Floor, 66 Prescot Street, London E1 4HG, United Kingdom. Local office: G1-G3, Ground Floor, IKG Building (Dog No. 194 Street No. 250), C Ring Road, Opposite Gulf Times, P. O. Box: 22157 (Doha), Qatar	
Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organization. To check this certificate validity please call: +974 40329729	
	
0008	
Page 1 of 8	



ISO/IEC 27001:2014 – SPAIN

AENOR**Certificado del Sistema
de Gestión de Seguridad de la Información****SI-0017/2012**

AENOR certifica que la organización

VODAFONE ESPAÑA, S.A.U.

dispone de un sistema de gestión de seguridad de la información conforme con la Norma UNE-ISO/IEC 27001:2014

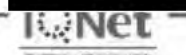
para las actividades: Los sistemas de información que dan soporte a los procesos de seguridad de la información (análisis de riesgos y verificación de requisitos de seguridad de productos, servicios, sistemas de información, infraestructura y red), fraude (abusos, prevención, reporting y monitorización) y seguridad física de Vodafone según el documento de aplicabilidad vigente a fecha de emisión del certificado.

que se realizan en: Oficinas centrales AV DE AMÉRICA, 115. 28042 - MADRID
CPD VODAFONE / ONO: CL. FRAY LUIS DE LEÓN, 11- 3 4º Pta. 28012 - MADRID
CPD ONO / VODAFONE: BASURI, 5. 28023 - ARAVACA (MADRID)
CPD ONO / VODAFONE: SAN SEVERO 22-24. 28042 - MADRID
CPD LEGANÉS - CALLE PALIER 48-50. 28914 - LEGANES (MADRID)

Fecha de primera emisión: 2012-03-23
Fecha de última emisión: 2018-03-23
Fecha de expiración: 2021-03-23

Original Efectivo

AENOR INTERNACIONAL S.A.U.
Genova, 6. 28004 Madrid, España
Tel. 91 432 60 00 - www.aenor.com



ANNEX A: SECURITY
PART C: KEY SUBCONTRACTOR'S CURRENT STORM SECURITY OVERVIEW
DOCUMENT



Crown
Commercial
Service

Core Terms (incl Special Terms)

1. Definitions used in the contract

1.1 Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.

2.2 CCS doesn't guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract.

2.3 CCS has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.

2.4 If the Buyer decides to buy Deliverables under the Framework Contract it must use Framework Schedule 7 (Call-Off Award Procedure) and must state its requirements using Framework Schedule 6 (Order Form Template and Call-Off Schedules). If allowed by the Regulations, the Buyer can:

- make changes to Framework Schedule 6 (Order Form Template and Call-Off Schedules)
- create new Call-Off Schedules
- exclude optional template Call-Off Schedules
- use Special Terms in the Order Form to add or change terms

2.5 Each Call-Off Contract:

- is a separate Contract from the Framework Contract
- is between a Supplier and a Buyer
- includes Core Terms, Schedules and any other changes or items in the completed Order Form
- survives the termination of the Framework Contract

2.6 Where the Supplier is approached by an eligible buyer requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this Framework Contract before accepting their order. The Supplier will promptly notify CCS if the eligible buyer won't use this Framework Contract.

Special Term 1: Core Terms Clause 2.6 – Deletes the last sentence: "The Supplier will promptly notify CCS if the eligible buyer won't use this Framework Contract."

2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

Core Terms

2.8 The Supplier won't be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

- verify the accuracy of the Due Diligence Information
- properly perform its own adequate checks

2.9 CCS and the Buyer won't be liable for errors, omissions or misrepresentation of any information.

2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

2.11 Special Term 2: Adds new clause: The Supplier shall operate the Catalogue in accordance with Framework Schedule 1 (Specification).

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

- that comply with the Specification, the Framework Tender Response and, in relation to a Call-Off Contract, the Call-Off Tender (if there is one)
- to a professional standard
- using reasonable skill and care
- using Good Industry Practice
- using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract
- on the dates agreed
- that comply with Law

3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

Special Term 3: Core Terms Clause 3.2.2 – deletes the Clause.

3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

Core Terms

3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

Special Term 4: Core Terms Clause 3.2.11 - Deletes the Clause.

3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with Clause 3. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.

3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.

Core Terms

3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4 Pricing and payments

4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.

4.2 CCS must invoice the Supplier for the Management Charge and the Supplier must pay it using the process in Framework Schedule 5 (Management Charges and Information).

4.3 All Charges and the Management Charge:

- exclude VAT, which is payable on provision of a valid VAT invoice
- include all costs connected with the Supply of Deliverables

4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

4.5 A Supplier invoice is only valid if it:

- includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer
- includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any)
- doesn't include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge)

4.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, CCS or the Buyer can publish the details of the late payment or non-payment.

4.8 If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables and that cost is reimbursable by the Buyer, then CCS or the Buyer may either:

Core Terms

- require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items
- enter into a direct agreement with the Subcontractor or third party for the relevant item

4.9 If CCS or the Buyer uses Clause 4.8 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

4.10 CCS and the Buyer's right to enter into a direct agreement for the supply of the relevant items is subject to both:

- the relevant item being made available to the Supplier if required to provide the Deliverables
- any reduction in the Framework Prices (and where applicable, the Charges) excludes any unavoidable costs that must be paid by the Supplier for the substituted item, including any licence fees or early termination charges

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they're ordered to do so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

- neither CCS or the Buyer can terminate a Contract under Clause 10.4.1
- the Supplier is entitled to reasonable and proven additional expenses and to relief from Delay Payments, liability and Deduction under this Contract
- the Supplier is entitled to additional time needed to make the Delivery
- the Supplier cannot suspend the ongoing supply of Deliverables

5.2 Clause 5.1 only applies if the Supplier:

- gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware
- demonstrates that the Supplier Non-Performance only happened because of the Authority Cause
- mitigated the impact of the Authority Cause

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

Core Terms

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the End Date.

6.3 The Supplier must allow any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit.

6.4 The Supplier must provide information to the Auditor and reasonable co-operation at their request.

6.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- tell the Relevant Authority and give reasons
- propose corrective action
- provide a deadline for completing the corrective action

6.6 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

- the methodology of the review
- the sampling techniques applied
- details of any issues
- any remedial action taken

6.7 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

7.1 The Supplier Staff involved in the performance of each Contract must:

- be appropriately trained and qualified
- be vetted using Good Industry Practice and the Security Policy
- comply with all conduct requirements when on the Buyer's Premises

7.2 Where a Buyer decides one of the Supplier's Staff isn't suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.

7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any

person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

- it has full capacity and authority to enter into and to perform each Contract
- each Contract is executed by its authorised representative
- it is a legally valid and existing organisation incorporated in the place it was formed
- there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract
- it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract
- it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract
- it is not impacted by an Insolvency Event
- it will comply with each Call-Off Contract

8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:

- wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract
- non-payment by the Supplier of any tax or National Insurance

8.4 All claims indemnified under this Contract must use Clause 26.

8.5 CCS or a Buyer can terminate the Contract for breach of any warranty or indemnity where they are entitled to do so.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

Special Term 5: Core Terms Clause 8.7 – Deletes current text and replace with:

"The Supplier shall assign to the Buyer, or if it is unable to do so, shall (to the extent it is legally able to do so) hold on trust for the sole benefit of the Buyer, all warranties and indemnities provided by third parties in respect of the Deliverables. Where any such warranties are held on trust, the Supplier shall enforce such warranties in accordance with

any reasonable directions that the Buyer may notify from time to time to the Supplier.”

9. Intellectual Property Rights (IPRs)

9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier’s Existing IPR to enable it to both:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier

9.2 Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.

9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

9.4 Neither Party has the right to use the other Party’s IPRs, including any use of the other Party’s names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer’s sole option, either:

- obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR
- replace or modify the relevant item with substitutes that don’t infringe IPR without adversely affecting the functionality or performance of the Deliverables

10. Ending the contract

10.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months’ written notice before the Contract expires.

10.3 Ending the contract without a reason

10.3.1 CCS has the right to terminate the Framework Contract at any time without reason

Core Terms

or liability by giving the Supplier at least 30 days' notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.3.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

Special Term 6: Core Terms Clause 10.3.2 - Deletes current text and replaces with the following:

“Each Buyer has the right to terminate their Call-Off Contract at any time by giving the Supplier not less than the minimum period of notice specified in the Order Form. Under such circumstances the Buyer agrees to pay the Supplier's reasonable and proven unavoidable Losses resulting from termination of the Call- Off Contract, provided that the Supplier takes all reasonable steps to minimise such Losses. The Supplier will give the Customer a fully itemised list of such Losses, with supporting evidence, to support their claim for payment. After the Call-Off Contract ends Clauses 10.5.2 to 10.5.7 will apply.”

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- there's a Supplier Insolvency Event
- there's a Contract Default that is not corrected in line with an accepted Rectification Plan
- the Relevant Authority rejects a Rectification Plan or the Supplier does not provide it within 10 days of the request
- there's any material default of the Contract
- there's a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract
- there's a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management)
- there's a Change of Control of the Supplier which isn't pre-approved by the Relevant Authority in writing
- there's a Variation to a Contract which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes)
- if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded
- the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations
- the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them

10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If there is a Default, the Relevant Authority can, without limiting its other rights, request that the Supplier provide a Rectification Plan.

10.4.4 When the Relevant Authority receives a requested Rectification Plan it can either:

- reject the Rectification Plan or revised Rectification Plan, giving reasons
- accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties

10.4.5 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

- must give reasonable grounds for its decision
- may request that the Supplier provides a revised Rectification Plan within 5 Working Days

10.4.6 If any of the events in 73 (1) (a) to (c) of the Regulations happen, the Relevant Authority has the right to immediately terminate the Contract and Clause 10.5.2 to 10.5.7 applies.

10.5 What happens if the contract ends

Where the Relevant Authority terminates a Contract under Clause 10.4.1 all of the following apply:

10.5.1 The Supplier is responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

10.5.2 The Buyer's payment obligations under the terminated Contract stop immediately.

10.5.3 Accumulated rights of the Parties are not affected.

10.5.4 The Supplier must promptly delete or return the Government Data except where required to retain copies by law.

10.5.5 The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.

Core Terms

10.5.6 The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

10.5.7 The following Clauses survive the termination of each Contract: 3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

Special Term 12: Core Terms – replace the existing Clause 10.5.7 as below:

10.5.7: The following Clauses survive the termination of each Contract: 3.2.10, 6, 7.5, 9, 11, 14, 15, 16, 17, 18, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.6 When the supplier can end the contract

10.6.1 The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6.2 If a Supplier terminates a Call-Off Contract under Clause 10.6.1:

- the Buyer must promptly pay all outstanding Charges incurred to the Supplier
- the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated
- Clauses 10.5.4 to 10.5.7 apply

Special Term 13: Core Terms – replace the existing Clause 10.6.2 as below:

10.6.2: If a Supplier terminates a Call-Off Contract under Clause 10.6.1:

- the Buyer must promptly pay all outstanding Charges incurred to the Supplier
- the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated. Clauses 10.5.3 to 10.5.7 apply.

10.7 When subcontracts can be ended

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

- there is a Change of Control of a Subcontractor which isn't pre-approved by the Relevant Authority in writing

Core Terms

- the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4
- a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority

10.8 Partially ending and suspending the contract

10.8.1 Where CCS has the right to terminate the Framework Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Call-Off Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

10.8.2 Where CCS has the right to terminate a Framework Contract it is entitled to terminate all or part of it.

10.8.3 Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.8.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.8.5 The Parties must agree any necessary Variation required by Clause 10.8 using the Variation Procedure, but the Supplier may not either:

- reject the Variation
- increase the Charges, except where the right to partial termination is under Clause 10.3

10.8.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.8.

11. How much you can be held responsible for

11.1 Each Party's total aggregate liability in each Contract Year under this Framework Contract (whether in tort, contract or otherwise) is no more than £100,000.

11.2 Each Party's total aggregate liability in each Contract Year under each Call-Off Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Call-Off Order Form

Special Term 7: Core Terms Clause 11.2 – amends “£5 million” to “£1 million”

11.3 No Party is liable to the other for:

Core Terms

- any indirect Losses
- Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect)

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

- its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors
- its liability for bribery or fraud or fraudulent misrepresentation by it or its employees
- any liability that cannot be excluded or limited by Law
- its obligation to pay the required Management Charge or Default Management Charge

11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3, 9.5, 12.2 or 14.9 or Call-Off Schedule 2 (Staff Transfer) of a Contract.

11.6 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

11.7 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

- Deductions
- any items specified in Clause 11.5

11.8 If more than one Supplier is party to a Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 The Supplier indemnifies CCS and every Buyer against any costs resulting from any Default by the Supplier relating to any applicable Law to do with a Contract.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint

Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

14. Data protection

14.1 The Relevant Authority is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation.

Special Term 8: Core Terms Clause 14.1 - Deletes the Clause and replaces with:

“The Parties acknowledge that for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor unless otherwise specified in Joint Schedule 11.”

14.2 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.3 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.4 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.5 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

Special Term 9: Core Terms 14.5 – deletes the Clause and replaces with:

“The Supplier shall ensure that any system on which the Supplier holds any Government Data, including backup data, is a secure system, and for Call-Off Contracts that it will comply with the relevant Buyer’s requirements in respect of Call-Off Schedule 9.”

14.6 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.7 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

- tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier
- restore the Government Data itself or using a third party

Core Terms

14.8 The Supplier must pay each Party's reasonable costs of complying with Clause 14.7 unless CCS or the Buyer is at fault.

14.9 The Supplier:

- must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request
- must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading
- must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice
- securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it
- indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

- keep all Confidential Information it receives confidential and secure
- not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent, except for the purposes anticipated under the Contract
- immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure
- if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party
- if the information was given to it by a third party without obligation of confidentiality
- if the information was in the public domain at the time of the disclosure
- if the information was independently developed without access to the Disclosing Party's Confidential Information
- to its auditors or for the purposes of regulatory requirements
- on a confidential basis, to its professional advisers on a need-to-know basis
- to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

15.4 CCS or the Buyer may disclose Confidential Information in any of the following cases:

- on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer
- on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to
- if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions
- where requested by Parliament
- under Clauses 4.7 and 16

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within the required timescales the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:

- publish the Transparency Information
- comply with any Freedom of Information Act (FOIA) request
- comply with any Environmental Information Regulations (EIR) request

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision, which does not need to be reasonable.

17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

- provides a Force Majeure Notice to the other Party
- uses all reasonable measures practical to reduce the impact of the Force Majeure Event

20.2 Either party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

20.3 Where a Party terminates under Clause 20.2:

- each party must cover its own Losses
- Clause 10.5.2 to 10.5.7 applies

21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier cannot assign a Contract without the Relevant Authority's written

Core Terms

consent.

23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Relevant Authority.

23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

- their name
- the scope of their appointment
- the duration of their appointment

24. Changing the contract

24.1 Either Party can request a Variation to a Contract which is only effective if agreed in writing and signed by both Parties

24.2 The Supplier must provide an Impact Assessment either:

- with the Variation Form, where the Supplier requests the Variation
- within the time limits included in a Variation Form requested by CCS or the Buyer

Special Term 10: Core Terms Clause 24.2 – adds the following additional text at the end of the Clause:

“If the Supplier needs resources other than those ordinarily used in the provision of the Service in order to complete an Impact Assessment requested by the Buyer, the Supplier must tell the Buyer before beginning the Impact Assessment. If the Buyer wants the Impact Assessment to go ahead, the Buyer shall pay any reasonable costs incurred by the Supplier in producing the Impact Assessment. To be clear, the Supplier will not be able to recover costs incurred during the Impact Assessment that the Buyer didn’t agree before the Impact Assessment began.”

24.3 If the Variation to a Contract cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

Core Terms

- agree that the Contract continues without the Variation
- terminate the affected Contract, unless in the case of a Call-Off Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them
- refer the Dispute to be resolved using Clause 34 (Resolving Disputes)

24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Framework Prices or the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, Framework Prices or a Contract and provide evidence:

- that the Supplier has kept costs as low as possible, including in Subcontractor costs
- of how it has affected the Supplier's costs

24.7 Any change in the Framework Prices or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address in the Framework Award Form.

25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.

25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

Core Terms

26.2 At the Indemnifier's cost the Beneficiary must both:

- allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim
- give the Indemnifier reasonable assistance with the claim if requested

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which cannot be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that doesn't damage the Beneficiary's reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

- the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money
- the amount the Indemnifier paid the Beneficiary for the Claim

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

- commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2)
- do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them

27.2 The Supplier must during the Contract Period:

- create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same
- keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request
- if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including

Core Terms

compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses

27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- been investigated or prosecuted for an alleged Prohibited Act
- been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency
- received a request or demand for any undue financial or other advantage of any kind related to a Contract
- suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.4 it must specify the:

- Prohibited Act
- identity of the Party who it thinks has committed the Prohibited Act
- action it has decided to take

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

- protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise
- any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- all applicable Law regarding health and safety

Core Terms

- the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

- the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant
- other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under a Call-Off Contract, the Supplier must both:

- comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions
- indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker

contains the following requirements:

- the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding
- the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer
- the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements
- the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

- Law
- Clause 12.1
- Clauses 27 to 32

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by

Core Terms

mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

- determine the Dispute
- grant interim remedies
- grant any other provisional or protective relief

34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

This Contract and any issues arising out of, or connected to it, are governed by English law.

36. Telecoms Expense Management

Special Term 11: Core Terms – add the following provision:

“The Supplier shall provide without charge to a TEM Provider nominated by CCS the detailed invoice data for each Buyer in receipt of Deliverables in an Electronic Data Interchange (EDI) format at the same frequency as it is received by that Buyer, subject to the TEM Provider agreeing to enter into a direct confidentiality agreement with the Supplier on terms equivalent to the terms set out in Clause 15 (What you must keep Confidential).”

Joint Schedules

Joint Schedule 1 (Definitions)
Crown Copyright 2018

Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In each Contract, unless the context otherwise requires:
 - 1.3.1 the singular includes the plural and vice versa;
 - 1.3.2 reference to a gender includes the other gender and the neuter;
 - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;
 - 1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
 - 1.3.5 the words **"including"**, **"other"**, **"in particular"**, **"for example"** and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words **"without limitation"**;
 - 1.3.6 references to **"writing"** include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
 - 1.3.7 references to **"representations"** shall be construed as references to present facts, to **"warranties"** as references to present and future facts and to **"undertakings"** as references to obligations under the Contract;
 - 1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
 - 1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided; and
 - 1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified.

Joint Schedule 1 (Definitions)

Crown Copyright 2018

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract.

1.3.12 Where the Buyer is a Crown Body it shall be treated as contracting with the Crown as a whole.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees ;
"Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and "Achieved" , "Achieving" and "Achievement" shall be construed accordingly;
"Additional Insurances"	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
"Affected Party"	the party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Ancillary Services"	means those components described in paragraph 1.2.4 of Part A of Framework Schedule 1 (Specification);
"Annex"	extra information which supports a Schedule;
"Approval"	the prior written consent of the Buyer and "Approve" and "Approved" shall be construed accordingly;
"Audit"	the Relevant Authority's right to: <ul style="list-style-type: none"> a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) where the Relevant Authority is a Buyer, and the value of the relevant Call-Off Contract is greater than £3 million, verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility),

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;</p> <p>f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables;</p> <p>g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;</p> <p>h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;</p> <p>i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts;</p> <p>j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources;</p> <p>k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;</p>
"Auditor"	<p>a) the Buyer's internal and external auditors;</p> <p>b) the Buyer's statutory or regulatory auditors;</p> <p>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;</p> <p>d) HM Treasury or the Cabinet Office;</p> <p>e) any party formally appointed by the Buyer to carry out audit or similar review functions; and</p> <p>f) successors or assigns of any of the above;</p>
"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;
"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"Buyer System"	has the meaning given to it in Schedule 6 (ICT Services);
"Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
"Call-Off Contract Period"	the Contract Period in respect of the Call-Off Contract;
"Call-Off Expiry Date"	the date of the end of a Call-Off Contract as stated in the Order Form;
"Call-Off Incorporated Terms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
"Call-Off Initial Period"	the Initial Period of a Call-Off Contract specified in the Order Form;
"Call-Off Optional Extension Period"	such period or periods beyond which the Call-Off Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form;
"Call-Off Procedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Procedure and Award Criteria);
"Call-Off Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
"Call-Off Start Date"	the date of start of a Call-Off Contract as stated in the Order Form;
"Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Catalogue"	the Supplier's catalogue of Deliverables available to Buyers to order without Further Competition;
"Catalogue Publication Portal"	the CCS online publication channel via which Buyers can view the Catalogue;
"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
"Central Government Body"	<p>a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <p>a) Government Department;</p> <p>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);</p> <p>c) Non-Ministerial Department; or</p> <p>d) Executive Agency;</p>
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
"Commercially Sensitive Information"	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
"Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
"Contract Period"	the term of either a Framework Contract or Call-Off Contract from the earlier of the: a) applicable Start Date; or b) the Effective Date until the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "Controlled" shall be construed accordingly;
"Controller"	has the meaning given to it in the GDPR;
"Core Network"	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;
"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<ul style="list-style-type: none"> ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; <p>b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</p> <p>c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables;</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</p> <p>but excluding:</p> <ul style="list-style-type: none"> a) Overhead; b) financing or similar costs; c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise; d) taxation; e) fines and penalties; f) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and g) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Subject Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Charge"	has the meaning given to it in Paragraph 7.1.1 of Framework Schedule 5 (Framework Management);
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "Deliver" and "Delivered" shall be construed accordingly;
"Direct Award Criteria"	means the award criteria to be applied for the direct award of Call-Off Contracts for Services set out in Framework Schedule 7 (Call-Off Award Procedure);
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable) for the period specified in the Order Form (for the purposes of this definition the "Disaster Period");
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);
"Dispute"	any claim, dispute or difference arises out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	<p>descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:</p> <ul style="list-style-type: none"> a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables b) is required by the Supplier in order to provide the Deliverables; and/or c) has been or shall be generated for the purpose of providing the Deliverables;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;
"EIR"	the Environmental Information Regulations 2004;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;
"End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
"Estimated Year 1 Contract Charges"	the anticipated total charges payable by the Supplier in the first Contract Year specified in the Call-Off Order Form;
"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : i) in the first Contract Year, the Estimated Year 1 Contract Charges; or ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
"Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
"Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
"FOIA"	the Freedom of Information Act 2000 as amended from time to time and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	<p>any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from:</p> <ul style="list-style-type: none"> a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract; b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of a Crown Body, local government or regulatory bodies; d) fire, flood or any disaster; or e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: <ul style="list-style-type: none"> i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"Framework Award Form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
"Framework Contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Framework Contract Period"	the period from the Framework Start Date until the End Date or earlier termination of the Framework Contract;
"Framework Expiry Date"	the date of the end of the Framework Contract as stated in the Framework Award Form;
"Framework Incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
"Framework Initial Period"	the initial term of the Framework Contract as specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Initial Period may be extended up to a maximum of the number of years in total specified in the Framework Award Form;
"Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
"Framework Start Date"	the date of start of the Framework Contract as stated in the Framework Award Form;
"Framework Special Terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
"Framework Tender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender Response);
"Further Competition Procedure" or "Further Competition"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679)
"General Anti-Abuse Rule"	a) the legislation in Part 5 of the Finance Act 2013 and; and b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	<p>a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:</p> <ul style="list-style-type: none"> i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; or <p>b) any Personal Data for which the Authority is the Controller;</p>
"Government Procurement Card"	the Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2 ;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"Health and Social Care Network or HSCN"	the government's network for health and social care, which helps all organisations involved in health and social care delivery to work together and interoperate; and as described at https://digital.nhs.uk/services/health-and-social-care-network ;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Environment"	the ICT systems related to a Call-Off Contract described in Call-Off Schedule 6 (ICT Services);
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"ICT Services"	the ICT related Services to be delivered under a Call-Off Contract described in Call-Off Schedule 6 (ICT Services);
"Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract;</p> <p>b) details of the cost of implementing the proposed Variation;</p> <p>c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;</p> <p>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and</p> <p>e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;</p>
"Implementation Plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;
"Insolvency Event"	<p>a) in respect of a person:</p> <p>b) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or</p> <p>c) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or</p> <p>d) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or</p> <p>e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or</p>

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>f) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or</p> <p>g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or</p> <p>h) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or</p> <p>i) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or</p> <p>j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;</p>
"Installation Works"	all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract;
"Intellectual Property Rights" or "IPR"	<p>a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;</p> <p>b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
"Invoicing Address"	the address to which the Supplier shall Invoice the Buyer as specified in the Order Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies ;
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of processing;
"Key Personnel"	the individuals (if any) identified as such in the Order Form;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	<p>any Subcontractor:</p> <p>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or</p> <p>c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract,</p> <p>and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;</p>
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;
"Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "Loss" shall be interpreted accordingly;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680)
"Man Day"	7.5 Man Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
"Man Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;
"Management Information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Management Charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
"Marketing Contact"	shall be the person identified in the Framework Award Form;
"MI Failure"	means when an MI report: <ul style="list-style-type: none"> a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date(including where a Nil Return should have been filed);
"MI Report"	means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
"MI Reporting Template"	means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task specified as such in the Implementation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
"Month"	a calendar month and "Monthly" shall be interpreted accordingly;
"National Insurance"	contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	<ul style="list-style-type: none"> a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; <p>but shall not include the Supplier's Existing IPR;</p>
"Occasion of Tax Non – Compliance"	<p>where:</p> <ul style="list-style-type: none"> a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: <ul style="list-style-type: none"> i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	<p>ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or</p> <p>b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;</p>
"OJEU Contract Notice"	has the meaning given to it in the Framework Award Form;
"Open Book Data"	<p>complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:</p> <p>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;</p> <p>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:</p> <p>i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;</p> <p>ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each manpower grade;</p> <p>iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and</p> <p>iv) Reimbursable Expenses, if allowed under the Order Form;</p> <p>c) Overheads;</p> <p>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</p> <p>e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;</p> <p>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;</p> <p>g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and</p>

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	h) the actual Costs profile for each Service Period;
"Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
"Order Form Template"	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);
"Other Contracting Authority"	any actual or potential Buyer under the Framework Contract;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "Parties" shall mean both of them where the context permits;
"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies ;
"Primary Services"	means the components described in paragraph 1.2.2 of Part A of Framework Schedule 1 (Specification);
Processor	takes the meaning given in the GDPR;
Processor Personnel:	all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
"Prohibited Acts"	<p>a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:</p> <ul style="list-style-type: none"> i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; <p>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or</p> <p>c) committing any offence:</p> <ul style="list-style-type: none"> i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or <p>d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;</p>
"Protective Measures"	<p>technical and organisational measures which must take account of:</p> <ul style="list-style-type: none"> a) the nature of the data to be protected b) harm that might result from Data Loss Event; c) state of technological development d) the cost of implementing any measures <p>including but not limited to pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;</p>

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Public Services Network or PSN"	the network of networks delivered through multiple service providers, as further detailed in the PSN operating model; and described at https://www.gov.uk/government/groups/public-services-network ;
"Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan Template) which shall include: a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time;
"Reimbursable Expenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and information derived from any of the above;
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in Annex 2 of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
"Schedules"	any attachment to a Framework or Call-Off Contract which contains important information specific to each aspect of buying and selling;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	<p>means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate) which shall be based on tests completed against a representative sample of Orders as specified in Framework Schedule 8 and must provide assurance that:</p> <ul style="list-style-type: none"> a) Orders are clearly identified as such in the order processing and invoicing systems and, where required, Orders are correctly reported in the MI Reports; b) all related invoices are completely and accurately included in the MI Reports; c) all Charges to Buyers comply with any requirements under this Framework Contract on maximum mark-ups, discounts, charge rates, fixed quotes (as applicable); and d) a number of additional sample of public sector orders identified in Framework Schedule 8 (Self Audit Certificate) from the Supplier's order processing and invoicing systems as orders not placed under this Framework Contract have been correctly identified as such and that an appropriate and legitimately tendered procurement route has been used to place those orders, and those orders should not otherwise have been routed via centralised mandated procurement processes executed by CCS
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Call-Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Offer"	a Deliverable made available to Buyers by the Supplier via the Catalogue;
"Service Offer Effective Date"	the date when the Service Offer will be available to Buyers on the Catalogue;
"Service Offer Expiry Date"	the date the Service Offer will be/was removed from the Catalogue;
"Service Offer Price Card"	means a list of prices, rates and other amounts for a specific Service Offer;
"Service Offer Template"	the template set out at Annex 1 to Part B of Framework Schedule 3 (Framework Prices);
"Service Period"	has the meaning given to it in the Order Form;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Services"	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	means: a) any delivery point for the Services (including the Buyer Premises, the Supplier's premises, third party premises, or any non-premises location, such as kerbside cabinets and bus shelters); or b) from to or at which i) the Services are (or are to be) provided; or ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or c) where any part of the Supplier System is situated; or a) d) any physical interface with the Buyer's System takes place
"Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

"Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of the Supplier related to a Contract
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;
"Supplier"	the person, firm or company identified in the Framework Award Form;
"Supplier Action Plan"	means a document, maintained by the Authority, capturing information about the relationship between the Parties including, but not limited to strategic objectives, actions, initiatives, communication channels, risks and supplier performance;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
"Supplier's Confidential Information"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	(or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;
"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or c) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supplier System"	has the meaning given to it in Schedule 6 (ICT Services);
"TEM Provider"	means a Supplier appointed by CCS to provide telecoms expense management;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
"Test Issue"	any variance or non-conformity of the Deliverables or Deliverables from their requirements as set out in a Call-Off Contract;
"Test Plan"	a plan: a) for the Testing of the Deliverables; and

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)

Crown Copyright 2018

	b) setting out other agreed criteria related to the achievement of Milestones;
"Tests and Testing"	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "Tested" shall be construed accordingly;
"Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Time and Materials"	a pricing mechanism whereby the Buyer agrees to pay the Supplier based upon the work performed by the Supplier's employees and Sub-Contractors, and for materials used in the project, no matter how much work is required to complete the project;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
"US-EU Privacy Shield Register"	a list of companies maintained by the United States of America Department for Commerce that have self-certified their commitment to adhere to the European legislation relating to the processing of personal data to non-EU countries which is available online at: https://www.privacyshield.gov/list ;
"Variation"	has the meaning given to it in Clause 24 (Changing the contract);
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 1 (Definitions)
Crown Copyright 2018

"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form.
----------------------	---

Joint Schedule 2 (Variation Form)

Crown Copyright 2018

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contact Details	
This variation is between:	[delete] as applicable: CCS / Buyer] (" CCS " " the Buyer ") And [insert] name of Supplier] (" the Supplier ")
Contract name:	[insert] name of contract to be changed] (" the Contract ")
Contract reference number:	[insert] contract reference number: Framework Contract reference/Call-Off Contract reference]
Details of Proposed Variation	
Variation initiated by:	[delete] as applicable: CCS/Buyer/Supplier]
Variation number:	[insert] variation number]
Date variation is raised:	[insert] date]
Proposed variation	
Reason for the variation:	[insert] reason]
An Impact Assessment shall be provided within:	[insert] number] days
Impact of Variation	
Likely impact of the proposed variation:	[Supplier to insert] assessment of impact]
Outcome of Variation	
Contract variation:	This Contract detailed above is varied as follows: <ul style="list-style-type: none"> [CCS/Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause]
Financial variation:	Original Contract Value: £ [insert] amount]
	Additional cost due to variation: £ [insert] amount]
	New Contract value: £ [insert] amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete]** as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 2 (Variation Form)
Crown Copyright 2018

Signed by an authorised signatory for and on behalf of the **[delete]** as applicable: CCS / Buyer]

Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature

Date

Name (in Capitals)

Address

Joint Schedule 3 (Insurance Requirements)
Crown Copyright 2018

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.1 – Vodafone Direct Award Version

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

3. What happens if you aren't insured

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

- 4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

- 5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.1 – Vodafone Direct Award Version

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

dealing with such claims including without limitation providing information and documentation in a timely manner.

- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

Joint Schedule 3 (Insurance Requirements)

Crown Copyright 2018

ANNEX: Required Insurances

1. The Supplier shall hold the following standard insurance cover from the Framework Start Date in accordance with this Schedule:
 - 1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);
 - 1.2 public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000); and
 - 1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).
 - 1.4 Product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000)

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.1 – Vodafone Direct Award Version

Joint Schedule 4 (Commercially Sensitive Information)
Crown Copyright 2018

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

- 1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

Joint Schedule 4 (Commercially Sensitive Information)
Crown Copyright 2018

No.	Date	Item(s)	Duration of Confidentiality
1.	31.01.2019	Document Name; Attachment 3 - RM3808 Framework Prices v1.4	31.01.2023
2.	Date of submission	Breakdown of pricing information to give input costs, capital and operating costs, overheads, revenue, margins and profits.	Expiry Date plus 6 years
3.	Call-Off Start Date	How any payments due to the Supplier on the termination of the whole or any part of the Call Off Contract have been or will be calculated but excluding the actual amounts of such payments.	Expiry Date plus 6 years
4.	Date of submission	Any financial data relating to the Supplier's business as a whole including the financial standing of the Supplier provided in connection with this Call Off Contract, including but not limited to any information relating to financial distress reporting.	Expiry Date plus 6 years

Joint Schedule 4 (Commercially Sensitive Information)
Crown Copyright 2018

5.	Date of submission	The cover and amounts of the Supplier's insurances.	Expiry Date plus 6 years
6.	Call-Off Start Date	How any service credits are financially calculated under the Call Off Contract, but excluding any details regarding the applicable service thresholds, or any performance related information or requirements, or information relating to the actual amounts of any service credits paid or credited to the Customer.	Expiry Date plus 6 years
7.	Date of submission	Technical details of the Supplier's network, (including topology, network diagrams, detailed network coverage, route maps, the Supplier's Points of Presence and/or street furniture/chambers etc.).	Expiry Date plus 6 years

Joint Schedule 4 (Commercially Sensitive Information)
Crown Copyright 2018

8.	Date of submission	Design documents relating to the Services and any notes or minutes of technical design meetings held in relation to the aforementioned but excluding any documents explicitly set out in the Call Off Contract as being Deliverables to the Customer.	Expiry Date plus 6 years
9.	Date of submission	The Supplier's own Business Continuity Plan, Business Incident Plans, and Disaster Recovery Manuals and Procedures, Security Plan and related Business Security Processes but excluding any Customer-specific plans or procedures to be provided by the Supplier under the Call Off Contract.	Expiry Date plus 6 years

Joint Schedule 5 (Corporate Social Responsibility)
Crown Copyright 2018

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

- 1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)
- 1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.
- 1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such reasonable corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time. Any necessary changes to the relevant Call-Off Contract shall be enacted via the Variation Procedure.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:
 - 2.1.1 eliminate discrimination, harassment or victimisation of any kind; and
 - 2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at <https://www.modernslaveryhelpline.org/report> or by telephone on 08000 121 700.

- 3.1 The Supplier:
 - 3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
 - 3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

- 3.1.3 warrants and represents that it has not been convicted of any slavery or human tracking offenses anywhere around the world.
- 3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human tracking offenses anywhere around the world.
- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human tracking offenses anywhere around the world.
- 3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
- 3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;
- 3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security**4.1 The Supplier shall:**

- 4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect to wages before they enter;
- 4.1.3 All workers shall be provided with written and understandable Information about their employment conditions in respect to wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 5 (Corporate Social Responsibility)

Crown Copyright 2018

- 4.1.4 not make deductions from wages:
 - (a) as a disciplinary measure
 - (b) except where permitted by law; or
 - (c) without expressed permission of the worker concerned;
- 4.1.5 record all disciplinary measures taken against Supplier Staff; and
- 4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

- 5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
- 5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- 5.1.3 ensure that use of overtime used responsibly, taking into account:
 - (a) the extent;
 - (b) frequency; and
 - (c) hours worked;by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

- 5.3.1 this is allowed by national law;
- 5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
appropriate safeguards are taken to protect the workers' health and safety; and
- 5.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

Framework Ref: RM3808

Project Version: v1.0

Model Version: v3.0 – Vodafone Direct Award Version

Joint Schedule 5 (Corporate Social Responsibility)
Crown Copyright 2018

6. Sustainability

- 6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:
<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>