



---

**UKEF Salesforce Delivery Partner**

**Call Off Order Form for Management Consultancy Services2, Lot 1, RM6008**

**Project** [REDACTED]

---

**FOR A CALL-OFF CONTRACT BETWEEN**

**UKEXPORT FINANCE**

**AND**

**KPMG LLP**

**FRAMEWORK SCHEDULE 4**

**CALL OFF ORDER FORM**

## PART 1 – CALL OFF ORDER FORM

### SECTION A

This Call Off Order Form is issued in accordance with the provisions of the Framework Agreement for the provision of Management Consultancy Services dated **04 September 2018**.

The Delivery Partner agrees to supply the Services specified below on and subject to the terms of this Call Off Contract.

For the avoidance of doubt this Call Off Contract consists of the terms set out in this Template Call Off Order Form and the Call Off Terms.



RM6008-MCF2-Call  
-off-terms-v61.pdf

Order Number		TBA
From	<b>UK Export Finance, ("CUSTOMER")</b>	1 Horse Guards Road, London SW1A 2HQ
To	<b>KPMG LLP ("DELIVERY PARTNER")</b>	15 Canada Square, London, E14 5GL
Date	<b>1 February 2021 ("DATE")</b>	



### SECTION B

#### 1. CALL OFF CONTRACT PERIOD

1.1.	<b>Commencement Date:</b> <b>1 February 2021</b>	
1.2.	<b>Expiry Date:</b>  End date of Initial Period: <b>31 January 2023</b>  End date of Extension Period: <b>31 January 2024</b>  Minimum written notice to Delivery Partner in respect of extension: <b>3 months</b>	
1.3.	<b>Maximum Contract Value</b> The maximum contract value is [REDACTED] excluding VAT, for the initial 2-year	

	duration, and [REDACTED] for the optional 1 year extension period.	
--	--	--

## 2. SERVICES

2.1.	<p><b>Services required:</b></p> <p>In Call Off Schedule 2 (Services)</p> <p>The Services to be provided under the Call-Off Contract are set out in the Statement of Requirement.</p> <p>The Customer is not committing to any guaranteed spend beyond the Design Phase. This is because over the Call-Off Contract Period, the funding position of the Customer may change. Equally, if the Customer and the Delivery Partner fail to agree a revised Milestone the Customer may terminate this Call-Off Contract.</p> <p>Each Milestone will be Approved by the Customer in accordance with the terms of the Call-Off Contract. It is envisaged that Approval of the next Milestone will occur during the firebreak period the Customer has proposed to allow the new functionality put in place under a previous Milestone to 'bed in'. If the Customer exercises its discretion to extend the Call-Off Contract, further indicative Milestones will be added to the Call-Off Contract via the Variation Procedure.</p>	<p>Requirements for the Design Phase are outlined in the Statement of Requirement (paragraphs 5.20 – 5.28), future phases of work (Milestones) will be agreed in accordance with paragraphs 5.18 – 5.19. This is also outlined in section 5 of the Statement of Requirement.</p> <p> Appendix%20B%20Statement%20of%20R</p> <p>The Delivery Partner will deliver the Services in accordance with the bid response document below save as agreed with the Customer in writing.</p> <p> UKEF Salesforce Delivery Partner_KPN</p>
------	--	---

## 3. PROJECT PLAN

3.1.	<p><b>Project Plan:</b> In Call Off Schedule 4 (Project Plan)</p> <p>The Delivery Partner shall provide the Customer with a draft Project Plan for Approval within seven (7) Working</p>	<p>The Delivery Partner's Project Plan are included in the Call-Off Contract bid response embedded above.</p>
------	--	---

	Days from the Call Off Commencement Date.	
	The Project Plan will refine the plan submitted with the tender and set out the Deliverables and Acceptance Criteria.	
<i>Milestones, Deliverables, Payments etc are outlined in the Statement of Requirements.</i>		


#### 4. CONTRACT PERFORMANCE

<b>4.1.</b>	<b>Standards:</b> As detailed in paragraph 5.1.22 of the Statement of Requirements	As detailed in the Delivery Partner's bid response document embedded above.
<b>4.2</b>	<b>Service Levels/Service Credits:</b> Not applied	<i>Not applicable.</i>
<b>4.3</b>	<b>Critical Service Level Failure:</b> Not applied	<i>Not applicable.</i>
<b>4.4</b>	<b>Performance Monitoring:</b> Not applied	<i>Not applicable.</i>
<b>4.5</b>	<b>Period for providing Rectification Plan:</b> In Clause 39.2.1(a) of the Call Off Terms	





#### 5. PERSONNEL

<b>5.1</b>	<b>Key Personnel:</b> <b>Account Manager</b>	As detailed in the Delivery Partner's bid response document embedded above.
<b>5.2</b>	<b>Relevant Convictions</b> (Clause 28.2 of the Call Off Terms): <b>N/A</b>	

#### 6. PAYMENT

6.1	<p><b>Call Off Contract Charges</b> (including any applicable discount(s), but excluding VAT):</p> <p>In Annex 1 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)</p>	<p>All as per the Delivery Partner's bid response document.</p>  <p>Appendix%20E%20Pricing%20Schedule% [REDACTED]</p> <p>Other charges as per the embedded pricing schedule.</p>
6.2	<p><b>Payment terms/profile</b> (including method of payment e.g. Government Procurement Card (GPC) or BACS):</p> <p>In Annex 2 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)</p>	BACS
6.3	<p><b>Reimbursable Expenses:</b></p> <p>Not permitted</p>	
6.4	<p><b>Customer billing address</b> (paragraph 7.6 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)):</p> <p>Valid Invoices should be submitted for payment to the following address:</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>	
6.5	<p>The prices submitted by the Delivery Partner as part of their Tender shall be fixed for (paragraph 8.2 of Schedule 3 (Call Off Contract Charges, Payment and Invoicing)):</p> <p><b>Three (3)</b> Call Off Contract Years from the Call Off Commencement Date</p>	
6.6	<p><b>Delivery Partner periodic assessment of Call Off Contract Charges</b> (paragraph 9.2 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)) shall not be carried out</p>	
6.7	<p><b>Delivery Partner request for increase in the Call Off Contract Charges</b> (paragraph 10 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)):</p> <p>Not Permitted</p>	

## 7. LIABILITY AND INSURANCE

7.1	<b>Estimated Year 1 Call Off Contract Charges:</b>	
7.2	<b>Delivery Partner's limitation of Liability</b> (Clause 37.2.1 of the Call Off Terms);	As set out in clause 37.2.1
7.3	<b>Insurance</b> (Clause 38.3 of the Call Off Terms): Minimum Five (5) Five million pounds for each of: Employers Liability Insurance Third Party Public & Products Liability Professional Indemnity Motor third party liability insurance	<div>  Employers Liability UK EL - GBP 10m - 20 </div> <div>  Indemnity SUMMARY OF INSURANCE </div> <div>  Public and Products Liability Primary PL 2 </div> <div>  KPMG Renewal Motor Certificate 202 </div>

## 8. TERMINATION AND EXIT

8.1	<b>Termination on material Default</b> (Clause 42.2 of the Call Off Terms):  In Clause 42.2.1(c) of the Call Off Terms	
8.2	<b>Termination without cause notice period</b> (Clause 42.7 of the Call Off Terms):  In Clause 42.7 of the Call Off Terms	
8.3	<b>Undisputed Sums Limit:</b>  In Clause 43.1.1 of the Call Off Terms	
8.4	<b>Exit Management:</b>  In Call Off Schedule 9 (Exit Management)	

## 9. DELIVERY PARTNER INFORMATION

--	--	--

<b>9.2</b>	<b>Commercially Sensitive Information:</b> [ ]	<i>Any KPMG pricing information or associated rate cards relating to this project</i>
------------	---	---

## 10. OTHER CALL OFF REQUIREMENTS

<b>10.1</b>	<b>Recitals</b> (in preamble to the Call Off Terms): Recitals B to E Recital C - date of issue of the Statement of Requirements: <b>05/11/2020</b> Recital D - date of receipt of Call Off Tender: <b>19/11/2020</b>	
<b>10.2</b>	<b>Call Off Guarantee (Clause 4 of the Call Off Terms):</b> Not required	
<b>10.3</b>	<b>Security:</b> The short form security requirements outlined in paragraphs 1 to 5 of Schedule 7 will apply.	
<b>10.4</b>	<b>ICT Policy:</b> The IT Strategy documents are included as Schedule 1 to Appendix B – Statement of Requirements The Delivery Partner is required to comply with this policy.  The Delivery Partner is also required to comply with the Customer's (UKEF) Security Framework Policy, added to the end of this Call-Off Order Form.	
<b>10.6</b>	<b>Business Continuity &amp; Disaster Recovery:</b>  In Call Off Schedule 8 (Business Continuity and Disaster Recovery)  <b>Disaster Period:</b> For the purpose of the definition of "Disaster" in Call Off Schedule 1 (Definitions) the "Disaster Period" shall be three (3) working days	
<b>10.7</b>	<b>NOT USED</b>	
<b>10.8</b>	<b>Protection of Customer Data</b> (Clause 35.2.3 of the Call Off Terms): <b>N/A</b>	
<b>10.9</b>	<b>Notices</b> (Clause 56.6 of the Call Off Terms): DIT's postal address: 3 Whitehall Place, London SW1A 2HP Customer's postal address: 1 Horse Guards Road, London SW1A 2HQ	



	Delivery Partner's postal address and email address: 15 Canada Square, London, E14 5GL [REDACTED]													
<b>10.10</b>	<b>Transparency Reports</b> In Call Off Schedule 13 (Transparency Reports)													
<table border="1"> <thead> <tr> <th>TITLE</th> <th>CONTENT</th> <th>FORMAT</th> <th>FREQUENCY</th> </tr> </thead> <tbody> <tr> <td><i>Performance and Performance Management</i></td> <td><i>Phases of work</i></td> <td><i>Meeting</i></td> <td><i>Weekly</i></td> </tr> <tr> <td><i>Call Off Contract Charges</i></td> <td><i>Milestone Payments / Payment Profile</i></td> <td><i>Meeting</i></td> <td><i>Weekly</i></td> </tr> </tbody> </table>			TITLE	CONTENT	FORMAT	FREQUENCY	<i>Performance and Performance Management</i>	<i>Phases of work</i>	<i>Meeting</i>	<i>Weekly</i>	<i>Call Off Contract Charges</i>	<i>Milestone Payments / Payment Profile</i>	<i>Meeting</i>	<i>Weekly</i>
TITLE	CONTENT	FORMAT	FREQUENCY											
<i>Performance and Performance Management</i>	<i>Phases of work</i>	<i>Meeting</i>	<i>Weekly</i>											
<i>Call Off Contract Charges</i>	<i>Milestone Payments / Payment Profile</i>	<i>Meeting</i>	<i>Weekly</i>											
<b>10.11</b>	<p><b>Alternative and/or Additional Clauses from Call Off Schedule 14 and if required, any Customer alternative pricing mechanism:</b></p> <p><b>Alternative pricing:</b> [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED].</p> <p><b>Additional clauses:</b></p> <p>Please see additional clauses contained in sections 10.16, 10.17 and 10.18 of this Order Form.</p> <p><b>1. Open Source Publication</b> Pursuant to clause 34.1.4 of the Call Off Terms, the Parties agree that materials provided by the Supplier shall not be published Open Source without prior consultation and written agreement between the Parties both acting reasonably.</p> <p><b>2. Working Papers and Reports</b> Reports 2.1 Notwithstanding any other provision of this Call Off Contract, except where required by the FOIA or EIR, the Customer shall not: 2.1.1 attribute any non-Supplier branded Deliverable to the Supplier; without the Supplier's prior written consent.</p> <p>Internal Working Papers 2.2 The parties agree that, unless requested by the Customer, during the Call Off Contract Period the Supplier may retain possession of any internal drafts, notes, analyses, and other working papers prepared or generated by the Supplier in connection with the Services (the 'Working Papers').</p> <p>For the avoidance of doubt, the parties agree that under the terms of the Call Off Contract the Working Papers fall within</p>													

	<p>the meaning of Project Specific IPR and may be requested by the Customer, from time to time, during the Call Off Contract Period.</p> <p>2.4 The Supplier shall:</p> <p>(i) provide the Customer with the Working Papers on an as-requested basis; and</p> <p>(ii) unless otherwise agreed by the Customer in advance, provide the Working Papers to the Customer as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Customer.</p> <p><b>3. Audit Independence</b></p> <p><i>The Supplier shall notify the Customer immediately if there is a change in law, rule, regulation, professional standard or circumstance which the Supplier believes could compromise or conflict with its auditor independence obligations. Where a potential conflict has been identified the Supplier shall use its reasonable endeavours to mitigate the impact of any such circumstances and seek a work-around solution with the Customer. Where the circumstance/ conflict can not be mitigated by the Supplier the Supplier may terminate this Call off Contract by providing the Customer with as much advance written notice as is reasonably practicable in the circumstances.</i></p> <p><b>4. Design Phase</b></p> <p>Any clarification of, or changes to, section 5.4 of the bid response document embedded above shall be agreed by the Parties in writing within 14 days of the Commencement Date.</p>	
<b>10.12</b>	<p><b>Call Off Tender:</b></p> <p>In Schedule 16 (Call Off Tender)</p>	
<b>10.13</b>	<p><b>Publicity and Branding (Clause 36.3.2 of the Call Off Terms)</b></p>	
<b>10.14</b>	<p><b>Staff Transfer</b></p> <p>Annex to Schedule 10, List of Notified Sub-Contractors (Call Off Tender).</p>	
<b>10.15</b>	<p><b>Processing Data</b></p> <p>Call Off Schedule 17</p>	
<b>10.16</b>	<p><b>Milestone Change- Clause 23.3</b></p> <p>The following are the Customer's changes to Clause 23 of the Contract.</p> <p>23.3 Milestone Change</p>	

	<p>23.3.1 The Delivery Partner acknowledges that the Customer is under no obligation to proceed with any Milestone (excluding the Design Phase).</p> <p>23.3.2 Prior to the commencement of each Milestone, the Customer shall review the Delivery Partner's proposed changes to the relevant Milestone, Milestone Payment, Deliverables and any Deliverable criteria due under that Milestone (the "Milestone Proposal") which shall be submitted by the Delivery Partner as a Deliverable under in the Project Plan.</p> <p>23.3.3 The Delivery Partner shall provide the Customer with such additional information as the Customer shall reasonably require to enable it to undertake its review of the Milestone Proposal.</p> <p>23.3.4 The Customer shall Approve the Milestone Proposal where it is satisfied that:</p> <ul style="list-style-type: none"> <li>(a) that the Customer has the budget for the relevant Milestone Payment (and such budget may be subject to such internal check points and approvals as the Customer considers necessary);</li> <li>(b) that the Milestone Payment offers the Customer value for money; and</li> <li>(c) that the Deliverables have been agreed in accordance with the Acceptance Criteria.</li> </ul> <p>23.3.5 The Customer shall consult with the Delivery Partner but may impose such conditions on the Milestone Proposal as the Customer considers appropriate.</p> <p>23.3.6 Where the Customer Approves the Milestone proposal the Customer shall submit a Variation Form to the Delivery Partner with the revised Project Plan and any conditions the Customer considers necessary attached. The parties shall agree the Variation in accordance with Clause 23.1 but the Customer shall not be entitled to request an Impact Assessment.</p> <p>23.3.7 Where the Customer does not Approve the Milestone proposal or the Delivery Partner does not sign the Variation Form the Customer may terminate this Call Off Contract in accordance with Clause 42.11.</p> <p>23.3.8 The Delivery Partner undertakes any work and incurs any costs in respect of a Milestone that has not been Approved at its own risk and the Customer shall not be liable for any Delivery Partner costs that arise in respect of a Milestone that is not Approved by the Customer.</p>	
<b>10.17</b>	<p><b>Termination Provisions</b></p> <p>42.11 Termination due to non-commencement of a Milestone</p>	

	In the event that the Customer does not Approve a Milestone in accordance with Clause 23.3, the Customer shall be entitled to terminate this Call Off Contract with immediate effect by issuing a Termination Notice to the Delivery Partner.	
<b>10.18</b>	<p>New Clause 46.3</p> <p>46.3A Consequences of termination under Clauses 42.11 (Termination due to non-commencement of a Milestone)</p> <p>Where the Customer terminates this Call Off Contract under Clause 42.11 (Termination due to non-commencement of a Milestone), the Customer shall not be liable to pay any costs incurred or monies committed by the Delivery Partner in relation to any un-Approved Milestone unless the Customer has expressly agreed to such costs or monies being incurred.</p>	

Contract Reference:	Project [REDACTED]
Date:	January 2021
Description Of Authorised Processing	
Identity of the Controller:  [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]  UK Export Finance, 1 Horse Guards Road, London SW1A 2HQ  [REDACTED]  Identity of Processor:  <i>KPMG LLP, 15 Canada Square, London, E14 5GL</i>	The Parties acknowledge that for the purposes of the Data Protection Legislation the Customer is the Controller and the Delivery Partner is the Processor under this Framework Agreement.
Use of Personal Data	Managing the obligations under the Call Off Contract Agreement, including exit management, and other associated activities,
Duration of the processing	For the duration of the Framework Contract plus 7 years.
Nature and purposes of the processing	KPMG will not handle or process any personal identifiable information (PII) of UKEF employees or UKEF customers. Any

	access to UKEF-related PII data will be through UKEF-controlled systems, and KPMG will only view the data. The data will not be exported, handled and processed by KPMG.	
Type of Personal Data	Data associated with users, leads, opportunities, accounts and contacts”.	
Categories of Data Subject	Staff, contractors and temporary workers whom the Customer wishes to have access to the software.	

## FORMATION OF CALL OFF CONTRACT

BY SIGNING AND RETURNING THIS CALL OFF ORDER FORM (which may be done by electronic means) the Delivery Partner agrees to enter a Call Off Contract with the Customer to provide the Services in accordance with the terms Call Off Order Form and the Call Off Terms.

The Parties hereby acknowledge and agree that they have read the Call Off Order Form and the Call Off Terms and by signing below agree to be bound by this Call Off Contract.

In accordance with paragraph 7 of Framework Schedule 5 (Call Off Procedure), the Parties hereby acknowledge and agree that this Call Off Contract shall be formed when the Customer acknowledges (which may be done by electronic means) the receipt of the signed copy of the Call Off Order Form from the Delivery Partner within two (2) Working Days from such receipt.

For and on behalf of the Delivery Partner:

Name and Title	
Signature	
Date	

**For and on behalf of the Customer:**

Name and Title	
Signature	
Date	

# UKEF - Security Framework Policy

Title	UK Export Finance (UKEF) Security Framework Policy
Reference	Security & Information Management Committee
Version	1.1
Date reviewed	10 October 2019
Author	██████████
Owner	██████████

## **1.0 Introduction**

The UK Export Finance (UKEF) Security Framework provides an overview of the departments approach to ensuring the security of our people, assets and information. The framework includes a description of the pan-government security environment, overarching principles, and a commentary on UKEF's approach to the mandatory security outcomes set out by the Cabinet Secretary, these are:

- a) Governance
- b) Culture & Awareness
- c) Risk Management
- d) Information
- e) Personnel Security
- f) Physical Security
- g) Preparing for and Responding to Security Incidents
- h) Technology & Services

The framework is closely aligned to the wider Civil Service approach to security and in particular the "Security Policy Framework<sup>1</sup> (2018) "developed by the Cabinet Office and the "Government Security: Roles and Responsibilities<sup>2</sup> (2018)" document.



## 2.0 Government Security Accountability

The Prime Minister and Cabinet are ultimately responsible for the security of Government. Practical responsibility is delegated across HMG to the Cabinet Secretary, respective Ministers, Permanent Secretaries and Management Boards or Executive Teams.

HMG works closely with the intelligence agencies and other organisations to keep government safe. In particular, HMG organisations will consult the full range of policy, advice and guidance provided by the Cabinet Office, National Cyber Security Centre (NCSC), Centre for the Protection of National Infrastructure (CPNI), and the UK National Authority for Counter-Eavesdropping (UKNACE), which are the UK National Technical Authorities for cyber, personnel, and physical security, and technical protective security, respectively.

The Government's clusters model is evolving and (as at September 2019) a Centre's of Excellent approach is being piloted where specialised consultancy and advisory services are offered by the lead departments.

- Cluster 1 (led by HMRC): Cyber advice and consultancy
- Cluster 2 (Home Office): Physical and Personnel advice and consultancy
- Cluster 3 (DWP): Education and Awareness advice and consultancy
- Cluster 4 (MoD and FCO): Defence and International advice and consultancies

UKEF is a member of Cluster 4, both the Director of Resources and the Head of Security are part of

the clusters formal governance arrangements. Other sources of international standards and good practice also shape business specific approaches.

1 [HMG Security Policy Framework Version 1.1](#)

2 [Government Security: Roles and Responsibilities Version 1.0](#)

### **3.0 Overarching Principles**

The following are the key principles identified by the Cabinet Office for implementing government

security: -

- The organisation's Accounting Officer is formally accountable, under the Security Policy Framework, for ensuring the security of the organisation and its assets;
- Organising and delivering effective security must be based on a clear understanding of the organisation's assets, for example, people, information, intellectual property or physical assets – and a strong security risk management culture which seeks to identify, manage and mitigate security risks in accordance with the security standards;
- Responsibility for the identification and management of security risks sits with the relevant Board or Executive Team member who is accountable for the delivery of that area of the department's business.
- In delivering against these principles, it is expected that the designated Board Member or Accountable Official, working with their Senior Security & Resilience Adviser, adhere to the principles set out in the minimum-security standards to ensure any security incidences and breaches are properly managed, recorded and reported.

This should be supported by an annual reporting process on security performance measurement and an appropriate level of commonality across government and should be linked to each organisation's internal audit and annual audit, and risk assurance governance and processes.

#### **4.0 Security Outcomes:**

##### **4.1 Governance:**

Each government organisation is required to have an appropriate security governance structure in place to support the Accounting Officer.

Formal governance at UKEF is provided via the Security & Information Management Committee (SIMC), this is chaired by the Director of Resources and the group's terms of reference are available on the staff intranet. SIMC is responsible for ensuring that the assets required for UKEF's business operations, systems and processes are appropriately secured in accordance with UKEF, legal, regulatory and central government requirements. It is a sub-committee of the Executive Committee (EC). SIMC is also responsible for ensuring that appropriate and effective risk managed policies and processes are in place across the eight Security Outcomes.

The Government Security Roles & Responsibilities document sets out a number of roles that

departments should have in place:

Appropriate Board Member, or Executive Director, to discharge oversight and responsibility for security risk management. In UKEF this is the Director of Resources who is also the Senior Information Risk Owner (SIRO).

Security & Resilience Adviser (SA): The Security Adviser is responsible for articulating the security needs of their department, overseeing and reporting on the delivery of services to agreed standards, including being the responsible owner for local security policies. They will be acting as an intelligent customer for their department appropriating services from their Cluster Security Unit as necessary.

The role supports the Department's security infrastructure and procedures through recognition of the security profession and its functional standards and by securing funding for professional training, qualifications and continuous development. In UKEF this role is undertaken by the Head of Security.

Risk Owners (RO): Heads of Division or other UKEF staff who on a day-to-day basis are responsible for the delivery of a function, service, programme or project, and who take operational decisions in direct response to risk, not just limited to security.

Information Asset Owners (IAO): Named senior individuals responsible for each identified information asset (e.g. database or ICT system) at the appropriate business level within a

Department/Agency.

UKEF's Information Asset Register including relevant IAO's is maintained by the Business Insight Centre and is available [on the staff intranet](#).

**Data Protection Officer (DPO):** An enterprise security leadership role required by data protection legislation. DPOs are responsible for advising accounting officers and senior boards (e.g. ExCo) about the organisation's compliance with data protection law and best practice including explaining residual risk and addressing privacy requirements. To avoid conflicts of interest, this role should not deliver or oversee design or implementation of data protection policies.

UKEF's Data Protection Officer is the Head of Compliance.

**Chief Information Security Officer (CISO):** The CISO should advise the Board on how best to exploit technology to deliver the organisation's strategic objectives and provide strong strategic leadership for the organisation's IT community and its investment in technology. They will be responsible for a departments IT strategy, IT architecture, IT policies and standards, technology assurance and IT professionalism. UKEF is not formally adopting the CISO role in its Security Framework but notes that the activities highlighted fall within the remit of the Head of Technology, Change & Innovation.

## **4.2 Culture & Awareness**

The Accounting Officer is responsible for maintaining a positive security culture at UKEF and is supported by a wide range of colleagues including the Head of Security in delivering against this objective.

A rolling programme of communications is in place to promote a strong security culture and this is subject to external measurement by the Cabinet Office.

Security related training is triaged via the UKEF Learning & Development team. This includes mandatory e-learning on handling information. [SAFE Security Training](#) is mandatory for staff travelling to locations identified as being high risk from a personal security perspective.

The Security team will work with colleagues from external agencies including NCSC, CPNI and the Met Police to deliver organisational wide learning on security related topics.

All UKEF's security related policies and procedures are available on the staff intranet and are the responsibility of the Security team.

## **4.3 Risk Management**

UKEF has an Assurance Framework and operates a "three lines of defence" model for risk management in the department. The model defines the sources of assurance into three broad categories:

- **First Line** - the business (all UKEF teams) own and manage the processes, procedures risks and controls on a day to day basis. Assurance is provided via outputs including performance indicators, management information, business metrics, supervisory checks and controls.

□ Second Line – is represented by teams including Risk Management Group, Legal, Compliance Security and some parts of Finance. These are Divisions which are part of the management chain but provide independent oversight of management activity. Assurance is provided via outputs objective assessments or reviews to determine whether compliance with defined requirements are being met.

□ Third Line – is represented by Internal and External Audit teams, and other Civil Service

(typically, HMT or Cabinet Office) or parliamentary scrutiny processes who provide independent and objective assurance of UKEF's governance, risk management and control environment. Assurance outputs include independent reviews of the highest areas of risk, or where there are gaps and weaknesses in business processes.

The UKEF Assurance Framework is a key management tool for Divisions in understanding their risks and controls and in focussing management attention on areas of risk or control requiring specific intervention to ensure the delivery of key business strategies.

It is a key component of the UKEF Enterprise Risk Framework and will be co-ordinated by the Enterprise Risk Division. It seeks to provide reliable assurance (evidence) on organisational stewardship and the management of major UKEF risks by sample testing & examining key controls detailed in the RACA (risk registers) & validating statements made in the self-certification process (CEC).

It provides Divisions with an independent review at a point in time as to whether key Divisional Policies, Processes & Procedures are being adhered to and Divisional controls are embedded as defined.

The Security team maintain a Risk Register for departmental wide security risks. Individuals

divisional risk registers also identify security related risks. This ensures the department has an understanding of security risks facing the organisation, have identified potential mitigatory actions and are aware of the level of residual risk remaining.

The Security Committee takes an overview all security and information related risks throughout UKEF via the centrally produced (Resources Division) Security Risk Register.

A Risk Appetite Statement is in place regarding Cyber and Fraud risk.

The department has a small security team who are specialists who provide advice on all security and resilience related activities.

#### **4.4 Information**

UKEF has an Information Management Framework which provides a high-level view of the

department's information management structure and direction for information management

practice in UKEF. The framework also includes details of roles and responsibilities for managing information in the department.

The Department also has a Data Protection Policy which sets out what UKEF is required to do to ensure that all staff who process personal data do so in accordance with the Data Protection Legislation.

UKEF's Information Asset Register including relevant IAO's is maintained by the Business Insight Centre and is available [on the staff intranet](#).

All staff are required to undertake training on managing information, the type of training undertaken is role specific. Standard government information classification system is employed by the department.

Risk assurance is provided in line with UKEF's Assurance Framework (2019) and via a 6-monthly reporting to the Security & Information Assurance Committee.

#### **4.5 Personnel Security**

The Security team are responsible for Personnel Security with support from colleagues in the Resources Division. The Department has a [Personnel Security Plan](#) which is available on the staff intranet.

Vetting procedures are in place and all UKEF staff are cleared to a minimum of Counter Terrorism Cleared (CTC) level. Role based risk assessments mean that a number of staff are required to be cleared to Security Check (SC) or Developed Vetting (DV) level.

Contractors who will be provided access to the UK Export Finance network must be cleared to SC level.

A risk-based assessment is undertaken on the results of any security clearance and where an individual is refused an appeals process is on place.

#### **4.6 Physical Security**

HM Treasury are responsible for providing all aspects of physical security at 1 Horse Guards Road.

The Head of Security acts as the UKEF lead for this contract and is a member of the buildings Incident Management Team. UKEF has [procedures in place for managing visitors](#) to the building and all staff are required to wear passes when in the building.

UKEF also has clear [procedures in place to support staff working remotely](#) and extensive advice relating to security whilst travelling abroad including a dedicated "[Travel Hub](#)" on the staff intranet.

The department has clear policies and procedures covering UKEF staff travelling and working overseas. A risk assessments process is in place which is completed prior to travelling. Staff visiting high risk locations are required to

undertake “SAFE” training. The department works closely with colleagues from across government including the CPNI and FCO to ensure robust security arrangements are in place.

The Security team are responsible for the security of UKEF devices both in the UK and overseas. The team monitor and report on loss or damage to devices.

#### **4.7 Preparing for and Responding to Security Incidents**

The Head of Security is responsible for coordinating business continuity arrangements to facilitate a rapid and effective response to recover from incidents.

Each Division at UKEF has a Business Continuity Plan and a named Business Continuity Coordinator.

The UKEF Incident Management Team is chaired by the Director of Resources and includes named representatives from across the department. UKEF also has an overarching Incident Management Plan in place.

The Head of Security is responsible for recording any security incidents or breaches including loss of IT equipment, loss of security passes, unauthorised disclosures and breaches of official information.

Mechanisms exist via the departmental Data Protection Officer to report relevant breaches to the Information Commissioner’s Office where required.

Further information regarding UKEF’s approach to business continuity and incident management is available on [the staff intranet](#).

#### **4.8 Technology and Services**

Responsibility for the security of IT assets and services is shared between the Technology Change & Innovation (TCI) Division and the Security team (Resources Division). A more detailed breakdown is provided in Table 1. UKEF does not have any technology or services that are part of the Critical National Infrastructure.

The TCI are responsible for the provision and maintenance of all IT equipment and standard services. Centrally provisioned applications are also the responsibility of TCI whether they are externally supplied or bespoke developments (excluding EUD’s). Within TCI the Service Delivery team support a number of security related activities.

The Security team are responsible for the safety of UKEFs assets and staff, whilst in the UK and overseas. To enhance the departments cyber security capability a Security Operations Centre has been created to monitor and detect threats to our IT infrastructure.

Table 1

	<b>Security Team</b>	<b>Technology Change &amp; Innovation</b>

Policy and procedures	Devising Security Framework and related policies including Email & Internet Acceptable User Policy, Mobile Devices Policy, UKEF Password Policy, Secure Remote Working Policy, Information Security Policy and Security Incidents Procedure.	Devising overall IT Strategy. Publication of users guide for UKEF hardware and centrally managed software.
Patch Management & Penetration Testing	Assurance role, monitoring the performance of the department on patching and reporting outcome to Security Committee. Responsible for pen testing as required.	Ensuring patching takes place as and when it becomes due for centrally managed IT contracts. This includes managing the 3 <sup>rd</sup> party providers responsible for patching.
Threat Management	A Security Operations Centre will become operational in November 2019 and will ensure that dedicated UKEF resources are allocated to horizon scanning, monitoring, detecting, containing and remediating IT threats across critical applications, devices and systems.	Working with Security and third-party suppliers to respond to and remedy identified issues
Incident Management Team (IMT)	Chair (Director of Resources), strategic lead and co-ordinate activities of the IMT.	Be represented at IMT, act as subject matter expert for IT, lead on IT operational response.
IT Assets, including phones and laptops	Protect assets from unauthorised access, misuse, manipulation or destruction. Record any loss of equipment and report findings to the Security and Information Management Committee.	Responsible for needs identification, procurement, configuration and allocation of IT assets. Providing technical advice to Security on wider implications of any solutions they wish to deploy.



Change related IT security	Undertaking risk assessments and responsible for pen testing process.	Support the wider change programme
Back up and restoration of systems	Provide advice and testing arrangements as necessary.	Ensure back up and restoration arrangements are actively in place for all UKEF IT system.
Wider Civil Service	“Own” relationship with Cluster 4, NCSC, CPNI, GCHQ and any other government bodies engaged in cyber security.	Work collaboratively with government bodies engaged in cyber security as and when necessary.