Requirement ID	Requirement Specification	Requirement Type
3.2	**Branding and Publicity**	
This section covers those requirements relating to strict guidelines regarding the use and display of ERDF logos on all publicity materials.		
A.7	The Supplier shall ensure that the DIT and ERDF corporate branding as set out in the ERDF Branding and Publicity Requirements and provided by DIT and MHCLG from time to time are used exclusively at all times across all Communications.	**Mandatory**
A.8	The Supplier shall ensure that all Branding and Publicity Requirements are complied with in line with EU Regulations and National ESIF Guidance. The consequences of non-compliance may lead to repayment of the total sum of the funding in accordance with clause 10.8 and 10.9 of the Agreement.	**Mandatory**
A.9	The Supplier shall ensure that all Branding and Publicity Requirements are complied with in line with EU Regulations and National ESIF Guidance. The consequences of non-compliance may lead to repayment of funding.	**Mandatory**
A.10	The Supplier shall establish and operate an ESIF compliant approach to all external communications with DIT, the EITA Supplier(s) and SME Applicants and any other party as nominated by DIT, taking account of DIT guidance on branding and promotion and ensuring compliance with EU regulations and National ESIF Guidance	**Mandatory**
3.3	**Reporting of grant information across government**	
This section covers those requirements relating to the recording and reporting of grant information across government via the Government Grants Information System (GGIS) which aims to provide accurate data to enable departments to manage grants efficiently and effectively, while actively reducing the risk of fraud. Full training in use of GGIS will be provided by Cabinet Office either in London or at the Supplier's own premises (subject to discussion).		
A.11	The Supplier shall ensure that all Data related to each ESIF Project and SME Applicant is published on GGIS under the relevant ESIF Project in accordance with the GGIS requirements (as updated from time to time).	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
A.12	The Supplier shall ensure that SME Applicants are notified that the Supplier needs to comply with the FOIA, which allows general right of access to all types of recorded information held by public authorities.	**Mandatory**
A.13	The Supplier shall ensure that the SME Applicants notify the Supplier of any information which they consider to be eligible for exemption from disclosure under the FOIA. Such information must be referred to as "Reserved Information" and identified in the SME Applications.	**Mandatory**
A.14	The Supplier shall ensure that Reserved Information and any other information which is classified as Reserved Information is redacted prior to publication by GGIS. All decisions relating to the exemption and disclosure of information shall be notified to the Applicant.	**Mandatory**
A.15	The Supplier shall ensure that grant awards are uploaded to the GGIS monthly or more frequently if volume of entries dictates.	**Mandatory**
A.16	The Supplier shall ensure each SME Applicant is allocated a unique reference number for all communications; this identifier shall have the following characteristics: • [redacted]	**Mandatory**
3.4 Managing ERDF Projects		
This section covers those requirements relating to the managing of ERDF Projects		
A.17	The Supplier shall comply with European Structural and Investment Funds counter fraud guidance (part of National ESIF Guidance) as may be amended or superseded by equivalent guidance from time to time.	**Mandatory**
A.18	The Supplier shall collaborate with DIT to manage each ESIF Project in accordance with the European Regional Development Fund requirements. This shall include but will not be limited to: • maintain a Risk Register by ESIF Project;	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
	• clear audit trails and financial management; • ensuring each ESIF Project is managed discretely (i.e. separate cost centres and reporting); and • monitoring and real-time reporting of co-financing availability (by LEP), and Enterprises Supported (by LEP) to DIT and the EITA Supplier(s) to manage SME Applications accordingly.	
A.19	The Supplier shall work collaboratively with DIT to ensure delivery of the ESIF outputs and compliance with the ESIF expenditure requirements.	**Mandatory**
A.20	The Supplier shall establish and operate a management information system for each ESIF Internationalisation Fund project, which captures all required electronic data to ensure ESIF compliance, and meets the data requirements set out by DIT in accordance with Schedule 11: Processing Personal Data; Schedule 8.4: Reports and Records Provisions; and Schedule 2.4: Security Management.	**Mandatory**
A.21	The Supplier shall ensure that the management information system allows DIT access to documentation relating to SME Applicants in an efficient and effective manner and supports DIT's sample checking process.	**Mandatory**
A.22	The Supplier shall allow DIT access to all ESIF Project related data and documentation at all times.	**Mandatory**
A.23	The Supplier shall ensure all ESIF Project documentation is managed, retained and stored in accordance with National ESIF guidance (as published and updated on gov.uk) and EU regulations; Schedule 11: Processing Personal Data; Schedule 8.4: Reports and Records Provisions; and Schedule 2.4: Security Management.	**Mandatory**
3.5 Summative assessments		
There is a requirement for all successful ESIF Applicants (in this case DIT) to undertake a summative assessment.		

Requirement ID	Requirement Specification	Requirement Type
A.24	The Supplier shall collaborate with DIT and the Summative Assessor to assist the delivery of a compliant Summative Assessment for each ESIF Internationalisation Fund project, including the capture of mandatory Summative Assessment data.	**Mandatory**
3.6 European Structural and Investment Funds: outputs and results		
The European Structural and Investment Funds Growth programme is funding for projects that create jobs and support local growth.		
A.25	The Supplier shall ensure that they record ESIF Outputs Data (subject always to this Agreement) to be evidenced in accordance with National ESIF Output guidance (as published and updated on gov.uk).	**Mandatory**
A.26	The Supplier shall supply real time updates on actual and forecast project expenditure and output performance at LEP levels (and at Category of Region level within the LEP, where applicable).	**Mandatory**
A.27	The Supplier shall work collaboratively with DIT to ensure delivery of the ESIF outputs and compliance with the ESIF expenditure requirements.	**Mandatory**

4. SME APPLICATION & AWARD

Requirement ID	Requirement Specification	Requirement Type
This section covers those requirements relating to how the Supplier will help the EITA Supplier(s) to identify suitable SMEs for ESIF Internationalisation Fund co-financing by providing guidance, training and other helpful interventions as agreed with DIT and the EITA Supplier(s).		
4.1 Facilitating with identifying suitable & eligible SME Applicants		
B.1	The Supplier shall develop and provide guidance on eligibility and suitability of SME Applicants for ESIF Internationalisation Fund co-financing for the EITA Supplier(s) to identify eligible and suitable SME Applicants. Any such guidance shall be updated from time to time as part of a continuous improvement process and in accordance with any amended National ESIF Guidance.	**Mandatory**
B.2	The Supplier shall develop and provide guidance on eligibility of Expenditure for ESIF Internationalisation Fund co-financing for the EITA Supplier(s) (from time to time as updated) in accordance with ESIF Internationalisation Fund guidelines.	**Mandatory**
4.2 Guidance for selecting private sector provider		
This section covers those requirements relating to how the supplier will help the SME Applicants identify or source suppliers for the support that required ESIF Internationalisation Fund co-funding.		
B.3	The Supplier shall develop and provide guidance to help the SME Applicants with a process of selecting a private sector provider with respect to the co-financing. Any such guidance shall be compliant with EU regulations and National ESIF Guidance.	**Mandatory**
B.4	The Supplier shall develop and make available best practice guidance to help SME Applicants manage private sector providers funded through the ESIF Internationalisation Fund.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
4.3 Reviewing SME Application(s)		
SMEs applying for ESIF Internationalisation Fund co-investment funding will be subject to a financial due diligence assessment. This assessment tests the financial health of the applicant organisation, its on-going sustainability, its ability to manage the cash flow requirements of ESIF Internationalisation Fund co-investment funding, and its ability to repay ESIF Internationalisation Fund co-investment funding if necessary. The due diligence assessment will include an assessment of whether the undertaking is an undertaking in difficulty. Organisations identified as being undertakings in difficulty are ineligible for ESIF Internationalisation Fund support and their application will be rejected. This section covers those requirements relating to how the Supplier will review SME Applicants' ESIF Internationalisation Fund co-investment funding.		
B.5	The Supplier shall develop and comply with processes in accordance with the ESIF Internationalisation Fund guidelines for the SME Application Process and shall submit such processes to DIT for Assurance before the Operational Service Commencement Date and operate for the Term of this Agreement.	**Mandatory**
B.6	The Supplier shall develop and provide guidance on the SME Application Process (ensuring compliance with EU Regulations and National ESIF Guidance) for SME Applicants and the EITA Supplier(s).	**Mandatory**
B.7	The Supplier shall develop and regularly communicate best practice approaches that help improve the quality of SME Applications for SME Applicants and the EITA Supplier(s).	**Desirable**
B.8	The Supplier shall develop and comply with processes in accordance with EU Regulations and National ESIF Guidance for checking eligibility and suitability of SME Applications, and shall submit such processes to DIT for Assurance before the Operational Service Commencement Date and operate for the Term of this Agreement.	**Mandatory**
B.9	The Supplier shall check the suitability of SME Applicants and the proposed activity to be funded.	**Mandatory**
B.10	The Supplier shall check the SME Application to ensure compliance with EU State Aid Regulations.	**Mandatory**
B.11	The Supplier shall establish and operate a process to ensure SME Applicants are not "in difficulty" as defined by EU State Aid Regulations.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
B.12	The Supplier shall check that the SME Applicant's project has not already started prior to an SME Application being submitted, ensuring compliance with GBER.	Mandatory
B.13	The Supplier shall, before awarding SME Applicant's co-funding, shall assess the SME's Application with reference to a set of mandatory exclusion grounds, equivalent to those set out in regulation 57(1)-(3) of the PCR, to determine the suitability of a SME Applicant. The detailed grounds for mandatory exclusion of an organisation are set out in Annex1 (Grounds for mandatory exclusion) of this Schedule as may be amended or superseded by equivalent legislation.	Mandatory
B.14	The Supplier shall check SME Applications for eligibility of proposed activity and related expenditure in line with EU Regulations and National ESIF Guidance.	Mandatory
B.15	The Supplier shall ensure the SME Application process identifies how the proposed activity to be co-financed by ESIF Internationalisation Fund co-investment funding addresses DIT barriers to export in a measurable and qualitative way.	Mandatory
B.16	The Supplier shall check the rules of Additionality for each SME Application.	Mandatory
B.17	The Supplier shall ensure that the SME Application process captures and reports the relevant equality and diversity information in accordance with the National ESIF Guidance and Schedule 11: Processing Personal Data.	Mandatory
B.18	The Supplier shall perform an assessment of SME Application(s) for either award or rejection of ESIF funding. Each outcome shall include a justification for the decision which must be communicated to the SME Applicant.	Mandatory
B.19	The Supplier shall resolve any SME Application errors with the SME Applicant, and inform the relevant EITA Supplier's Personnel responsible for supporting the SME Applicant.	Mandatory

Requirement ID	Requirement Specification	Requirement Type
4.4	**Carry out due – diligence (including fraud risk assessment)**	
B.20	The Supplier shall establish and operate a process to verify the professional standing of private sector providers suppliers.	**Mandatory**
B.21	The Supplier shall establish and operate a process to prevent potentially fraudulent activity related to SME co-investment awards and report any findings or concerns to DIT.	**Mandatory**
B.22	The Supplier shall supply DIT with the required volume of approved SME Applications to meet DIT Sample Checking Requirements.	**Mandatory**
4.5	**Agree co-investment conditions**	
B.23	The Supplier shall establish comprehensive funding Terms and Conditions which shall include as a minimum a full right of audit and an obligation to provide impact data and participate in any project surveys.	**Mandatory**
4.6	**Award co-investment funding**	
B.24	The Supplier shall develop and issue an ESIF compliant Funding Offer to individual SME Applicants, ensuring the relevant EITA Supplier's Personnel is informed.	**Mandatory**
B.25	The Supplier shall establish and operate a transparent funding rejection process.	**Mandatory**
4.7	**Appeals & Complaints**	
This section sets out the requirements for processing appeals and complaints		
B.26	The Supplier shall ensure that the process for receiving and processing Appeals is the same for all the ESIF Internationalisation Fund regional projects	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
B.27	The Supplier shall submit to DIT for Approval (prior to being implemented) its proposals for and, when Approved, implement a process for dealing with SME Applicant complaints in accordance with DIT's complaints process and procedure.	**Mandatory**
B.28	The Supplier shall submit to DIT for Approval (prior to being implemented) its proposals for and, when Approved, implement a process for dealing with SME Applicant appeals with respect to the co-financing decision in accordance with DIT's complaints process and procedure.	**Mandatory**
B.29	The Supplier shall process and respond to appeals made by the SME Applicants	**Mandatory**

5. CLAIMS, PAYMENT & CLOSE-OUT

Requirement ID	Requirement Specification	Requirement Type
5.1	**Monitor the co-investment & conditions**	
C.1	The Supplier shall establish and operate a variation process where a SME Applicant can request an increase or decrease in amount of co-financing offered, within acceptable parameters to be defined by the Supplier in accordance	**Mandatory**
C.2	The Supplier shall establish and operate a system to monitor funding variations, funding attrition levels and lapsed offers.	**Mandatory**
5.2	**Validate & Pay Award (Co-financing Claim Process)**	
C.3	The Supplier shall develop and provide guidance on the Co-financing Claim Process (from time to time as ESIF National guidelines are updated and amended) for SME Applicants and the EITA Supplier(s).	**Mandatory**
C.4	The Supplier shall submit to DIT for Approval (prior to being implemented) its proposals for and, when Approved, implement a Co-financing Claim Process in accordance with ESIF National guidelines.	**Mandatory**
C.5	The Supplier shall ensure that the ESIF Internationalisation Fund Co-financing Claim Process only allows one claim per SME Applicant.	**Mandatory**
C.6	On receipt of a Co-Financing Claim by the SME Applicant the Supplier shall assess and verify eligibility and accuracy of the claim in accordance with ESIF Internationalisation Fund guidelines.	**Mandatory**
C.7	The Supplier shall ensure all SME claims include all required supporting evidence in accordance with ESIF Internationalisation Fund guidelines.	**Mandatory**
C.8	The Supplier shall resolve any SME claim errors with the SME Applicant and inform the relevant personnel from the EITA Supplier.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
C.9	Where an SME Applicant claim is Approved, the Supplier shall make payment within thirty (30) calendar days.	Mandatory
C.10	The Supplier shall record the authorisation of payments.	Mandatory
C.11	The Supplier shall establish and operate a claim rejection process.	Mandatory
C.12	The Supplier shall retain all SME claim and payment evidence in accordance with ESIF Internationalisation Fund guidelines.	Mandatory
C.13	The Supplier shall supply DIT with the required volume of approved SME claims to meet DIT sample checking requirements.	Mandatory
5.3 Evaluate & Close-out		
C.14	The Supplier shall develop and carry out a suitable SME evaluation and close out process to ensure ESIF compliant evidence of all ESIF Internationalisation Fund outputs is collected and retained in accordance with Schedule 11: Processing Personal Data; Schedule 8.4: Reports and Records Provisions; and Schedule 2.4: Security Management.	Mandatory
C.15	The Supplier shall record and monitor ESIF Internationalisation Fund output performance for all individual SME Applicants in accordance with Schedule 11: Processing Personal Data; Schedule 8.4: Reports and Records Provisions; and Schedule 2.4: Security Management.	Mandatory

6. POST - AWARD

Requirement ID	Requirement Specification	Requirement Type
6.1	**Reclaiming Funds from MHCLG**	
D.1	The Supplier shall complete monthly Transaction List templates to support DIT's claims to MHCLG.	**Mandatory**
D.2	The Supplier shall assist DIT in making its quarterly claims to MHCLG, including the desk based administrative check (such as to help DIT respond to any challenges from MHCLG).	**Mandatory**
6.2	**Resolve Queries**	
D.3	The Supplier shall assist DIT in answering specific MHCLG enquiries in a timely manner to ensure DIT meet MHCLG timescales.	**Mandatory**
D.4	The Supplier shall, where requested by DIT, attend meetings with MHCLG or other auditors.	**Mandatory**
D.5	The Supplier shall assist DIT in any Project Change Request process with MHCLG.	**Mandatory**
6.3	**Award & Benefit Reporting**	
D.6	The Supplier shall record SME total project costs, funding sought and match contributions and the data points from the SME Application.	**Mandatory**
D.7	The Supplier shall capture SME Postcodes, LEP Area, Category of Region, business activity, any rural establishments and LEP sector data.	**Mandatory**
D.8	The Supplier shall assist DIT with its monitoring and reporting by assembling comprehensive evidence / narratives of business impacts achieved.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
D.9	The Supplier shall work with DIT Analysts to continuously improve reporting of business impacts.	Mandatory
D.10	On request the Supplier shall supply all required information and data to the Summative Assessment contractor.	Mandatory
D.11	The Supplier shall allow DIT access to all project management information and project documentation at all times.	Mandatory
D.12	The Supplier shall monitor and report progress on sustainability and equal opportunity data in line with MHCLG requirements.	Mandatory
D.13	The Supplier shall capture all Summative Assessment data requirements using the template provided by DIT from MHCLG.	Mandatory
6.4 Accounting		
D.14	The Supplier shall supply real time updates on actual and forecast project expenditure and output performance at LEP level.	Mandatory
D.15	The Supplier shall work collaboratively with DIT to ensure delivery of ESIF expenditure and outputs.	Mandatory
6.5 Audit & Manage Compliance		
D.16	The Supplier shall work with DIT to maintain the project Risk Register.	Mandatory
6.6 Request Co-Investment Reimbursement		
D.17	The Supplier shall send individual project invoices covering the most recent month's activity to DIT by the end of the first working week of the following month.	Mandatory
D.18	Not Used	~~Mandatory~~

ENGROSSED CONTRACT FINAL v2.0

Requirement ID	Requirement Specification	Requirement Type
D.19	The Supplier shall ensure each invoice includes a separate line showing the total amount of ESIF SME Funding expenditure defrayed in the relevant period.	**Mandatory**

7. REPORTING & OPERATIONS

Requirement ID	Requirement Specification	Requirement Type
7.1 Reporting & Operations		
E.1	The Supplier shall establish and operate a process which identifies and reports any present and emerging issues to DIT.	**Mandatory**
E.2	The Supplier shall establish and operate a continuous improvement approach to support the EITA Supplier(s) in delivering eligible, suitable and quality SME funding applications, including addressing any training needs.	**Mandatory**
E.3	The Supplier shall establish, operate and monitor a system to manage levels of funding attrition, lapsed offers and funding variations and provide monthly reports to DIT.	**Mandatory**
E.4	The Supplier shall establish and operate a project reporting system which ensures DIT is able to meet all DIT Internal, MHCLG, External Auditor, LEP or any other partner or stakeholder requirements	**Mandatory**
E.5	The Supplier shall provide monthly reports for DIT. This shall include but not be limited to: • Number of Applications received per LEP area (and, where relevant, Category of Region within that LEP area) • Number of Funding Offers made per LEP area (and, where relevant, Category of Region within that LEP area)	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
	• Number of Applications rejected per LEP area (and, where relevant, Category of Region within that LEP area) • Number of SME Applicant claims paid per LEP area (and, where relevant, Category of Region within that LEP area) • Total Value of Funding Offered per LEP area (and, where relevant, Category of Region within that LEP area) • Total Value of Funding Paid per LEP area (and, where relevant, Category of Region within that LEP area) • Number of Enterprises Supported per LEP area (and, where relevant, Category of Region within that LEP area) • Total Value of Private Sector Match Funding per LEP area (and, where relevant, Category of Region within that LEP area) • Increase in Employment per LEP area (and, where relevant, Category of Region within that LEP area) • Number of New Enterprises Supported (London ESIF Internationalisation Fund project only) This report should include monthly and cumulative data and shall be subject to amendment in accordance with the provision set out in Schedule 8.1 (Governance).	
E.6	The Supplier shall provide relevant EITA Suppliers' personnel real time access to information. This shall include but not be limited to: • Number of Applications Received • Number of Funding Offers made	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
	• Total Value of Funding Offered • Total Value of Funding Paid • Number of Enterprises Supported and (for London ESIF Internationalisation Fund project only Number of New Enterprises Supported), for any LEP area and (where relevant) Category of Region within that LEP area.	
E.7	On request the Supplier shall prepare reports to meet MHCLG and DIT internal and external needs.	**Mandatory**
E.8	The Supplier shall assist with quarterly reporting to regional ESIF Project Advisory Groups, LEPs and Growth Hubs.	**Mandatory**
E.9	The Supplier shall establish and operate an ESIF compliant approach to external communications with DIT, the EITA Supplier(s) and SME Applicants and any other party as nominated by DIT, taking account of DIT guidance on branding and promotion.	**Mandatory**
E.10	Where required, the Supplier shall support DIT with all external interactions, with but not limited to, MHCLG, LEPs and Growth Hubs.	**Mandatory**
E.11	Where required, the Supplier shall support DIT with all internal interactions and requests, with but not limited to, other DIT directorates, regional Heads of Export, regional teams, ministerial briefings and policy developments.	**Mandatory**
E.12	The Supplier shall attend all meetings as requested by DIT, including but not limited to Project Initiation Visits, ESIF Project Advisory Groups, DIT contract meetings, and meetings with MHCLG or external Auditors.	**Mandatory**
E.13	The Supplier shall create a central point of contact for all project related enquiries from DIT and EITA Supplier(s).	**Mandatory**
E.14	The Supplier shall be responsible and accountable for the provision of competent personnel and staff employed by any sub-contractor.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
E.15	The Supplier shall develop a suite of guidance materials for SME beneficiaries and ITAs to support the delivery of a compliant, efficient and quality fund administration process, including a comprehensive set of FAQs.	**Mandatory**
E.16	The Supplier shall create all required project documentation, including associated terms and conditions to ensure compliant delivery of a fully managed ESIF Internationalisation Fund service.	**Mandatory**
E.17	In collaboration with DIT, the Supplier shall develop an ESIF compliant impact evidence collection approach which takes account of the impact and outcomes listed in the project logic model.	**Mandatory**
E.18	The Supplier may be required to collaborate with DIT to develop a project brand for the external presentation of the project.	**Desirable**
E.19	The Supplier shall help DIT meet or exceed all ERDF Output Targets (in accordance with Annex 3: ESIF output and allocation summary), whilst ensuring that LEP level fund allocations are not exceeded.	**Mandatory**
E.20	The Supplier shall be required to provide an SME Funding application decision to beneficiaries within five (5) days of receipt.	**Mandatory**
E.21	The Supplier shall be required to respond to all DIT, SME and EITA Supplier(s)' enquiries within twenty-four (24) hours of receipt.	**Mandatory**
E.22	The Supplier shall be required to demonstrate how all SME Applicant processes are designed to ensure the minimum burden on business.	**Mandatory**
E.23	The Supplier shall ensure that all monthly and quarterly reports are delivered no later than five (5) Working Days after the reporting period end date.	**Mandatory**

8. INFORMATION GOVERNANCE

Requirement ID	Requirement Specification	Requirement Type
This section covers the generic requirements applicable to the Supplier in relation to Information Governance.		
8.1	**Data Retention**	
F.1	The Supplier shall comply with all DIT's specific requirements relating to retention periods for all Data to be agreed during implementation, ensuring compliance with EU Regulations and National ESIF Guidance.	**Mandatory**
F.2	The Supplier shall securely delete all Data at the expiry of its retention period, in accordance with Schedule 11: Processing Personal Data; Schedule 8.4: Reports and Records Provisions; and Schedule 2.4: Security Management.	**Mandatory**
F.3	The Supplier shall ensure that all Data deleted at the expiry of its retention period cannot be accessed by anyone. Data held on paper shall be securely shredded and Data held electronically.	**Mandatory**
8.2	**Data Protection**	
F.4	The Supplier shall ensure that the Virtual Library complies with this Service Description, and Schedule 8.4 (Reports and Records Provisions).	**Mandatory**
F.5	The Supplier shall collect and process Personal Data only in accordance with the instructions and directions given by DIT and in accordance with Data Protection Legislation.	**Mandatory**
F.6	The Supplier shall protect all Personal Data against unauthorised and unlawful processing, accidental loss, alteration, destruction and damage in accordance with Data Protection Legislation.	**Mandatory**
F.7	The Supplier shall use a Privacy Notice in the format to be agreed with DIT.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
F.8	The Supplier shall ensure that the Privacy Notice is updated upon request by DIT within five (5) days of such request at no cost to DIT.	**Mandatory**
F.9	The Supplier shall immediately escalate and report all complaints relating to unauthorised and unlawful processing of accidental loss of, alteration, destruction and damage to Personal Data to DIT in accordance with Schedule 2.4: Security Management and this Service Description.	**Mandatory**
F.10	The Supplier shall notify DIT within five (5) Working Days of all changes to all processes and activities (including locations where they may be undertaken) that will require DIT to update its notification on the ICO Register of Data Controllers.	**Mandatory**
8.3 Data Protection Audit		
F.11	The Supplier shall submit to DIT for Approval, and when Approved, comply with, a Data Protection audit plan. The plan shall include: • timescales for preparation and conduct of the annual audit; and • the audit strategy and planned outputs.	**Mandatory**
F.12	The Supplier shall comply with the Data Protection Audit Plan.	**Mandatory**
F.13	The Supplier shall ensure that a comprehensive Data Protection audit is carried out by an independent Third Party and/or DIT in accordance with Schedule 11: Processing Personal Data.	**Mandatory**
F.14	The Supplier shall undertake a Data Protection audit every twelve (12) months (or such other frequency as DIT may require) and report the findings to DIT.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
F.15	The Supplier shall implement any recommendations from any Data Protection audits within timescales set by DIT.	**Mandatory**
8.4	**Reporting of Data Protection Breaches**	
F.16	The Supplier shall report all breaches of Data Protection Legislation and all other data security incidents within the period specified in Schedule 2.2: Performance Level and the Incident Management Process.	**Mandatory**
8.5	**Storage**	
F.17	The Supplier shall develop and comply with processes that ensure that the transmission of SME Application Records over a public network is done securely in accordance with security measures equivalent to those used by major financial institutions for the protection of financial data and shall submit such processes to DIT for Assurance.	**Mandatory**
F.18	The Supplier shall ensure that the storage of SME Application Records complies with DIT's security requirements as specified in Schedule 2.4: Security Management.	**Mandatory**
8.6	**Individual Rights**	
F.19	The Supplier shall submit to DIT for Approval, and when Approved, comply with, a procedure for processing Individual Rights request (i.e. subject access requests (SARs)) in accordance with Data Protection Legislation.	**Mandatory**
F.20	Where the Supplier is required to supply information to DIT to enable them to respond to Individual Rights requests, the Supplier shall cooperate within such time and in such form as reasonably requested by DIT. Where no period of time is specified in the request, the Supplier shall action the request within ten (10) Working Days from the date the request is made to the Supplier (unless a longer period is specified in advance by DIT).	**Mandatory**

9. SECURITY

Requirement ID	Requirement Specification	Requirement Type
9.1	**Security Management**	
This section covers those requirements relating to Security including the Security Policy. This section should be read in conjunction with Schedule 2.4: Security Management		
G.1	The Supplier shall manage the Incident Management Process in accordance with Schedule 2.4: Security Management.	**Mandatory**
G.2	The Supplier shall ensure that all measures necessary to comply with Data Protection Legislation are in place to control access to Personal Data by the Supplier's Personnel in accordance with Schedule 11: Processing Personal Data	**Mandatory**
G.3	The Supplier shall allow DIT Personnel to monitor the Supplier's compliance and obligations under this Agreement without hindrance. This shall include allowing authorised DIT Personnel to enter the Premises at any time in order to inspect the operation, maintenance and equipment used in the provision of the Services.	**Mandatory**
G.4	The Supplier shall put in place Data management procedures to ensure that Data is periodically assessed for deletion in accordance with Schedule 11: Processing Personal Data.	**Mandatory**
G.5	DIT may carry out audits of the Supplier's quality management systems (including Quality Plans and any quality manuals and procedures) at agreed times. The Supplier shall develop and comply with auditing procedures for audits of the quality management systems and shall submit such procedures to DIT for Assurance.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
G.6	The Supplier shall provide full co-operation for any audit including access to all relevant Documentation and Personnel.	**Mandatory**
G.7	The Supplier shall develop and comply with an audit methodology for monitoring and controlling all business processes and hand-offs to each business function and shall submit such audit methodology to DIT for Assurance.	**Mandatory**
G.8	The Supplier shall develop and comply with an Audit Schedule covering all audits, together with the scope of each Audit, and shall submit such an Audit Schedule to DIT for Assurance prior to the Planned Operational Service Commencement Date.	**Mandatory**
G.9	The Supplier shall submit to DIT for Approval, the proposed security audits to be carried out and, when Approved, carry out such security audits in accordance with Schedule 2.4: Security Management.	**Mandatory**
G.10	The Supplier shall provide DIT with reports, in electronic format when requested by DIT, from the incident log including full details of: • Incidents; • Security Incidents; • Changes; and • Any other incidents.	**Mandatory**
G.11	The Supplier shall distinguish between: • Incidents; • Defects; • Changes; • Security Incidents; • Key Performance Indicator Incidents and;	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
	• Closed, where the Incident is deemed to be in none of these classifications.	
G.12	The Supplier shall analyse and report on trends of incidents.	**Mandatory**

10. QUALITY ASSURANCE

Requirement ID	Requirement Specification	Requirement Type
10.1 Quality Assurance and Quality Plan		
This section covers those requirements relating to		
H.1	The Supplier shall develop and comply with a Quality Assurance process and shall submit such a process to DIT for Assurance.	**Mandatory**
H.2	The Supplier shall develop a Quality Plan, that ensures that all aspects of the Services are the subject of quality management systems; and is consistent with ISO 9001:2015 or any standard which is generally recognised as being equivalent to it.	**Mandatory**
H.3	The Supplier shall submit to DIT for Approval the date by which it can deliver the Quality Plan, prior to the Operational Service Commencement Date, and once Approved, shall deliver the Quality Plan on or before such Approved Date.	**Mandatory**
H.4	The Supplier shall submit the Quality Plan to DIT for Assurance within the Approved timescale, and once Assured, comply with the Quality Plan.	**Mandatory**
H.5	The Supplier shall provide the Services in accordance with the Quality Plan.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
H.6	The Supplier shall develop and comply with a Quality Plan and shall submit such a Quality Plan together with any proposed changes to DIT for Assurance.	**Mandatory**
H.7	The Supplier shall ensure continuity in the management of quality assurance during the term of the Agreement.	**Mandatory**
H.8	The Supplier shall be responsible for the quality of the services supplied and be required to provide quality controls and measures to monitor these in accordance with the Quality Plan.	**Mandatory**
H.9	The Supplier shall nominate two (2) named persons as representatives who shall be responsible for the overall quality and timeliness of the Services to be provided	**Mandatory**
H.10	The Supplier shall, during the life of the Agreement, look to develop, maintain and improve efficiency and quality of the services provided to enhance the overall delivery of the Project.	**Mandatory**

11. CAPACITY PLANNING

Requirement ID	Requirement Specification	Requirement Type
11.1	**Managing Capacity**	
	This section covers those requirements relating to managing capacity of the SME Application throughput. The Supplier shall design the Services, to be capable of being scaled smoothly from the initial deployment, which supports only the defined Services in this Agreement, to support Services with up to two (2) times the current steady state operational volumes as set out in Annex 2 – Estimate Cashflow Forecasts.	

Requirement ID	Requirement Specification	Requirement Type
I.1	The Supplier shall provide the Capacity Plan(s) to DIT for Assurance prior to the implementation of the Services.	**Mandatory**
I.2	The Supplier shall review and maintain the Capacity Plan(s) at intervals of not more than six (6) months, in the event of a Change Control Request and at the request of DIT, to reflect Services performance in relation to volume, technical and operational changes and future volume projections.	**Mandatory**
I.3	The Supplier shall at its cost provide a Change Control Request in accordance with Schedule 8.2: Change Control Request Procedure for any increases in Capacity where the Supplier predicts Capacity to be insufficient to meet demand.	**Mandatory**

12. DOCUMENTATION

Requirement ID	Requirement Specification	Requirement Type
12.1	**Document Management Approach**	
This section covers those requirements relating to Documentation. This includes system Documentation and operational Documentation. Requirements applying to both are contained in the general section. This section should be read in conjunction with Schedule 6.1: Implementation Plan.		
J.1	The Supplier shall develop and comply with procedures for maintenance and support and shall submit such procedures to DIT for Assurance.	**Mandatory**
J.2	The Supplier shall develop, review, update and comply with procedures for maintenance and support when Changes are made to the Services and shall submit such procedures including any updates to DIT for Assurance within four (4) weeks of the Change.	**Mandatory**
J.3	The Supplier is responsible for identifying all documents, including procedures, impacted by planned and agreed Changes, and notifying DIT of these documents before the Change is agreed with DIT.	**Mandatory**
J.4	The Supplier shall ensure all documentation described in Schedule 6.1: Implementation Plan Milestones and all other Documentation requested by DIT, is provided to DIT for review as and when modified during the Term.	**Mandatory**
J.5	The Supplier shall submit to DIT for Approval, a Review Schedule and, when Approved, comply with such Review Schedule. The Review Schedule shall allow time for: • DIT reviewers to read the document(s) to be reviewed, including any referenced supporting documentation, and • record and return review comments to the Supplier; • assuming no less than two (2) revisions of each document • avoiding the simultaneous release of each document.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
J.6	The Supplier shall provide electronic copies (or allow access) of Documentation in Microsoft Office (Word, Visio, Excel or PowerPoint) and/or PDF formats as requested by DIT from time to time.	**Mandatory**
J.7	The Service Provider shall ensure documentation for Operational Processes and Procedures is provided for all tasks to be undertaken by the Supplier from the Operational Service Commencement Date. This shall, without limitation comprise: • procedures for operation of the Services; • procedures for maintenance and support of the Services; and • references to relevant systems Documentation.	**Mandatory**

13. FACILITIES, PERSONNEL, STAFFING & TRAINING

Requirement ID	Requirement Specification	Requirement Type
This section lists the requirements related to the provision of facilities. This section also covers requirements for Personnel (both the Supplier's, EITA Supplier(s)' and DIT's), as well as their recruitment and training.		
13.1 Organisation		
K.1	The Suppliers shall collaborate with the EITA Supplier(s) to manage the resolution of incidents.	**Mandatory**
K.2	The Supplier shall ensure a support plan is provided which details the support services that will be provided to DIT and the EITA Supplier(s) to ensure a seamless service.	**Mandatory**
K.3	The Supplier shall establish and operate a continuous improvement approach to support the EITA Supplier(s) Personnel in delivering eligible, suitable and quality SME Applications, including addressing any training needs.	**Mandatory**
K.4	The Supplier shall attend regular meetings with DIT and any related Third Parties upon request from DIT.	**Mandatory**
K.5	The Supplier shall ensure that its organisation is structured to ensure focus on excellence in customer service and compliance with this Agreement.	**Mandatory**
K.6	The Supplier shall promote clear, accurate and regular communications between the Supplier's Personnel and the EITA Supplier(s)' Personnel.	**Mandatory**
K.7	The Supplier shall ensure that person(s) are nominated to be responsible for the delivery of the Services and are contactable by DIT during normal business hours.	**Mandatory**
K.8	The Supplier shall ensure that DIT is advised on a rolling weekly basis of the name(s) and contact details of the appointed person(s) responsible for the delivery of the Services and shall ensure that they are available for contact by DIT during normal business hours.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
13.2 Personnel		
K.9	The Supplier shall ensure that only appropriately qualified Personnel are employed to provide the support service and maintenance.	**Mandatory**
K.10	The Supplier shall ensure that the scope of the identified job roles clearly identifies the responsibilities and accountability for outputs and hand-offs.	**Mandatory**
K.11	The Supplier shall ensure that DIT is notified immediately of the occurrence of any of the following regarding the Supplier's Personnel: • suspensions; • disciplinary proceedings; • dismissals; and/or • Key Personnel appointments	**Mandatory**
K.12	The Service Provider shall ensure that appropriate and relevant Personnel security checks are performed for new Service Provider Personnel prior to the commencement of their employment.	**Mandatory**
13.3 Supplier's Personnel Training		
K.13	The Supplier shall include, without limitation, a detailed review of the following areas in the induction course referred to in J.14 below: • Data Protection Legislation; • National ESIF guidelines;	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
	• FOI Legislation; • obligations, codes and procedures for its Personnel; • Environmental Information Regulations; • Computer Misuse Act 1990; • security processes and procedure; • Premises rules and regulations; • methods to ensure Personnel have a clear understanding of their duties and hours; and • methods to ensure Personnel are competent to use all necessary Equipment and supplier system(s) in a safe and efficient manner.	
K.14	The Supplier shall submit to DIT for Approval and, when Approved, comply with the contents of and materials to be used for a formal induction course for new Personnel.	**Mandatory**
K.15	The Supplier shall submit to DIT for Approval and, when Approved, comply with a detailed training plan for all The Supplier Personnel involved in the delivery of the Services. The plan shall cover the following areas, such as but not limited to: • the Supplier's approach to training; • the Supplier's proposals for induction training; and • the Supplier's proposals for periodic refresher training and Personnel development training. The Training Plan shall include any specific training requirements as Approved by DIT.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
K.16	The Supplier shall provide all necessary induction and on-going training and supporting materials to all its Personnel for any changes made to the Services. For the avoidance of doubt, this shall include, but not be limited to training on the following: • FAQs; • SME Application and Claims guidance • Customer service; • SME Application guidelines; and • training and materials relevant to the operation of the Services; and • all other required guidance	**Mandatory**
K.17	The Supplier shall ensure that all training manuals and courses are updated to reflect changes to operational practices and lessons learned.	**Mandatory**
K.18	The Supplier shall ensure that its Personnel have access to all Documentation appropriate to the performance of any role to which they are assigned.	**Mandatory**
13.4 Supplier Recruitment and Staffing		
K.19	The Supplier shall provide job descriptions for those roles identified by the Supplier to be necessary for the delivery of Services to DIT for Approval as part of the Detailed Design. At a minimum, this shall include job descriptions for those Key Personnel outlined in Schedule 11: Key Personnel.	**Mandatory**
K.20	The Supplier shall provide job descriptions of its Personnel to DIT upon request. Job descriptions must include as a minimum, details of: • key accountabilities; • key competencies;	**Mandatory**

ENGROSSED CONTRACT FINAL v2.0

Requirement ID	Requirement Specification	Requirement Type
	• scope of each role; and • minimum qualifications and experience necessary for the individual to fulfil the role.	
K.21	The Supplier shall request DIT approval for the replacement of any Key Personnel in accordance with Schedule 11: Key Personnel.	**Mandatory**

14. FINANCE

Requirement ID	Requirement Specification	Requirement Type
14.1	**Fraud Detection**	
L.1	The Supplier shall provide all required and requested Data and statements directly to the relevant enforcement authority (or appropriate relevant authority) for the purposes of credit card fraud and other investigations, unless otherwise specifically requested by DIT.	**Mandatory**
L.2	The Supplier shall provide any requested Data and statements to the relevant police service (or appropriate relevant authority) within the timescales specified by DIT and at no cost to DIT. A log of such events shall be maintained, providing traceability to the Data provided, and this log should be provided to DIT for inspection on request.	**Mandatory**
L.3	The Supplier shall ensure that the Supplier's system(s) logs all Data provided to the relevant police service.	**Mandatory**
14.2	**Audit**	
L.4	Access is required by internal and external DIT auditors to the Supplier's systems and documents. Regular audits need to be carried out by the Supplier in order to give assurance on the creditability of its operations, reporting and financial statements.	**Mandatory**
L.5	The Supplier shall (at no cost to DIT) co-operate fully with any DIT audit pursuant to Clause 11 including providing access to all relevant Supplier documentation and personnel.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
L.6	The Supplier shall allow DIT access to all audit data, reports and results from audits commissioned by the Supplier which relate (in whole or in part) to the Services.	**Mandatory**
L.7	The Supplier shall use a risk-based approach to routinely carry out internal audits to provide assurance that effective controls are in place. The Supplier shall submit a plan for its audit programme to DIT for Assurance and provide DIT with access to the final report.	**Mandatory**
14.3 Process & Control		
The Supplier shall obtain DIT Approval of the design of any finance procedures, processes and controls for assurance purposes. This section details the specific controls and processes required in order to operate each ESIF Project effectively.		
L.8	The Supplier shall ensure that all financial processes and controls are developed in accordance with ESIF Internationalisation Fund guidelines (as updated and amended from time to time).	**Mandatory**
L.9	The Supplier shall ensure that all financial data provided to DIT is complete, correct and consistent with the underlying operational activity.	**Mandatory**
L.10	The Supplier shall produce and maintain an issues log detailing all discrepancies in the financial data. This shall be provided to DIT at the end of each Period (to be agreed with DIT).	**Mandatory**
L.11	The Supplier shall submit the design of all procedures, processes and controls relating to financial data to DIT for Assurance (prior to implementation).	**Mandatory**
L.12	The Supplier shall maintain a system of internal controls to provide the right level of checks and balances to verify reconciliation of financial data.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
L.13	The Supplier shall ensure that the finance system(s) contain a system of internal controls to provide the right level of checks and balances to verify reconciliation of financial data.	**Mandatory**
L.14	The Supplier shall document and perform periodic checks and reconciliations to prove the completeness and integrity of Data entered into the finance system(s).	**Mandatory**
L.15	The Supplier shall use the log for monitoring money laundering and shall ensure that all irregularities are thoroughly investigated and actioned.	**Mandatory**
L.16	The Supplier shall produce finance user guides and finance process documents on how they will assure their operation and submit such guides and process documents to DIT for Assurance, and (when Assured) comply with such guides and process documents.	**Mandatory**
L.17	The Supplier shall ensure that all transactions in related to a SME Applicant are cross referenced to related documents, transactions, and authorisations in order to provide a full audit trail for all SME Applicant(s) related transactions.	**Mandatory**
L.18	The Supplier shall design and operate processes to ensure that rebates can be made for the following: • overpayments; • duplicate payments; and • payment errors.	**Mandatory**
L.19	The Service Provider shall ensure that the finance system(s) shall record the reason for a rebate as being due to one of the following: • overpayments;	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
	• duplicate payments; and • payment errors.	
14.4 Financial Reporting		
Management and financial reporting requirements (including frequency and scope) are detailed in this section		
L.20	The Supplier shall ensure that Supplier Personnel responsible for managing the finance function attend Periodic meetings with DIT.	**Mandatory**
L.21	The Supplier shall communicate all limitations, errors, missing data and anomalies in the underlying financial data to DIT immediately.	**Mandatory**
L.22	The Supplier shall ensure that all accounting journals are at all times created using the latest version of the DIT journal upload template and in a format to be agreed.	**Mandatory**
L.23	The Supplier shall ensure the Risk Register includes financial risks and documented mitigations and controls from time to time.	**Mandatory**
L.24	The Supplier shall provide financial reports separating each different ESIF Project.	**Mandatory**
L.25	The Supplier shall provide DIT ad-hoc extracts of the financial reports within two (2) Working Days of the request being issued by DIT.	**Mandatory**

Requirement ID	Requirement Specification	Requirement Type
14.5 Staff and Training		
The Supplier shall ensure that all Supplier Personnel have all relevant and required skill and knowledge through training and experience to enable them to perform their duties competently.		
L.26	The Supplier shall ensure that Supplier Personnel responsible for managing the finance function are qualified accountants holding a current recognised Chartered Accounting Qualification and (at no additional cost to DIT) are fully trained to enable them to perform their duties competently.	**Mandatory**
L.27	The Supplier shall nominate a dedicated Qualified Accountant who is responsible for managing the financial deliverables under this Agreement in accordance with Schedule 9.2: Key Personnel.	**Mandatory**
L.28	The Supplier shall (at no additional cost to DIT) provide annual internal fraud detection and prevention training to all Service Provider Personnel involved in processing payments to successful SME Applicant(s).	**Mandatory**

15. CLOSE-OUT SUPPORT AND OUTPUT EVIDENCE COLLECTION - DURING EXIT

- The Supplier shall be required to provide close-out support and output evidence collection for all outstanding requirements that are outside the ESIF Project timeline (beyond June 2023) in accordance with Schedule 7.1(Charges and Invoicing) and Schedule 8.5 (Exit Management).

SCHEDULE 2.2

PERFORMANCE LEVELS

Performance Levels

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"Performance Monitoring Report"	has the meaning given in Paragraph 1.1(a) of Part B;
"Performance Review Meeting"	the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Agreement, as further described in Paragraph 1.5 of Part B;
"Repeat KPI Failure"	has the meaning given in Paragraph 3.1 of Part A;
"Satisfaction Survey"	has the meaning given in Annex 1;

PART A: PERFORMANCE INDICATORS AND SERVICE CREDITS

1 INTRODUCTION

1.1 The objective of the performance management regime is to encourage the Supplier to meet defined service levels by measuring performance against a range of key performance indicators (each a "Key Performance Indicator" or "KPI").

1.2 The KPIs have been selected to reflect areas of the Services which are essential in order to deliver an acceptable level of customer service for the SME Applicant, and to avoid exposing the Authority to significant financial or reputational risk.

1.3 Service Points and therefore Service Credits have been set for each KPI, to reflect the relative impact of failure to meet the acceptable service level for the KPI.

2 PERFORMANCE INDICATORS

1.4 **Table 1** in Annex 1 to this Schedule ("**Table 1**") sets out the sets out the performance management regime parameters for each of the Key Performance Indicators.

1.5 The Supplier shall monitor its performance against each Key Performance Indicator and shall send the Authority a report detailing the level of service actually achieved in accordance with Part B (Performance Monitoring).

1.6 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 4 of Part A (Performance Indicators and Service Credits).

2 SERVICE POINTS

2.1 If the level of performance of the Supplier during a Service Period achieves the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.

2.2 If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Paragraph 2.3.

2.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as detailed in **Table 1** (Annex 1) . The number of Service Points accumulated depends on the extent to which the Supplier has failed to meet the Target Performance Level for each KPI. For each Key Performance Indicator there are three (3) bands of Service Points as follows:

(a) a Minor KPI Failure; or

(b) a Serious KPI Failure; or

(c) a Severe KPI Failure;or

2.4 Where the KPI Failure is a Repeat KPI Failure which means the Severe KPI points shall accure in accordance with the provisions of Paragraph 3.2 shall apply.

2.5 The Service Points shall be totalled for all KPIs at the end of each Month and the corresponding Service Credit deductions shall be calculated in accordance with paragraph 3.1 of Part C of Schedule 7.1 (Charging and Invoicing).

2.6 The value of the Service Credits Deductions shall be capped each Month at an amount equivalent to 10% of the Monthly Service Fees of each respective ESIF Projects (i.e NP201, ME201, SE201 and LO201) in accordance with the table in paragraph 5 in Schedule 7.1 (Charging and Invoicing). ("**Monthly Service Credit Cap**")

2.7 The value of the Service Credits Deductions shall be subject to annual Indexation in accordance with paragraph 5.1 of Schedule 7.1 (Charging and Invoicing).

Calculation of Working Days

2.8 When measuring the timeliness of any item subject to a KPI based on Working Days the following rules will apply:

(a) any complete Working Day between the item Start Point and End point shall be included in the Working Day count;

(b) any part Working Day which contains Working Hours between the item Start Point and End point shall be included in the Working Day count;

(c) when an item is correctly escalated to DIT during Working Hours, then that Working Day and any subsequent complete Working Day the item is with DIT shall be excluded in the Working Day count; and

(d) when an item is correctly escalated to DIT outside of Working Hours, then any subsequent complete Working Day the item is with DIT shall be excluded in the Working Day count.

Worked Example:
An item was received on Friday 02 November at 10:25. This item was correctly escalated to DIT on Wednesday 07 November at 17:50. A response was received back from DIT on Friday 09 November at 10:15. The item was responded to on Monday 12 November at 18:30.

Date	Supplier Working Day?	Description
Fri 02 Nov	Yes	Item received during Working Hours
Sat 03 Nov	No	Non Working Day
Sun 04 Nov	No	Non Working Day
Mon 05 Nov	Yes	Item with Supplier
Tue 06 Nov	Yes	Item with Supplier
Wed 07 Nov	No	Correctly escalated to DIT during Working Hours
Thu 08 Nov	No	Item with DIT
Fri 09 Nov	Yes	Returned from DIT during Working Hours
Sat 10 Nov	No	Non Working Day

Sun 11 Nov	No	Non Working Day
Mon 12 Nov	Yes	Response sent from Supplierat 18:30
Total	**5 Working Days**	

3 REPEAT KPI FAILURES AND RELATED KPI FAILURES

Repeat KPI Failures

3.1 If a KPI Failure occurs in respect of the same Key Performance Indicator in any two (2) consecutive Measurement Periods, the second and any subsequent KPI Failures shall be a "Repeat KPI Failure". The KPI Failure shall be applied in accordance with the table below.

3.2 The Repeat KPI Failure count shall be reset to zero (0) once there have been two (2) consecutive Measurement Periods in which the Target Performance Level has been met.

3.3 A worked example is set below:

Counting Repeat KPI Failures

	Measurement Period											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Failure to meet Target Performance Levels for a KPI (F)	F	F	✓	F	✓	✓	F	✓	F	F	✓	F
No. of Repeat Failures	0	1		2			0		1	2		3

3.4 For any failure to meet Target Performance Levels for each KPI which is a Repeat Failure, the Service Points applicable shall be applied as follows:

Repeat KPI Failure count applicable to the Measurement Period	**Applicable Service Points by Severity Level of each KPI**			
	Minor KPI Failure	**Serious KPI Failure**	**Severe KPI Failure**	**KPI Service Threshold**
0	1	2	3	4
1	2	3	4	
2	3	4		
3	4			
4 above				

3.5 For the avoidance of doubt, Repeat KPI Failures that are accruing Service Points equivalent to or more than the Service Points applied to a Serious KPI Failure, shall be deemed a Material KPI Failure.

4 SERVICE CREDITS

4.1 Schedule 7.1 (Charges and Invoicing) sets out the mechanism by which Service Points shall be converted into Service Credits.

4.2 The Authority shall use the Performance Monitoring Reports provided pursuant to Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

PART B: PERFORMANCE MONITORING

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 Within 10 Working Days of the end of each Service Period, the Supplier shall provide:

(a) a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.2 (the "**Performance Monitoring Report**"); and

(b) a report to the Authority's senior responsible officer which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the "**Balanced Scorecard Report**").

Performance Monitoring Report

1.2 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each Key Performance Indicator, the actual performance achieved over the Service Period, and that achieved over the previous 3 Measurement Periods;

(b) a summary of all Performance Failures that occurred during the Service Period;

(c) the severity level of each KPI Failure which occurred during the Service Period and whether each PI Failure which occurred during the Service Period fell below the PI Service Threshold;

(d) which Performance Failures remain outstanding and progress in resolving them;

(e) for any Material KPI Failures or Material PI Failures occurring during the Service Period, the cause of the relevant KPI Failure or PI Failure and the action being taken to reduce the likelihood of recurrence;

(f) the status of any outstanding Rectification Plan processes, including:

(i) whether or not a Rectification Plan has been agreed; and

(ii) where a Rectification Plan has been agreed, a summary of the Supplier's progress in implementing that Rectification Plan;

(g) for any Repeat Failures, actions taken to resolve the underlying cause and prevent recurrence;

(h) the number of Service Points awarded in respect of each KPI Failure;

(i) the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;

(j) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;

(k) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement;

(l) such other details as the Authority may reasonably require from time to time; and

Information in respect of previous Service Periods

(m) a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;

(n) the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;

(o) the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan; and

Information in respect of the next Quarter

(p) any scheduled Service Downtime for Permitted Maintenance and Updates that has been agreed between the Authority and the Supplier for the next Quarter.

Balanced Scorecard Report

1.3 The Balanced Scorecard Report shall be presented in the form of a dashboard and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period, including details of the following:

(a) financial indicators;

(b) the Target Performance Levels achieved;

(c) behavioural indicators;

(d) performance against its obligation to pay its Sub-contractors within 30 days of receipt of an undisputed invoice;

(e) Milestone trend chart, showing performance of the overall programme; and

(f) sustainability and energy efficiency indicators, for example energy consumption and recycling performance.

1.4 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Meeting held in accordance with Paragraph 1.5.

1.5 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Scorecard Reports. The Performance Review Meetings shall (unless otherwise agreed):

(a) take place within 5 Working Days of the Performance Monitoring Report being issued by the Supplier;

(b) take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and

(c) be attended by the Supplier Representative and the Authority Representative.

1.6 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure and/or PI Failure.

2 PERFORMANCE RECORDS

2.1 The Supplier shall keep appropriate documents and records (including Help Desk records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

2.2 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.

2.3 The Supplier shall ensure that the Performance Monitoring Report, the Balanced Scorecard Report and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.

ANNEX 1: KEY PERFORMANCE INDICATORS

PART I: KEY PERFORMANCE INDICATORS TABLES

The Key Performance Indicators that shall apply to the Operational Services are set out below:

1 Key Performance Indicators

Table 1 - Key Performance Indicator Table

KPI ID	Key Performance Indicator Title	Definition	Start Point	End point	Frequency of Measurement	Target Performance Level	Severity Levels			
							Minor KPI Failure	Serious KPI Failure	Severe KPI Failure	KPI Service Threshold
KPI1	Timely processing of SME Applications	% of Funding Award decisions made within three (3) Working Days of receipt of SME Application	The start of the first Working Day after receipt of a SME Application or where the SME Application is either incomplete or has errors, the SME Application shall be put on Hold and the Start Point shall be at the start of the first Working Day after receipt of a SME Application resubmission	Date and time SME Applicant is notified of Funding Award decisions	Monthly	95%	[redacted]	[redacted]	75% - 84.9%	below 75%
							1 Service Point	2 Service Points	3 Service Points	4 Service Points
KPI2	Timely issuing of offer letters	% of Funding Offer Letters issued within forty-eight (48) hours of funding award decision	Date and time of a funding award decision being notified to the SME Applicant	Date and time a funding Offer Letter is successfully sent to the SME Applicant	Monthly	95%	[redacted]	[redacted]	75% - 84.9%	Below 75%
							1 Service Point	2 Service Points	3 Service Points	4 Service Points
KPI3	Timely processing of SME Claims	% of SME Claim Approval and payments made or Error notifications sent to SME Applicants within five (5) days	Date and time a SME Claim is received by the Supplier	Date and time an SME Claim is processed (payment is received by SME) or error notified to the SME	Monthly	95%	[redacted]	[redacted]	75% - 84.9%	Below 75%
							1 Service Point	2 Service Points	3 Service Points	4 Service Points
KPI4	Timely collection of close out reports	% of SME Applicant close out reports completed and submitted to DIT within six (6) months of claim payment	N/A	N/A	Monthly	95%	[redacted]	[redacted]	75% - 84.9%	75%
							1 Service Point	2 Service Points	3 Service Points	4 Service Points
KPI5	Delivery of compliant SME Applicant projects	% of SME Applicant claims which are reimbursed by MHCLG without claw-back or retrospective review by either DIT or MHCLG	N/A	N/A	Monthly	98%	[redacted]	[redacted]	85% - 92.9%	Below 85%
							1 Service Point	2 Service Points	3 Service Points	4 Service Points
KPI6	Close-out Satisfaction Survey	% of SME Applicants scoring positively four (4) or five (5) in a close out report cost benefit analysis. Negative scores will require further detail and only scores which are explicitly associated with the Fund Administrator will be taken into account.	N/A	Satisfaction score four (4) or five (5) out of five (5	Monthly	90%	[redacted]	[redacted]	80% - 89.9%	below 80%
							1 Service Point	2 Service Points	3 Service Points	4 Service Points

Further Details relating to the KPIs

KPI1 - Timely processing of SME Applications

(a) The Supplier shall be assessed on the percentage of all Funding Award decisions which are made within the stipulated timeframe.

(b) The KPI measure shall be based upon all reports with an end point during the Month

KPI2 - Timely issuing of offer letters

(a) The Supplier shall be assessed on the percentage of all Funding Offer Letters which are issued within the stipulated timeframe.

(b) The KPI measure shall be based upon all reports with an end point during the Month

KPI3 - Timely processing of SME Claims

(a) The Supplier shall be assessed on the percentage of all SME claims processed and paid or assessed to have errors where the errors have been notified to the relevant SME Applicant within the stipulated timeframe.

(b) The KPI measure shall be based upon all reports with an end point during the Month

KPI4 - Timely collection of close out reports

(a) The Supplier shall be assessed on the percentage of close out reports which have been completed 6 months after the payment of valid and approved claims.

(b) The KPI measure shall be based upon the number of claims paid during the month 6 months prior to the current month.

KPI5 - Delivery of compliant SME Applicant projects

(a) The Supplier shall be assessed on the percentage of all SME Applicant projects which are reimbursed by MHCLG without clawback or retrospective review by either DIT or MHCLG

(b) The KPI measure shall be based upon all reports with an end point during the Month

KPI6 - Close-out Satisfaction Survey

(a) This KPI asseses the SME Applicant beneficiary cost/benefit perception of funding application process at close out stage.

(b) The Supplier shall be assessed on the percentage of all SME close out reports where the cost benefit analysis scores either four (4) or five (5).

(c) The KPI measure shall be based upon all reports with an end point during the Month

SCHEDULE 2.3

STANDARDS

Standards

1. DEFINITIONS

In this Schedule, the following definitions shall apply:

"Standards Hub"	the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/; **and**
"Suggested Challenge"	a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2. GENERAL

2.1. Throughout the term of this Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

2.2. Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

2.3. Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

3. TECHNOLOGY AND DIGITAL SERVICES PRACTICE

3.1. The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.

4. OPEN DATA STANDARDS & STANDARDS HUB

4.1. The Supplier shall comply to the extent within its control with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

4.2. Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Agreement or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at http://standards.data.gov.uk/). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Agreement, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

4.3. The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

5. TECHNOLOGY ARCHITECTURE STANDARDS

5.1. The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with TOGAF 9.1 or its equivalent, then this shall be deemed acceptable.

6. ACCESSIBLE DIGITAL STANDARDS

6.1. The Supplier shall comply with (or with equivalents to):

(a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.0 Conformance Level AA; and

(b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

7. SERVICE MANAGEMENT SOFTWARE & STANDARDS

7.1. Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:

(a) ITIL v3 2011;

(b) ISO/IEC 20000-1:2011 "ITSM Specification for Service Management";

(c) ISO/IEC 20000-2:2012 "ITSM Code of Practice for Service Management";

(d) ISO 10007 "Quality management systems – Guidelines for configuration management"; and

(e) BS25999-1:2006 "Code of Practice for Business Continuity Management" and, ISO/IEC 27031:2011, ISO 22301 and ISO/IEC 24762:2008 in the provision of "IT Service Continuity Strategy" or "Disaster Recovery" plans.

7.2. For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to "Bronze Level", then this shall be deemed acceptable.

8. ENVIRONMENTAL STANDARDS

8.1. The Supplier warrants that it has obtained ISO 14001 (or equivalent) certification for its environmental management and shall comply with and maintain certification requirements throughout the Term. The Supplier shall follow a sound environmental management policy, ensuring that any Goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.

8.2. The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).

8.3. The Supplier shall (when designing, procuring, implementing and delivering the Services) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

8.4. The Supplier shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency. The Supplier shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

8.5. The Supplier shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

9. HARDWARE SAFETY STANDARDS

9.1. The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:

(a) any new hardware required for the delivery of the Services (including printers), shall conform to BS EN 60950-1:2006+A12:2011 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;

(b) any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN 60065:2002+A12:2011 or any subsequent replacements;

(c) any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2007 or any subsequent replacements ; and

(d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 41003:2009 or any subsequent replacements.

9.2. Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Agreement in accordance with the relevant health and safety regulations.

SCHEDULE 2.4

SECURITY MANAGEMENT

1. Definitions

In this Schedule, the following definitions shall apply:

"Risk Management Documentation"	has the meaning given in Paragraph 6.3;
"Information Management System"	means the Core Information Management System and the Wider Information Management System;
"Accreditation"	the assessment of the Core Information Management System in accordance with Paragraph 6 by the Authority or an independent information risk manager/professional appointed by the Authority, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Authority, taken in accordance with the process set out in Paragraph 6, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	the Supplier's plan to attain an Accreditation Approval Statement from the Authority, which is prepared by the Supplier and approved by the Authority in accordance with Paragraph 6.4;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; and/or

	(c) any part of the Supplier System ceasing to be compliant with the Certification Requirements,
	in each case as more particularly set out in the security requirements in Schedule 2.1 (*Services Description*) and the Baseline Security Requirements;
"Certification Requirements"	the requirements set out in Paragraph 7;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources, which the Authority has determined in accordance with Paragraph 4 shall be subject to Accreditation;
"IT Health Check"	has the meaning given Paragraph 8.1.1;
Personal Data	has the meaning given in the Data Protection Legislation;
Personal Data Breach	has the meaning given in the Data Protection Legislation;
Personal Data Processing Statement	sets out: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier in accordance with Paragraph 6.4 of Schedule 2.4 (Security Management) and included in the Risk Management Documentation;
"Process Authority Data"	any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing,

	structuring, transmitting or otherwise using Authority Data;
"Required Changes Register"	is a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Authority shall be made to the Core Information System and/or the Risk Management Documentation as a consequence of the occurrence of any of the events set out in Paragraph 6.10.1 to 6.10.8 together with the date on which each such change shall be implemented and the date on which each such change was implemented;
"Risk Management Approval Statement"	a notice issued by the Authority which sets out the information risks associated with using the Core Information Management System and confirms that the Authority is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority;
"Risk Management Reject Notice"	has the meaning given in Paragraph 6.6.6;
"Security Test"	has the meaning given Paragraph 8.1; and
"Statement of Information Risk Appetite"	has the meaning given in Paragraph 5.1;.
"Vulnerability Correction Plan"	has the meaning given in Paragraph 8.4.3(a); and
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data which have not been determined by the Authority to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources.

ENGROSSED CONTRACT FINAL v2.0

2. Introduction

2.1 This Schedule sets out:

2.1.1 the principles which the Supplier shall comply with when performing its obligations under this Agreement in order to ensure the security of the Authority Data, the IT Environment, the Supplier Solution and the Information Management System;

2.1.2 the process which shall apply to the Accreditation of the Core Information Management System in Paragraph 6;

2.1.3 the Certification Requirements applicable to the Wider Information Management System in Paragraph 7;

2.1.4 the Security Tests which the Supplier shall conduct during the Term in Paragraph 8;

2.1.5 the Security Tests which the Authority may conduct during the Term in Paragraph 8.7;

2.1.6 the requirements to patch vulnerabilities in the Core Information Management System in Paragraph 9;

2.1.7 the obligations on the Supplier to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in Paragraph 10; and

2.1.8 each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 11.

3. Principles of Security

3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

3.1.1 the IT Environment;

3.1.2 the Supplier Solution; and

3.1.3 the Information Management System.

3.2 Notwithstanding the involvement of the Authority in the Accreditation of the Core Information Management System, the Supplier shall be and shall remain responsible for:

3.2.1 the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors;

3.2.2 the security of the Supplier Solution; and

3.2.3 the security of the Information Management System.

3.3 The Risk Management Board shall, in addition to its responsibilities set out in Schedule 8.1 (Governance), monitor and may also provide recommendations to the Supplier on the Accreditation of the Core Information Management System.

3.4 Each Party shall provide access to members of its information assurance personnel to facilitate the Supplier's design, implementation, operation, management and continual improvement of the Risk Management Documentation and the security of the Supplier Solution and Information Management System and otherwise at reasonable times on reasonable notice.

4. Information Management System

4.1 The Authority shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Authority to make such determination, the Supplier shall provide the Authority with such documentation and information that the Authority may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Sub-contractor to Process Authority Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Authority shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

4.2 Any proposed change to the component parts of and/or boundary of the Core Information Management System shall be notified and processed in accordance with the Change Control Procedure.

5. Statement of Information Risk Appetite and Baseline Security Requirements

5.1 The Supplier acknowledges that the Authority has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services (the **"Statement of Information Risk Appetite"**).

5.2 The Authority's Baseline Security Requirements in respect of the Core Information Management System are set out in Annex 1.

5.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Accreditation of the Core Information Management System.

6. Accreditation of the Core Information Management System

6.1 The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 6.

6.2 The Accreditation shall be performed by the Authority or by representatives appointed by the Authority.

6.3 Prior to the Operational Services Commencement Date, the Supplier shall prepare and submit to the Authority the risk management documentation for the Core Information Management System, which shall comply with, and be subject to approval by the Authority in accordance with, this Paragraph 6 (the "**Risk Management Documentation**").

6.4 The Risk Management Documentation shall be structured in accordance with the template as set out in Annex 3 and include:

6.4.1 the Accreditation Plan, which shall include:

(a) the dates on which each subsequent iteration of the Risk Management Documentation will be delivered to the Authority for review and staged approval; and

(b) the date by which the Supplier is required to have received a Risk Management Approval Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority Responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 6.7.1

6.4.2 a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

6.4.3 a completed ISO 27001:2013 Statement of Applicability for the Core Information Management System; the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

6.4.4 unless such requirement is waived by the Authority, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Supplier in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

6.4.5 the Required Changes Register;

6.4.6 evidence that the Supplier and each applicable Sub-contractor is compliant with the Certification Requirements; and

6.4.7 a Personal Data Processing Statement.

6.5 If the Risk Management Documentation submitted to the Authority pursuant to Paragraph 6.3 (or Paragraph 6.10, as applicable) is approved by the Authority,

it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Risk Management Documentation is not approved by the Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the Risk Management Documentation on the grounds that it does not comply with the requirements set out in Paragraph 6.4 shall be deemed to be reasonable.

6.6 To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Authority and its authorised representatives with:

6.6.1 access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and

6.6.2 such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

6.6.3 to enable the Authority to establish that the Core Information Management System is compliant with the Risk Management Documentation.

6.6.4 The Authority shall, by the relevant date set out in the Accreditation Plan, review the identified risks to the Core Information Management System and issue to the Supplier either:

6.6.5 a Risk Management Approval Statement which will then form part of the Risk Management Documentation, confirming that the Authority is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority; or

6.6.6 a rejection notice stating that the Authority considers that the residual risks to the Core Information Management System have not been reduced to a level acceptable by the Authority and the reasons why ("**Risk Management Rejection Notice**").

6.7 If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:

6.7.1 address all of the issues raised by the Authority in such notice; and

6.7.2 notify the Authority that the Core Information Management System is ready for an Accreditation Decision.

6.8 If the Authority determines that the Supplier's actions taken pursuant to the Risk Management Rejection Notice have not reduced the residual risks to the Core Information Management System to an acceptable level and issues a further

Risk Management Rejection Notice, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 30.2(b).

6.9 The process set out in Paragraph 6.7 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Agreement.

6.9.1 The Supplier acknowledges that it shall not be permitted to use the Core Information Management System to Process Authority Data prior to receiving a Risk Management Approval Statement.

6.9.2 The Supplier shall keep the Core Information Management System and Risk Management Documentation under review and shall update the Risk Management Documentation annually in accordance with this Paragraph and the Authority shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 6.10.

6.10 The Supplier shall notify the Authority within 2 Working Days after becoming aware of:

6.10.1 a significant change to the components or architecture of the Core Information Management System;

6.10.2 a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

6.10.3 a change in the threat profile;

6.10.4 a Sub-contractor failure to comply with the Core Information Management System code of connection;

6.10.5 a significant change to any risk component;

6.10.6 a significant change in the quantity of Personal Data held within the Core Information Management System;

6.10.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

6.10.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns,

update the Required Changes Register and provide the updated Required Changes Register to the Authority for review and approval within 2 Working Days after the initial notification or such other timescale as may be agreed with the Authority.

6.11 If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and the Supplier shall:

6.11.1 immediately cease using the Core Information Management System to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to Process Authority Data in accordance with the Authority's written directions; and

6.11.2 where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 30.2(b).

6.12 The Supplier shall review each Change Request against the Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.

6.13 The Supplier shall be solely responsible for the costs associated with developing and updating the Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Accreditation process.

7. Certification Requirements

7.1 The Supplier shall ensure, at all times during the Term, that the Supplier and any Sub-contractor with access to Authority Data or who will Process Authority Data are certified as compliant with:

7.1.1 ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

7.1.2 Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Authority Data. Any exceptions to the flow-down of the certification requirements to third party suppliers and sub-contractors must be agreed with the Authority.

7.2 The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

7.2.1 securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

7.2.2 are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

7.3 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.

7.4 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

7.4.1 immediately ceases using the Authority Data; and

7.4.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements.

8. Security Testing

8.1 The Supplier shall, at its own cost and expense:

8.1.1 procure a CHECK IT Health Check of the Core Information Management System (an "**IT Health Check**") by a NCSC approved member of the CHECK Scheme:

(a) prior to it submitting the Risk Management Documentation to the Authority for an Accreditation Decision;

8.2 if directed to do so by the Authority in accordance with Paragraph 8.3; and

(a) once every 12 months during the Term.

8.2.2 conduct vulnerability scanning and assessments of the Core Information Management System monthly;

8.2.3 conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a Supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

8.2.4 conduct such other tests as are required by:

(a) any Vulnerability Correction Plans;

(b) the ISO27001 certification requirements;

(c) the Risk Management Documentation; and

(d) the Authority following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

(each a "**Security Test**").

8.3 The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

8.4 In relation to each IT Health Check, the Supplier shall:

8.4.1 agree with the Authority the aim and scope of the IT Health Check;

8.4.2 promptly, following receipt of each IT Health Check report, provide the Authority with a copy of the IT Health Check report;

8.4.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(a) prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied;

(iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

8.5 The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to the Supplier complying with this Paragraph 8.5, if a Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.6 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 8.4, the Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

8.7 The Authority and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information System and/or the Supplier's compliance with the Risk Management Documentation ("**Authority Security Tests**"). The Authority shall take reasonable steps to notify the Supplier prior to carrying out such Authority Security Test

to the extent that it is reasonably practicable for it to do so taking into account the nature of the Authority Security Test.

8.8 The Authority shall notify the Supplier of the results of such Authority Security Tests after completion of each Authority Security Test.

8.9 The Authority Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If an Authority Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be granted relief in respect of such Performance Failure for that Measurement Period.

8.10 Without prejudice to the provisions of Paragraph 8.4.3, where any Security Test carried out pursuant to this Paragraph 8 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Core Information Management System and/or the Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Supplier shall implement such changes to the Core Information Management System and/or the Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible.

8.11 If the Authority unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Risk Management Documentation in accordance with Paragraph 8.8 above, the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:

8.11.1 has arisen as a direct result of the Authority unreasonably withholding its approval to the implementation of such proposed changes; and

8.11.2 would have been avoided had the Authority given its approval to the implementation of such proposed changes.

8.12 For the avoidance of doubt, where a change to the Core Information Management System and/or the Risk Management Documentation is required to remedy non-compliance with the Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

8.13 If any repeat Security Test carried out pursuant to Paragraph 8.10 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 30.2(b).

8.14 The Supplier shall, by 31 March of each year during the Term, provide to the Authority a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

8.14.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Agreement; and

8.14.2 the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

9. Vulnerabilities and Corrective Action

9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

9.2 The severity of vulnerabilities for Supplier COTS Software and Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Risk Management Documentation and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ("Moderate" and "Low") respectively.

9.3 Subject to Paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Core Information Management System within:

9.3.1 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

9.3.2 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

9.3.3 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

9.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 9.3 shall be extended where:

9.4.1 the Supplier can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;

9.4.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

9.4.3 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Risk Management Documentation.

9.5 The Risk Management Documentation shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing.

9.6 The Supplier shall:

9.6.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;

9.6.2 promptly notify NCSC of any actual or sustained attempted Breach of Security;

9.6.3 ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.6.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;

9.6.5 pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Risk Management Documentation;

9.6.6 from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Authority with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Paragraph 9.3 for applying patches to vulnerabilities in the Core Information Management System;

9.6.7 propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;

9.6.8 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Information Management System); and

9.6.9 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.

9.7 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Supplier shall immediately notify the Authority.

9.8 If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 9.3, such failure shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 30.2(b).

10. Malicious Software

10.1 The Supplier shall install and maintain anti-Malicious Software or procure that latest versions of anti-virus definitions and anti-Malicious Software is installed and maintained on any part of the Information Management System, which may Process Authority Data and ensure that such anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

10.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

10.3 any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the Parties as follows:

10.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier (except where the Authority has waived the obligation set out in Clause 20.3) or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

10.3.2 otherwise by the Authority.

11. Breach of Security

11.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Risk Management Documentation.

11.2 The security incident management process set out in the Risk Management Documentation shall, as a minimum, require the Supplier upon becoming aware of a Breach of Security or an attempted Breach of Security to:

11.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority which shall be completed within such timescales as the Authority may reasonably require) necessary to:

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

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet any Performance Indicator, the Supplier shall be granted relief against the failure to meet such affected Performance Indicator for such period as the Authority, acting reasonably, may specify by written notice to the Supplier; and

(d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

11.2.2 as soon as reasonably practicable and, in any event, within 24 Hours, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

11.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the Information System and/or the Risk Management Documentation with the Baseline Security Requirements and/or this Agreement, then such action and any required change to the Information System and/or Risk Management Documentation shall be completed by the Supplier at no cost to the Authority.

11.4 If the Supplier fails to comply with its obligations set out in this Paragraph 11, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Authority, shall permit the Authority to terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 30.2(b).

12. Data Processing, Storage, Management and Destruction

12.1 In addition to the obligations on the Supplier set out Clause 20 (Protection of Personal Data) in respect of Processing Personal Data and compliance with the Data Protection Legislation , the Supplier shall:

12.1.1 Process Authority Data only at the Sites and such Sites must not located outside of the European Union except where the Authority has given its consent to a transfer of the Authority Data to outside of the European Union in accordance with Clause 20;

12.1.2 on demand, provide the Authority with all Authority Data in an agreed open format;

12.1.3 have documented processes to guarantee availability of Authority Data in the event of the Supplier ceasing to trade;

12.1.4 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority; and

12.1.5 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as directed by the Authority.

Annex 1: Baseline Security Requirements

1. Security Classification of Information

If the provision of the Services requires the Supplier to Process Authority Data which is classified as:

1.1 OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or

1.2 SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2. End User Devices

2.1. The Supplier shall ensure that any Authority Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.

2.2. The Supplier shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

3. Networking

3.1. The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.

4. Personnel Security

4.1. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

4.2. The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access

to IT systems which Process Authority Data or data which is classified as OFFICIAL-SENSITIVE.

4.3. The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

4.4. The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.

4.5. The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.

5. Identity, Authentication and Access Control

5.1. The Supplier shall operate an access control regime to ensure:

5.1.1. all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

5.1.2. all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

5.1.3. The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.

5.1.4. The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.

6. Audit and Protective Monitoring

6.1. The Supplier shall collect audit records which relate to security events in [Core] Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the [Core Information

Management System], to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

6.2. The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

6.3. The retention periods for audit records and event logs must be agreed with the Authority and documented **in the Risk Management Documentation.**

7. Secure Architecture

7.1. The Supplier shall design the Core Information Management System in accordance with:

7.2. the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

7.3. the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

7.4. the **NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:**

(a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;

(j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors;

(n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

Annex 2

CORE INFORMATION MANAGEMENT SYSTEM DIAGRAM

[To be included as a Milestone Acceptance Criteria for **Ready to Commence Service within Milestone Payment – IMPM2**]

Annex 3

Risk Management Documentation Template

[To be included as a Milestone Acceptance Criteria for **Ready to Commence Service within Milestone Payment – IMPM2**]

Author:

Owner:

Date:

Version:

1 EXECUTIVE SUMMARY

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

Change History

Version Num-ber	Date of Change	Change made by	Nature and reason for change

References, Links and Dependencies

This document is dependent on the supporting information and assurance provided by the following documents.

ID	Document Title	Reference	Date
1.			
2.			
3.			

2 SYSTEM DESCRIPTION

2.1 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

< Who owns the system and operates the system and the organisational governance structure.This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

3 RISK ASSESSMENT

3.1 **Accreditation/Assurance Scope**

<This section describes the scope of the Accreditation/Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 **Risk appetite**

<A risk appetite should be agreed with the SIRO/SRO and included here.>

3.3 **Business impact assessment**

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 **Risk assessment**

<The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inher-ent risk level	Vulnerability	Controls	Resid-ual risk level

3.5 **Controls**

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

3.6 **Residual risks and actions**

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4 IN-SERVICE CONTROLS

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO27001 certification should be included. This section should include at least:

a) information risk management and timescales and triggers for a review;

b) contractual patching requirements and timescales for the different priorities of patch;

c) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;

d) configuration and change management;

e) incident management;

f) vulnerability management;

g) user access management; and

h) data sanitisation and disposal.>

5 SECURITY OPERATING PROCEDURES (SYOPS)

< If needed any SyOps requirements should be included and referenced here.>

6 MAJOR HARDWARE AND SOFTWARE AND END OF SUPPORT DATES

< This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

7 INCIDENT MANAGEMENT PROCESS

<The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

8 SECURITY REQUIREMENTS FOR USER ORGANISATIONS

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9 REQUIRED CHANGES REGISTER

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third	Authority name	11/11/2018	Jul-2019	Open

		Party supplier XXXX will be performing the print capability				

10 PERSONAL DATA PROCESSING STATEMENT

<This should include: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach.>

11 ANNEX A. ISO27001 AND/OR CYBER ESSENTIAL PLUS CERTIFICATES

<Any certifications relied upon should have their certificates included>

12 Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached>

13 Annex C. Protecting Bulk Data assessment if required by the Authority/Customer

<A spreadsheet may be attached>

14 Annex E. Latest ITHC report and Vulnerability Correction Plan

SCHEDULE 2.5

INSURANCE REQUIREMENTS

Insurance Requirements

1. OBLIGATION TO MAINTAIN INSURANCES

1.1. Without prejudice to its obligations to the Authority under this Agreement, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 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 the date on which the relevant risk commences.

1.2. The Insurances shall be maintained in accordance with Good Industry Practice and (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.

1.3. The Insurances shall be taken out and maintained with insurers who are:

(a) of good financial standing;

(b) appropriately regulated;

(c) regulated by the applicable regulatory body and is in good standing with that regulator; and

(d) except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.

1.4. The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

2. GENERAL OBLIGATIONS

Without limiting the other provisions of this Agreement, the Supplier shall:

(a) take or procure the taking of all reasonable risk management and risk control measures in relation to the Services 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;

(b) promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

(c) 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.

3. FAILURE TO INSURE

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 any of the Insurances or maintain any of the Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. EVIDENCE OF INSURANCES

The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Agreement.

5. CANCELLATION

5.1. Subject to Paragraph 6.2, the Supplier shall notify the Authority in writing at least 5 Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

5.2. Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 6.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

6. INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

6.1. The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Agreement for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services and/or this Agreement, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.

6.2. The Supplier shall maintain a register of all claims under the Insurances in connection with this Agreement and shall allow the Authority to review such register at any time.

6.3. Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

6.4. 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 Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Agreement or otherwise.

ANNEX 1: REQUIRED INSURANCES

PART A: INSURANCE CLAIM NOTIFICATION

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within 20 Working Days after any insurance claim in excess of £100,000 relating to or arising out of the provision of the Services or this Agreement 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 Authority) full details of the incident giving rise to the claim.

PART B: THIRD PARTY PUBLIC AND PRODUCTS LIABILITY INSURANCE

1. Insured

The Supplier

2. Interest

To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental:

(a) death or bodily injury to or sickness, illness or disease contracted by any person; and

(b) loss of or damage to physical property;

happening during the period of insurance (as specified in Paragraph 5)and arising out of or in connection with the provision of the Services and in connection with this Agreement.

3. Limit of indemnity

[redacted]

4. Territorial limits

United Kingdom

5. Period of Insurance

From the date of this Agreement for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing.

6. Cover features and extensions

6.1. Indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

7. Principal exclusions

7.1. War and related perils.

7.2. Nuclear and radioactive risks.

7.3. Liability for death, illness, disease or bodily injury sustained by employees of the Insured arising out of the course of their employment.

7.4. Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.

7.5. Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.

7.6. Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.

7.7. Liability arising from the ownership, possession or use of any aircraft or marine vessel.

7.8. Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

8. Maximum deductible threshold

[redacted]

PART C: UNITED KINGDOM COMPULSORY INSURANCES

The Supplier shall meet its insurance obligations under applicable Law in full, including, United Kingdom employers' liability insurance and motor third party liability insurance.

PART D: ADDITIONAL INSURANCES

PROFESSIONAL INDEMNITY INSURANCE

1. **Insured**

   The Supplier

2. **Interest**

   To indemnify the Insured for all sums which the Insured shall become legally liable to pay (including claimant's costs and expenses) as a result of any claim or claims first made against the Insured during the Period of insurance by reason of any act, error and/or omission arising from or in connection with professional services relevant to this Agreement.

3. **Limit of indemnity**

   [redacted]

4. **Territorial limits**

   United Kingdom

5. **Period of insurance**

   From the date of this Agreement for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing and a period of six (6) years following the expiry or termination of this Agreement whichever occurs earlier..

6. **Cover features and extensions**

   6.1. Loss of documents and computer records extension.

   6.2. Legal liability assumed under contract, duty of care agreements and collateral warranties.

   6.3. Retroactive cover from the date of this Agreement or retroactive date no later than the date of this Agreement in respect of any policy provided on a claims made form of policy wording.

7. **Principal exclusions**

   7.1. War and related perils.

   7.2. Nuclear/radioactive risks.

   7.3. Insolvency of the Insured (as set out in paragraph 4.1 above)

7.4. Bodily injury, sickness, disease or death sustained by any employee of the Insured (as set out in paragraph 4.1 above) arising out of the course of their employment.

8. Maximum deductible threshold

[redacted]

CRIME INSURANCE

1. **Insured**

   The Supplier

2. **Interest**

   To indemnify the Insured in respect of a direct financial loss sustained by the Insured resulting from either;

   2.1. fraud or dishonesty committed by any employee of the Insured acting alone or in collusion with others; or

   2.2. a fraudulent act committed by any other person that is not a director, officer, partner, trustee or employee of the Insured which is committed with the principal intent to cause the Insured to sustain such loss and is first discovered by the Insured during the Period of insurance.

3. **Limit of indemnity**

   [redacted]

4. **Territorial limits**

   United Kingdom

5. **Period of Insurance**

   From the date of this Agreement for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing and a period of six (6) years following the expiry or termination of this Agreement whichever occurs earlier..

6. **Cover features and extensions**

   6.1 Retroactive cover from the date of this Agreement or retroactive date no later than the date of this Agreement

   6.2. Money or securities belonging to any other individual or organisation that is not the Insured but is in the care custody and control of the Insured

   6.3. Physical loss damage or destruction of money or securities, including damage to safes or vaults

   6.4. Theft of money or securities, including whilst in transit and whilst in the care, custody and control of a security company

7. **Principal exclusions**

   7.1. War and related perils.

   7.2. Nuclear/radioactive risks.

   7.3. Consequential loss

   7.4. Credit risks

7.5. Acts of directors, partners or major shareholders of the Insured

7.6. Fines, penalties or damages

7.7. Loss sustained after knowledge

7.8. Physical loss destruction or damage of the premises of the Insured

7.9. Proprietary information, trade secrets and intellectual property

7.10. Voluntary exchange or purchase 8.

8. Maximum deductible threshold

[redacted]

Insurance Table class of insurance	Insurer identity (including any excess layer insurers)	Supplier proposed maximum deductible threshold	Agreement to the requirements of Schedule 2.5 (Insurance Requirements) clauses 1 to 6	Agreement to the requirements of Annex 1 of Schedule 2.5
[redacted]		[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]

SCHEDULE 2.6

SOCIAL VALUE

Social Value

1. Scope

1.1. This Schedule 2.6 (Social Value) sets out the provisions with regards to the Social Value themes of:

(A) Diverse Supply Chains and Inclusion, Mental Health and Well-Being are set out in Part A (Equality and Supplier Diversity);

(B) Skills and Employment is set out in Part B (Strategic Labour Needs and Training); and

(C) Safe Supply Chains is set out in Part C (Ethical Sourcing) and Schedule 2.4 (Security Management).

PART A

Equality and Supplier Diversity

2. Compliance

2.1. Without limiting any other provision of this Agreement, the Supplier shall, in relation to the Services:

(A) not unlawfully discriminate; and

(B) procure that the Supplier's Personnel do not unlawfully discriminate,

within the meaning and scope of the Equality Act 2010 (the "**Equality Act**") and any other relevant enactments in force from time to time relating to discrimination in employment.

3. The General Equality Duty

3.1. The Supplier acknowledges that under section 149 of the Equality Act DIT is under a duty to have due regard for the need to, amongst other things:

(A) eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by or under the Equality Act;

(B) advance equality of opportunity between people who share a relevant protected characteristic and persons who do not share it; and

(C) foster good relations between people who share a relevant protected characteristic and persons who do not.

3.2. As at the Effective Date, the nine (9) protected characteristics as set out in the Equality Act are: (i) age; (ii) disability; (iii) gender reassignment; (iv) marriage and civil partnership; (v) pregnancy and maternity; (vi) race; (vii) religion and belief; (viii) sex; and (ix) sexual orientation.

3.3. In the performance of this Agreement, the Supplier shall, and shall procure that its Sub-Contractors shall, assist and co-operate with DIT to the greatest extent possible in satisfying this duty.

3.4. DIT's fair treatment at work policy (the "**Fair Treatment at Work Policy**") as updated from time to time and notified to the Supplier requires DIT's own staff and those of its contractors to comply fully with the Fair Treatment at Work Policy to eradicate harassment in the workplace. The Supplier shall:

(A) ensure that its staff, and those of its Sub-Contractors who are engaged in the performance of this Agreement (including Key Sub-Contractors) are fully conversant with the requirements of the Fair Treatment at Work Policy;

(B) fully investigate allegations of workplace harassment in accordance with the Fair Treatment at Work Policy; and

(C) ensure that appropriate, effective action is taken where harassment is found to have occurred.

4. Approved Equality and Diversity Plan

4.1. The Supplier shall ensure that the Virtual Library at all times includes up-to-date versions of the Approved Strategic Equality and Diversity Plan, the Approved Equality and Diversity Training Plan and the Approved Supplier Diversity Plan.

5. Strategic Equality and Diversity Plan

5.1. The Supplier shall comply with the Approved Strategic Equality and Diversity Plan and shall procure that each of its Sub-Contractors:

(A) adopts and implements; and

(B) in respect of other tiers of sub-contractors beneath the Sub-Contractors ("**Indirect Sub-Contractors**"), procures that those Indirect Sub-Contractors adopt and implement,

an equality and diversity policy in respect of their respective employees engaged in relation to the performance of this Agreement which is at least as extensive in scope as the Approved Strategic Equality and Diversity Plan.

6. Equality and Diversity Training Plan

6.1. During the Term, the Supplier shall comply with the Approved Diversity Training Plan in relation to all of its Personnel and shall procure that each of its Sub-Contractors:

(A) adopts and implements; and

(B) in respect of its Indirect Sub-Contractors, procures that those Indirect Sub-Contractors adopt and implement,

a diversity training plan in respect of their respective employees engaged in relation to the performance of this Agreement which is at least as extensive in scope as the Approved Equality and Diversity Training Plan.

7. Supplier Diversity

7.1. During the Term, the Supplier shall at all times comply with the Approved Supplier Diversity Plan. The Supplier shall procure that each of its Sub-Contractors:

(A) adopts and implements; and

(B) in respect of its Indirect Sub-Contractors, procures that each such Indirect Sub-Contractor adopt and implement,

a supplier diversity plan in relation to the performance of this Agreement which is as least as extensive as the Approved Supplier Diversity Plan.

8. Monitoring and Reporting

8.1. Subject to paragraph 8.2, the Supplier shall provide to DIT on the Effective Date and subsequently every six (6) months thereafter (or at such lesser or greater intervals as determined by DIT acting reasonably and notified to the Supplier) the following information:

(A) the proportion of Supplier employees, agents and consultants and, to the extent reasonably possible, the employees of its Sub-Contractors and Indirect Sub-Contractors engaged pursuant to the terms of the relevant subcontracts in the performance of this Agreement, who are:

(1) female;

(2) of non-white British origin or who classify themselves as being non-white British;

(3) from the local community; and/or

(4) disabled; and

(5) the proportion of its Sub-Contractors and Indirect Sub-Contractors that are Small or Medium Enterprises and/or Black and Minority Ethnic Businesses (BMEs).

8.2. The Supplier shall ensure at all times that it, its Sub-Contractors and its Indirect Sub-Contractors comply with the requirements of the General Data Protection Regulation (as may be amended) in the collection and reporting of the information to DIT pursuant to paragraph 8.1.

9. Diversity Infractions

9.1. If the Supplier or any of its Sub-Contractors commits a Diversity Infraction, DIT shall be entitled (but shall not be obliged) to:

(A) without prejudice to any other right or remedy it might have under this Agreement and where a Diversity Infraction is committed by the Supplier, serve written notice upon the Supplier identifying in reasonable detail the nature of the Diversity Infraction and the Supplier shall cease committing and remedy such Diversity Infraction within thirty (30) calendar days of receipt of such notice (or such longer period as may be specified by DIT in the notice); or

(B) where the Diversity Infraction is committed by a Sub-Contractor of the Supplier, serve written notice upon the Supplier identifying in reasonable detail the nature of the Diversity Infraction, and the Supplier shall procure that the relevant Sub-Contractor ceases committing and remedies the Diversity Infraction within thirty (30) calendar days of receipt by the Supplier of such notice (or such longer period as may be specified by DIT in the notice).

9.2. If the Supplier fails to procure the remedy of any Diversity Infraction referred to in paragraph 9.1(A), DIT may (in its sole discretion) serve a further written notice upon the Supplier and within thirty (30) calendar days of receipt of such further notice (or such longer period as may be specified by DIT in the notice), the Supplier shall terminate the engagement of its Sub-Contractor under the relevant Sub-Contract and procure performance of the affected works or services by another Sub-Contractor and DIT may, in its sole discretion, require that the Supplier provides evidence to substantiate such Sub-Contractor's compliance with the obligations specified in paragraphs 2 to 7 of this schedule.

10. Equality and Diversity Audit

10.1. DIT (or such Third Party as may be nominated by DIT) may undertake an audit of any and/or all information relating to the Supplier's compliance with paragraphs 2 to 7 of this schedule in accordance with Clause 2.1 (a)(Records, Reports, Audits & Open Book Data) of this Agreement.

10.2. The Supplier shall, and shall procure that each of its Sub-Contractors shall and, where applicable subject to the provisions of paragraphs 2 to 6, its Indirect Sub-Contractors shall, maintain and retain the Minimum Records for a minimum of six (6) years with respect to all matters relating to the performance of paragraphs 2 to 7. The Supplier shall procure that each Sub-Contract between it and its Sub-Contractors and, where applicable, subject to the provisions of paragraphs 2 to 6, each sub-contract between its Sub-Contractor and any Indirect Sub-Contractor of the Supplier and each sub-contract between the Supplier's Indirect Sub-Contractors shall contain rights of audit in favour of and enforceable by DIT substantially equivalent to those granted by the Supplier pursuant to paragraph 10.1.The Supplier shall promptly provide, and shall procure that its Sub-Contractors shall and, where applicable subject to the provisions of paragraphs 2 to 6, its indirect sub-contractors shall, promptly provide all reasonable co-operation to DIT or its nominated Third Party in relation to any audit including, to the extent reasonably possible in each particular circumstance:

(A) granting or procuring the grant of access to any premises used in the Supplier's performance of this Agreement or in the relevant Sub-Contractor's or Indirect Sub-Contractor's performance of its sub-contract, whether on the Supplier's own premises or otherwise;

(B) granting or procuring the grant of access to any equipment (including all computer hardware and software and databases) used (whether exclusively or non-exclusively) in the performance of the Supplier's or relevant Sub-Contractor's or Indirect Sub-Contractors obligations specified in paragraphs 2 to 7, wherever situated and whether the Supplier owns the equipment or otherwise; and

(C) complying with DIT 's (or its nominated Third Party's) reasonable requests for access to the Supplier's senior Personnel (including Key Personnel) engaged

in the performance of this Agreement or the relevant Sub-Contractor's or Indirect Sub-Contractor's performance of its sub-contract.

PART B

Strategic Labour Needs and Training

11. Introduction

11.1. Without prejudice to the other provisions in this Agreement relating to Supplier's Personnel this Schedule sets out the Supplier's obligations in respect of:

(A) supporting the DIT Group (and Third Parties nominated by the DIT Group) in the implementation of the Skills and Employment Strategy; and

(B) ensuring that the Supplier attracts, develops and retains Personnel with the skills necessary to deliver the Services throughout the Term.

12. SLNT Plan

12.1. Upon receiving comments from DIT in relation to the Initial SLNT Plan, the Supplier shall within twenty (20) Working Days:

(A) develop an updated strategic labour needs and training plan based on the Initial SLNT Plan and taking into account DIT 's comments and requirements; and

(B) submit a revised copy of the Initial SLNT Plan to DIT for Approval.

12.2. . If the Initial SLNT Plan developed in accordance with paragraph 12.1 is:

(A) Approved, the Supplier shall adopt such plan immediately as the Agreed SLNT Plan and shall append the Agreed SLNT Plan to this Schedule in place of the Initial SLNT Plan in accordance with the Change Control Procedure (and such plan shall only be required to be appended once);

(B) not Approved, the Supplier shall amend the Initial SLNT Plan and resubmit it to DIT for Approval within twenty (20) Working Days of being informed by DIT that such plan is not Approved.

12.3. If DIT does not Approve the Initial SLNT Plan following its resubmission, the matters preventing such Approval shall be resolved in accordance with the Dispute Resolution Procedure set out in Schedule 8.3 (*Dispute Resolution Procedure*) of this Agreement.

12.4. Without limiting any other provision of this Agreement, the Supplier shall:

(A) comply with provisions of the Agreed SLNT Plan; and

(B) at no additional cost to DIT and subject to the provisions of paragraph 12.5 below, review and amend the Agreed SLNT Plan and Implementation Plan:

(1) as a minimum, every twelve (12) months following the Operational Commencement Date or at such other times as may be requested by DIT , to reflect:

(a) Good Industry Practice;

(b) any changes to the nature of the Services;

(c) any amendments proposed by DIT .

12.5. Any changes or amendments to the Agreed SLNT Plan shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by DIT.

13. SLNT Co-ordinator

13.1. Within twenty (20) Working Days of the Effective Date, the Supplier shall nominate a member of it's Personnel with the necessary skills and authority to:

(A) be responsible for the implementation and on-going development and maintenance of the Agreed SLNT Plan; and

(B) act as the single point of contact between DIT Personnel on all matters concerning the Agreed SLNT Plan,

the ("**SLNT Co-ordinator**").

13.2. The Parties shall add the SLNT Co-ordinator to the list of Key Personnel set out Schedule 9.2 (Key Personnel).

14. Monitoring and Reporting

14.1. The Supplier shall provide the Contract and Operational Board with a Monthly SLNT Monitoring Report (in accordance with paragraph 6.1(i) of Schedule 8.1(Governance) detailing the Supplier's performance against the Agreed SLNT Plan.

14.2. The Supplier shall ensure at all times that it complies with Schedule 11 (*Processing Personal Data*) of this Agreement in the collection and reporting of information to DIT pursuant to paragraph 14.1above.

15. SLNT Infractions

17.1 If the Supplier fails to:

(A) ensure that each SLNT Output for the monitoring period is delivered in accordance with Agreed SLNT Plan; and/or

(B) review the Agreed SLNT Plan in accordance with paragraph 12.4 of this Schedule (Social Value),then the Supplier's Chief Executive shall attend a meeting with DIT to explain the reasons for such failure.

16. SLNT Audit

16.1. DIT may from time to time undertake any audit or check of any and all information regarding the Supplier's compliance the provisions of this Schedule in accordance with Clause 2.1 (a)(*Records, Reports, Audits & Open Book Data*).

16.2. The Supplier shall maintain and retain records relating to the Agreed SLNT Plan and its compliance with the provisions of this Schedule for a minimum of six (6) years.

PART C

Ethical Sourcing

17. Introduction to Ethical Sourcing

17.1. DIT is committed to ensuring that workers employed in its supply chains throughout the world are treated fairly, humanely and equitably. In the course of complying with this Agreement, the Supplier shall comply with and shall procure that its sub-contractors (as applicable) comply with those principles of the Ethical Trading Initiative (ETI) Base Code as are detailed here http://www.ethicaltrade.org/resources/key-eti- resources/eti-base-code , or an equivalent code of conduct (the "Ethical Sourcing Principles") in relation to the provision of the Services.

17.2. The Supplier shall conduct risk analysis of (i) human rights issues, and (ii) labour conditions, of the supply chains used in the fulfilment of this Agreement, and shall agree with DIT a process for managing high-risk supply chains. This may include where appropriate the carrying out of social audits and the agreement of corrective action plans.

17.3. During the course of this Agreement, if DIT has reasonable cause to believe that the Supplier is not complying with any of the Ethical Sourcing Principles, DIT shall notify the Supplier and the Parties shall agree an action plan with appropriate timeframes for compliance by the Supplier (the "**Action Plan**"), such Action Plan to be agreed by the Parties by no later than 20 (twenty) Working Days from the date of DIT notifying the Supplier that remedial action is required or such other period as the Parties may otherwise agree in writing. The costs of the creation and implementation of the Action Plan shall be borne by the Supplier.

17.4. During the course of this Agreement, DIT has the right to request the Service Provider to carry out one or more audits in accordance with Clause 2.1 (a)(*Records, Reports, Audits & Open Book Data*). to verify whether the Supplier is complying with the Ethical Sourcing Principles (or any associated Action Plan).

ANNEX 1 TO SCHEDULE 2.6

Equality and Inclusion Policy –DIT's fair treatment at work policy (the "Fair Treatment at Work Policy") as updated from time to time.

ANNEX 2 TO SCHEDULE 2.6

SLNT Template

The SLNT Template shall take the form set out in this Annex.

SLNT Activity Breakdown

[To be included in the Document Library prior to Ready to Commence Service within Milestone Payment – IMPM2]

ANNEX 3 TO SCHEDULE 2.6

Initial SLNT Plan

[To be included in the Document Library prior to Ready to Commence Service within Milestone Payment – IMPM2]

ANNEX 4 TO SCHEDULE 2.6

[redacted]

SCHEDULE 3

AUTHORITY RESPONSIBILITIES

Authority Responsibilities

1. INTRODUCTION

1.1. The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Agreement. Any obligations of the Authority in Schedule 2.1 (Services Description) and Schedule 4.1 (Supplier Solution) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be "Authority Responsibilities" and cross referenced in the table in Paragraph 3.

1.2. The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2. GENERAL OBLIGATIONS

The Authority shall:

(a) perform those obligations of the Authority which are set out in the Clauses of this Agreement and the Paragraphs of the Schedules (except Schedule 2.1 (Services Description) and Schedule 4.1 (Supplier Solution));

(b) use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority's staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;

(c) provide sufficient and suitably qualified staff to fulfil the Authority's roles and duties under this Agreement as defined in the Implementation Plan;

(d) use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Agreement provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority; and

(e) procure for the Supplier such agreed access and use of the Authority Premises (as a licensee only) and facilities (including relevant IT systems) as is reasonably required for the Supplier to comply with its obligations under this Agreement, such access to be provided during the Authority's normal working hours on each Working Day or as otherwise agreed by the Authority (such agreement not to be unreasonably withheld or delayed).

3 SPECIFIC OBLIGATIONS

The Authority shall, in relation to this Agreement perform the Authority's responsibilities identified as such in this Agreement the details of which are set out below:

Document	Paragraph (Location)
Schedule 2.1 *(Services Description)*	1. As part of the Joint Service Design, and to support the solution development and the Authority audit processes, the Authority shall confirm, no later than one (1) Week after being provided with a final version of the eligibility criteria by the Supplier, that the eligibility criteria accurately represents the criteria developed during of Joint Service Design. The eligibility criteria will form the basis for checking and validating the eligibility of SME Applications and the Authority audit processes. 2. The Authority in accordance with the Detailed Implementation Plan (or a schedule of Joint Service Design activities agreed between the Parties) shall provide the Supplier with access to the appropriate DIT personnel to participate in workshops and to provide guidance to the Supplier as part of validation of the related rules and guidance related to the SME Applicant and SME Application. DIT will make reasonable efforts to support the Supplier in recruiting assistance from other key stakeholders such as MHCLG, LEPS and SMEs, to participate in workshops and provide guidance (related to the SME Applicant and SME Application) to the Supplier as part of the Joint Service Design. 3. The Authority in accordance with the Detailed Implementation Plan (or a schedule of Joint Service Design activities agreed between the Parties) shall participate in Joint Service Design and support the solution development. The Joint Service Design is part of the Parties' approach to assuring that the solution meets the requirements of this Agreement and for the Authority to approve the Supplier's procedures and system design configuration as being in accordance with the Authority's Requirements as set out in Schedule 2.1, in the following areas (but not limited to): • Scheme Governance (section 3.1 Standards, working practices and principles), in particular establishing objective criteria for the assessment of value for money to be applied as part of the Supplier's solution. • Branding & Publicity (section 3.2 Branding and Publicity) • FOIA (section 3.3 Reporting of grant information across government) • ESIF Management Processes & Documents (section 3.4 Managing ERDF Projects) and (section 3.6 European Structural and Investment Funds: outputs and results)

	• Summative assessments' compliance process (section 3.5 Summative assessments) • Reporting of business impacts (section 4 SME Application & Award) and (section 6 Post-Award) • Claims and payments process (section 5 Claims, Payment & Close-out) • Reporting of business impacts (section 6 Post-Award) and (section 7.1 Reporting & Operations) • Reporting, and evidence collection approach (section 7.1 Reporting & Operations) 4. The Authority shall present the output of the Joint Service Design, including the eligibility criteria, to MHCLG and shall seek comment or feedback. Any feedback received shall be shared with the Supplier on receipt. 5. The Authority shall use best endeavours to give reasonable notice of any meetings that the Supplier is requested to attend and any Project Change requests requiring Supplier assistance 6. The Supplier shall ensure that the Summative Assessor attends key Joint Service Design meetings as required. 7. The Authority shall approve the approach to branding and promotion (as may be updated from time) and shall: a) provide the Supplier with DIT guidance on branding and promotion. b) confirm all proposed outbound communications; and support the Supplier with signposting ESIF branding guidance. 8. The Authority shall utilise the self-serve capability to obtain any project related data or documentation in electronic format providing the following conditions are satisfied: a) The Supplier has provided the necessary training and guidance to the authorised DIT users. b) During acceptance testing of the solution the self-serve capability is tested by DIT users to test any required reports specified during the Joint Service Design. c) Thorough testing is carried out on all processes with any resulting defects being resolved prior to the

	Operational Service Commencement Date. Authorised DIT users shall be involved throughout such Testing and shall have the opportunity give feedback on the design and test required reports. d) The self-serve solution has the capability to generate pre-defined reports specified during Joint Service Design and ad hoc reports consistent with the reporting requirements set out variously in Schedule 2.1 can be created by a reasonably competent user. e) The self-serve solution allows a reasonably competent user to produce analytical queries(as set out in Schedule 2.1) f) Reasonable support and assistance is provided to authorised DIT users as required throughout the Term of the Contract. 9. Requirement F15 - The Authority shall set reasonable timescales to address recommendations from Data Protection audits, reflecting the materiality of the issue and the complexity and scale of the action required 10. Requirement D13- The Authority shall provide the template for Summative Assessment data within one (1) month of the Effective Date and ensure data requirements are provided during service design to ensure Summative Assessment needs are included. 11. The Authority shall provide reasonable notice of any reports required to meet MHCLG and the Authority's needs. 12. Requirement L.22 - The Authority shall provide the Supplier with the journal upload template for journals relating to the Authority's financial accounts as described in L.22 of Schedule 2.1 (Service Description) no later than 30 days after the Effective Date, and then as and when updated.
Schedule 4.1 (Supplier Solution)	1. [redacted]

	3. [redacted]
	[redacted]
	[redacted]
	[redacted]
	7. [redacted]

SCHEDULE 4.1

SUPPLIER'S SOLUTION

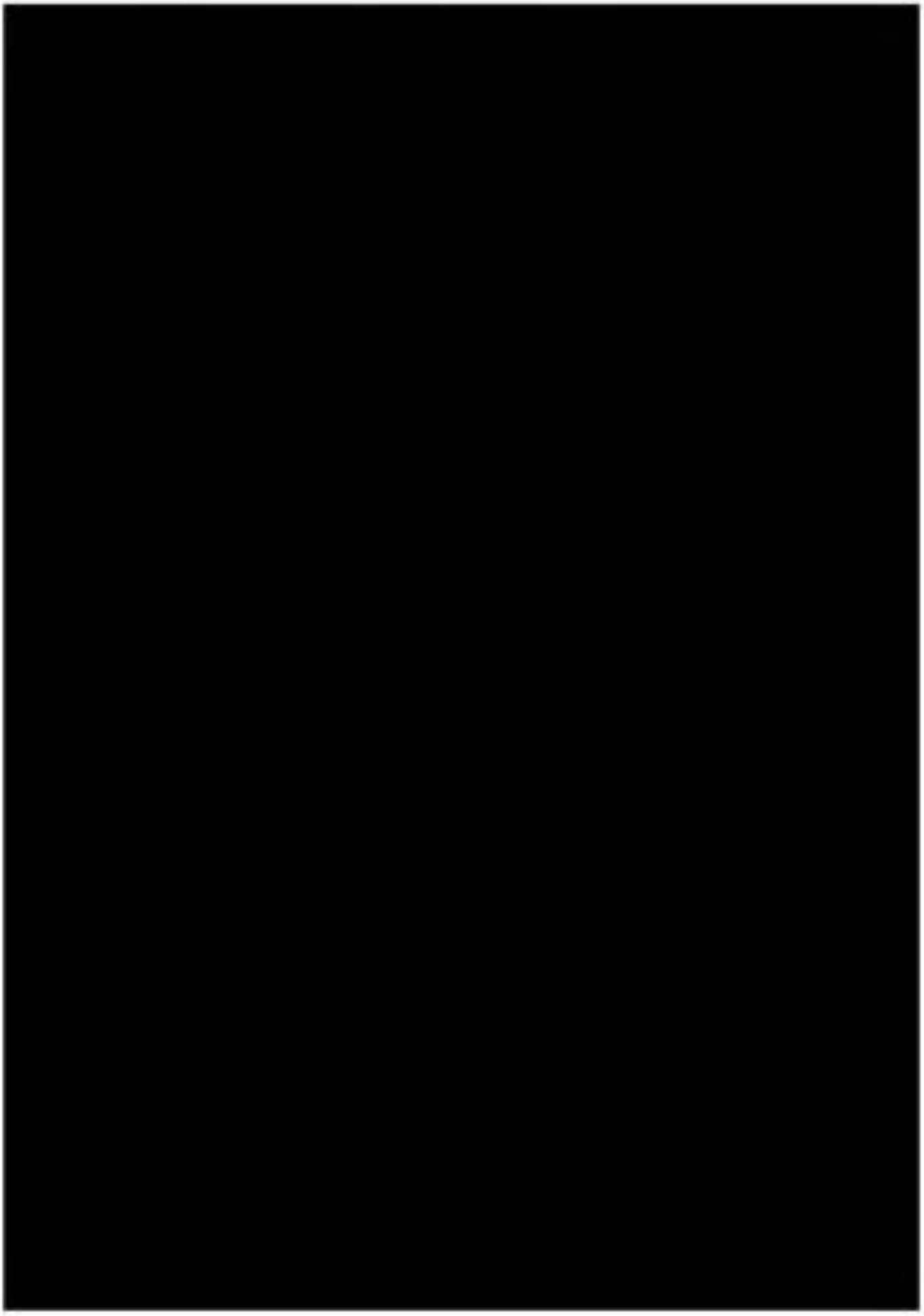
Contents

[redacted]

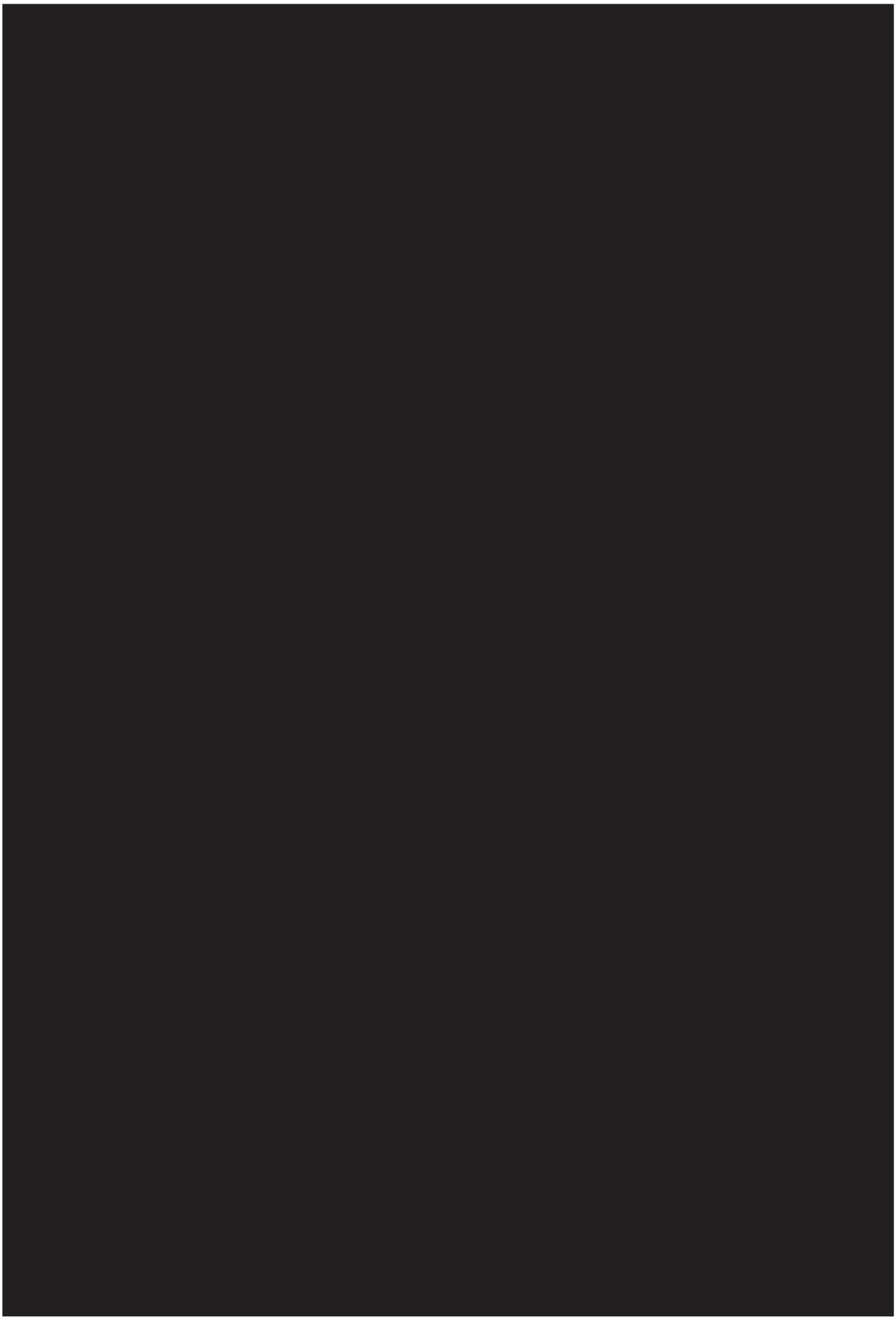
[redacted]

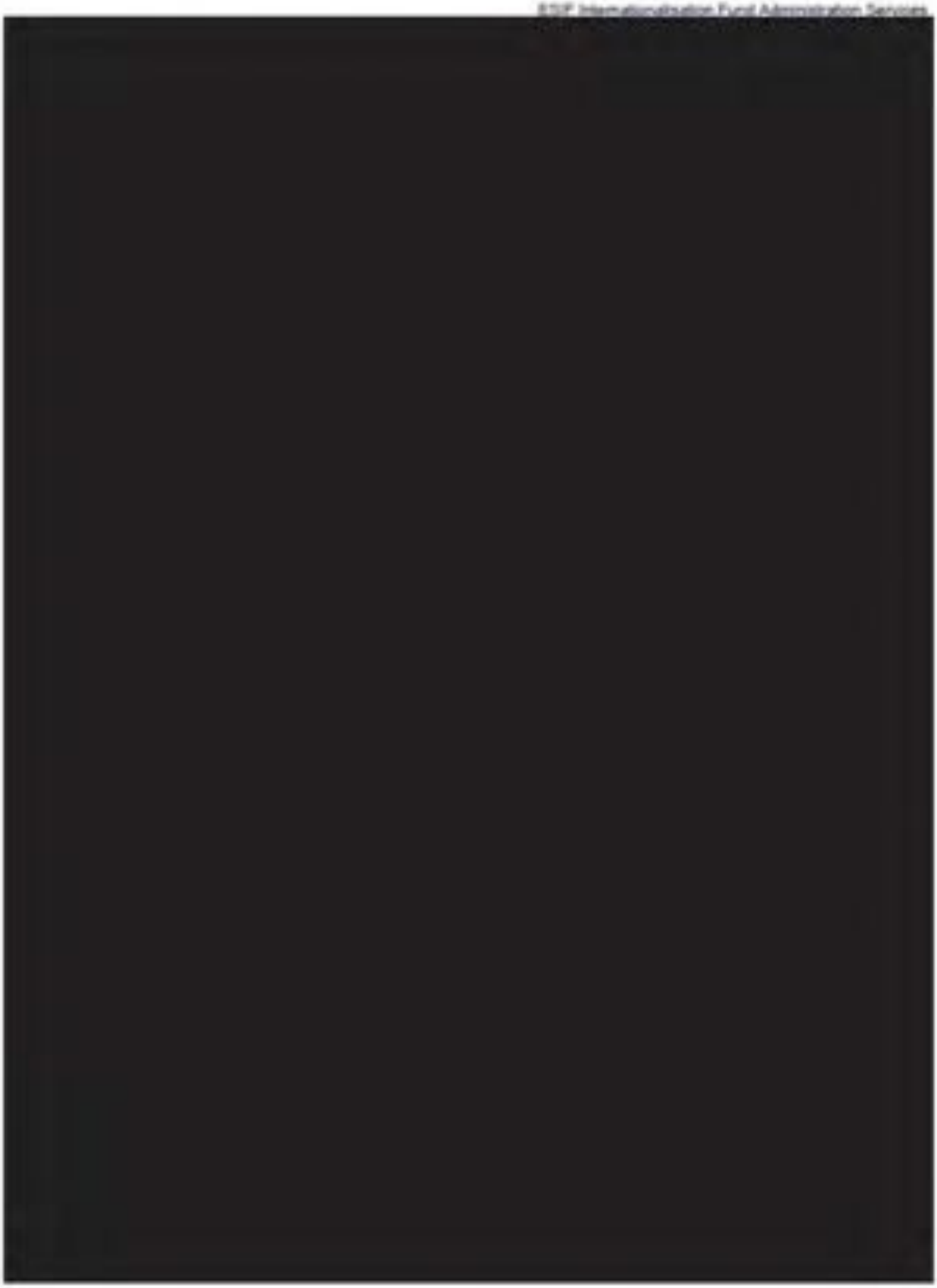
[redacted]

[redacted]



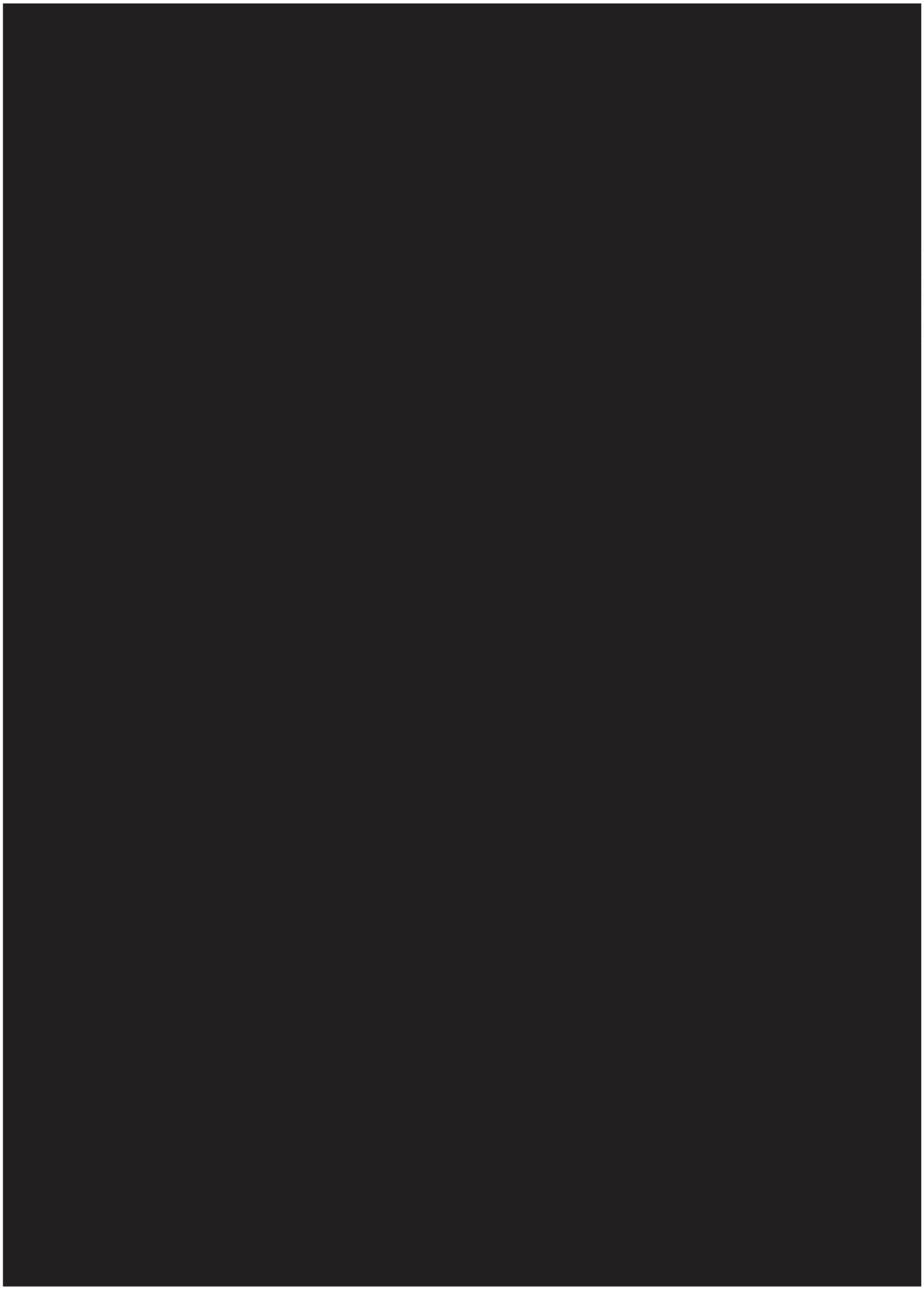
3. Module Sv - Subsection 3: Ethical Sourcing





[redacted]

[redacted]



[redacted]

1 [redacted]

[redacted]

2 [redacted]

[redacted]

3 [redacted]

4 [redacted]

5 [redacted]

6

6. Module Da – Subsection 3: Service Delivery and Quality Controls & Assurance

1 [redacted]

[redacted]

2 [redacted]

[redacted]

3 How [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

7 [redacted]

[redacted]

8 [redacted]

[redacted]

[redacted]

[redacted]

1 Application Overview

[redacted]

1.1 [redacted]

[redacted]

1.1.1 [redacted]

[redacted]

1.1.2 [redacted]

[redacted]

1.1.3 [redacted]

[redacted]

1.2 [redacted]

[redacted]

1.2.1 [redacted]

[redacted]

[redacted]

1.2.2 [redacted]

[redacted]

1.2.3 [redacted]

[redacted]

1.2.4 [redacted]

[redacted]

2 [redacted]

2.1 [redacted]

[redacted]

2.2 [redacted]

[redacted]

[redacted]

2.3 [redacted]

[redacted]

2.3.1 [redacted]

[redacted]

2.4 [redacted]

[redacted]

2.5 [redacted]

[redacted]

3 [redacted]

3.1 [redacted]

[redacted]

3.2 [redacted]

[redacted]

3.3 [redacted]

[redacted]

[redacted]

3.4 [redacted]

[redacted]

3.5 [redacted]

[redacted]

4 [redacted]

[redacted]

4.1 [redacted]

[redacted]

4.2 [redacted]

4.2.1 [redacted]

4.2.2 [redacted]

4.2.3 [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

4.2.4 [redacted]

[redacted]

4.2.5 [redacted]

[redacted]

4.2.6 [redacted]

[redacted]

[redacted]

4.2.7 [redacted]

[redacted]

4.2.8 [redacted]

[redacted]

[redacted]

4.2.9 [redacted]

[redacted]

5 [redacted]

[redacted]

[redacted]

5.1 [redacted]

[redacted]

[redacted]

5.2 [redacted]

[redacted]

5.3 [redacted]

[redacted]

6 [redacted]

6.1 [redacted]

[redacted]

[redacted]

6.2 [redacted]

[redacted]

[redacted]

7 [redacted]

7.1 [redacted]

[redacted]

7.1.1 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

7.1.2 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

7.1.3 [redacted]

[redacted]

7.1.4 [redacted]

[redacted]

7.2 [redacted]

[redacted]

7.2.1 [redacted]

[redacted]

7.2.2 Security

[redacted]

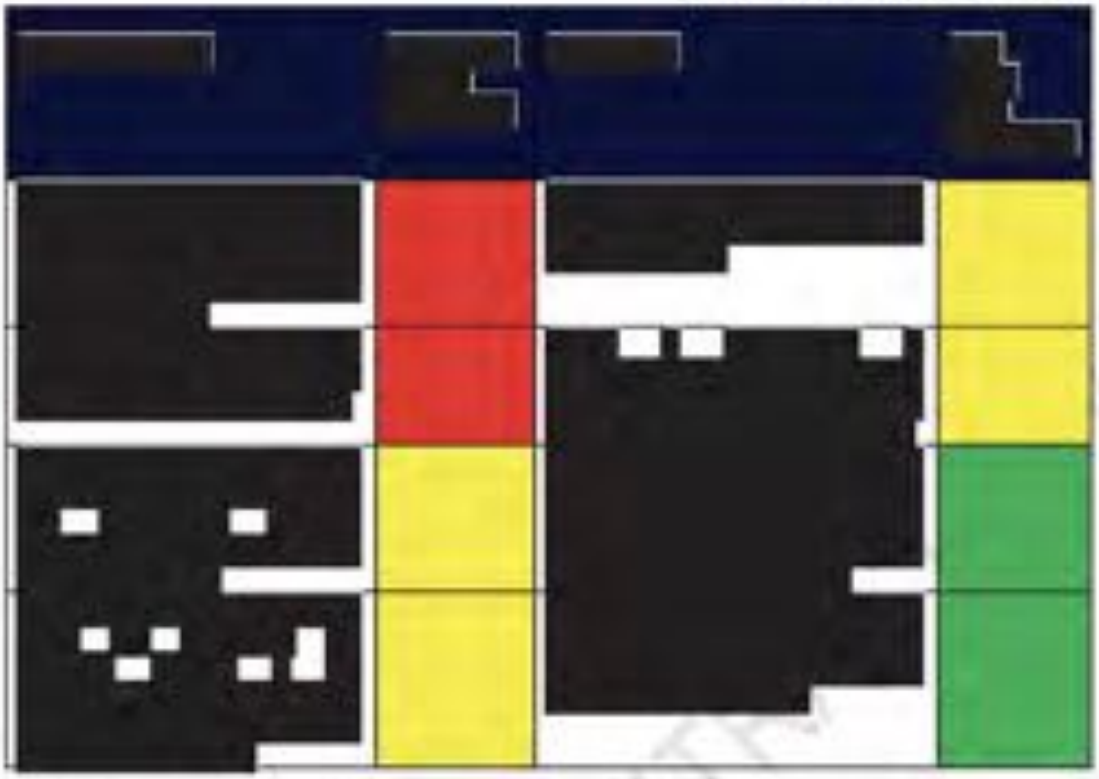
7.2.3 [redacted]

[redacted]

8 [redacted]

8.1 [redacted]

[redacted]

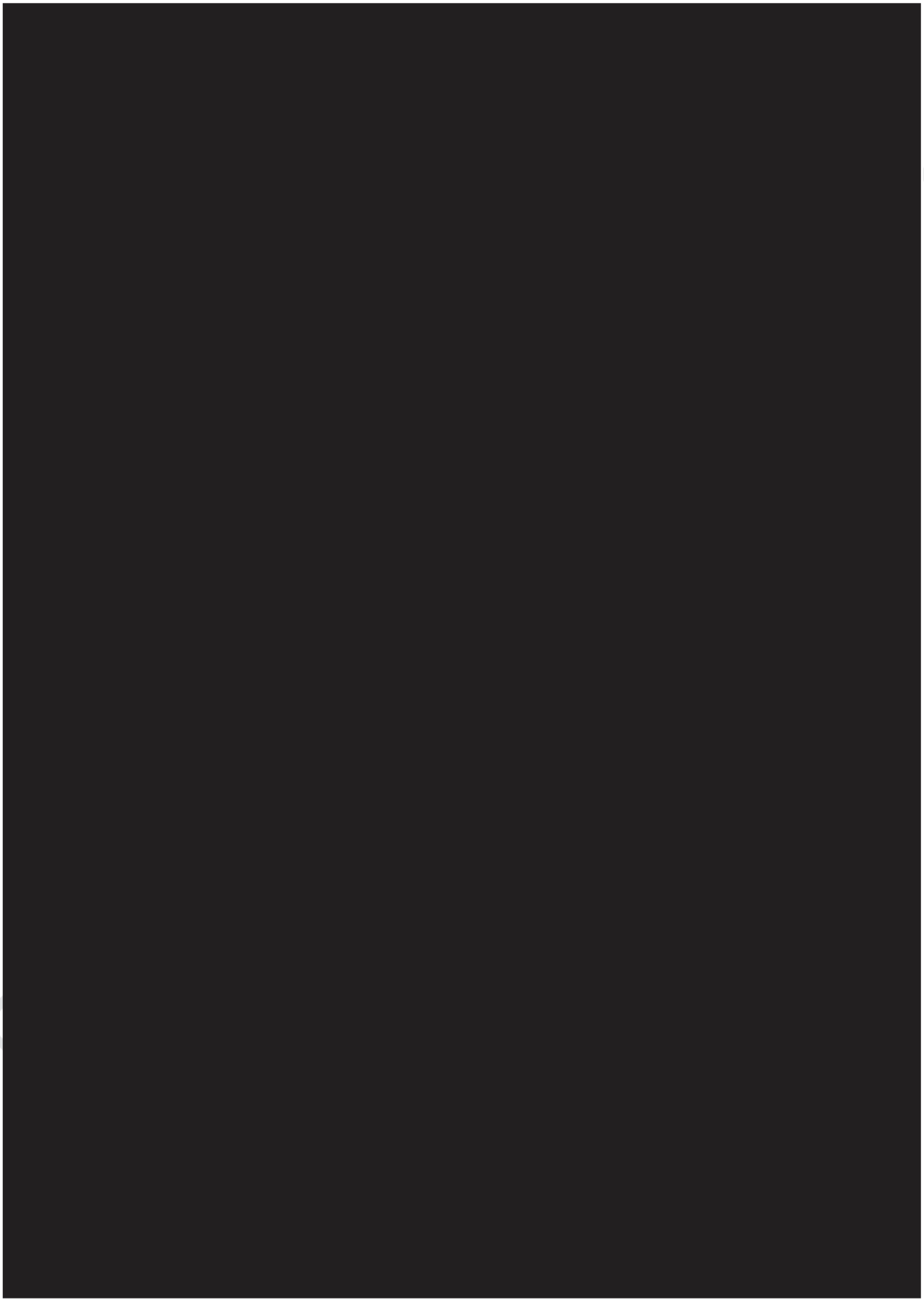


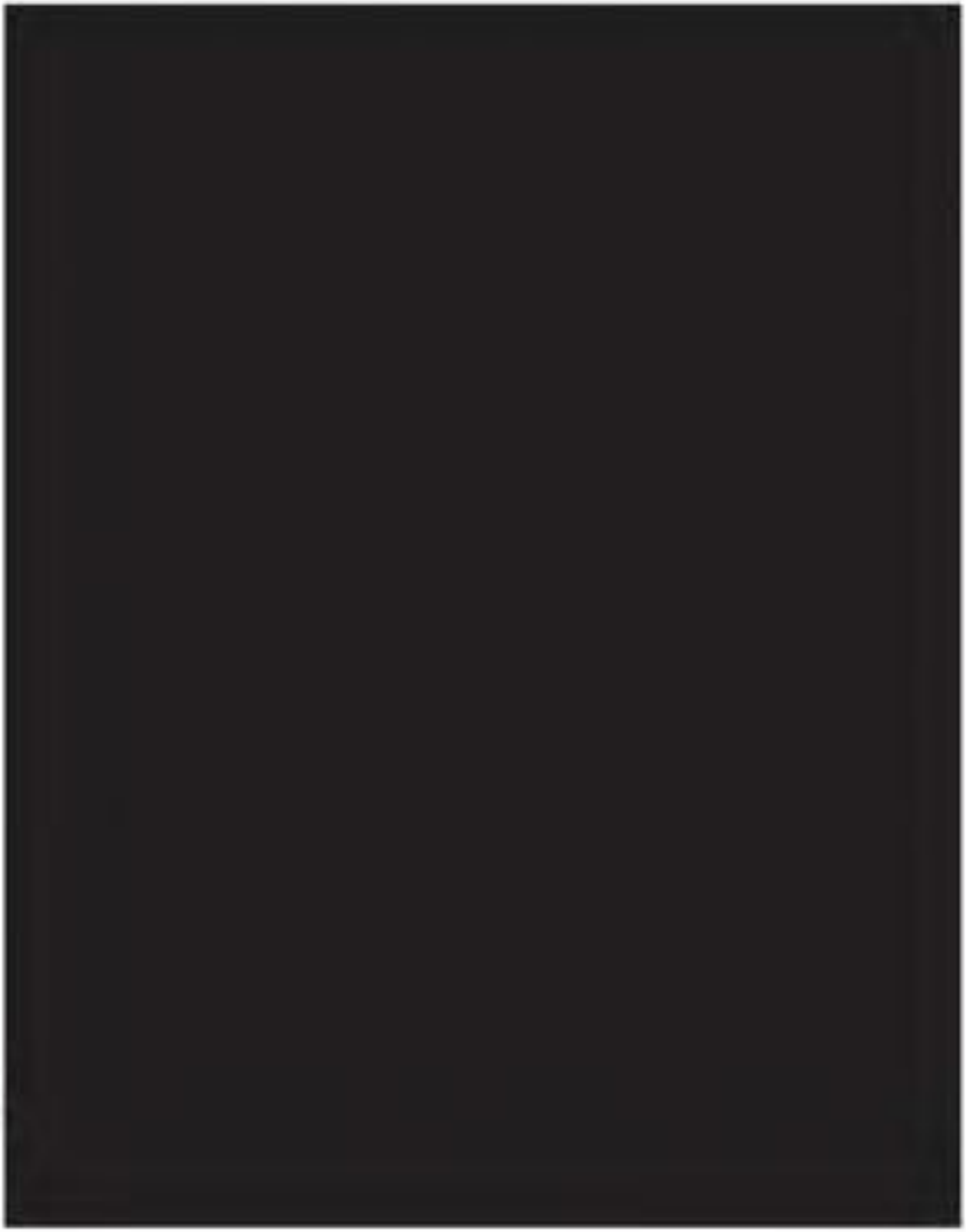
8.2

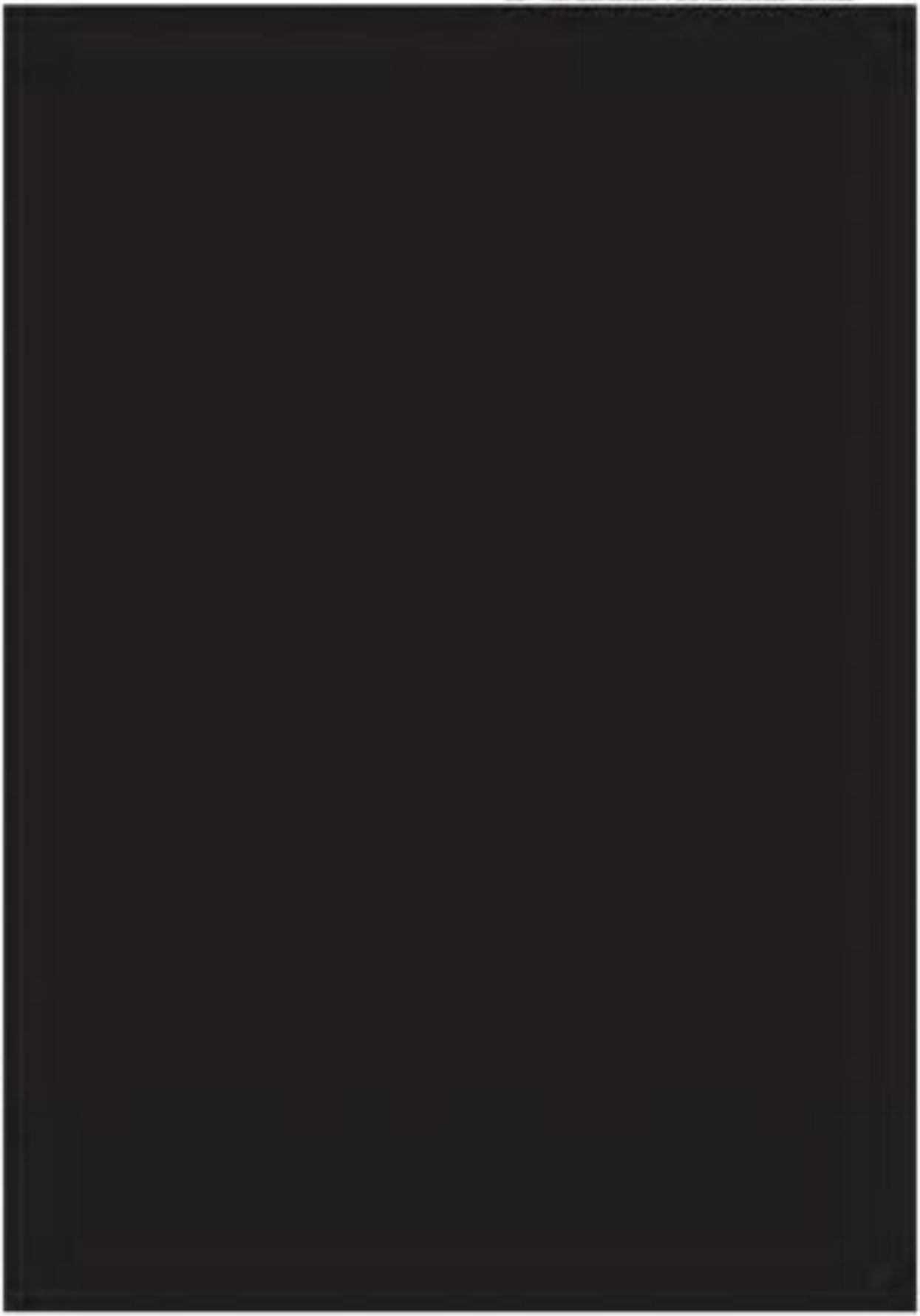
8.3

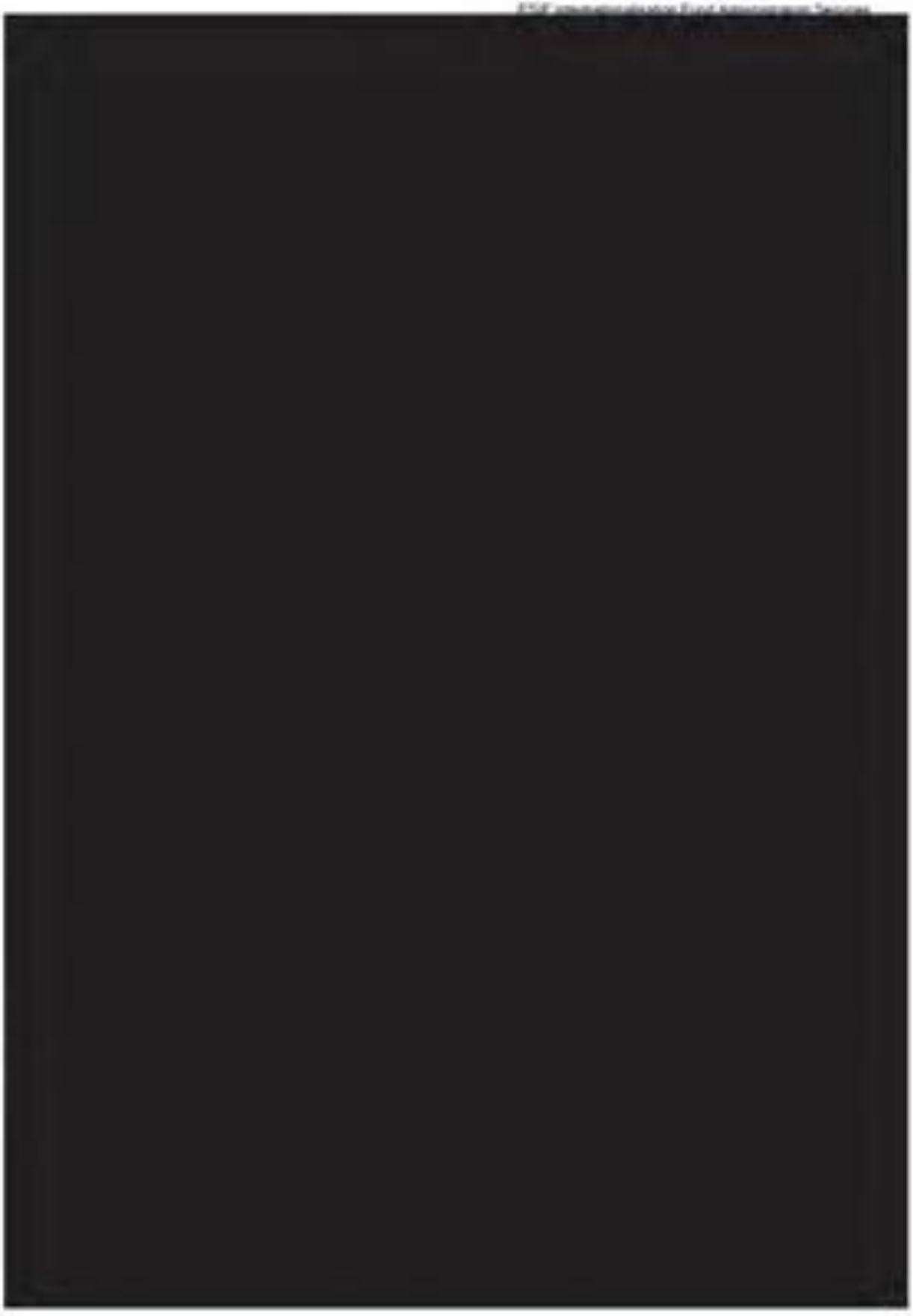
[redacted]

[redacted]



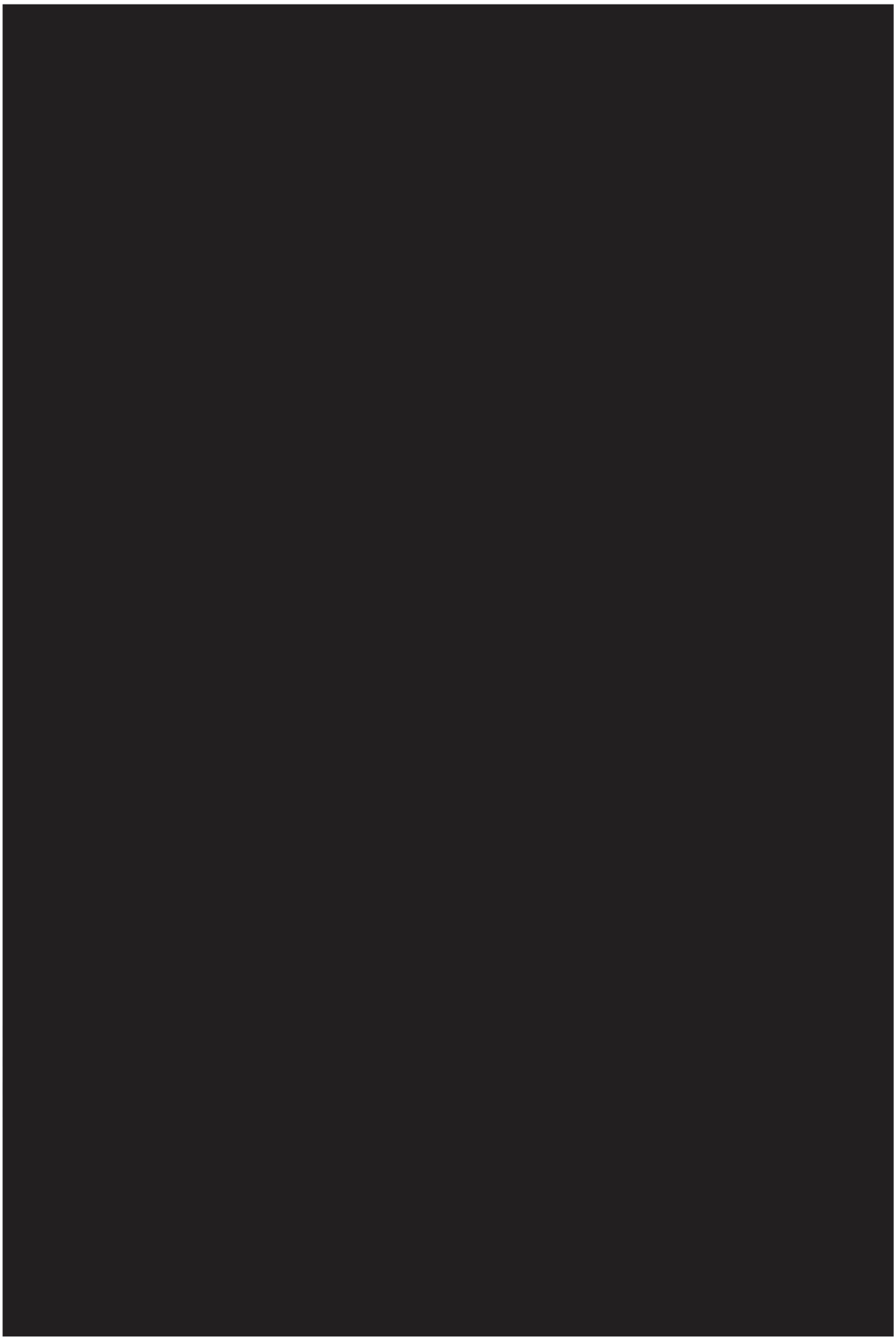


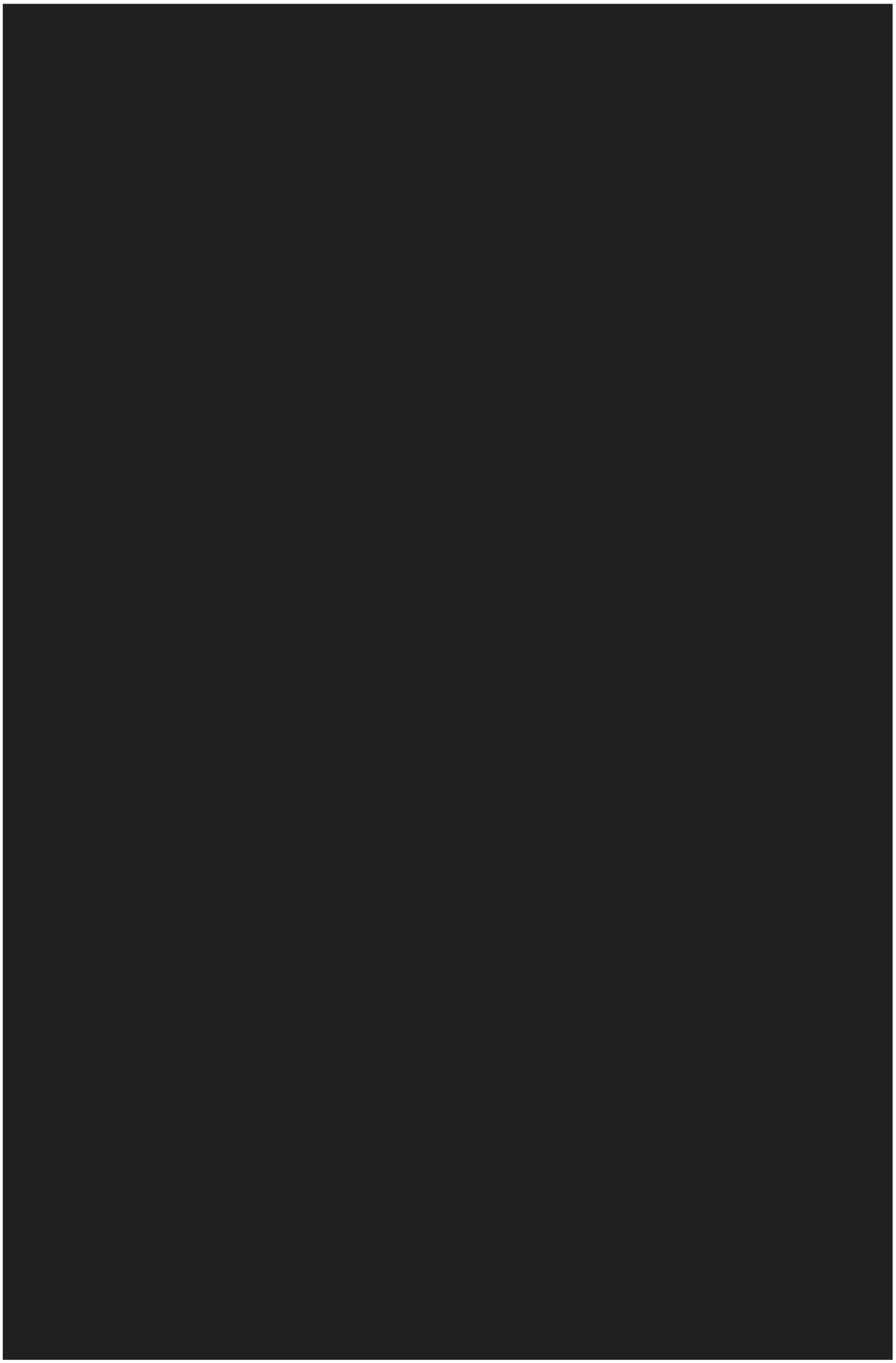




[redacted]

[redacted]





10. Module Dc – Subsection 3: Financial Controls and Fraud Prevention

11. Module Dd – Interoperability & Interactions

1 [redacted]

2 [redacted]

3 [redacted]

[redacted]

4 [redacted]

[redacted]

5 [redacted]

[redacted]

6 [redacted]

[redacted]

1 [redacted]

[redacted]

2 [redacted]

[redacted]

3 [redacted]

3.1 [redacted]

[redacted]

3.2 [redacted]

[redacted]

[redacted]

3.3 [redacted]

[redacted]

3.4 [redacted]

[redacted]

3.5 [redacted]

[redacted]

[redacted]

4 [redacted]

[redacted]

[redacted]

1 [redacted]

[redacted]

[redacted]

[redacted]

1.1 [redacted]

[redacted]

1.2 [redacted]

[redacted]

[redacted]

1.3 [redacted]

[redacted]

[redacted]

[redacted]

1.4 [redacted]

[redacted]