Schedule 9

Information Security and Accreditation

1. Introduction

1.1 This Schedule 9 (**Information Security and Accreditation**) sets out:

1.1.1 the principles of information security to be applied in delivering the Services;

1.1.2 wider aspects of security relating to the Services;

1.1.3 the creation and maintenance of the Security Management Plan;

1.1.4 the development, implementation, operation, maintenance and continual improvement of an ISMS;

1.1.5 the creation and maintenance of the Security Exit Management Plan;

1.1.6 testing of ISMS compliance with the security requirements as set out in Schedule 2 (**Authority's Service Requirements**);

1.1.7 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC 27002 (Information Security Code of Practice);

1.1.8 the formal risk assessment and implementation of proportionate controls to enable Accreditation of the Services;

1.1.9 the documentation, review and maintenance of Accreditation, including production and maintenance of a formal Risk Management Accreditation Document Set (RMADS);

1.1.10 obligations in the event of actual, potential or attempted Security Incidents, including incident reporting and post incident investigations; and

1.1.11 the requirement to establish, and the outline responsibilities of, a joint Supplier/Authority Security Working Group.

2. Principles of Information Security

2.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of information and consequently on the security assurance provided by an effective implementation of an ISMS.

2.2 The Supplier shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:

2.2.1 is in accordance with Good Industry Practice, Laws and this Agreement including this Schedule;

2.2.2 complies with the Security Policy;

2.2.3 complies with at least the minimum set of security measures and standards as determined by the HMG Security Policy Framework (Tiers 1-4) and any other applicable HMG publications notified to the Supplier; including, but not limited to, applicable CESG Information Assurance Standards and CESG Good Practice Guides;

2.2.4 meets any specific security threats to the Information Storage/Processing Environment(s) through which the Supplier stores, passes and/or processes any Authority data;

2.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 4;

2.2.6 complies with Authority Accreditation requirements in accordance with paragraph 6;

2.2.7 complies with the security requirements as set out in Schedule 2 (**Authority's Service Requirements**); and

2.2.8 complies with the Authority's ICT standards.

2.3 The references to standards, guidance and policies set out in paragraph 2.2 shall be deemed to be references to such items as developed and updated and to any successor to, or replacement for, such standards, guidance and policies, from time to time.

2.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Authority of such

inconsistency immediately upon becoming aware of the same, and the Authority shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with. Timescales for implementation will be agreed between the Parties.

3. ISMS and Security Management Plan

3.1 Introduction

3.1.1 The Supplier shall develop, implement, operate, maintain, assure and continuously improve an ISMS in accordance with ISO/IEC 27001 for, without prejudice to paragraph 2.2, approval by the Authority. The correct operation of this ISMS shall be assured via a robust Internal Audit Programme developed and executed by the Supplier and additional audit and checks performed by the Authority or its Authorised Representatives.

3.1.2 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the Term.

3.1.3 The Supplier shall comply with its obligations set out in the Security Management Plan.

3.1.4 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the Authority, aim to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Supplier's Sites, the Supplier Systems and any ICT, 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.

3.1.5 The Supplier shall develop and maintain a Security Exit Management Plan in accordance with this Schedule to apply at the end of the Term.

3.1.6 The Supplier shall ensure that its Subcontractors comply in all respects with the Security Management Plan and the Security Exit Management Plan and with the Supplier's obligations under the Security Management Plan and the Security Exit Management Plan.

3.2 Development of the Security Management Plan

3.2.1 Within thirty (30) Working Days after the Effective Date and in accordance with paragraph 3.4 (Amendment and Revision), the Supplier shall prepare and deliver to the Authority for approval a fully complete and up to date Security Management Plan which shall be based on the outline Security Management Plan set out in Appendix 2.

3.2.2 If the Security Management Plan, or any subsequent change to it which in accordance with paragraph 3.4 (Amendment and Revision) is subject to this paragraph, is approved by the Authority it shall be adopted immediately (and in the case of any change shall replace or update the previous version of the Security Management Plan). If the Security Management Plan (or any such change) is not approved by the Authority the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Authority and re-submit 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 fifteen (15) Working 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 Security Management Plan (or such change) 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 3.2.2 may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan (or such change) on the grounds that it does not comply with the requirements set out in paragraph 3.3.4 shall be deemed to be reasonable.

3.3 Content of the Security Management Plan

3.3.1 The Security Management Plan shall set out the security measures to be implemented and maintained by the Supplier and its Subcontractors in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply

with the provisions of this Schedule (including the principles set out in paragraph 2.2).

3.3.2 The Security Management Plan (including the draft version) should also set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the Supplier's ISMS at the date set out in the Schedule 5 (**Overall Implementation Plan**) for the Supplier to meet the full obligations of the security requirements in Schedule 2 (**Authority's Service Requirements**).

3.3.3 The Security Management Plan shall be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules of this Agreement which cover specific areas included within that standard.

3.3.4 The Security Management Plan shall be written in plain English and in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Services and shall only reference documents which are in the possession of the Authority or whose location is otherwise specified in this Schedule.

3.4 Amendment and Revision of the ISMS and Security Management Plan

3.4.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier annually to reflect the following, or at more frequent intervals if one of the following arises:

3.4.1.1 emerging changes in Good Industry Practice;

3.4.1.2 any change or proposed change to the Supplier Systems, the Services and/or associated processes;

3.4.1.3 any new perceived or changed security threats;

3.4.1.4 any reasonable request by the Authority and;

3.4.1.5 any findings resulting from ongoing monitoring activities and/or the testing referred to in paragraphs 4 and 5.

3.4.2 The Supplier shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and shall amend the ISMS and Security Management Plan at no

additional cost to the Authority. The results of the review should include, without limitation:

3.4.2.1 suggested improvements to the effectiveness of the ISMS;

3.4.2.2 updates to the risk assessments;

3.4.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS and;

3.4.2.4 suggested improvements in measuring the effectiveness of controls.

3.4.3 On receipt of the results of such reviews, the Authority shall approve any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph 3.2.2.

3.4.4 Any change which the Supplier proposes to make to the ISMS or Security Management Plan as a result of an Authority request or change to the Schedule 2 (**Authority's Service Requirements**) or otherwise shall be notified to the Security Working Group. If the Accreditor, or the Accreditor's designated representative on the Security Working Group, deems such proposed change to be significant, the proposed change shall be subject to the Authority's review and approval as set out in paragraph 3.2.2 before any such change or amendment is implemented, unless otherwise agreed between the Parties. If the Accreditor, or the Accreditor's designated representative on the Security Working Group, deems such proposed change not to be significant, it shall be approved and implemented in accordance with the decision of the Security Working Group.

3.5 Security Exit Management Plan

3.5.1 Within twelve (12) months after the Effective Date the Supplier shall prepare and deliver to the Authority for approval a fully complete and up to date Security Exit Management Plan which shall be based on the outline Security Exit Management Plan set out in Appendix 3 and shall be based on the principles set out in

Schedule 10 (**Exit Management**). The Security Exit Management Plan shall be subject to Authority approval in accordance with the same process as set out at paragraph 3.2.2 in relation to approval of the Security Management Plan.

3.5.2 The Security Exit Management Plan shall be fully reviewed and updated by the Supplier annually to reflect the following, or at more frequent intervals if one of the following arises:

3.5.2.1 emerging changes in Good Industry Practice;

3.5.2.2 any change or proposed change to the Supplier Systems, the Services and/or associated processes;

3.5.2.3 any new perceived or changed security threats;

3.5.2.4 any reasonable request by the Authority and;

3.5.2.5 any findings resulting from ongoing monitoring activities and/or the Testing referred to in paragraphs 4 and 5.

3.5.3 Following any such review, the Supplier shall notify the Authority in writing of its proposals, if any, to update the Security Exit Management Plan and the Authority shall approve any amendments or revisions in accordance with the same process as set out at paragraph 3.2.2 in relation to revisions of the Security Management Plan.

4. Conformance to ISO/IEC 27001 and 27002

4.1 The Supplier shall conduct Security Tests on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority not less than annually through the production of an Internal Audit Plan that articulates the Supplier's proposed Internal Audit Programme for at least the following twelve (12) months.

4.2 The Supplier shall provide the Authority with the results of such tests (in a form approved by the Authority in advance and including copies of any reports and associated documentation) as soon as practicable after completion of each Security Test.

4.3 If, as a result of such tests, the Supplier finds issues or risks in the operation of the ISMS, the Supplier shall promptly report such issues and risks to the Security Working Group.

4.4 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority and/or its Authorised Representatives shall be entitled to carry out such Security Tests as it may deem necessary to confirm the correct operation of the ISMS and the Supplier's compliance with the Security Management Plan, the principles and practices of ISO 27001, and applicable HMG security standards and policies. Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services, and shall specifically not extend to technical penetration tests of the Supplier Systems by the Authority. If such tests adversely affect the Supplier's ability to deliver the Services to the agreed Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the tests. The Authority may notify the Supplier of the results of such Security Tests after their completion.

4.5 Where any Security Test carried out pursuant to paragraphs 4.1 or 4.4 above reveals any actual, suspected or potential Security Incident, the Supplier shall:

4.5.1 report the Security Incident, suspected Security Incident or potential Security Incident to the Authority in accordance with paragraph 7 of this Schedule;

4.5.2 investigate the Security Incident, suspected Security Incident or potential Security Incident in accordance with paragraph 8 of this Schedule; and

4.5.3 prepare a Security Improvement Plan in order to correct any failure or weakness, or prevent any potential failure or weakness from resulting in a Security Incident in future.

4.6 The Supplier shall additionally promptly notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to prevent such failure or weakness re-occurring. Subject to the Authority's approval in accordance with paragraph 3.4.4 the Supplier shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably practicable. For the avoidance of doubt, the preparation of a Security Improvement Plan and any

changes made to the ISMS or Security Management Plan shall be at no cost to the Authority.

4.7 If, on the basis of observations made or other evidence obtained during Security Tests, it is the Authority's reasonable opinion that the ISMS is not in full compliance with the principles and practices of ISO/IEC 27001 or paragraph 2.2 or applicable HMG standards and policies, then the Authority shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to correct such non-compliances.

5. Penetration Testing

5.1 The Supplier shall commission a penetration test of any and all Supplier Systems, and those of the Supplier's Subcontractor(s), that shall store or process Authority Data or the Authority Confidential Information or otherwise contribute to the Supplier's delivery of the Services (including any back-up, business continuity or disaster recovery components), from a CESG-approved CHECK 'Green Light' penetration testing body that is independent of the Supplier and the Supplier's Subcontractor(s).

5.2 The Supplier shall notify the Authority of the penetration testing body that the Supplier proposes to commission prior to the commencement of any penetration test.

5.3 The Supplier shall document the proposed scope of any and all penetration tests in terms of the Supplier Systems, and those of the Supplier's Subcontractor(s), that shall be tested and the types and depth of testing to which each Supplier System shall be subjected in conjunction with the penetration testing body, and shall submit the proposed scope for the Authority's approval prior to the commencement of any penetration test.

5.4 Penetration tests shall be:

5.4.1 initially completed in full within such time after the Effective Date that there is sufficient time available to implement any corrective actions and recommendations identified in the penetration test report prior to the Commencement Date;

5.4.2 subsequently repeated in part for any and all individual Supplier System(s) that undergo(es) significant change, where the definition of 'significant' shall be at the sole discretion of the

Accreditor, within one (1) month of such a change being made and;

5.4.3 repeated in full within twelve (12) months of the completion of the last full penetration test.

5.5 The Supplier shall provide the Authority with full and unedited copies of any and all penetration test reports and associated documentation provided to the Supplier by the penetration testing body, including the details of any corrective action proposed by the penetration testing body as a result of such penetration test(s), within ten (10) Working Days of receiving such reports and associated documentation.

5.6 The Supplier shall present the findings of any and all penetration tests, including the corrective actions proposed by the penetration testing body as a result of such penetration test(s), to the Security Working Group within thirty (30) Working Days of the Supplier receiving such from the penetration testing body. The Supplier shall indicate whether it proposes to implement or not implement each proposed corrective action, and the timeline for implementation where applicable, for the Authority's approval through the Security Working Group.

5.7 The Supplier shall implement any and all corrective actions arising from penetration tests that are approved by the Authority through the Security Working Group within the timelines stipulated by the Authority through the Security Working Group.

6. Accreditation

6.1 The Services provided to the Authority by the Supplier shall undergo a formal Accreditation process, led by the Authority, in compliance with HMG Security Policy Framework. The Supplier shall enable Accreditation of the Services to take place prior to the Commencement Date. Accreditation is a mandatory prerequisite to commencing a new information storage/processing activity.

6.2 The Supplier shall promptly provide to the Authority any and all information relevant to the Services and/or the Supplier's provision of the Services that may be required by the Accreditation process.

6.3 Accreditation shall be managed by the Accreditor within the scope of the Accreditor's delegated authority, and otherwise by the relevant Senior Information Risk Owner (SIRO) (including where the risks applicable to a

given environment fall outside of the SIRO's Risk Appetite, in which case the Accreditor must escalate the Accreditation decision to the Senior Information Risk Owner (SIRO), usually facilitated through the production of a risk acceptance case (also known as a risk balance case) that details the specific risk to be accepted).

6.4 The Supplier shall manage the risks identified during the Accreditation process to a level of Residual Risk which is acceptable to the SIRO. The Supplier shall additionally demonstrate the effectiveness of any and all controls implemented to manage such risks in such a manner and to such an extent as are necessary to satisfy the Accreditor and SIRO.

6.5 The Supplier shall carry out such activities and provide such assurances as are required by the Accreditor for the purposes of maintaining such Accreditation for the duration of the Agreement, in compliance with HMG Security Policy Framework and all other applicable HMG security policies and standards notified to the Supplier.

7. Security Event/Incident Reporting and Management

7.1 The Supplier shall agree a common taxonomy and methodology for categorising Security Events and Security Incidents by their type and severity with the Authority within the security incident management process. The Supplier shall additionally identify the combinations of Security Events, including any temporal criteria around the timing of their occurrence, which the Supplier shall use in identifying the occurrence of Security Incidents.

7.2 The Supplier shall agree the process(es), format(s) and timeline(s) by which the occurrence of Security Events and Security Incidents of each type and severity shall be notified to the Security Working Group, or other Authority stakeholders, with the Authority, within the security incident management process.

7.3 The Supplier shall report any and all Security Events and Security Incidents to the Authority in the agreed format(s), to the agreed person(s) and within the prescribed timeline(s) applicable to the type and severity of each incident/event. The Authority shall notify the Supplier in accordance with the agreed security incident management process, as defined by the ISMS, upon becoming aware of any Security Incident or any potential or attempted Security Incident affecting the Supplier Systems.

7.4 The Supplier shall take immediate action to stop, limit or correct Security Incidents as soon as they are detected, in accordance with the incident handling procedures that form part of the ISMS, and within the bounds pre-authorised by the Authority.

7.5 The Supplier shall provide a high-level summary of Security Events and Security Incidents that have occurred since the last Security Working Group, and any related security management information, to the Authority as a standing agenda item at each Security Working Group, or more frequently if directed by the Authority.

8. Post Incident Investigation

8.1 The Supplier shall investigate any and all Security Incidents reaching or exceeding an incident severity threshold that shall be stipulated by the Authority, and shall provide an incident investigation report to the Authority within one (1) calendar month of the occurrence of any such incidents that includes:

8.1.1 an assessment of the Security Incident's impact(s);

8.1.2 a root-cause analysis of how and why the Security Incident occurred;

8.1.3 any information which may assist in identifying the perpetrator(s) of the Security Incident;

8.1.4 the Supplier's recommendations for preventing re-occurrence of the Security Incident, or similar Security Incidents, in the future; including the relevant advantages and disadvantages applicable to each recommendation; and

8.1.5 any other Security Incident investigation aspects identified by the Security Incident handling or investigation policies within the ISMS.

10. Security Working Group

10.1 The Supplier shall be responsible for the establishment of a Security Working Group within twenty (20) Working Days of the Effective Date which shall include key stakeholders from both the Supplier (including representatives from the Supplier's Subcontractor(s) where applicable and where approved by the Authority) and the Authority. The Security Working Group shall meet not less than quarterly or as otherwise agreed between the Parties.

10.2 The Security Working Group shall report to the Authority and its remit shall include, but not be limited to:

10.2.1 the management and review of security issues and risks identified through Security Tests, audits and/or through the Accreditation process;

10.2.2 the recording and ongoing management of security issues and risks within a risk register, and the recording and execution of any corresponding risk management decisions and/or activities;

10.2.3 the reporting of security issues and risks to the Authority's stakeholders (including Authority Customers) at a frequency agreed with the Authority;

10.2.4 the review of security management information (the scope and content of which is to be agreed between the Parties) provided by the Supplier;

10.2.5 ensuring compliance to ISO/IEC 27001 and that Accreditation of the Services is maintained throughout the duration of the Agreement;

10.2.6 recommending and facilitating where applicable any identified and necessary changes to ISMS, security policy and Security Management Plan and Security Exit Management Plan, and (subject to the Authority's approval) approve or reject these as appropriate;

10.2.7 reviewing any potential, attempted or actual Security Incident or any other Security Events that may have information security implications for the Services or the Authority, and to review measures that are proposed to prevent re-occurrence; and

10.2.8 sharing the Supplier's and the Authority’s views on changes in the prevailing threat environment between Security Working Group meetings, both in the context of the Government Banking Service and in relation to the financial services sector more broadly; including the identification of prevalent threat actors/groups and the analysis of trends in their motives, methods and preferred attack vectors.

11. TIMESCALES

11.1 Notwithstanding the timescales set out in this Schedule, the Parties shall be at liberty to agree at any time an alternative timescale in which the relevant act is to be completed.

APPENDIX 1

Security Policy

APPENDIX 2

Example Structure of Security Management Plan

1. **EXECUTIVE SUMMARY**
2. **INTRODUCTION TO SECURITY**
3. **STATEMENT OF APPLICABILITY**
4. **SCOPE OF SERVICES AND TECHNOLOGY**
5. **DURATION OF SERVICE**
6. **ASPECTS OF SECURITY**
7. **SECURITY REQUIRMENTS AND CONTROLS**
8. **SECURITY RISK ASSESSMENT AND GAP ANALYSIS**
9. **RISK MITIGATION**
10. **SECURITY TEAMS AND RESPONSBILITIES**
11. **PROCEDURES**
12. **TRAINING**
13. **MAINTENANCE**
14. **AUDITING**
15. **SUBCONTRACTORS**

APPENDIX 3

Example Structure of Security Exit Management Plan

1. **EXECUTIVE SUMMARY**
2. **STATEMENT OF APPLICABILITY**
3. **SCOPE OF SERVICES AND TECHNOLOGY**
4. **DURATION OF TRANSITION**
5. **ASPECTS OF SECURITY**
6. **TRANSITION SECURITY REQUIRMENTS AND CONTROLS**
7. **TRANSITION SECURITY RISK ASSESSMENT AND GAP ANALYSIS**
8. **TRANSITION RISK MITIGATION**
9. **SECURITY TEAM RESPONSBILITIES**
10. **PROCEDURES**
11. **MAINTENANCE**
12. **SUBCONTRACTORS**