Key	Supporting documentation	Attached?	Name(s) of attachment(s) / description
I.01	Overview description of the IT environment	Select	
I.02	Network diagram and Infrastructure overview	Select	
I.03	System diagram and functional overview	Select	
I.04	IT function organogram	Select	
I.05	List of key business processes supported by IT including short summary for each process	Select	
I.06	List of key applications with functional summary	Select	
I.07	List of IT-relevant internal / external audit findings with actions currently outstanding	Select	
I.08	Copies of key IT documentation (Latest IT Strategy, Information Security, Business Continuity, Change Management, any other considered relevant for submission to demonstrate controls in place within the environment)	Select	
I.09	Please describe the key changes to your IT environment that will support the regulated activity permissions that you are seeking (if no changes to established IT environment have been required please note this and explain why). You can attach a document to provide this information if you prefer	Select	

Section 1	Governance and Risk Management	Response	Supporting narrative (required)	Response Guidelines
Objectives	*A) IT governance is likely to ensure that IT meets the needs of the business.* *B) IT governance is likely to ensure that IT risks are managed proportionately.*			
1.A.01	Is the governance of the IT function well defined? (e.g. governance terms of reference, operating model, organisation charts, job responsibilities, and the terms of reference of any committees)?	Select		Your response could include references to governance structures and processes that are in place to ensure appropriate oversight of technology services. This could include descriptions of, • Governance, Compliance and Risk Control - Structure and Roles/Resp • Org Chart, Job Responsibilities and Operating Model • Procedures for reviewing IT issues with the board, • Business strategies and how they are scoped into IT budget and strategy.
1.A.02	Is the governance of the IT function linked to the governance of the business as a whole?	Select		Please state how you comply with the control
1.A.03	Do you have a documented IT Strategy and Budget that are approved by senior IT and business management?	Select		Your response could include references to mechanism and frequency of management reviews / strategy updates
1.A.04	Is there a mechanism for identifying and assessing IT risk, and determining appropriate mitigating actions?	Select		Responses could include references to risk management guidelines. These could be processes, policies and lines of defence to identify, manage, mitigate, escalate and reporting of risks related to the system and related people / processes.
1.A.05	Is there a mechanism for reporting the results of this process to appropriate levels of management?	Select		Responses could include references to risk management guidelines. These could be • Processes and policies related to internal and external escalation mechanisms, • Internal and External Communication processes on crystallisation of risks.

Section 2	Reviews and audits		Supporting narrative (required)	Response Guidelines
Objectives	*A) The system will be subject to satisfactory independent reviews.*			
2.A.01	Were the systems relating to this application reviewed in the last 12 months, or will they have been reviewed in the 12 months before launch by internal audit, external audit, or an independent and qualified third party?	Select		Please state how you comply with the control
2.A.02	Are IT systems and controls subject to regular reviews / audit / self-assessments / validation by an independent and qualified audit function with appropriate management oversight?	Select		Responses could include references to, • Audit / Validation / Self-Assessment / Compliance Assessment frequency and reports • Process to ensure that audit actions are remediated • Management oversight, reporting and escalation mechanism of outstanding audit issues & breaches

Section 3	Change Management		Supporting narrative (required)	Response Guidelines
Objectives	*A) Change and project management frameworks are designed to deliver systems that meet the needs of the business and its customers, on time and within budget.* *B) Change controls adequately mitigate the risk of failures caused by faulty code or configuration changes.*			
3.A.01	Do you have documented project and change management policies that ensure that business, IT, and project objectives are aligned; changes and projects are managed in a controlled manner and risks are identified in a timely manner?	Select		Responses could include references to methodologies to control and govern changes to the IT landscape. This could include descriptions of • Change management policies, governance and control • Project organisation, Project methodologies and Risk management • Formal development methodologies • Impact assessment and communication to external and internal stakeholders • Senior management approval and sign-off mechanisms
3.A.02	Do documented change control procedures require changes to IT systems (including emergency and vendor-provided fixes) receive appropriate validation and quality assurance testing (including user acceptance testing if required by the approved test model).	Select		This could include descriptions of • Emergency patching / fix process • Authorisation and risk assessment process for changes • Validation, simulation and conformance testing process and reports • Version control and tracking (track development and production software versions / builds at any point of time / rollback changes) • Process for updating stakeholders, system architecture, operating manuals and configuration manuals after changes (e.g. security, disaster recovery, customers, suppliers, documentation, communication to internal and external stakeholders and staff training)
3.A.03	Is a system in place to maintain a full audit trail of changes and to detect unauthorised changes to systems and revert systems back to their original state?	Select		Responses could include a description of tools and processes to detect unauthorised changes
3.A.04	Are there separate development, testing and live environments?	Select		• Responses could include references to system and applications environments management and control. • This could include descriptions on segregation of production, development and testing controls. If automated tools are used please describe the controls used to manage risks associated with implementation of changes. • If these environments are also used by external clients / members, explain their usage, scope, reporting and oversight mechanisms.
3.A.05	Are key vendor software packages protected by escrow agreements?	Select		Yes / No
3.A.06	If systems required for the service under consideration are newly-implemented or in the process of going live is the testing of the proposed business systems needed to support the activities for which authorisation is sought, planned, in progress or completed? Were all bugs that could cause data errors or unacceptable performance resolved before the system went live?	Select		Please state how you comply with the control.
3.A.07	Did designated testers and relevant senior IT and business management formally sign-off on planned testing before the system went live?	Select		Responses could include references to • Business testing and sign-off (incl. 3rd parties & customers) • Approvals for testing scope and plans • Approval and Sign-off procedures before go-live

Section 4	Operational resilience and business continuity		Supporting narrative (required)	Response Guidelines
Objectives	*A) The system has sufficient built-in resilience and support to prevent harmful service interruptions.* *B) If there is an interruption, an effective recovery plan is in place.*			
4.A.01	Has the business defined the systems Availability / Unavailability target (i.e. % up-time during normal business hours) required to support business activities?	Select		Please state how you comply with the control
4.A.02	Do you have a formal documented process to perform stress testing at least annually to test critical systems' ability to accommodate at least twice the historical peak [or twice the projected peak if a new system] of activity and resolve any issues in a timely manner?	Select		Responses should include references to • End to End Stress testing - frequency, scope and methodology. • System sizing, latency and load balancing, • Component stress testing based on simulated market conditions • Demand forecast, capacity and performance adjustment capabilities. • Capacity / Performance monitoring capabilities
4.A.03	Are key components duplicated to eliminate single points of failure that could cause interruptions resulting in unacceptable harm to customers? (Consider power suppliers, communications lines, processors, disk drives, routers, switches, air conditioning, etc.)	Select		Responses could include references to procedures related to, • Identification of single point of failures • Alternative ways for customers to perform transactions
4.A.04	Are procedures and processes in place to log and monitor actual or potential availability, system performance, capacity problems or market abuse and manage them?	Select		• Responses should include references to • Process / Procedures around monitoring services (staff, operational manuals and access restrictions.) • Order management and threshold monitoring (Pre/Post trade monitoring and controls if applicable). • Specifics of delay between actual and reported event. • Specifics of proactive monitoring and event correlation • Descriptions of monitoring, reporting and communications around availability of systems / interfaces. • Related policies to identify risks as well as mitigation plans including mechanisms to constrain or halt processing if required.
4.A.05	Do you have mechanisms to perform appropriate on-boarding / due-diligence process for clients / members that connect / use your systems or any other interfaces that your systems may integrate with.	Select		Responses could include references to , • Member / client complaince or onboarding policy • Due Diligence and on-boarding policy for clients / members • Mointoring and ensuring complaince to the firms policieis and e • Process to off-board clients / members
4.A.06	Are adequately trained systems support staff available throughout both business and subsequent hours, to resolve problems before the next business day?	Select		Responses could include references to procedures related to policies to ensure that staff and authorised and well trained to deal with operational issues.
4.A.07	Is there a business continuity plan that provides for critical systems to recover within the maximum period the business has defined as acceptable? Is there appropriate management oversight over the strategy and implementation of these plans	Select		Responses should include references to recovery plans for key systems. This could include • Business Continuity and Disaster Recovery Plans and Policies • Communication plan to internal / external stakeholders to deal with disruptive incidents • Description of scenario testing including scenarios that have been explicitly excluded. • Disaster recovery tests and compliance to recovery time (RTO) and recovery point objectives (RPO) for the systems relating to this application. • Plans to address disruptions of outsourced activities where the supplying firm's services become unavailable BCP / DR Testing frequency and management reporting. •Review process / frequency of BCP / DR process and methodologies.
4.A.08	Are staff trained in the operation of business continuity arrangements, with roles and responsibilities clearly defined?	Select		Responses should include references to staff training arrangements and guidance for roles and responsibilities.
4.A.09	Will the effectiveness of the disaster recovery plan be validated by successful pre-launch testing on the systems as they will be at launch, and at least annually thereafter, with any failures corrected and retested within six months?	Select		Please state how you comply with the control
4.A.10	Is the disaster recovery plan updated at least annually or when any system change affects it?	Select		Please state how you comply with the control

Section 5	Information security and controls		Supporting narrative (required)	Response Guidelines
Objectives	*A) There is a satisfactory information security policy, adequately supported by standards and an effective information security function.* *B) Effective basic information security measures are in place, security is effectively monitored.* *C) Users' access to systems is controlled effectively.* *D) System security is tested.*			
5.A.01	Is there a well defined Information Security policy based ib a recognised standard (e.g. BS7799, ISO27001.)	Select		Please state how you comply with the control
5.A.02	Is a named and experienced person, independent of IT management, responsible for information security with the role and responsibilities defined in writing? (State name and summarise role, responsibilities and experience.)	Select		State Name, Summarise Role and Responsibilities
5.A.03	Are there mechanisms to check that policies and procedures are complied with?	Select		Responses should include references to a review / report of systems, controls and compliance by internal audit.
5.A.04	If so, does this also apply to functions outsourced to service providers or other parts of the group, whether in the UK or overseas?	Select		Yes / No
5.A.05	Does the firm's Data Protection Act registration cover all the applicable uses, sources, and disclosures of personal data?	Select		Yes / No
5.A.06	What logical and physical security measures have been implemented to protect the technology and business environment (e.g. firewalls, IDS, IPS, anti-virus, DLP, encryption, etc.)?	Select		Responses could include references to, • Monitor and alert of security issues • Logical / physical security network security • Policies to prevent users from installing software or connecting unauthorised drives • Control over datacentre access
5.A.07	Are internal networks, including wireless networks, protected from unauthorised access, e.g. by password protection and by keeping communications equipment in secure areas?	Select		Responses could include references to, • Network Protection and secure communication • User password policies (e.g. complexity and frequency of change) • Admin password policies (e.g. complexity and frequency of change)
5.A.08	Please describe what measures have been implemented to address risk of data loss, data theft, and data leakage of data in transit and data at rest.	Select		Responses should include references to measures that protect against data loss/theft onsite, offsite , during transit and at rest.
5.A.09	Please specify what encryption measures are implemented. Please specify algorithms and key lengths.	Select		Responses should include references usage of encryption and related technologies for, • Protection of sensitive data • Secure transmission of data over public networks, such as the internet • Protection of data stored in portable devices / removable media
5.A.10	Does creating new users, or amending the access rights of existing users, require formal authorisation?	Select		Responses could include references to, • Leaver / Joiner processes including but not limited to authorisations to grant role and user access to systems and services. • Role / access review process along with mechanisms to prevent unauthorised access. • Initial / Periodic user training on security policies
5.A.11	Is logical access to applications granted on the principle of least privilege, and is it given in a way that enforces segregation of duties? (i.e. does it ensure that separate persons can access functions that need to be separate for control purposes, e.g. inputting and releasing payments?).	Select		Responses could include user access control policies and procedures. Response could contain references to, • Role based access control and capabilities to identify user activities. • Process to ensure segregation of duties (e.g. between administrators, developers and users) • The ability to identify / monitor usage of all users who have access to critical IT systems
5.A.12	Are there appropriate procedures to handle security breaches	Select		Response could contain references to, • Communication process to deal with internal and external stakeholders (e.g. regulators, clients etc.) • Descriptions of containment mechanisms • Incident management policy and escalation mechanisms
5.A.13	When users leave or their responsibilities change, are the access rights or profiles they no longer need promptly deleted? Is user access to business systems reviewed by appropriate line managers on a regular basis and any access rights that are no longer required removed? (If yes, how often?)	Select		Please state how you comply with the control
5.A.14	Will an independent penetration test of the network be carried out, and all significant weaknesses corrected, before launch and at least annually thereafter? Will the penetration tests include an internal vulnerability assessment and external penetration testing?	Select		Responses should include references to independent audits and penetration tests. Related information could frequency, remediation of issues and monitoring of key system components for changes that may impact security

Section 6	Outsourcing		Supporting narrative (required)	Response Guidelines
Objectives	*A) Agreements with vendors and service providers are in accordance with good industry practice.*			
6.A.01	Do you outsource significant IT functions? If the answer to this question is No, please do not complete the remainder of this section.	Select		See SYSC 8.1 for our outsourcing requirements for firms.
6.A.02	Have you exercised due skill, care, and diligence in entering into the outsourcing arrangement, to obtain assurance that an appropriate standard of service will be provided?	Select		Responses should include references to sourcing and selection strategy along with oversight arrangements to govern suppliers. Related information could include references to vetting mechanism, capability measures and review cycles.
6.A.03	Does the service provider have the ability, capacity, and any authorisation required by the law to perform the outsourced functions, services or activities reliably and professionally?	Select		Responses could include references to sourcing due diligence processes and guidelines to ensure that potential suppliers meet relevant legal and regulatory obligations.
6.A.04	Do you have the expertise and methods required for assessing the standard of performance of the service provider, supervising the service provider, and initiating corrective actions?	Select		Responses should include references to areas of the contractual agreements containing oversight and measurement criteria to evaluate and monitor supplier performance.
6.A.05	Can you terminate the arrangement for outsourcing where necessary without impairing the continuity and quality of your services to your customers?	Select		Responses should include references to the ability to terminate suppliers without impacting service
6.A.06	Does the contract give your, your auditors, us and any other relevant competent authority the right to audit the service provider?	Select		Responses should include references pertaining to cooperation with competent authorities to review/audit/assess activities/data/systems of the sourcing provider.
6.A.07	Does the contact require the service provider to protect any confidential information about you and your customers? For transfer to non-EU states does the contract mirror the EU model clauses?	Select		Responses should include references to data protection agreements with the sourcing provider(s). This could include descriptions of confidential data protection, non-disclosure and anti-piracy agreements
6.A.08	Does the contract require you and the service provider to establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities?	Select		Responses should include supplier specific contingency / DR / backup plans. Related information could include descriptions of contingency planning for outsourced functional areas