FINTECH SERVICE PROVIDERS (“FSP”) COMPLIANCE READINESS FRAMEWORK

15 May 2020

Version 1.0

SFA | SINGAPORE FINTECH ASSOCIATION

TABLE OF CONTENTS

OVERVIEW

Eight in ten FinTechs in Singapore partner with a Financial Institution (FI) to enhance the FI's offerings or provide technology solutions to the FIs. As such there is a need for these FinTechs to adopt an efficient approach to demonstrate their compliance levels to the FIs while maintaining a baseline level of governance, rigor and consistency over their activities. To do so, the Singapore FinTech Association has undertaken a phased approach to enhancing the compliance maturity of these FinTechs by establishing the 'Fintech Service Provider ("FSP") Compliance Readiness Framework'.

The primary objective of this framework is to promote a sustainable outsourcing relationship between the FSPs and FIs, by helping the FSPs understand the minimum compliance requirements that they need to put in place to operate within the FI industry. The self-assessment accompanying this framework will allow FSPs to be aware of the maturity of their control environment against the minimum compliance requirements.

This framework also enhances the FIs' comfort level in partnering with the FSPs. Based on MAS Outsourcing and TRM guidelines, FIs are expected to adopt their own approach/strategy to manage the risk of outsourcing to FSPs and understand any residual risk that management is accepting. With this framework, FIs would be able to use the results of the self-assessment performed by FSPs as part of their vendor due diligence and perform onboarding of these FSPs with the condition of the FSPs resolving any gaps identified within the self-assessment and eventually obtaining a third-party assurance report over their controls.

The framework includes a set of minimum base requirements from OSPAR, the Monetary Authority of Singapore ("MAS") Technology Risk Management ("TRM") Consultation Paper and the MAS Cyber Hygiene Notice, that the FSPs are expected to comply with, as a starting point for servicing FIs. The framework has been streamlined to take into consideration the FSP's scale, operating model and their gradually evolving ability to eventually comply with the OSPAR, TRM requirements and the MAS Cyber Hygiene Notice. The detailed approach on how the framework was built from existing guidelines and frameworks is outlined in the section below.

Approach to building the 'FSP Compliance Readiness Framework'

The starting point for the creation of the FSP Compliance Readiness Framework is the Guidelines on Control Objectives and Procedures for Outsourced Service Providers v 1.1 dated June 2017, issued by the Association of Banks in Singapore.

Using the ABS guidelines / OSPAR framework as a basis the following approach was taken to develop this FSP Compliance Readiness Framework:

1) Certain ABS OSPAR controls criteria were initially set aside based on the following principles –
   a) Policy related controls criteria - Controls criteria that outline requirements to have a formal established policy (with periodic review) have been set aside for now, with the principle that as long as a process has been implemented to address the corresponding policy expectation, this process provides adequate comfort over the control environment. As an alternative an overall requirement to have formal documented policies has been included as a new criteria within the Entity Level Controls section of this version of the framework.
   b) Repetitive control criteria - Certain controls criteria are indicated as repetitive, for which another existing control criteria is identified (in a more relevant control domain) that addresses the underlying/associated risk. Essentially similar/duplicate controls criteria have been included only once within this version of the framework.
   c) Relevance of control criteria - Considering the desire to implement the requirements of the ABS guidelines / OSPAR framework using a progressive step-by-step approach and that the preliminary objective is the establishment of a baseline level of governance, rigor and consistency over the outsourced processes, certain controls criteria are set aside that are considered too ambitious for this initial version of the framework. For example, controls related to the business transaction processing (which will be specific to the nature of service provided by the FSP) have been set aside for future consideration. As an alternative, an overall requirement to have SLA tracking and periodic reporting to FIs has been included as a new criteria within the Entity Level Controls section of this version of the framework.

2) The controls criteria that have not been set aside, are classified as 'key' or 'complementary'. Key controls criteria are considered the more desirable option for compliance within the current version of this framework. Complementary controls criteria are included as an option alongside a key control criteria (which the former complements) such that the FSPs are able to rely on the complementary controls criteria, as an interim measure, while they devise action plans to implement the key controls criteria.

3) In addition to the base requirements adopted from the ABS guidelines / OSPAR framework, some additional requirements are included from the recent TRM Consultation Paper (issued 7 March 2019) and the Cyber Hygiene Notice (issued 6 August 2019) that were identified as relevant for FSPs.

4) The identified controls criteria from points (1), (2) and (3) have been revised/reworded to make them suitable and sustainable within an FSP environment.

5) As part of future stages/phases of the evolution of this framework, elements that have been set aside (for now) will be re-evaluated for inclusion with a view to eventual compliance to the ABS guidelines / OSPAR framework using a progressive step-by-step approach.

6) Whilst we have considered the MAS TRM Consultation Paper (issued on 7 March 2019) and Cyber Hygiene Notice (issued on 6 August 2019) in the development of the framework, given the phased approach, only controls that are the minimum base requirements for servicing FIs, from these documents have been included. Please refer to Appendix for the list of requirements from MAS TRM Consultation Paper guidelines that were not included within this framework.

I. ENTITY LEVEL CONTROLS

Entity level controls are internal controls to ensure that the FSP's management directives pertaining to the entire entity are carried out. The controls include the following components:

(a) Control Environment.
(b) Risk Assessment.
(c) Information and Communication.
(d) Monitoring.
(e) Practices related to Sub-Contracting.

The following is a brief description of the components:

(a) Control Environment

The control environment sets the priority and culture for the FSP, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Aspects of the FSP's control environment may affect the services provided to the FIs. The control environment that an FSP should consider implementing includes the following components:

i. Establishing workplace conduct standards and enforcement procedures

ii. Conducting pre-employment checks on candidates

iii. Defining organisational structures, reporting lines, authorities and responsibilities. Key responsibilities such as the expectations of the person responsible for information security should be defined

iv. Personnel having the qualifications and resources to fulfil their responsibilities

(b) Risk Assessment

The FSP's risk assessment process may affect the services provided to FIs. The following is a list of risk assessment factors that the FSP should consider as part of a regular risk assessment program:

i. Rapid growth – If the FSP gains a substantial number of new customers, the operating effectiveness of certain controls could be affected.

ii. New technology – If the FSP implements a new technology, its risks and impact to the FIs should be assessed.

iii. New business models, products, or activities – The diversion of resources to new activities from existing activities could affect the operating effectiveness of certain controls at the FSP.

iv. Corporate restructurings – A change in ownership or internal reorganisation could affect reporting responsibilities or the resources available for services to the FIs.

(c) Information and Communication

The FSP should implement formalised documentation of policies for all the underlying processes and controls related to various functions such as IT, Business Operations, Human Resource, etc.

Adequate information and effective communication are essential to the proper functioning of internal control.

i. The FSP should establish an internal communication channel to communicate to its staff, roles and responsibilities and significant matters related to the services provided to FIs.
ii. The FSP should establish a communication channel with FIs for reporting exceptions, changes to operating environment and other significant matters (e.g. engaging a sub-contractor) and also allow for FIs to respond with any feedback/complaints on the services.

FSPs should conduct initiatives to enhance awareness of information security and relevant regulatory requirements among their staff. For example, this could include sessions on phishing awareness, document encryption expectations, responsibilities relating to confidentiality/non-disclosure of client information, etc.

(d) Monitoring

i. FSPs should monitor their processes relevant to services provided to FIs to identify issues and concerns. For example, this could include a self-evaluation of its processes to assess compliance maturity against the FSP Compliance Readiness Framework and subsequently proceed to employ independent auditors to evaluate effectiveness of controls.

ii. FSPs should implement formalised documentation of policies for the underlying processes and controls related to various functions such as IT, Business Operations, Human Resources, etc.

FSPs should implement periodic tracking and reporting on SLA compliance and service lapses relating to service provisioning to FIs.

(e) Practices related to Sub-Contracting

FSPs that engage sub-contractors as part of service provisioning to FIs should:

i. be able to demonstrate due diligence and risk assessment of sub-contractors prior to onboarding

ii. monitor the sub-contractor's activities that affect service provisioning to FIs on an ongoing basis

iii. ensure contractual terms in sub-contracting arrangements should align to the FSP’s contract with the FIs

II. GENERAL INFORMATION TECHNOLOGY ("IT") CONTROLS

This section applies to the IT systems/applications that store, host or process FI's/FI clients' data and as such are instrumental in delivering the services that the FSP provides to the FIs. General IT Controls are internal controls to mitigate IT, financial reporting and operational risks.

(a) Logical Security

These controls provide reasonable assurance that logical access to programmers, data and operating system software is restricted to authorised personnel on a need-to-have basis.

1.	**Logical access to programmes, data, and operating system software is restricted to authorised personnel on a need-to-have basis.**	i. IT systems are configured to require key security settings (e.g. password complexity, lockout settings, password history) over passwords used for access. ii. Access to IT systems software (including API services connecting to FIs) is only granted based on a documented and approved request, and on a 'need-to-use' basis. As an alternative, the FSP may review access to IT systems software (including API services connecting to FIs), including sub-contractors' access, on a periodic basis to verify that access has been granted on a 'need-to-use' basis. iii. Access to IT systems software (including API services connecting to FIs) is revoked or disabled promptly when the access is no longer required. As an alternative, the FSP may review access to IT systems software (including API services connecting to FIs), including sub-contractors' access, on a periodic basis to verify that access has been granted on a 'need-to-use' basis. iv. Strong logical controls are used to identify, segregate and protect individual FI's information. Such controls should survive the tenure of the contract. For API services accessing FI data, these sessions should be logged to identify the third parties making the API connections and the data being accessed by the third party.

v. FI's data (including data that has been backed up exists within UAT) should be securely destroyed or removed as per agreed retention and destruction protocols as well as upon termination of contractual arrangements.

vi. Industry-accepted cryptography standards (e.g. cryptographic algorithms and encryption key length) agreed with FIs, are deployed to protect FIs' customer information and other sensitive data in accordance with the MAS Technology Risk Management (TRM) Guidelines section 12.1.3. These standards would apply for all FIs' customer information and other sensitive data that is:

(a) Stored in all type of authorised end-point devices, e.g. notebooks, personal computers, portable storage devices and mobile devices.

(b) Transmitted between terminals and hosts, through networks (e.g. internet, cloud and APIs) and between sites, e.g. primary and recovery sites.

(c) Stored in computer storage, including servers, databases, backup media and storage platforms, e.g. storage area network ("SAN")

(d) Electronically transmitted to external parties (where permissible). When transmitted electronically to external parties, e.g. via email, the decryption keys are communicated to the intended recipient via a separate channel, e.g. via telephone call.

vii. Where the FSP owns cryptographic keys, the FSP should ensure cryptographic keys are securely generated and protected from unauthorised disclosure (including during transmission). Access to generate keys is restricted.

viii. Where the FSP owns cryptographic keys, the FSP should store the cryptographic keys in systems that are hardened and tamper resistant (e.g. hardware security module).

ix. Users with elevated access privileges (including administrative account and accounts which can deploy changes into production) in respect of any operating system, database, application, security appliance or network device and accounts on any system used by the relevant entity to access customer information through the internet are implemented with two-factor authentication (2FA).

x. In addition, users with elevated access privileges are subjected to strict controls such as:

    (a) Split-password control, never-alone principle etc.

    (b) Passwords are changed regularly.

    (c) Activities performed of privileged users are logged

xi. Where possible, activities logged are reviewed by an independent personnel.

(b) Physical Security

These controls provide reasonable assurance that Data Centre ("DC")/Controlled Areas are resilient and physically secured from internal and external threats.

1. Data Centre/Controlled Areas are physically secured from internal and external threats.	i.	If the FSP utilises cloud services or has engaged a third party data centre provider, the FSP should conduct an assessment of these third party services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks as stipulated in the "Entity Level Controls - (f) Practices related to Sub-Contracting". As an alternative, for FSPs that manages their own data centre or server room, the below Physical Security controls would apply. (a) Access is physically restricted (e.g. via card access, biometric systems, ISO standard locks) to authorised personnel on a need-to-have basis only. Access mechanisms may include 'anti-passback' feature to prevent the use of card access for multiple entries and mantraps to prevent tailgating. (b) Requests for access to DCs by employees, contractors and third parties must be approved and documented. (c) All visitors must be registered. Visitors are issued with clear identification (e.g. an ID badge) and escorted by authorised personnel at all times. or as an alternative the FSP reviews the access rights to data centre/controlled areas on a periodic basis to verify that access is granted to authorised personnel on a need-to-have basis only.
	ii.	For FSPs that manage their own data centre all access points, including

		windows, to controlled areas are fitted with audible intruder alarms that are monitored by FSP personnel. Doors are fitted with door-ajar alarms. The alarm system is tested regularly, and the test documentation is retained.
	iii.	For FSPs that manage their own data centre, entries and exits to secure areas have an audit trail (e.g. entry/exit log from door access system, CCTV footage, manual log-book with visitor's name, date, time, purpose, escort's name, etc.).
	iv.	For FSPs that manage their own data centre, all physical access credentials are revoked or disabled promptly when not required. Inventory of security access cards is managed, and damaged or lost cards are invalidated or revoked in the access control system promptly. As an alternative, the FSP reviews the access rights to data centre/controlled areas on a periodic basis to remove access that is no longer required.
2. Data Centre/Controlled areas are resilient to protect IT assets	i.	For FSPs that manage their own data centre, the following environmental control features are installed at the data centre: (a) Locked cabinets for systems and network equipment. (b) Uninterruptible power supply and backup generators. (c) Air conditioning and humidity control systems. (d) Temperature and humidity sensor. (e) Fire and smoke detection systems. (f) Water sprinkler system (dry-piped). (g) FM200 or other fire suppression system.

(h) Raised floor.

(i) CCTV cameras.

(j) Water leakage detection system.

(k) Hand-held fire extinguisher.

ii. For FSPs that manage their own data centre, the environmental control equipment are inspected, tested and maintained regularly.

(c) Change Management

These controls provide reasonable assurance that changes to applications, system software and network components are assessed, approved, tested, implemented and reviewed in a controlled manner.

1. Changes to applications, system software and network components are assessed, approved, tested, implemented and reviewed in a controlled manner.	i.	The following controls exist for changes applied to the FSPs production environment: (a) Changes are initiated through a formal change request process and classified according to the priority, risk and impact of the changes. (b) Change requests are approved in accordance to an established Change Authority Matrix (includes internal and FIs' approvals), as agreed with FIs. (c) A risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems is performed to determine approval requirements. (d) All changes are tested and appropriate approvals are obtained prior to implementation. System Integration Testing ("SIT") and User Acceptance Testing ("UAT") test plans are prepared and signed off in accordance to the established Change Authority Matrix. (e) Emergency change escalation protocols (e.g. by telephone and email) and approval requirements are established in the change approval matrix (includes internal and FI approvals) as agreed with FIs. Documented approvals are obtained after the emergency change. (f) A rollback plan (which may include a backup plan) is prepared and

approved prior to changes being made.

ii. (a) Segregation of environments for development, testing, staging and production is established. UAT data are anonymised. If UAT contains production data, the environment must be subject to appropriate production level controls.

(b) Segregation of duties is enforced so that no single individual has the ability to develop, compile and migrate object codes into the production environment.

(c) Where the FSPs uses DevOps processes, the respective DevOps activities are logged and reviewed in a timely manner.

iii. Source code reviews are conducted on an-going basis for higher risk systems and applications changes (including APIs) to identify security vulnerabilities (including list of known components with "known vulnerabilities") and deficiencies, coding errors, defects and malicious codes before these changes are implemented.

iv. Where the FSP uses agile development framework, a mixture of static, dynamic and interactive application security testing methods is used to validate the security of the software application. Where applicable, the FSP should include fuzzing or fuzz testing as part of its dynamic or interactive application security testing.

v. Where the FSP uses agile development framework, automated static or dynamic software scanning should be implemented to detect security vulnerabilities or coding issues, and configurations that can impact the security of IT systems. Any issues or software defects discovered from source code review and application security testing should be tracked and remediated before production deployment.

(d) Incident Management

These controls provide reasonable assurance that all system and network processing issues are resolved in a timely and controlled manner.

1. System and network processing issues are resolved in a timely and controlled manner.	i.	When an incident is detected or reported, the defined incident management process is initiated by authorised personnel. The incident severity level and escalation process are pre-agreed with FIs. FIs should be notified immediately upon discovery and an Incident Report should be provided post-event.
	ii.	Incidents are recorded and tracked with the following information: (a) Severity. (b) Client/FI information. (c) Description of incident/problem. (d) Date and time of incident/problem. (e) Incident type. (f) Application, systems and / or network component impacted. (g) Escalation and approvals. (h) Actions taken to resolve the incident or problem, including date and time action was taken. (i) Root-cause analysis to prevent recurrence

iii. The FSP should design and implement its systems to achieve the level of system availability that is commensurate with its business needs. FSPs should proactively measure and monitor the utilisation of its system and network resources against a set of pre-defined thresholds to ensure that IT resources are adequate to meet business needs.

iv. The FSP should review its network architecture on a periodic basis to identify any potential single point of failure and implement appropriate measures to address and mitigate the risk of disruption.

(e) Backup and Disaster Recovery

These controls provide reasonable assurance that business and information systems recovery and continuity plans are documented, approved, tested and maintained. Backups are performed and securely stored.

1. Backups are performed and securely stored.	i.	Backup and restoration processes are implemented such that FIs' critical information systems can be recovered. Backup procedures are formally documented based on the data backup and recovery requirements of FIs. These include a data retention policy and procedures designed to meet business, statutory and regulatory requirements as agreed with FIs. Where the FSP owns cryptographic keys, the FSP should maintain backups of cryptographic keys for recovery purposes and accord them a high level of protection.
	ii.	System level backups are securely stored at off-site storage facilities.
	iii.	Follow-ups are completed to resolve exceptions noted during the back-up process, if applicable (e.g., a signature or initials on the document, written explanations, checkmarks, or other indications of follow up, such as an email etc.).
	iv.	Backup copies (or other media) are periodically tested to validate recovery capabilities.
2. Business and information systems recovery and continuity plans are documented, approved, tested and maintained	i.	A Disaster Recovery strategy and business continuity plan is established and maintained based on business, operational and information technological needs of the FSP and FIs that they service. These should be tested at least every 12 months. Operational considerations include geographical requirements, on-site and off-site redundancy requirements.

(a) Different scenarios such as major system outages, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary processing centre are considered in a DR plan.

(b) DR facilities should be able to accommodate the capacity for recovery as agreed with FIs.

(c) The FSP should notify the FIs of any substantial changes in the FSPs' BCP plans and of any adverse development that could substantially impact the services provided to the FIs.

In consultation with FIs testing may be conducted more frequently depending on the changing technology conditions and operational requirements. FIs should also be permitted to participate in DR and BCP tests as appropriate.

ii. The DR exercise (i.e. testing plans and results) should be documented with action plans to resolve and retest exceptions. The results of BCP and DR exercises should be communicated to the FIs.

iii. Recovery plans should include established procedures to meet recovery time objectives (RTO) and recovery point objectives (RPO) of systems and data. Applied definitions and actual objectives related to RTO and RPO are reviewed on a periodic basis by appropriate FSP Management to ensure alignment with FIs' expectations and applicable MAS regulations (e.g. MAS Outsourcing Guideline Business Continuity Management ("BCM") section 5.7.2 and MAS TRM Guideline section 8.2.4). Defined RTO, RPO and resumption operating capacities should be validated by management during the annual test of the DR strategy and BCP.

(f) Network and Security Management

These controls provide reasonable assurance that systems and network controls are implemented based on FIs' business needs.

1.	**Systems and network controls are implemented based on clients' business needs.**	i. Security baseline standards (i.e. system security baseline settings and configuration rules) are defined for the various middleware, operating system, databases, virtual instances and network devices to ensure consistent application of security configurations and hardening of systems to the required level of protection. Regular enforcement checks against baseline standards should be carried out to monitor compliance.
		ii. Anti-virus/anti-malware software are installed and updated regularly on every system. Detected threats are quarantined and removed appropriately.
		iii. FSP maintains an up-to-date inventory of hardware and software platforms used (including open source platforms) to facilitate patching and vulnerability monitoring, timely monitoring, reviewing, testing and application of vendor provided patches, and prioritizing security patches to address known vulnerabilities. Implementing patches should be performed in a timely manner. Where no security patch is available to address a vulnerability, the FSP will ensure that controls are instituted to reduce any risk posed by such vulnerabilities to such a system.
		iv. File integrity checks are in place to detect unauthorised changes (e.g. databases, files, programmes, system configuration, open source software downloaded from the internet).
		v. Network security controls are deployed to protect the internal network (including virtual network/cloud). These include firewalls and intrusion detection-prevention devices (including denial-of-service security appliances where appropriate)

between internal and external networks as well as between geographically separate sites, if applicable. Network surveillance and security monitoring procedures (e.g. network scanners, intrusion detectors and security alerts) are also established.

If the FSP uses IoT devices, the network that hosts IoT devices should be secured using strong authentication and network access controls to limit the cyberattack surface.

vi. Rules for network security devices are backed up regularly.

vii. Security system events are logged, retained and monitored.

(g) Security Incident Response

These controls provide reasonable assurance that appropriate personnel within the FSP are contacted and immediate action is taken in response to a security incident.

1. Appropriate personnel are contacted and immediate action taken in response to a security incident	i. Security incident response procedures (for cyber, physical or system security) should be documented and tested every 12 months.

(h) System Vulnerability Assessments

These controls provide reasonable assurance that vulnerability assessments and penetration testing are conducted regularly to detect and remediate security vulnerabilities in the IT environment.

1. Vulnerability Assessments	i.	The FSP continually monitors emergent security exploits, and performs regular VAs of its IT environment against common and emergent internal and external security threats. The frequency of a VA should be commensurate with the criticality of the system and the security risk to which it is exposed.
2. Penetration Testing	i.	PTs are performed to simulate attacks of the IT systems. The frequency of PT should be determined based on factors such as system criticality and the system's exposure to cyber risks. PTs of Internet facing systems are performed at least every 12 months.
3. Timely Remediation	i.	Issues identified via the VAs and PTs are remediated promptly and revalidated to ensure that the identified gaps are fully resolved. The process should minimally include the following: (a) severity assessment and classification of an issue; (b) definition of timeframe to remediate issues of different severity; and (c) risk assessment and mitigation strategies to manage deviations from the framework.

(i) Technology Refresh Management

These controls provide reasonable assurance that software and hardware components used in the production and disaster recovery environment are refreshed timely.

1.	**Production and disaster recovery systems and software are replaced timely**	i. An up-to-date inventory of software and hardware components used in the production and disaster recovery environments supporting FIs is maintained to facilitate the tracking of IT resources. The inventory includes all relevant associated warranty and other supporting contracts related to the software and hardware components. For IoT devices, it should include the networks they are connected to and their physical locations. ii. The FSP actively manages its IT systems and software supporting FIs so that outdated and unsupported systems which significantly increase its exposure to security risks are replaced timely. Close attention should be paid to the products' end-of-support ("EOS") dates.

III. Appendix

This appendix lists down those requirements from the MAS TRM Consultation Paper that were not included within this framework.

S/N	Domain	Reference	Clause
1	Software Application Development and Management	6.1.3	The FI should ensure its software developers are trained to apply the standards when developing software.
2	Software Application Development and Management	6.4.4	The FI should perform risk assessment before allowing third parties to connect to its systems via APIs, and ensure the security implementation for each API is commensurate with the sensitivity and business criticality of the data being exchanged, and the confidentiality and integrity requirements of the data.
3	Software Application Development and Management	6.4.8	Real-time monitoring and alerting capabilities should be instituted to provide visibility of the usage and performance of APIs and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access token in the event of a breach.

S/N	Domain	Reference	Clause
4	Software Application Development and Management	6.4.9	The FI should implement measures to handle high volumes of API call requests by legitimate applications, and mitigate denial-of-service attacks. The measures to be implemented should be commensurate with the criticality and availability requirements of the application.
5	Software Application Development and Management	6.5.1	The prevalence of common business application tools and software on the Internet has enabled end user computing, where business users develop or use simple applications to automate their operations, such as perform data analysis and generate reports. Any applications developed or acquired by end users should be approved by the relevant business and IT management, and managed as part of the FI's information assets.

S/N	Domain	Reference	Clause
6	Software Application Development and Management	6.5.2	The FI should establish a process to assess the importance of end user developed or acquired applications to the business, and ensure appropriate controls and security measures are implemented to address the associated risks. The FI should ensure proper review and testing of the programme codes, scripts and macros before they are deployed and used.
7	Software Application Development and Management	6.5.3	Shadow IT or IT applications acquired and used in the FI's environment without the approval of relevant business and IT management increase the FI's exposure to risks, such as leakage of sensitive data, or malware infection. The FI should establish measures to monitor and detect the use of shadow IT in its environment. End user should not be allowed to use shadow IT until they have been properly assessed and approved for use.

S/N	Domain	Reference	Clause
8	IT Service Management	7.7.7	The FI should establish a communications plan that covers the process and procedures to apprise its customers of IT incidents that may impede the FI's delivery of financial services to them, and to handle any media or public queries. The FI should identify the spokespersons and subject matter experts to address the media or public queries as well as the platforms to disseminate information.
9	IT Resilience	8.5.4	The FI's disaster recovery or secondary DC should be geographically separated from its primary DC so that both sites will not be impacted by a disruption to the underlying infrastructure (e.g. telecommunications and power) in a particular area.
10	Access Control	9.1.8	The FI should subject its service providers, who are given access to the FI's information assets, to the same monitoring and access restrictions on the FI's personnel.

S/N	Domain	Reference	Clause
11	Cryptography	10.1.4	The FI should monitor development in the area of cryptanalysis and where necessary, update or change the cryptographic algorithms or increase the key lengths, to ensure they remain resilient against evolving threats.
12	Cryptography	10.2.3	The FI should determine the appropriate lifespan of each cryptographic key based on the sensitivity of the data and the criticality of the system to be protected. The cryptographic key should be securely replaced, before it expires at the end of its lifespan.

S/N	Domain	Reference	Clause
13	Cryptography	10.2.7	When cryptographic keys have expired or have been revoked, the FI should use a secure key destruction method to ensure the keys would not be recoverable.
14	Operational Infrastructure Security	11.1.5	Security measures should be implemented to prevent and detect the use of unauthorised internet services which allow users to communicate or store confidential data such as social media sites, cloud-based internet storage sites, and web-based emails.

S/N	Domain	Reference	Clause
15	Operational Infrastructure Security	11.2.7	Systems with internet access are more susceptible to cyber threats. In this regard, the FI should perform a risk assessment and implement Internet surfing separation by isolating systems, including end-user computers and devices, which handle critical business and system functions or contain sensitive data, from the Internet and other systems connected to the Internet.
16	Operational Infrastructure Security	11.3.7	When implementing Bring Your Own Device (BYOD22), the FI should conduct a comprehensive risk assessment and implement appropriate measures to secure its BYOD environment before allowing staff to use their personal devices to access the corporate network. Refer to Annex B on the security measures for BYOD.
17	Operational Infrastructure Security	11.4.3	The FI should establish policies and standards to manage virtual machines images and snapshots. The standards should include details that govern the security, creation, distribution, storage, use, retirement and destruction of virtual images and snapshots so as to protect these assets against unauthorised access or modification.

S/N	Domain	Reference	Clause
18	v	11.5.2	Many IoT devices are designed without or with minimal security controls, if compromised, these devices can be used to gain unauthorised access to the FI's network and systems or as a launch pad for cyber attacks on the FI. The FI should assess and implement processes and controls to mitigate risks arising from IoT. The security controls should be commensurate with the function and criticality of the data that is collected, stored and processed by the IoT devices.
19	Cyber Surveillance and Security Operations	12.1.1	To maintain good cyber situational awareness, the FI should establish a process to collect, process and analyse cyber-related information for its relevance and potential impact to the FI's business and IT environment. Cyber-related information would include cyber events, cyber threat intelligence and information on system vulnerabilities.
20	Cyber Surveillance and Security Operations	12.1.2	The FI could consider procuring cyber intelligence monitoring services, as well as participating in cyber threat information-sharing arrangements with trusted parties.
21	Cyber Surveillance and Security Operations	12.1.3	The FI should use cyber threat intelligence to facilitate its risk assessment on prevailing cyber threats and implement the necessary measures to mitigate the attendant risks.
22	Cyber Surveillance and Security Operations	12.1.4	A process should be established for timely dissemination of cyber related information with internal stakeholders for their awareness or necessary action.

S/N	Domain	Reference	Clause
23	Cyber Surveillance and Security Operations	12.1.5	The FI should establish a process to detect and respond to misinformation related to the FI that are propagated via the cyberspace. The FI may consider engaging external media monitoring services that use technologies, such as machine learning, to facilitate evaluation and identification of online misinformation.
24	Cyber Surveillance and Security Operations	12.2.2	As compromised devices often attempt to establish connections via the Internet to Command and Control (C2) servers, the FI should proactively monitor and block callbacks, which can be tell-tale signs of intrusions.

S/N	Domain	Reference	Clause
25	Cyber Surveillance and Security Operations	12.2.4	Correlation of multiple events registered on system logs should be performed to identify suspicious or anomalous system activity trend or user behavioural patterns.
26	Cyber Surveillance and Security Operations	12.2.10	To facilitate continuous monitoring and analysis of cyber events; as well as prompt detection and response to cyber incidents, the FI should consider establishing a security operations centre with cyber surveillance and incident response capability.
27	Cyber Security Assessment	13.1.2	When performing system VA, the scope should minimally include vulnerability discovery, identification of weak security configurations, as well as applications and services that are not approved by business, IT management and other key stakeholders. For web-based systems, the scope of VA should include checks on common web-based vulnerabilities, such as SQL injection and cross-site scripting.

S/N	Domain	Reference	Clause
28	Cyber Security Assessment	13.2.1	The FI should carry out penetration testing 30 (PT) to obtain an in-depth evaluation of its cyber security defences. A combination of blackbox and greybox testing should be conducted for online financial services. 30 The 2 common types of penetration testing are: a) blackbox testing, which refers to testing without any prior knowledge of the environment except for the IP address ranges and known URLs; and b) greybox testing, which refers to testing with credentials. The security assessor is authenticated using the same rights as a normal customer
29	Cyber Security Assessment	13.2.2	A bug bounty programme is another mean by which an FI could discover vulnerabilities in their systems by inviting and incentivising ethical or "white hat" hackers to test their systems. The FI may consider conducting a bug bounty programme to test the security of its IT infrastructure to complement its PT.
30	Cyber Security Assessment	13.4.1	The FI is encouraged to perform an adversarial attack simulation exercise34 to test and validate the effectiveness of its cyber defence and response plan against prevalent cyber threats.

S/N	Domain	Reference	Clause
31	Cyber Security Assessment	13.4.2	The objectives, scope and rules of engagement should be defined before the commencement of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities carried out by the red team do not disrupt the FI's production systems.
32	Cyber Security Assessment	13.5.1	To simulate realistic adversarial attacks on an FI during a red team exercise, the threat scenario should be designed and based on real cyber incidents
33	Cyber Security Assessment	13.5.2	As an alternative, the FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.
34	Online Financial Services	14.1.1	Online financial services refer to banking, trading, insurance, or other financial and payment services that are provisioned via the Internet . In delivering online financial services, the FI should implement security and control measures which commensurate with the risk involved to ensure data confidentiality and integrity, and the security, availability and resilience of the online services.

S/N	Domain	Reference	Clause
35	Online Financial Services	14.1.2	The FI should secure the communications channel by using strong cryptographic controls to safeguard the confidentiality and integrity of confidential data during transmission such as using encryption and digital signatures.
36	Online Financial Services	14.1.3	Adequate measures should also be taken to minimise exposure of the FI's online financial services to common attack vectors such as code injection attack, cross-site scripting, man-in-the-middle attack (MITMA), distributed denial of service (DDoS), malware and spoofing attacks.
37	Online Financial Services	14.1.4	An FI offering online financial services access via a mobile device should be aware of the risks unique to mobile applications. Specific measures aimed at addressing the risk of mobile applications should be put in place. Refer to Annex C for guidance on Mobile Application Security.
38	Online Financial Services	14.1.5	Distribution of mobile applications or software to customers should only be performed through official mobile application stores or other secure delivery channels.
39	Online Financial Services	14.1.6	The FI should actively monitor the Internet, mobile application stores, social media websites, emails or text messages (e.g. SMS) for phishing campaigns targeting the FI and its customers. Immediate action should be taken to report the phishing attempts to the service providers and law enforcement agencies to facilitate removal of the malicious content. The FI should alert its customers of such campaigns.

S/N	Domain	Reference	Clause
40	Online Financial Services	14.1.7	Rooted or jailbroken mobile devices should be blocked from accessing the FI's mobile applications to perform financial transactions as such devices are more susceptible to malware and security vulnerabilities.
41	Online Financial Services	14.2.1	Multi-factor authentication should be deployed at login for online financial services to secure the customer authentication process. Multi-factor authentication can be based on any two or more of the following factors, i.e. what you know (e.g. personal identification number or password), what you have (e.g. OTP generator) and who you are (e.g. Biometrics).
42	Online Financial Services	14.2.2	End-to-end encryption at the application layer should be implemented for the transmission of customer passwords so that they are not exposed at any intermediate nodes between the customer mobile application or browser and the system where passwords are verified.
43	Online Financial Services	14.2.3	The FI should implement transaction-signing (e.g. digital signatures) for authorising high risk activities to protect the integrity of customer accounts' data and transaction details. High-risk activities include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details, high value funds transfers and revision of funds transfer limits.

S/N	Domain	Reference	Clause
44	Online Financial Services	14.2.4	Besides login and transaction-signing for high-risk activities, the FI may apply a risk-based approach and implement appropriate risk-based or adaptive authentication that presents customers with authentication options that commensurate with the risk level of the transaction and sensitivity of the information.
45	Online Financial Services	14.2.5	When implementing time-based one-time-passwords (OTPs), the FI should establish a validity period that is as short as practicable to lower the risk of a stolen OTP being used for fraudulent transactions.
46	Online Financial Services	14.2.6	Where biometric technologies and customer passwords are used for customer authentication, the FI should ensure the biometrics information and authentication credentials are encrypted in storage and during transmission.
47	Online Financial Services	14.2.7	The performance of the biometrics solution, based on false acceptance rate and false rejection rate , should be calibrated to commensurate with the risk associated with the online activity.
48	Online Financial Services	14.2.8	A soft token is a software-based two-factor authentication mechanism installed on a general-purpose device . Where soft token is used for customer authentication, appropriate measures, such as verifying the identity of the customer, detecting and blocking rooted or jailbroken devices, and performing device binding , should be implemented for the soft token provisioning process.

S/N	Domain	Reference	Clause
49	Online Financial Services	14.2.9	Diversification of cryptographic keys can greatly limit the impact of a key exposure. A unique cryptographic key should be used to generate each type of authentication factors. For instance, the cryptographic key for generating the OTP for login should be different from the one that is used to generate the transaction-signing code.
50	Online Financial Services	14.2.10	A process should be implemented to secure the issuance and enrolment of the authentication or transaction signing mechanism so as to prevent the theft of the mechanism for unauthorised access to the FI's customer's online account.
51	Online Financial Services	14.2.11	The FI should ensure the authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. In the event of interference, the FI should put in place measures to detect and terminate the session. To prevent an attacker from maintaining a hijacked session indefinitely, online session should be automatically terminated after a pre-defined time.
52	Online Financial Services	14.2.12	Where alternate controls and processes (e.g. maker-checker function) are implemented for corporate or institutional customers to authorise transactions, the FI should perform a security risk assessment to ascertain these controls or processes commensurate with the risk of the activities that are being carried out.
53	Online Financial Services	14.3.1	The FI should implement real-time fraud monitoring or surveillance systems to identify and block suspicious or fraudulent online transactions.

S/N	Domain	Reference	Clause
54	Online Financial Services	14.3.2	follow-up process should be established to ensure suspicious transactions or payments are investigated and issues are adequately and promptly addressed.
55	Online Financial Services	14.3.3	The FI should notify customers of suspicious activities or fund transfers above a threshold that is defined by the FI or customers to facilitate detection and response to fraudulent transactions in a timely manner. The notification should contain meaningful information such as type of transaction and payment amount, as well as instructions to report suspicious activities or unauthorised transactions.
56	Online Financial Services	14.4.1	Customers should be informed about the risks of using online financial services before they subscribe to such services and whenever changes are made to the security features of the services.
57	Online Financial Services	14.4.2	The FI should advise their customers on the means to report security issues, suspicious activities or fraud.
58	Online Financial Services	14.4.3	The FI should alert their customers to cyber threats and incidents, and educate their customers of their responsibilities to take appropriate security measures to secure the electronic devices that are used to access online financial services.

S/N	Domain	Reference	Clause
59	IT Audit	15.1.1	Audit plays an important role to assess the effectiveness of the controls, risk management and governance process in the FI. The FI should ensure IT audit is performed to provide the board of directors and senior management an independent and objective opinion of the adequacy and effectiveness of the FI's risk management, governance and internal controls relative to its existing and emerging technology risk.
60	IT Audit	15.1.2	A comprehensive set of auditable areas for technology risk should be identified so that an effective risk assessment could be performed during audit planning. Auditable areas should include all IT operations, functions and processes.
61	IT Audit	15.1.3	The frequency of IT audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process.
62	IT Audit	15.1.4	The FI should ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented