Monetary Authority of Singapore

COMPLIANCE CHECKLIST
FOR
INTERNET BANKING AND TECHNOLOGY RISK MANAGEMENT GUIDELINES 3.0

TABLE OF CONTENTS

SECTION

A COMPLIANCE CHECKLIST

1. Each guideline description in the checklist should be evaluated in the context of the relevant sections in the Internet Banking and Technology Risk Management Guidelines Version 3.0. Some item descriptions in this checklist have been condensed and may not be verbatim with the Guidelines.

2. For each item, place an “X” in the appropriate column to indicate whether the financial institution is fully compliant, partially compliant, or not compliant with the guideline description. Otherwise, place an “X” in the NA column.

3. If full compliance has not been achieved, explain in Section B how and when remedial action would be made.

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
	2.0	**RISK MANAGEMENT FRAMEWORK**				
1.	2.0.1	A sound and robust risk management framework is established. Such a framework includes the identification of information systems assets, security threats and vulnerabilities; estimation of the likelihood of exploitation or attacks; assessment of potential losses associated with these risk events; and the implementation of appropriate security measures and controls for asset protection.	☐	☐	☐	☐
2.	2.0.3	Risks associated with internet banking and the launch of new products or services are assessed and resolved during the conceptualisation and developmental stages. Risk control procedures and security measures are put in place prior to or at the implementation phase.	☐	☐	☐	☐
3.	2.0.4	The oversight of technology risk management is the responsibility of the Board of Directors and Senior Management. The monitoring and reporting of risk management effectiveness and compliance eventually flow upwards to the Chief Executive Officer and the Board of Directors.	☐	☐	☐	☐

* Explain in Section B why full compliance has not been achieved; indicate what and when remedial action will be made.

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
4.	2.0.5	Policies, procedures and practices to define risks, stipulate responsibilities, specify security requirements, implement safeguards to protect information systems, administer internal controls and enforce compliance are set up as essential specifications of the risk management framework.	☐	☐	☐	☐
5.	2.0.5	Periodic security risk assessments are conducted by management to identify internal and external threats that may undermine system integrity, interfere with service or result in the disruption of operations.	☐	☐	☐	☐
6.	2.0.5	Security awareness, training and education programmes are conducted internally and externally to promote and nurture a security-conscious environment.	☐	☐	☐	☐
7.	2.0.6	Various scenarios of operational disruption or system breakdown are identified by the financial institution and catered for in the disaster recovery plan.	☐	☐	☐	☐
8.	2.0.7	Periodic testing and validation of recovery requirements and readiness at the backup site are carried out and assessed for adequacy, effectiveness and personnel ability to execute contingency procedures and restore operational capability.	☐	☐	☐	☐
9.	2.2.2	During the risk identification process, consideration is given to both the internet applications and their interfaces with the back-end and the supporting systems. Risks and threats associated with such systems and their interdependencies are taken into account.	☐	☐	☐	☐
10.	2.2.3	Security threats such as denial of service attacks, internal sabotage and malware infestation can cause severe disruption to the operations of a financial institution with consequential losses for all parties affected. Such mutating and growing risks are vigilantly monitored within the risk management process.	☐	☐	☐	☐
11.	2.3.1	Following the task of risk identification, the potential effects and consequences of these risks on the overall business and operations are analysed and quantified by management. In the event that certain risks are not quantifiable, these risks are defined and steps are taken to understand their potential impact and consequences should adverse incidents occur.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		With this information, the risks are prioritised, cost-benefit analysis is performed, and risk mitigation decisions are made.				
12.	2.4.1	For each type of material risks identified and analysed, risk mitigation and control strategies that are consistent with the value of the information asset and level of risk tolerance, are developed and implemented by management. Risk mitigation entails a methodical approach in prioritising, evaluating and implementing appropriate risk-reduction controls and security measures that emanate from the risk assessment process.	☐	☐	☐	☐
13.	2.4.3	An ongoing risk monitoring and compliance regime is instituted by management to ascertain the performance and effectiveness of the risk management process. When risk parameters change, the risk process is updated and enhanced accordingly. Re-evaluation of past risk-control equations, renewed testing and auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken are conducted.	☐	☐	☐	☐
	3.0	**TYPES OF INTERNET FINANCIAL SERVICES**				
14.	3.1.3	For financial institutions that provide basic information service on the internet by purchasing advertisement space on other websites hosted by third parties, regular monitoring is made not only of the financial institution's advertisement, but also the associated contents of the service provider.	☐	☐	☐	☐
	4.0	**SECURITY AND CONTROL OBJECTIVES**				
15.	4.1.2	The strength and type of encryption algorithm adopted by the financial institution are commensurate with the degree of confidentiality and integrity required for its internet systems.	☐	☐	☐	☐
16.	4.1.2	Only encryption algorithms that are well-established international standards are used by the financial institution. Such algorithms should be subjected to rigorous scrutiny by an international community of cryptographers; or approved by authoritative professional bodies, reputable security vendors or government agencies.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
17.	4.1.3	All cryptographic keys are created, stored, distributed and changed under the most stringent conditions. No single individual has knowledge of the entire key, or have access to all the constituents making up these keys.	☐	☐	☐	☐
18.	4.1.3	The frequency at which cryptographic keys are changed is based on the sensitivity of the encrypted data and operational criticality.	☐	☐	☐	☐
19.	4.1.4	Hardware security modules and similar tamper-resistant devices are used to perform encryption and decryption functions.	☐	☐	☐	☐
20.	4.1.5	Encryption of customer PINs and other sensitive data is maintained end-to-end at the application layer. The encryption process is kept intact from the point of data entry to the final system destination where decryption and/or authentication takes place.	☐	☐	☐	☐
21.	4.2.3	Monitoring or surveillance systems are deployed to alert the financial institution of any erratic system activities or unusual online transactions taking place.	☐	☐	☐	☐
22.	4.3.2	For financial institutions that provide internet banking services, ample resources and capacity in terms of hardware, software and other operating capabilities are monitored so as to deliver consistently reliable services. Such monitoring extends to the financial institution's service providers and vendors.	☐	☐	☐	☐
23.	4.3.3	In the context of online banking, the interfacing support systems are just as important as the hosting system. The availability of both front-end and backend systems are monitored to provide the level of reliability and consistency of service expected by customers.	☐	☐	☐	☐
24.	4.3.4	Standby hardware, software and network components are maintained to provide the capability for fast recovery.	☐	☐	☐	☐
25.	4.3.5	Procedures and monitoring tools to track system performance, server processes, traffic volumes, transaction duration and capacity utilisation on a continual basis are put in place to ensure a high level of availability of internet banking services.	☐	☐	☐	☐
26.	4.4.2	Two-factor authentication at login for all types of internet banking systems and for authorising transactions is implemented.	☐	☐	☐	☐
27.	4.4.3	For high value transactions or for changes to sensitive customer data (e.g., customer office and home address, email and telephone contact details) during a login session, the repeated use	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		of the second authentication factor (e.g., one-time passwords) by the customer is implemented.				
28.	4.4.3	An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. In the event of interference, controls are in place to terminate the session and reverse out the affected transactions. The customer is promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.	☐	☐	☐	☐
29.	4.4.4	Cryptographic functions, algorithms and protocols are used to authenticate logins and protect communication sessions between the customer and the financial institution.	☐	☐	☐	☐
30.	4.4.5	Confirmatory second channel procedures are applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits, to enhance online processing security. In devising these security features, their efficacy and differing customer preferences for additional online protection are taken into account.	☐	☐	☐	☐
31.	4.4.6	Authentication of the financial institution's web site by the customer is implemented using security mechanisms such as personal assurance messages/images, exchange of challenge response security codes or the secure sockets layer (SSL) server certificate verification.	☐	☐	☐	☐
32.	4.5.2	Controls are implemented to ensure that a customer is properly identified and authenticated before access to sensitive customer information or online banking functions is permitted. Sensitive customer information includes customer personal particulars or account details that can be used to identify a customer.	☐	☐	☐	☐
33.	4.5.4	As an integral part of the two-factor authentication architecture, appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack, are implemented.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
34.	4.5.6	Distribution of software to customers via the internet or through a web-based system is prohibited unless adequate security and safeguards for the customers are provided.	☐	☐	☐	☐
	5.0	**SECURITY PRINCIPLES AND PRACTICES**				
35.	5.1.1	Stringent selection criteria and thorough screening procedures are established for appointing personnel to internet operations and security functions.	☐	☐	☐	☐
36.	5.1.1	Personnel involved in developing, maintaining and operating websites and systems are adequately trained in security principles and practices.	☐	☐	☐	☐
37.	5.1.2	Sensitive and critical IT operations are jointly carried out by more than one person or performed by one person and immediately checked by another.	☐	☐	☐	☐
38.	5.1.2	Segregation of duties is established for operating systems function, systems design and development, application maintenance programming, computer operations, database administration, access control administration, data security, librarian and backup data file custody.	☐	☐	☐	☐
39.	5.1.2	Job rotation and cross training for security administration functions are instituted.	☐	☐	☐	☐
40.	5.1.2	Transaction processes are designed such that no single person can initiate, approve, execute and enter transactions into a system in a manner that would enable fraudulent actions to be perpetrated and processing details to be concealed.	☐	☐	☐	☐
41.	5.1.2	Access rights and system privileges are provided based on job responsibility and the necessity to have them to fulfil one's duties.	☐	☐	☐	☐
42.	5.1.4	No one is provided concurrent access to both production systems and backup systems, particularly data files and computer facilities.	☐	☐	☐	☐
43.	5.1.4	Access to backup files or system recovery resources are duly authorised for a specific reason and a specified time only.	☐	☐	☐	☐
44.	5.1.5	Personnel from vendors and service providers, including consultants, who have been given authorised access to the organisation's critical network and computer resources are subject to close supervision, monitoring and access	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		restrictions, similar to those applying to internal personnel.				
45.	5.1.7 (a)	Two-factor authentication is implemented for privileged users (systems, technical, operations, development, programming, support etc).	☐	☐	☐	☐
46.	5.1.7 (b)	Strong controls are implemented for remote access by privileged users.	☐	☐	☐	☐
47.	5.1.7 (c)	The number of privileged users is restricted.	☐	☐	☐	☐
48.	5.1.7 (d)	Privileged access is granted on a "need-to-have" basis.	☐	☐	☐	☐
49.	5.1.7 (e)	Audit logging of system activities performed by privileged users are maintained.	☐	☐	☐	☐
50.	5.1.7 (f)	Privileged users do not have access to systems logs in which their activities are being captured.	☐	☐	☐	☐
51.	5.1.7 (g)	Regular audits or management reviews of the logs are conducted.	☐	☐	☐	☐
52.	5.1.7 (h)	Sharing of privileged IDs and their access codes is prohibited.	☐	☐	☐	☐
53.	5.1.7 (i)	Vendors and contractors are disallowed from gaining privileged access to systems without close supervision and monitoring.	☐	☐	☐	☐
54.	5.1.7 (j)	Backups of data are protected from unauthorised access.	☐	☐	☐	☐
	5.2.1	The following security practices are implemented:				
55.	5.2.1 (a)	Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.	☐	☐	☐	☐
56.	5.2.1 (b)	Install firewalls between internal and external networks as well as between geographically separate sites.	☐	☐	☐	☐
57.	5.2.1 (c)	Install intrusion detection-prevention devices (including denial-of-service security appliances where appropriate).	☐	☐	☐	☐
58.	5.2.1 (d)	Develop built-in redundancies for single points of failure which can bring down the entire network.	☐	☐	☐	☐
59.	5.2.1 (e)	Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.	☐	☐	☐	☐
60.	5.2.1 (f)	Engage independent security specialists to assess the strengths and weaknesses of	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff who are operationally or functionally responsible for the system or activity.				
61.	5.2.1 (g)	Conduct penetration testing at least annually.	☐	☐	☐	☐
62.	5.2.1 (h)	Establish network surveillance and security monitoring procedures with the use of network scanners, intrusion detectors and security alerts.	☐	☐	☐	☐
63.	5.2.1 (i)	Implement anti-virus software.	☐	☐	☐	☐
64.	5.2.1 (j)	Conduct regular system and network configurations review and data integrity checks.	☐	☐	☐	☐
65.	5.2.1 (k)	Maintain access security logs and audit trails.	☐	☐	☐	☐
66.	5.2.1 (l)	Analyse security logs for suspicious traffic and intrusion attempts.	☐	☐	☐	☐
67.	5.2.1 (m)	Establish an incident management and response plan.	☐	☐	☐	☐
68.	5.2.1 (n)	Test the predetermined response plan relating to security incidents.	☐	☐	☐	☐
69.	5.2.1 (o)	Install network analysers which can assist in determining the nature of an attack and help in containing such an attack.	☐	☐	☐	☐
70.	5.2.1 (p)	Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.	☐	☐	☐	☐
71.	5.2.1 (q)	Maintain a rapid recovery capability.	☐	☐	☐	☐
72.	5.2.1 (r)	Conduct security awareness education and programs.	☐	☐	☐	☐
73.	5.2.1 (s)	Require frequent ICT audits to be conducted by security professionals or internal auditors who have the requisite skills.	☐	☐	☐	☐
74.	5.2.1 (t)	Consider taking insurance cover for various insurable risks, including recovery and restitution costs.	☐	☐	☐	☐
75.	5.2.1 (u)	Provide separate physical or logical environments for systems development, testing, staging and production; connect only the production environment to the internet.	☐	☐	☐	☐
76.	5.2.1 (v)	Implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
77.	5.2.1 (w)	Implement two-factor authentication at login for all types of internet banking systems and a specific OTP or digital signature for each value transaction above a specified amount selectable by the customer or pre-determined by the financial institution.	☐	☐	☐	☐
78.	5.2.1 (x)	Deploy strong cryptography and end-to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.	☐	☐	☐	☐
79.	5.2.1 (y)	Encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.	☐	☐	☐	☐
80.	5.2.1 (z)	Deploy strong user authentication in wireless local area networks and protect sensitive data with strong encryption and integrity controls.	☐	☐	☐	☐
	6.0	**SYSTEM DEVELOPMENT AND TESTING**				
81.	6.0.1	For major projects, a steering committee, consisting of various management, development and user stakeholders, is established to provide oversight and to monitor the progress of the project, including the deliverables to be realised at each phase of the project and the milestones to be reached according to the project timetable.	☐	☐	☐	☐
82.	6.1.1	In the system development life cycle framework, the tasks and processes for developing or acquiring new systems include the assignment and delineation of responsibilities and accountabilities for system deliverables and project milestones. User functional requirements, systems design and technical specifications and service performance expectation are adequately documented and approved at appropriate management levels.	☐	☐	☐	☐
83.	6.1.2	Besides business functionalities, security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, security event tracking and exception handling are clearly specified. Such security requirements are checked against the financial institution's security standards and regulatory requirements for compliance.	☐	☐	☐	☐
84.	6.1.3	A methodology approved by management is established to specify how and what system	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		testing should be conducted. The scope of the tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions. Full regression testing is performed before major system rectification or enhancement is implemented. The outcomes of the tests are reviewed and signed off by the users whose systems and operations are affected by the new changes.				
85.	6.1.4	Penetration testing is conducted prior to the commissioning of a new system that offers internet accessibility and open network interfaces. Vulnerability scanning is conducted at least quarterly, and penetration testing at least yearly.	☐	☐	☐	☐
86.	6.1.5	Separate physical or logical environments are maintained for unit, integration, system and user acceptance testing (UAT) to control the migration of new systems or changes to the production environment. Vendor and developer access to the UAT environment are strictly monitored.	☐	☐	☐	☐
87.	6.2.4	Based on the financial institution's risk analysis, specific application modules and their security safeguards are rigorously tested with a combination of source code review, exception testing and compliance review to identify errant coding practices and systems vulnerabilities that could lead to security problems, violations and incidents.	☐	☐	☐	☐
88.	6.2.4 (a)	Sensitive information such as cryptographic keys, account and password details, system configurations and database connection strings should not be disclosed. Potential sources of information leakages like verbose error messages and banners, hard-coded data, files and directories operations are scrutinised for inappropriate information disclosure.	☐	☐	☐	☐
89.	6.2.4 (b)	The security test methodology includes the review of all input validation routines and the assessment of their effectiveness against known vulnerabilities.	☐	☐	☐	☐
90.	6.2.4 (c)	The security test methodology includes the identification of insecure programming practices, such as the use of vulnerable function calls, inadequate memory management, unchecked argument passing, inadequate logging and comments, use of relative paths, logging of	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		passwords and authentication credentials, and inappropriate access privilege assignment.				
91.	6.2.4 (d)	Critical modules containing authentication and session management functions are vetted for discrepancies between the code design and implementation.	☐	☐	☐	☐
92.	6.2.4 (e)	When exception or abnormal conditions occur, adequate controls are in place to ensure resulting errors do not allow users to bypass security checks or obtain core dumps. Sufficient processing details are logged at the source of the exception to assist problem diagnosis. However, system or application details such as stack pointers are not revealed.	☐	☐	☐	☐
93.	6.2.4 (f)	Only cryptographic modules based on authoritative standards and reputable protocols are installed. Functions involving cryptographic algorithms and crypto-key configurations are vetted for deficiencies and loopholes. This review should also evaluate the choice of ciphers, key sizes, key exchange control protocols, hashing functions and random number generators.	☐	☐	☐	☐
	7.0	**RECOVERY AND BUSINESS CONTINUITY**				
94.	7.0.1	Recovery and business resumption priorities are defined and contingency procedures are tested and practised so that business and operating disruptions arising from a serious incident are minimised.	☐	☐	☐	☐
95.	7.0.1	The recovery plan and incident response procedures are evaluated periodically and updated as and when changes to business operations, systems and networks occur.	☐	☐	☐	☐
96.	7.0.3	A recovery site geographically separate from the primary site is established to enable the restoration of critical systems and resumption of business operations should a major disruption occur at the primary site.	☐	☐	☐	☐
97.	7.0.3	A hotsite rapid recovery capability is established and maintained. The required speed of recovery will depend on the criticality of resuming business operations, the type of online services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
98.	7.0.4	A predetermined action plan to address public relations issues is included in the incident response procedures.	☐	☐	☐	☐
99.	7.0.5	Incident response, disaster recovery and business continuity preparations are regularly reviewed, updated and tested to ensure their effectiveness and that responsible staff are capable of undertaking emergency and recovery procedures when required.	☐	☐	☐	☐
100.	7.0.5	The disaster recovery plan includes the scenario whereby the primary computer site experiences a total shutdown or incapacitation.	☐	☐	☐	☐
101.	7.0.6	For financial institutions that have network and systems linked to specific service providers and vendors, bilateral or multilateral recovery testing is conducted to ensure that inter-dependencies are also fully catered for.	☐	☐	☐	☐
102.	7.0.7	A predetermined action plan for countering and containing denial of service attacks is established as part of the disaster recovery plan.	☐	☐	☐	☐
	8.0	**OUTSOURCING MANAGEMENT**				
103.	8.1.1	Before an outsourcing vendor is appointed, due diligence is carried out to determine the viability, capability, reliability, track record and financial position of the outsourcing vendor.	☐	☐	☐	☐
104.	8.1.1	The contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all the contracting parties are carefully and properly defined in written agreements.	☐	☐	☐	☐
105.	8.1.2	The contractual agreement with the outsourcing vendor includes the provision of access to all parties nominated by the financial institution to its systems, operations, documentation and facilities to carry out any review or assessment for regulatory, audit or compliance purpose.	☐	☐	☐	☐
106.	8.1.2	The power of regulatory authorities under the Banking Act to carry out any inspection, supervision or examination of the service provider's role, responsibilities, obligations, functions, systems and facilities is specified in the contractual agreement.	☐	☐	☐	☐
107.	8.1.3	Financial institutions and outsourcing vendors must observe the requirements of banking secrecy under the Banking Act. The contracts and arrangements with outsourcing vendors take into account the need to protect the	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		confidentiality of customer information as well as the necessity to comply with all applicable laws and regulations.				
108.	8.2.1	The outsourcing vendor is required to implement security policies, procedures and controls that are at least as stringent as the financial institution's own operations.	☐	☐	☐	☐
109.	8.2.1	The security practices and processes of the outsourcing vendor is reviewed and monitored on a regular basis.	☐	☐	☐	☐
110.	8.2.1	A process of monitoring service delivery, performance reliability and processing capacity of the outsourcing vendor is established for the purpose of gauging ongoing compliance with agreed service levels and the viability of the outsourced operations.	☐	☐	☐	☐
111.	8.3.1	A disaster recovery contingency framework which defines the role and responsibilities of the outsourcing vendor is defined. The framework includes documentation, maintenance and testing of the outsourcing vendor's contingency plans and recovery procedures. The disaster recovery plan is reviewed, updated and tested regularly in accordance with changing technology conditions and operational requirements.	☐	☐	☐	☐
112.	8.3.2	A contingency plan is established based on credible worst-case scenarios whereby the outsourcing vendor is not able to continue operations or render the services required. The plan incorporates the identification of viable alternatives for resuming the financial institution's internet banking operations elsewhere.	☐	☐	☐	☐
	9.0	**DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)**				
113.	9.1.1	For financial institutions that provide internet banking services, appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems are deployed.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
114.	9.1.2	Firewalls, intrusion detection/prevention systems, routers and other specialised network equipment (that alert security personnel and divert and/or filter network traffic in real-time once a DDoS attack is suspected or confirmed) are deployed.	☐	☐	☐	☐
115.	9.1.3	Potential bottlenecks and single points of failure vulnerable to DDoS attacks could be identified through source code review, network design analysis and configuration testing.	☐	☐	☐	☐
	9.2.2	In the ISP selection process, the following factors are taken into consideration:				
116.	9.2.2 (a)	Whether an ISP offers DDoS protection or clean pipe services to assist in detecting and deflecting malicious traffic;	☐	☐	☐	☐
117.	9.2.2 (b)	The ability of the ISP to scale up network bandwidth on demand;	☐	☐	☐	☐
118.	9.2.2 (c)	The adequacy of an ISP's incident response plan; and	☐	☐	☐	☐
119.	9.2.2 (d)	The ISP's capability and readiness in responding quickly to an attack.	☐	☐	☐	☐
120.	9.3.1	An incident response framework is established and routinely validated to facilitate fast response to a DDoS onslaught or an imminent attack. The framework should include a plan detailing the immediate steps to be taken to counter an attack, invoke escalation procedures, activate service continuity arrangements, trigger customer alerts, as well as report to MAS and other authorities.	☐	☐	☐	☐
121.	9.3.2	The ISPs' incident response plans are analysed and assimilated into the financial institution's incident response framework. A communication protocol is established between the financial institution and the ISPs. Periodic joint incident response exercises are conducted together with the ISPs.	☐	☐	☐	☐
	10.0	**BANK DISCLOSURE**				
122.	10.0.1	Customers are provided information about the risks and benefits of using internet banking before they subscribe to internet banking services. Customers are also informed clearly and precisely on the respective rights, obligations and responsibilities of the customers and the financial institution on all matters	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
		relating to online transactions, and in particular, any problems that may arise from processing errors and security breaches.				
123.	10.0.2	The terms and conditions applying to online banking products and services are readily available to customers within the internet banking application. On initial logon or subscription to a particular service or product, a positive acknowledgement of the terms and conditions is required from the customer.	☐	☐	☐	☐
124.	10.0.3	The customer privacy and security policy are published on the financial institution's website. Customer dispute handling, reporting and resolution procedures, including the expected timing for the financial institution's response are clearly defined.	☐	☐	☐	☐
125.	10.0.4	Security measures and reasonable precautions that customers should take when accessing their online accounts are explained and published on the financial institution's website.	☐	☐	☐	☐
126.	10.0.5	On the contingency that security breaches may occur and customer online accounts might have been fraudulently accessed and unauthorised transactions made, the process for resolving the problem or dispute, as well as the conditions and circumstances in which the resultant losses or damages would be attributable to the financial institution or the customers are explained and published on the financial institution's websites.	☐	☐	☐	☐
	11.0	**CUSTOMER EDUCATION**				
127.	11.0.2	When new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to online delivery channels, sufficient instructions to properly utilise such new features are provided to the customers.	☐	☐	☐	☐
128.	11.0.3	To raise security awareness, the need to protect customer PINs, security tokens, personal details and other confidential data are clearly communicated to the customers. PIN and OTP security instructions are displayed prominently in the user login page or the USER ID, PIN and OTP entry page.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
	11.0.3	The following advice is included:				
129.	11.0.3 (a)	PINs should be at least 6 digits or 6 alphanumeric characters, without repeating any digit or character more than once.	☐	☐	☐	☐
130.	11.0.3 (b)	PINs should not be based on user-id, personal telephone number, birthday or other personal information.	☐	☐	☐	☐
131.	11.0.3 (c)	PINs must be kept confidential and not be divulged to anyone.	☐	☐	☐	☐
132.	11.0.3 (d)	PINs must be memorised and not be recorded anywhere.	☐	☐	☐	☐
133.	11.0.3 (e)	PINs should be changed regularly.	☐	☐	☐	☐
134.	11.0.3 (f)	The same PIN should not be used for different websites, applications or services, particularly when they relate to different entities.	☐	☐	☐	☐
135.	11.0.3 (g)	The customer should not select the browser option for storing or retaining user name and password.	☐	☐	☐	☐
136.	11.0.3 (h)	The customer should check the authenticity of the financial institution's website by comparing the URL and the financial institution's name in its digital certificate or by observing the indicators provided by an extended validation certificate.	☐	☐	☐	☐
137.	11.0.3 (i)	The customer should check that the financial institution's website address changes from http:// to https:// and a security icon that looks like a lock or key appears when authentication and encryption is expected.	☐	☐	☐	☐
138.	11.0.3 (j)	The customer should not allow anyone to keep, use or tamper with his OTP security token.	☐	☐	☐	☐
139.	11.0.3 (k)	The customer should not reveal the OTP generated by his security token to anyone.	☐	☐	☐	☐
140.	11.0.3 (l)	The customer should not divulge the serial number of his security token to anyone.	☐	☐	☐	☐
141.	11.0.3 (m)	The customer should check his bank account balance and transactions frequently and report any discrepancy.	☐	☐	☐	☐
	11.0.4	The following security precautions and practices are provided to the customers:				
142.	11.0.4 (a)	Install anti-virus, anti-spyware and firewall software in their personal computers, particularly when they are linked via broadband connections, digital subscriber lines or cable modems.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
143.	11.0.4 (b)	Update the anti-virus and firewall products with security patches or newer versions on a regular basis.	☐	☐	☐	☐
144.	11.0.4 (c)	Remove file and printer sharing in their computers, especially when they have internet access via cable modems, broadband connections or similar set-ups.	☐	☐	☐	☐
145.	11.0.4 (d)	Make regular backup of critical data.	☐	☐	☐	☐
146.	11.0.4 (e)	Consider the use of encryption technology to protect highly sensitive data.	☐	☐	☐	☐
147.	11.0.4 (f)	Log off the online session and turn off the computer when not in use.	☐	☐	☐	☐
148.	11.0.4 (g)	Do not install software or run programs of unknown origin.	☐	☐	☐	☐
149.	11.0.4 (h)	Delete junk or chain emails.	☐	☐	☐	☐
150.	11.0.4 (i)	Do not open email attachments from strangers.	☐	☐	☐	☐
151.	11.0.4 (j)	Do not disclose personal, financial or credit card information to little-known or suspect websites.	☐	☐	☐	☐
152.	11.0.4 (k)	Do not use a computer or a device which cannot be trusted.	☐	☐	☐	☐
153.	11.0.4 (l)	Do not use public or internet café computers to access online banking or perform financial transactions.	☐	☐	☐	☐
	Appendix A	**COUNTERING MAN-IN-THE-MIDDLE ATTACKS**				
	A.1	As part of the two-factor authentication infrastructure, financial institutions should consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in the middle attacks:				
154.	A.1 (a)	Each new payee is authorised by the customer based on an OTP from a second channel which also shows payee details or the customer's handwritten signature from a manual procedure which is verified by the financial institution.	☐	☐	☐	☐
155.	A.1 (b)	Each value transaction or an approved list of value transactions above a certain dollar threshold determined by the customer requires a new OTP. All payment and fund transfer transactions are encrypted at the application layer.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
156.	A.1 (c)	For challenge-based and time-based OTPs, the OTP time window does not exceed 100 seconds on either side of the server time.	☐	☐	☐	☐
157.	A.1 (d)	Digital signatures and key-based message authentication codes (KMAC) for payment or fund transfer transactions could be used for the detection of unauthorised modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him. This means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.	☐	☐	☐	☐
158.	A.1 (e)	The financial institution notifies the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.	☐	☐	☐	☐
159.	A.1 (f)	An online session is automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained.	☐	☐	☐	☐
160.	A.1 (g)	Security awareness is provided to internet banking customers such that customers are made aware of and shown how to react to SSL server certificate warnings. The customers should terminate a login session if a SSL certificate does not belong to the bank and a warning is given to this effect. Customers should inform the financial institution immediately after logging off.	☐	☐	☐	☐
	Appendix B	**SYSTEM SECURITY TESTING**				
	B.1	The following specifications are included in system security testing:				
161.	B.1 (a)	Tests are carried out on network systems to detect security loopholes or vulnerabilities that can be exploited to gain system entry.	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
162.	B.1 (b)	Tests are carried out to detect errors in business logic.	☐	☐	☐	☐
163.	B.1 (c)	Authentication testing is performed to ensure that security requirements (credential expiry, revocation, reuse, etc.) are implemented correctly, and that the protection of security functions and cryptographic keys is robust.	☐	☐	☐	☐
164.	B.1 (d)	Tests are conducted to verify that the security access matrix works correctly in various permutations.	☐	☐	☐	☐
165.	B.1 (e)	Input data validation testing is performed.	☐	☐	☐	☐
	B.1 (e)	Proper data validation should include the following:				
166.	B.1 (e) (i)	Every input to the applications is validated.	☐	☐	☐	☐
167.	B.1 (e) (ii)	All forms of data (such as text boxes, select boxes and hidden fields) are checked.	☐	☐	☐	☐
168.	B.1 (e) (iii)	The handling of null and incorrect data input is verified.	☐	☐	☐	☐
169.	B.1 (e) (iv)	Content formatting is checked.	☐	☐	☐	☐
170.	B.1 (e) (v)	The maximum length for each input field is validated.	☐	☐	☐	☐
171.	B.1 (f)	Stringent tests on exception and error handling are performed to facilitate fail-safe processing under various error and exception conditions.	☐	☐	☐	☐
172.	B.1 (g)	Tests are performed to ensure secure session management.	☐	☐	☐	☐
	B.1 (g)	The following conditions should be specified:				
173.	B.1 (g) (i)	Sensitive information that is passed in the cookies is encrypted.	☐	☐	☐	☐
174.	B.1 (g) (ii)	The session identifier should be random and unique.	☐	☐	☐	☐
175.	B.1 (g) (iii)	The session should expire after a pre-defined length of time.	☐	☐	☐	☐
176.	B.1 (h)	Cryptography is employed to protect sensitive data. The implementation of cryptography is rigorously tested to cover all cryptographic functions (encryption, decryption, hashing, signing) and key management procedures (generation, distribution, installation, renewal, revocation and expiry).	☐	☐	☐	☐

Item	IBTRM Section	Guideline Description	Full Compliance	Partial Compliance*	Non-compliance*	NA
177.	B.1 (i)	Logging functionality is tested for correct implementation to avoid security defects as well as facilitate follow-up investigation and troubleshooting when a system incident occurs.	☐	☐	☐	☐
	B.1 (i)	The requirements and specifications below would apply:				
178.	B.1 (i) (i)	Sensitive data such as passwords and authentication credentials should not be logged in transaction or system activity files.	☐	☐	☐	☐
179.	B.1 (i) (ii)	The maximum data length for logging is pre-determined.	☐	☐	☐	☐
180.	B.1 (i) (iii)	Successful and unsuccessful authentication attempts are logged.	☐	☐	☐	☐
181.	B.1 (i) (iv)	Successful and unsuccessful authorisation events are logged.	☐	☐	☐	☐
182.	B.1 (j)	The performance and the stability of a system under erratic conditions, such as abnormal traffic rates or frequent reboots, are verified. Stress testing outside the stated limits of the systems is conducted to ensure that the application still works correctly albeit with degraded service levels.	☐	☐	☐	☐

B DESCRIPTION OF REMEDIAL ACTION

1. If full compliance has not been achieved for any of the items in Section A, please explain how and when remedial action will be made. The item number and the corresponding IBTRM Guidelines in Section A should be shown in the table below. Additional space should be added where necessary.

2. Please attach an organisational chart showing technology risk management and IT security responsibilities at the Board level down to operational and functional levels.

Item	**IBTRM Section**	**Description of Remedial Action for Partially-compliant and Non-compliant Items**

Item	IBTRM Section	Description of Remedial Action for Partially-compliant and Non-compliant Items