GUIDELINES ON

CONTROL OBJECTIVES AND PROCEDURES FOR OUTSOURCED SERVICE PROVIDERS

1 June 2017

Version 1.1

TABLE OF CONTENTS

VERSION HISTORY

VERSION	DESCRIPTION	DATE
1.0	Issuance of initial GUIDELINES ON CONTROL OBJECTIVES AND PROCEDURES FOR OUTSOURCED SERVICE PROVIDERS.	25 July 2015
1.1	Updated the GUIDELINES ON CONTROL OBJECTIVES AND PROCEDURES FOR OUTSOURCED SERVICE PROVIDERS based on the new MAS Guidelines on Outsourcing (issued on 27 July 2016) and industry feedback.	1 June 2017

INTRODUCTION

Outsourcing continues to be prevalent in today's business landscape. In outsourcing, Financial Institutions ("FIs") rely on the outsourced service providers to perform certain business functions. While outsourcing has proven to be effective; FIs should ensure that their service providers maintain the same level of governance, rigour and consistency as if the services were still managed by themselves.

Loss of customer information or confidential data, or disruptions to critical bank services may result in reputational risk impacts or regulatory breaches. Outsourcing risks must be managed to safeguard the FIs' operations and customers. The service can be outsourced, but the risk cannot.

To address this, the Association of Banks in Singapore ("ABS") has established these Guidelines on Control Objectives and Procedures for the FIs' Outsourced Service Providers ("OSPs") operating in Singapore. These Guidelines form the minimum/baseline controls that OSPs which wish to service the FIs should have in place. However, FIs with specific needs should continue to liaise with their OSPs on a bilateral basis to impose any additional specific requirements. Where the OSPs deem necessary, OSPs are encouraged to supplement these minimum/baseline controls with specific controls as they relate to the security, availability, processing integrity and/or confidentiality of their service. Examples of such controls are included in Section III 'Service Controls', item (b) 'Authorising and Processing Transactions'.

By complying with the Guidelines, OSPs can assure the FIs that their controls are designed and operating effectively to meet the control objectives that are relevant in the provision of the outsourced services.

SCOPE

These Guidelines should be adopted by all OSPs in Singapore that undertake material outsourcing arrangements for FIs in Singapore.

AUDITS AND INSPECTIONS

I. ENGAGEMENT OF EXTERNAL AUDITOR

The OSP should engage a qualified auditor to perform audits in accordance with these Guidelines on the services rendered to the FIs.

In the event that an OSP decides to change the external auditor or decides to appoint a different external auditor for validation of remediation activities (refer to section "V. REPORTING AND HANDLING OF CONTROL FAILURE / QUALIFICATION OF CONTROL OBJECTIVES"), the OSP must ensure that there is a proper hand-over from the outgoing auditor to the incoming auditor to ensure that the interests of the FIs remain protected.

II. CRITERIA FOR QUALIFICATION EXTERNAL AUDITOR

The appointed external auditor should demonstrate a sound understanding of outsourcing risks pertinent to the banking industry as well as fulfil the following criteria:

1. The audit firm must have audited at least 2 commercial banks operating in Singapore in the last 5 years; and
2. The engagement partner, who signs off the Audit Report, must have audited at least 2 commercial banks operating in Singapore in the last 5 years.

III. FREQUENCY OF AUDIT

The audit should be performed once every 12 months. To be useful to FIs relying on the report, the samples selected for testing the operating effectiveness of controls should cover the entire period since the previous audit, with a minimum testing period of 6 months. If the period is less than 6 months, the reasons for the shorter period should be provided in the report.

IV. AUDIT REPORT

The appointed external auditor should issue the audit report in the format stated in the Outsourced Service Provider Audit Report ("OSPAR") template. The OSP must furnish a copy of its audit report to its FI clients.

V. REPORTING AND HANDLING OF CONTROL FAILURE / QUALIFICATION OF CONTROL OBJECTIVES

Where the auditor identifies a failure in the design and/or operating effectiveness of a control activity in relation to a control objective, the auditor should assess the potential impact of the failure on the services provided to the FIs. The auditor should be guided by the relevant auditing standards which specify the procedures for qualification of a control objective.

OSPs should notify the FIs of significant issues and concerns, and the remediation plans no later than the OSPAR release date. However, OSPs should notify the FIs immediately if the issues could potentially lead to a prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the FI's customer information.

The OSP should develop remediation plans to address the issues identified by the audit. If the issues require an extended time period to correct, the OSP should identify short term measures to mitigate the risks. The remediation measures should be validated by the auditor or other competent independent party.

VI. RIGHTS OF FIs and MAS

The MAS and FIs retain the right to audit the OSP, as well as the OSP's sub-contractors.

I. ENTITY LEVEL CONTROLS

Entity level controls are internal controls to ensure that the OSP'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) Information Security Policies.
(f) Human Resource Policies and Practices.
(g) 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 OSP, influencing the control consciousness of its people. It is the foundation for all the other components of internal control, providing discipline and structure. Aspects of the OSP's control environment may affect the services provided to the FIs. For example, the OSP's hiring and training practices may affect the quality and ability of the OSP's personnel to provide services to the FIs.

The control environment includes the following elements:

i. Communication and enforcement of integrity and ethical values.
ii. Commitment to competence.
iii. Management's philosophy and operating style.
iv. Organisational structure as well as assignment of authority and responsibility.

(b) Risk Assessment

The OSP's risk assessment process may affect the services provided to FIs. The following is a list of risk assessment factors and examples of how they might relate to the OSP:

i. Changes in the operating environment – Prior to introducing changes to the operating environment (including technology components), OSP should assess the materiality of the changes to the FI's outsourced arrangement using a change management framework and should notify and/or seek approval from FIs. This is applicable to sub-contractors used by the OSP.

ii. New personnel – New personnel without adequate training and / or background screening may increase the risk that controls may not be performed effectively.

iii. New or revamped information systems – The OSP may incorporate new functions into its systems or implement new systems that could affect the FIs' outsourced arrangements.

iv. Rapid growth – If the OSP gain a substantial number of new customers, the operating effectiveness of certain controls could be affected.

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

vi. 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 OSP.

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

viii. Expanded foreign operations – The OSP that use personnel in foreign locations may have difficulties responding to changes in the FI's requirements.

ix. Environmental scan – The OSP should scan for emerging threats that may impact its operations or services (e.g. cyber threats, geographic risks, etc.).

(c) Information and Communication

Adequate information and effective communication are essential to the proper functioning of internal control. The OSP's information and communication component of internal control include the following:

i. The information system must be documented with procedures for initiating, authorising, recording, processing and reporting FIs' transactions for proper accountability.

ii. Communication involves how the OSP communicates its roles and responsibilities, significant matters relating to the services provided to the FIs, including communication within its organisation, with the FIs and regulatory authorities. This may include the OSP's communication to its staff on how its activities impact the FIs, escalation procedures for reporting exceptions within the OSP and to the FIs, and seeking FIs' approval prior to any sub-contracting.

(d) Monitoring

Many aspects of monitoring may be relevant to the services provided to FIs. For example, the OSP may employ internal auditors or other personnel to evaluate the effectiveness of controls over time, either by ongoing activities, periodic evaluations, or combinations of the two. OSPs should have processes in place to bring significant issues and concerns identified through such evaluation to the OSPs' senior management and additionally, if impacting the services provided, e.g. adverse developments, to the FIs.

The OSP's monitoring of its sub-contractors' activities that affect the services provided to the FIs is another example of monitoring. This form of monitoring may be accomplished through visiting the sub-contractors' organisation, obtaining and reading reports containing detailed description of the sub-contractors' controls, or conducting an independent assessment of whether the controls in place are suitably designed and operating effectively throughout the specified period. Copies of any such reports and findings made on the OSP and/or its sub-contractors, in relation to the outsourcing arrangement, must be provided to the FIs. Results should be discussed as part of ongoing service discussions.

Monitoring external communications, such as customer complaints and communications from regulators, would be important and results of such monitoring should be provided to FIs. Often, these monitoring activities are included as control activities for achieving a specific control objective.

(e) Information Security Policies

Information Security ("IS") policies and procedures are established, documented and reviewed at least every 12 months or as and when there are changes. IS policies and procedures should state the person(s) responsible for information security management.

These documents are reviewed and approved by management. Specific security controls for systems and networks are defined to protect the confidentiality, integrity and availability of systems and data. Any identified deviations are documented, tracked and remediated. Deviations which impact the services rendered should be communicated to the FIs immediately.

An information security awareness training programme should be established. The training programme should be conducted for OSP's staff, sub-contractors and vendors who have access to IT resources and systems regularly to refresh their knowledge.

(f) Human Resource Policies and Procedures

The OSP should establish standards for workplace conduct, implement candidate background screening procedures, and conduct enforcement procedures to enable it to meet its commitments and requirements as they relate to the ABS controls objectives and MAS Guidelines on Outsourcing.

OSP's staff (including sub-contractor staff) involved in delivering the outsourced services to FIs should understand their responsibilities and be suitable for the roles for which they are employed. The OSP should ensure that individuals considered for employment are adequately screened for experience, professional capabilities, honesty and integrity. Screening should include background checks to assess character, integrity and track record. The following are non-exhaustive examples of OSP staff screening requirements:

i. Subject of any past or current proceedings of a disciplinary or criminal nature;

ii. Convicted of any offence (in particular, that associated with a finding of fraud, misrepresentation or dishonesty);

iii. Accepted civil liability for fraud or misrepresentation; and

iv. Are financially sound.

The listed examples are non-exhaustive and do not necessarily preclude an individual from taking on a particular role within an OSP organisation as screening procedures should be commensurate with the role that the employees are performing.

Contracts with OSP's staff (including sub-contractor staff) should specify their responsibilities for maintaining confidentiality of customer information in accordance with s47 of the Banking Act (Chapter 19) on Banking Secrecy.

(g) Practices related to Sub-Contracting

FIs expect sub-contractors of OSPs to be managed with the same rigour as the OSPs themselves. Thus, OSP should require and ensure that their sub-contractors adhere to the requirements of these Guidelines. OSPs in managing sub-contractors should:

i. Obtain approvals from the FIs before engaging sub-contractors.

ii. Be able to demonstrate due diligence and risk assessment of the sub-contractors.

iii. Implement processes to inform and consult the FIs on material changes to the sub-contractors' operating environment.

iv. Conduct a review of its sub-contractors every 12 months.

v. Monitor the performance and risk management practices of the sub-contractors.

Due diligence and risk assessments of sub-contractors should involve evaluation of relevant information as specified in section 5.4.3 of the MAS Guidelines on Outsourcing, e.g. experience and capability of the sub-contractor to implement and support the outsourcing arrangement over the contracted period and financial strength and resources of the sub-contractors. Sub-contracting within the OSP's group should be subjected to similar due diligence.

OSPs should take note of the requirements of section 5.10 of the MAS Guidelines on Outsourcing when outsourcing to a sub-contractor that is operating outside Singapore.

II. GENERAL INFORMATION TECHNOLOGY ("IT") CONTROLS

(a) Logical Security

These controls provide reasonable assurance that logical access to programmes, 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.	Logical access requirements to IT systems, i.e. programmes, data and operating system software are defined, as agreed with FIs. Logical access requirements include the following, where applicable: (a) Definition of the "least privilege" required by each user group, including privileged users, to: • Production and backup data. • Sensitive information, including FI's customer information. • Commands, services, e.g. application, web and network services, and sensitive files, e.g. system logs and audit trails. • Non-production systems, e.g. UAT and DR environments. (b) Password management rules and parameters (e.g. password complexity, lockout settings, password history) in line with the FI's password management requirements; and (c) Procedures to manage privileged / system administration accounts (including emergency usage).
	ii.	Access to IT systems software is only granted based on a documented and approved request, and on a need-to-use basis.

iii. All users' access to IT systems, including sub-contractors' access, are reviewed periodically in accordance with a frequency agreed with the FIs.

iv. Access to IT systems are revoked or disabled promptly in accordance with the SLA when the access is no longer required.

v. Strong physical or logical controls are used to identify, segregate and protect individual FI's information. Such controls survive the tenure of the contract.

vi. Procedures are established to securely destroy or remove the FI's data as per the agreed retention and destruction policies as well as well upon termination. This requirement also applies to backup data.

vii. Industry-accepted cryptography standards agreed with FIs are deployed to protect FIs' customer information and other sensitive data in accordance with the MAS Technology Risk Management ("TRM") Guidelines:

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

(b) Transmitted between terminals and hosts, through networks 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 key are communicated to the intended recipient via a separate channel, e.g. via telephone call.

	viii.	Password management controls for applications/systems are periodically reviewed with FIs according to the agreed information security requirements / standards.
	ix.	Users with elevated access privileges are subjected to strict controls such as: (a) Split-password control, never-alone principle, two-factor authentication ("2FA"), etc. (b) Passwords are changed regularly and access is removed when no longer required. (c) Timely review of privileged users' activities.

(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.	Access to data centre/controlled areas is restricted: (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 mechanism may include 'anti-passback' feature to prevent 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.

ii. All access points, including windows, to controlled areas are fitted with audible intruder alarms that are monitored by security personnel. Doors are fitted with door-ajar alarms. The alarm system is tested regularly and the test documentation is retained.

iii. 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. Access rights to data centre/controlled areas are reviewed at a frequency agreed with FIs. Access violations are monitored, followed up and reported to FIs in accordance with the SLA.

v. 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.

vi. An appropriate risk assessment, such as a Threat and Vulnerability Risk Assessment ("TVRA") is performed for the data centre, server room and any other controlled areas housing FIs' customer or sensitive information (e.g. hardcopy FIs' customer information, FIs' procedural documents, contractual documentation, etc.).

If an OSP shares premises with other organisations, a risk-based TVRA or similar appropriate risk assessment is performed to assess the relevant control areas, e.g. data centre, server room and/or any other relevant physical premises. The scope of the assessment is agreed with the FIs and include, at a minimum, the physical perimeter and surrounding environment of the premises. The assessment includes various threat scenarios such as theft, explosives, arson and internal sabotage.

Gaps identified by the risk assessment are remediated timely.

			Note: Before FIs procure DC services from the OSP, FIs will ensure that all identified risks are adequately addressed. Subsequent assessments may also be conducted at a frequency commensurate with the level and type of risk to which *a DC is exposed as well as the criticality of the DC to the FIs. FIs will obtain and assess the TVRA report from the OSP on the DC facility.*
2.	**Data Centre/Controlled areas are resilient to protect IT assets.**	i.	The following environmental control feature 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 sensors (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 extinguishers
		ii.	Environment 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.	A formal change management process is established, documented and reviewed at least every 12 months or when there are changes to the process. The change management process is reviewed and approved by management. Segregation of change management duties is also specified.
	ii.	The following controls exist for changes applied to the 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. (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.

(g) System logging is enabled to record activities that are performed during the migration process.

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

(i) Disaster recovery environment versions are updated timely after production migration is successfully completed.

iii. Change risk categories are used to determine approval requirements in accordance with the defined change management process. Appropriate escalation levels and approvals are established and documented in the Change Authority matrix for changes.

iv. 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.

v. Source code reviews are conducted for higher risk systems and applications changes to identify security vulnerabilities and deficiencies, coding errors, defects and malicious codes before these changes are implemented.

(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.	A formal documented incident management process exists. The process is reviewed at least every 12 months, or when there are changes to the process, and updated and approved accordingly.
	ii.	Roles and responsibilities of staff involved in the incident management process are clearly documented in the procedures, including recording, analysing, remediating and monitoring of problem and incidents.
	iii.	Clear escalation and resolution protocols and timelines are documented. FIs are notified of incidents and the notifications are tracked and reported to FIs in accordance with the SLA.
	iv.	Incidents are recorded and tracked with the following information: (a) Severity. (b) Client/FI information. (c) Date and time of incident/problem. (d) Description 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)	Post-mortem on incidents that includes root-cause analysis.
	v.	Problems attributing to the incidents are analysed to address root cause and to prevent recurrence. Trend analysis of past incidents is performed to facilitate the identification and prevention of similar problems.

(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 policies and procedures are documented. The policies and procedures are reviewed and updated at least every 12 months or whenever there are changes impacting backup procedures.
	ii.	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.
	iii.	System level backups are securely stored at off-site storage facilities.
	iv.	Backup logs associated with system level backups are generated and remedial action is taken for unsuccessful backups.
	v.	Data backed up to external media such as tapes are encrypted using industry-standard cryptography.
	vi.	Tape (or other media) tracking/management system is used to manage the physical location of backup

tapes. This includes a full inventory of all tapes on and off site, tapes retention periods and tapes due for rotation.

vii. Tape (or other media) inventory checks are performed at least every 12 months such that all tapes are accounted for.

viii. Backup tapes (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

Disaster Recovery ("DR") refers to disaster recovery capabilities as a whole for services rendered and not specific to information technology ("IT") disaster recovery only.

i. A DR strategy and business continuity plan are established and maintained based on the business, operational and information technology needs of the FIs. Operational considerations include geographical requirements and on-site / 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 shall accommodate the capacity for recovery as agreed with FIs

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

ii. DR strategy and business continuity plan, including activation and escalation process are reviewed, updated and tested at least every 12 months. In consultation with FIs this 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.

iii. DR exercises (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.

iv. Recovery plans 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 OSP management to ensure alignment with FIs' expectations and applicable MAS regulation (e.g. MAS Outsourcing, Business Continuity Management ("BCM") and MAS TRM). Defined RTO, RPO and resumption operating capacities should be validated by management during the annual test of the DR strategy and BCP.

v. Redundancy plans for single points of failure which can bring down the entire system or network are developed and implemented.

(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.	Specific security controls for systems and networks are defined to protect the confidentiality, integrity and availability of systems and data. These controls are documented, reviewed and updated at least every 12 months.
	ii.	Security baseline standards (i.e. system security baseline settings and configuration rules) are defined for the various middleware, operating system, databases and network devices to ensure consistent application of security configurations and harden systems to the required level of protection. Regular enforcement checks against baseline standards are carried out to monitor compliance.
	iii.	Procedures are implemented to ensure that anti-virus/anti-malware software are installed and updated regularly. Detected threats are quarantined and removed appropriately.
	iv.	Patch management procedures are established and include maintaining 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 prioritising security patches to address known vulnerabilities. The timeframe for implementing patches on critical system and security vulnerability is agreed with the FIs.
	v.	Deviations from security policies/standards are documented and mitigating controls are implemented to reduce the risks. Deviations are tracked and remediated appropriately. Outstanding deviations are reviewed at least every 12 months. Deviations which impact the services rendered to the FIs should be reported to the FIs.

	vi.	File integrity checks are in place to detect unauthorised changes (e.g. databases, files, programmes and system configuration).
	vii.	Network security controls are deployed to protect the internal network. 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.
	viii.	Rules for network security devices are backed up and reviewed regularly for appropriateness and relevance.
	ix.	Security system events are logged, retained and monitored.

(g) Security Incident Response

These controls provide reasonable assurance that appropriate personnel within the OSP are contacted and immediate action is taken in response to a security incident. Requirements in the relevant notices such as the MAS TRM Notice are adhered to.

1.	**Appropriate personnel are contacted and immediate action taken in response to a security incident**	i. An Incident Response Plan that establishes and documents specific procedures that govern responses to security incidents (physical or system security) is documented. The roles and responsibilities of staff involved in responding to security incidents are clearly defined. ii. Security response procedures are reviewed and tested every 12 months and the Incident Response Plan is updated where necessary. iii. 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.

(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.	Vulnerability assessment ("VA") policies and procedures are documented and reviewed at least every 12 months or whenever there are changes.
	ii.	The OSP continually monitors emergent security exploits, and perform regular VAs of its IT environment against common and emergent internal and external security threats. The frequency of the VAs is agreed with FIs based on the FIs' risk assessments.
2. Penetration Testing	i.	Penetration testing ("PT") policies and procedures are documented and reviewed at least every 12 months or whenever there are changes.
	ii.	PTs are performed to simulate attacks of the IT systems. 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.
	ii.	Procedures for fixing issues identified by VAs and PTs are documented and reviewed at least every 12 months or whenever there are changes.

(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.	Technology Refresh Management plan and procedures are documented and reviewed at least every 12 months or whenever there are changes.
	ii.	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.
	iii.	The OSP actively manages its IT systems and software supporting FIs so that outdated and unsupported systems which significantly increase exposure to security risks are replaced timely. Close attention is paid to products' end-of-support ("EOS") dates.
	iv.	The OSP should inform FIs on identification of any systems to be decommissioned or replaced.
	v.	When decommissioning IT systems, the OSP should ensure that the FI's information is securely destroyed / purged from the system to prevent data leakage. Evidence of the secure destruction / purge should be provided to the FI.
	vi.	A risk assessment of systems approaching EOS is conducted to assess the risks of continued usage and establish effective risk mitigation controls where necessary.

III. SERVICE CONTROLS

(a) Setting-up of New Clients/Processes

These controls provide reasonable assurance that client contracting procedures are defined and monitored, and client processes are set up and administered in accordance with client agreements/instructions.

1. OSP contracting procedures are defined and monitored	i.	In considering, amending, renegotiating or renewing an outsourcing arrangement, the OSP provides accurate and timely information to FIs so that they can perform an appropriate due diligence to assess the risks associated with the outsourcing arrangements. Information provided includes: (a) Experience and capability to implement and support the outsourcing arrangements over the contracted period. (b) Financial strength and resources. (c) Corporate governance, business reputation and culture, compliance, and pending or potential litigation. (d) Security and internal controls, audit coverage, reporting and monitoring environment. (e) Risk management frameworks and capabilities, including in technology risk management and business continuity management in respect of the outsourcing arrangements. (f) Disaster recovery arrangements and disaster recovery track records. (g) Reliance on and success in dealing with sub-contractors. (h) Insurance coverage.

(i) External factors (such as the political, economic, social and legal environment of the jurisdiction in which the OSP operates, and other events) that may impact service performance.

(j) Ability to comply with applicable laws and regulations and track records in relation to its compliance with applicable laws and regulations.

ii. Contractual terms and conditions governing relationships, functions, obligations (including minimal insurance coverage of assets), responsibilities, rights and expectations of all contracting parties are set out fully in written agreements, e.g. Outsourcing Agreement with Service Level Agreements ("SLA").

iii. The outsourcing agreements between the OSP and FIs have provisions to address the following:

(a) The scope of the outsourcing arrangement.

(b) The performance, operational, internal control and risk management standards.

(c) Confidentiality and security (i.e. roles and responsibilities, liability for losses in the event of breach of security/confidentiality and access to and disclosure of), including a written undertaking to protect, isolate and maintain the confidentiality of FIs information and other sensitive data.

(d) Business resumption and contingency requirements. The OSP is required to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

(e) Processes and procedures to monitor performance, operational, internal control and risk management standards.

(f) Notification of adverse developments or breaches of legal and regulatory requirements. The outsourcing agreement should specify the type of events and the circumstances under which the

OSPs should report such events to the FIs.

(g) Dispute resolution (i.e. protocol for resolving disputes and continuation of contracted services during disputes as well as the jurisdiction and rules under which disputes are to be settled). The outsourcing agreement should specify the resolution process, events of default, and the indemnities, remedies and recourse of the respective parties.

(h) Default termination and early exit by all parties.

Note: FIs have the right to terminate the outsourcing arrangement in the event of default, ownership change, insolvency, breach of security or confidentiality, or serious deterioration of service quality.

(i) Sub-contracting (i.e. restrictions on sub-contracting, and clauses governing confidentiality of data).

(j) FIs' contractual rights to remove or destroy data stored at the OSP's systems and backups in the event of contract termination.

(k) Ownership and access (i.e. ownership of assets generated, purchased or acquired during the outsourcing arrangements and access to those assets).

(l) Provisions that allow the FIs to conduct audits on the OSP and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the FIs; and to obtain copies of any report and findings made on the OSP and its sub-contractors, in relation to the outsourcing arrangements and to allow such copies of any report or finding to be submitted to the Monetary Authority of Singapore ("MAS").

(m) Provisions that allow the MAS, or any agent appointed by the MAS, where necessary or expedient, to exercise the contractual rights of the FIs to access and inspect the OSP and its sub-contractors, to obtain records and documents of transactions, and information given to the OSP, stored at or

processed by the OSP and its sub-contractors, and the right to access and obtain any report and finding made on the OSP and its sub-contractors.

(n) Provisions for the OSP to comply with FIs' security policies, procedures and controls to protect the confidentiality and security of the FIs' sensitive or confidential information, such as customer data, computer files, records, object programmes and source codes.

(o) Provisions for the OSP to implement security policies, procedures and controls that are at least as stringent as the FIs'.

(p) Provisions to ensure that an audit is completed for any new application/system before implementation that will address the FIs' information asset protection interests. The audit should at least cover areas like system development and implementation life cycle, the relevant documentation supporting each cycle phase, business user (including client where applicable) involvement and sign-off obtained on testing and penetration testing outcomes for application/ system and compliance with pre-agreed security policies with FIs.

(q) Provisions for sub-contracting of material outsourcing arrangements to be subjected to prior approval of the FIs.

(r) Applicable laws, i.e. choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes under the laws of a specific jurisdiction.

iv. In sub-contracting arrangements where the sub-contractors are providing services to support the OSP's outsourcing arrangement with the FI, the contractual terms in the sub-contracting arrangements should align with the OSP's contract with FIs.

2. OSP's processes are set up and administered in accordance with FIs agreements/instructions.	i.	Implemented process control activities are agreed with the FIs. The types of these controls are appropriate for the nature and materiality of the outsourcing arrangements.
	ii.	Operating procedures are documented, reviewed and updated at least every 12 months and made available to appropriate personnel.

(b) Authorising and Processing Transactions

These controls provide reasonable assurance that services of the OSP are authorised, recorded and subjected to internal checks to ensure completeness, accuracy and validity on a timely basis. Services are processed in stages by independent parties such that there is segregation of duties from inception to completion.

1. Services and related processes are authorised and recorded completely, accurately and on a timely basis.	i.	Services provided to the FIs and related automated and manual processes, including controls, are set up and administered in accordance with mutually agreed instructions between OSP and FI. Such agreement might include standard operating procedures ("SOP") or other types of instructions.
	ii.	Service procedures are documented, kept current and made available to appropriate personnel.
2. Services are subjected to internal checks to reduce the likelihood of errors.	i.	All services are recorded and checked against the FIs' specifications as defined in documented procedures. Errors or omissions are rectified promptly. All breaches and incidents (IT and non-IT) are tracked and escalated as per the SLA. Root cause analysis is conducted and, where appropriate, remedial actions are implemented to prevent recurrence.
	ii.	Error prevention and detection controls, e.g. reconciliations and "maker-checker" reviews, and error correction mechanisms are in place for key processes.
	iii.	Management Information reports are generated as per the agreed procedure to report on the status of tasks performed. Key performance indicators ("KPIs") are monitored as per the agreed procedures.
3. Services are processed in stages by independent	i.	Appropriate segregation of duties is implemented for transaction processing through logical and/or physical access controls.

	parties such that there is segregation of duties from inception to completion	ii. Access to record, authority to post and authorise transactions or services is restricted. Only authorised users have access to update customer service records.
4.	**Sample Controls for Data Entry Services** **Data entry procedures are performed in an accurate and timely manner.**	*Note: The following controls apply to data entry service providers only. Add this section if it is relevant to the service provided to the FIs.* i. Input forms are stamped with the date/time of receipt. ii. Input forms are batched and batch totals, e.g. number of forms are calculated and logged. iii. Batch totals are re-calculated upon data entry and reconciled with the log. Discrepancies are investigated and remediated. iv. Processed input forms are clearly marked to prevent re-input. v. Keyed data are verified against the original input forms to verify accuracy of data entry. vi. The identities of the maker and checker are recorded for accountability.
5.	**Sample Controls for Debt Collection Services** **Collections and monies received are posted to customer accounts in an accurate and timely**	*Note: The following controls apply to debt collection service providers only. Add this section if it is relevant to the service provided to the FIs.* i. Debt collection procedures are documented to guide personnel in the debt collection process. ii. Debt collection instructions are scanned into a document imaging application for archiving and retrieval.

	manner.	iii. The outstanding amounts in debt collection instructions are recorded and reconciled to the collected amounts before posting to the FIs' accounts. iv. The debt collection report is reviewed by the checker before the posting is approved. v. The identities of the maker and checker are recorded for accountability.
6.	**Sample Controls for Physical and Electronic Statement Printing Services** **Customer Statements are printed accurately and sent timely to FIs' customers.**	*Note: The following controls apply to physical and electronic statement printing service providers only. Add this section if it is relevant to the service provided to the FIs.* i. Statement printing procedures are documented to guide personnel in the statement printing process. ii. A statement schedule outlines when statements are required to be printed and mailed for each customer. iii. System reports with batch and hash totals are reconciled to ensure the completeness and accuracy of printed statements. iv. The identities of the checker and verifier of system reconciliation reports are recorded for accountability.

(c) Maintaining Records

These controls provide reasonable assurance that the OSP classifies data according to sensitivity, which determines protection requirements, access rights and restrictions, and retention and destruction requirements.

1. Data are classified according to sensitivity, which determines protection requirements, access rights and restrictions, and the retention and destruction requirements.	i.	Policies for data classification, retention and destruction are implemented. Retention is as required by local law (governing the FIs) or as required by the FIs.
	ii.	Data held with the OSP (both in physical and electronic forms) are stored in appropriate media where the level of backups is determined based on the classification of data. For information/records held in electronic storage media (including cloud based storage services), the OSP should ensure that appropriate levels of data/record segregation exist to prevent co-mingling of data. Logical segregation is an acceptable form of control to segregate customer information held electronically.
	iii.	Procedures on retention of information and data should be implemented. These procedures should clearly state retention guidelines based on the classification of information/data, applicable laws and agreed with the FIs.
	iv.	Procedures on destruction of information and data by the OSP should be implemented. These procedures should clearly state the secured destruction process based on the classification of information held. The procedures should be agreed with the FIs.
	v.	For terminated arrangements, the OSP should provide the FIs with relevant evidence that demonstrates that all forms of data/records/information (both electronic and physical) held by the OSP have been promptly removed or deleted, destroyed or rendered unusable.

(d) Safeguarding Assets

These controls provide reasonable assurance that physical assets held by the OSP are safeguarded from loss, misappropriation and unauthorised access.

1. Physical assets are safeguarded from loss, misappropriation and unauthorised access.	i.	Physical access to the operational OSP's office/facilities is restricted to authorised personnel at all times. Entrances to offices/facilities are secured via access control systems.
	ii.	Access to offices/facilities after normal business hours is pre-approved. Access is monitored 24 hours a day, 365 days a year.
	iii.	Physical assets (e.g. office equipment, storage media) are tagged and are assigned to custodians. Fixed assets counts are performed every 12 months and movements of assets are tracked and recorded.

(e) Service Reporting and Monitoring

These controls provide reasonable assurance that OSP's engagement with FIs and sub-contractors handling material outsourcing and FIs' customer information are properly managed.

1. Outsourced activities are properly managed and monitored.	i.	A governance framework supported by policies, procedures, guidelines and standards is established to manage and deliver its services.
	ii.	Due diligence and risk assessments of sub-contractors providing sub-contracted services are performed every 12 months. The due diligence includes the review of independent audit/expert assessment reports. The frequency of independent audit/expert assessment is agreed with the FIs.
	iii.	The governance procedures include regular training for employees and sub-contractors to ensure that employees and sub-contractors are aware of relevant regulatory requirements, e.g. anti-bribery and banking secrecy.
	iv.	SLAs with FIs and sub-contractors clearly define performance monitoring (e.g. performance measures and indicators such as system uptime and turnaround time for document processing) and reporting requirements. Achievements of agreed key performance indicators ("KPIs") and key risk indicators ("KRIs") are tracked and monitored.
	v.	Procedures are established for service recovery and reporting of lapses relating to the agreed service standards, including processes ensuring regular exchange of information and communication of critical issues.
	vi.	The OSP arranges regular meetings with FI clients and sub-contractors to discuss performance and service delivery outcomes. Corrective actions and plans are prepared and agreed with FI clients and sub-contractors to address performance and service delivery gaps.

DEFINTIONS

The following definitions are based on the definitions in the MAS Guidelines on Outsourcing:

"auditor" means – an external audit who is qualified to conduct OSPAR audits.

"customer" means – in relation to a bank, means a person (whether a natural person, legal person or legal arrangement):

(a) with whom the bank establishes or intends to establish business relations; or

(b) for whom the bank undertakes or intends to undertake any transaction without an account being opened.

"customer information" means – in the case of a bank, information that relates to its customers and these include customers' accounts, particulars, transaction details and dealings with the bank, but does not include any information that is public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred.

"commercial banks" means – banks in Singapore licensed by MAS under the Banking Act (Cap 19).

"material outsourcing arrangement" means – an outsourcing arrangement:

(a) which, in the event of a service failure or security breach, has the potential to either materially impact a bank's:
    (i) business operations, reputation or profitability; or
    (ii) ability to manage risk and comply with applicable laws and regulations,

or

(b) which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on a bank's customers.

“outsourcing agreement” means – a written agreement setting out the contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in an outsourcing arrangement.

“outsourcing arrangement” means – an arrangement in which a service provider provides the bank with a service that may currently or potentially be performed by the bank itself and which includes the following characteristics:

(a) the bank is dependent on the service on an ongoing basis; and

(b) the service is integral to the provision of a financial service by the bank or the service is provided to the market by the service provider in the name of the bank.

“service provider” or “outsourced service provider” means – any party which provides a service to a bank operating in Singapore.

“sub-contracting” means – an arrangement where a service provider which has an outsourcing arrangement with a bank, further outsources the services or part of the services covered under the outsourcing arrangement to another service provider.

“sub-contractor” means – a party to whom a service provider has further outsourced the services or part of the services covered under an outsourcing arrangement.