



GUIDELINES ON CONTROL OBJECTIVES & PROCEDURES FOR OUTSOURCED SERVICE PROVIDERS

26 June 2015

Version 1.0

THE ABS GUIDELINES ON CONTROL OBJECTIVES & PROCEDURES FOR OUTSOURCED SERVICE PROVIDERS

INTRODUCTION	3
SCOPE	4
AUDITS & INSPECTIONS	5
I. ENTITY LEVEL CONTROLS	6
II. GENERAL INFORMATION TECHNOLOGY (IT) CONTROLS	
(a) Logical Security	10
(b) Physical Security	11
(c) Change Management	13
(d) Incident Management	14
(e) Backup and Disaster Recovery	15
(f) Network & System Security and Monitoring	16
(g) Security Incident Response	18
(h) System Vulnerability Assessments	18
(i) Technology Refresh Management	19
III. SERVICE CONTROLS	
(a) Setting up of New Clients/Processes	20
(b) Authorising and Processing Transactions	22
(c) Maintaining Records	24
(d) Safeguarding Assets	25
(e) Service Reporting and Monitoring	25
DEFINITIONS	27

INTRODUCTION

Outsourcing continues to be prevalent in today's business landscape. In outsourcing, Financial Institutions (FIs) rely on the outsourced service providers (OSPs) to handle certain business functions. Outsourcing has proven to be effective; however FIs should ensure that their service providers maintain the same level of governance, rigour and consistency as themselves.

Loss of bank sensitive/customer data or loss of service capability may result in reputation risk or regulatory breaches. Outsourcing risks must be managed, to not adversely affect 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 this industry set of standards and controls 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 would continue liaise with their OSPs on a bilateral basis to impose any additional specific requirements.

Establishing a banking industry standard baseline will assure FIs' of the appropriate design of their OSP's internal controls and the effectiveness of those controls.

SCOPE

These Guidelines should be adopted by all Outsourced Service Providers (OSPs) in Singapore that undertake material outsourcing arrangements for FIs in Singapore or involve FIs' customer information. These Guidelines also applies to the OSP's subcontractors that provide the services or part of the services covered under the outsourcing arrangement with the FIs.

AUDITS AND INSPECTIONS

I. ENGAGEMENT OF EXTERNAL AUDITOR

The OSP needs to engage an external auditor to perform audits against these Guidelines on its services rendered to the FIs.

To this effect, the FI and MAS reserve the rights to audit the OSP (and its sub-contractors directly) and also on any additional FI's specific requirement.

II. CRITERIA OF EXTERNAL AUDITOR

The appointed external auditor should demonstrate a sound understanding of outsourcing risks pertinent to the banking industry as well as fulfilling 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 and the sampling data covers a period of 12 months.

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. RIGHTS OF FIs and MAS

FIs and MAS reserve the right to audit the OSP, as well as the OSP's sub-contractors, where they deem fit.

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) Information Security Policies
- e) Monitoring
- f) Information Security Policies
- g) Other HR and Sub-contracting Specific Controls

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
- v. Assignment of authority and responsibility
- vi. Human resource policies and practices

(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 - If the OSP provide services to FIs, a change in regulations may necessitate a revision to existing processes which may require additional or revised controls
- ii. New personnel - New personnel may increase the risk of controls not performed effectively
- iii. New or revamped information systems – the OSP may incorporate new functions into its systems that could affect the FIs
- 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 – the OSP may implement a new technology whereby its risks and impact to the FIs would need to be assessed
- vi. New business models, products, or activities - The diversion of resources to new activities from existing activities could affect 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 difficulty responding to changes in user requirements
- ix. Environmental scan – the OSP scans for emerging threats that may impact its operations or services (e.g. cyber threats, 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 process 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.

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 by visiting the sub-contractors' organisation, obtaining and reading a report containing detailed description of the sub-contractors' controls, or conducting an independent assessment of whether the controls are placed are suitably designed and operating effectively throughout the specified period.

Monitoring external communications, such as customer complaints and communications from regulators, generally would be relevant to the services 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 annually 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 to the FIs should be communicated immediately.

(f) Other HR & Sub-contracting Specific Controls

These controls should provide reasonable assurance that the management of the OSP provides oversight, ensures segregation of duties, and guides consistent implementation of security practices. Staff and sub-contractors of the OSP understand their responsibilities and are suitable for the roles for which they are considered.

- (i) OSP's staff and sub- contractors understand their responsibilities and are suitable for the roles for which they are considered
 - The OSP should ensure that individuals considered for employment are adequately screened for experience, professional capabilities, honesty and integrity. Screening should include background employment checks to assess character, integrity and track record.

- An information security awareness training program should be established. The training program should be conducted for OSP's staff, sub-contractors and vendors who have access to IT resources and systems.
- Contracts with staff and sub-contractors of the OSP should include non-disclosure clauses protecting confidentiality clauses which would apply staff and sub-contractors of the OSP working for its FI clients on and off premises.

(ii) The OSP's sub-contracting are properly managed and monitored

- Sub-contracting or use of sub-contractors is at the approval of the FIs and is subjected to and due diligence as agreed with the FIs.

II. GENERAL INFORMATION TECHNOLOGY (IT) CONTROLS

(a) Logical Security

These controls should provide reasonable assurance that logical access to programs, data, and operating system software is restricted to authorised personnel within the OSP and these applies to new and existing systems.

1. Logical access to programs, data, and operating system software is restricted to authorised personnel.

- (i) Information Security (IS) policies and procedures are established, documented and reviewed at least annually or when there are changes. IS policies and procedures are reviewed and approved by management. Logical access requirements to programs, data and operating system software are defined, as agreed with FIs.
- (ii) Access to systems and network devices is only granted based upon a documented and approved request and on a need basis.
- (iii) Access to production & backup data and sensitive information is granted on a 'least privilege' basis. Access to sensitive files (including system logs), commands and services are restricted and protected from manipulation on both production & non-production (consisting of FIs' customer information) systems.
- (iv) Access to systems (i.e. applications, operating systems, databases) and network devices by end users and IT Staff are reviewed periodically, frequency as agreed with FIs.
- (v) OSP's staff and sub-contractors off-boarding process includes revoking access from systems and network devices upon termination or when no longer required.
- (vi) Encryption, access privilege management, reconciliation and traceability IT security and control protocols are in place to protect the processing, transmission and storage of confidential information (including data at endpoint such as notebooks and mobile devices).
- (vii) Individual FI information is not merged with those of other OSP's clients. Appropriate technological measures are established to isolate, control and clearly identify FIs' data, information system assets, documents and records. 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.
- (viii) Industry-accepted cryptography standards agreed with FIs are deployed to protect FIs' information and

other sensitive data transmitted between terminals and hosts, including networks and in storage, as defined in the MAS Technology Risk Management (TRM) guidelines.

- (ix) Electronically transmitted FI's data to external parties (where permissible) is encrypted and industry-accepted cryptography standards is applied.
- (x) Industry-accepted password construction rules and parameters (e.g. complex password, lockout settings, password history) are implemented. The password controls for applications/systems are reviewed according to the agreed information security requirements/standards.
- (xi) Procedures are established to manage privilege system administration accounts (including emergency usage). Privileged access requested is documented and approved.
- (xii) Privileged access are reviewed at least annually and subjected to restricted controls such as dual control, never alone principle, two-factor authentication ("2FA"), etc. Passwords are changed regularly and access removed when no longer required. Changes made via privileged access must also be logged and monitored by an appropriate staff within the organisation.
- (xiii) Password should be stored in a secured manner (e.g. encrypted, access controlled etc).

(b) Physical Security

These controls demonstrate that the OSP restrict physical access to Data Centre/Controlled (DC) areas and have put in place environmental controls to protect the IT assets hosted at its data centres.

1. Physical access to Data Centre/Controlled areas is restricted to authorised individuals

- (i) Access to data centre/controlled areas is restricted:
 - a. Access is physically restricted (e.g. card access, biometric systems, ISO standard locks) to authorised personnel on a needs basis only. Access mechanism may include 'anti-passback' feature to prevent use of card access for multiple entries.
 - b. Access granted to employees, contractors and third parties to must be approved, documented and provided on a need to basis only.
 - c. All visitors must be registered and entry/exit recorded. Visitors should be issued with clear identification (e.g. an ID badge) and escorted by authorised personnel at all times.

- (ii) For controlled areas that have emergency exits, they must audible alarms and are monitored by security personnel. Periodic verification that of the alarms are functioning must be performed and documentation retained.
- (iii) Entry and exit to secure areas must have an audit trail (i.e. include CCTV footage / user id / name, date and time). Access rights to data centre/controlled areas are reviewed at least annually and as agreed with FI. Monitoring of access violations should be conducted on a monthly basis.
- (iv) Physical access right granted to employees, contractors and thirds parties are removed upon termination or when no longer required.
- (v) Threat and Vulnerability Risk Assessment (“TVRA”) should be performed for the data centre. The assessment criteria should be specified and should include at a minimum the data centre’s perimeter and surrounding environment and modelled on various scenarios of threats such as, theft and explosives.

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 that 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. Environmental controls are in place to protect the IT assets hosted at the data centre/ controlled areas.

- (i) The following physical and environmental control feature are minimally available at the data centre:

<ul style="list-style-type: none"> a. Systems and network equipment locked up in cabinet b. Uninterruptible power supply c. Air conditioning system d. Temperature and Humidity sensor e. Fire detector f. Smoke detector 	<ul style="list-style-type: none"> g. Water sprinkler (dry-piped or wet-piped) h. FM200 or other fire suppression system i. Raised floor j. CCTV k. Water leakage detection system l. Fire extinguisher
---	---
- (ii) The OSP should ensure that the perimeter of the DC, the DC building, facility, and equipment room are physically secured and monitored. The OSP should employ physical, human and procedural controls such as the use of security guards, card access systems, mantraps and bollards where appropriate
- (iii) The OSP should deploy security systems and surveillance tools, where appropriate, to monitor and record

activities that take place within the DC. The OSP should establish physical security measures to prevent unauthorised access to systems and equipment.

(c) Change Management

These controls provide reasonable assurance that the OSP documents and approves all changes to the system software and network components.

1. Changes to the system software and network components are documented and approved

- (i) A formal change management process is established, documented and reviewed at least annually or when there are changes to the process. The change management process is reviewed and approved by management. Segregation of change management duties should also be specified.
- (ii) The following controls exist for changes applied to the production environment:
 - a. Changes should be initiated through a formal change request process and classified according to different severity levels.
 - 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 should be performed.
 - d. All changes must be tested and appropriate approvals must be obtained prior to implementation. System Integration Testing ("SIT") and User Acceptance Testing ("UAT") test plans should be prepared and signed off in accordance to the established Change Authority Matrix.
 - e. Emergency change escalation protocols (e.g. by phone and email) and approval requirements should be established in the change approval matrix (includes internal and FI approvals) as agreed with FIs. Documented approval must still be 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 should be 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 must be anonymised. If UAT contains production data, the environment must be subject to appropriate production level controls.

(d) Incident Management

These controls provide reasonable assurance that the OSP resolves all system and network processing issues in a timely manner.

1. System and network processing issues (once input into the incident and problem management tool) are resolved in a timely manner

- (i) A formal documented incident management process exists. The process is reviewed at least annually or when there are changes to the process. The procedures documentation should be reviewed, updated and approved accordingly.
- (ii) Clear roles and responsibilities of staff involved in the incident management process should be outlined in the procedures, including recording, analysing, remediating and monitoring of problem and incidents.

Clear escalation and resolution protocols, including timelines should be documented. The need for incident notification to the FIs; and all these notifications should be tracked and reported to the FIs regularly.
- (iii) Incidents are recorded and tracked with the following information:
 - a. Severity
 - b. Client information
 - c. Date and time raised; description of incident or problem
 - d. Incident type
 - e. Application, systems and / or network component impacted
 - f. Escalation and approvals
 - g. Actions taken to resolve the incident or problem, including date and time action was taken
 - h. Post-mortem on incidents that includes root-cause analysis.
- (iv) Problems attributing to the occurrence of the incidents should be identified to address root cause and to prevent recurrence. Trend analysis of past incidents should be performed to facilitate the identification and

prevention of similar problems. Problems and incidents occurrence, root cause and resolution are tracked, monitored and reported to FIs.

(e) Backup and Disaster Recovery

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

1. Backups are performed and securely stored.

- (i) Backup and restoration processes have been implemented such that FIs' critical system information can be recovered. Backup procedures are formally documented based on the data backup and recovery requirements of FIs. These should include a data retention policy and procedures designed to meet business, statutory and regulatory requirements as agreed with FIs.
- (ii) System level backups are securely stored at off-site storage facilities.
- (iii) Backup logs associated with system level backups are generated and remedial action is taken for unsuccessful backups.
- (iv) Data backed up to external media such as tapes is encrypted and industry-accepted cryptography standards is applied.
- (v) 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.
- (vi) Tape (or other media) inventory checks are performed at least annually such that all tapes are accounted for.
- (vii) Backup tapes (or other media) are periodically tested to validate recovery capabilities.

2. Business and information systems recovery and continuity plans are

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

**documented, approved,
tested and maintained**

- (i) A DR strategy and business continuity plan is established and maintained based on business, operational and information technology needs of FI. Operational considerations include geographical requirements, on-site and off-site redundancy requirements.
 - a. Different scenarios such as major system outages, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary processing centre should be considered in a DR plan
 - b. DR facilities shall accommodate the capacity for recovery as agreed with FIs
- (ii) DR strategy and business continuity plan, including activation and escalation process is reviewed, updated and tested at least annually. In consultation with FIs this may be conducted more frequent depending on the changing technology conditions and operational requirements.
- (iii) DR exercise (i.e. testing plans and results) should be documented with action plans to resolve and retest exceptions.
- (iv) Recovery plans include established procedures to meet recovery time objectives (RTO) and recovery point objectives (RPO) of systems and data.
- (v) Redundancies for single point of failure which can bring down the entire network are considered and implemented.

(f) Network & Security and Monitoring

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

1. Systems and network controls are implemented based on client and business needs.

- (i) Information Security (IS) policies and procedures are established, documented and reviewed at least annually or when there are changes. IS policies and procedures 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.
- (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. Regular checks against baseline standards should be carried out to monitor compliance.
- (iii) Systems are 'hardened' (i.e. system security settings configured to the required level of protection) and

meet established baseline standards. This should include changing of all default passwords and protection against known vulnerabilities.

- (iv) Anti-virus/ malware detection programs are installed and operational. Procedures should include the timely detection and removal of known viruses/malware.
- (v) Patch management procedures include the monitoring, review, testing and timely application of vendor patches, prioritising security patches to address known vulnerabilities.
- (vi) Any identified deviations of security policy/standards are documented, tracked and remediated. Deviations which impact the services rendered to the FIs should be communicated.
- (vii) File integrity checks are in place to detect unauthorised changes (e.g. databases, files, programs and system configuration).
- (viii) Network security controls should be 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. Review for obsolete and duplicate firewall rules should be carried out at least half-yearly.
- (ix) Network surveillance and security monitoring procedures (e.g. network scanners, intrusion detectors and security alerts) are established.
- (x) Security system events are logged, retained and monitored.
- (xi) Two-factor authentication at login for all online financial systems and transaction signing for authorising high risk transactions is implemented.
- (xii) Internal Network Vulnerability Assessment ("VA") should be conducted quarterly to detect security vulnerabilities, including common web vulnerabilities. A combination of automated tools and manual techniques should be deployed. The scope, results (i.e. number of critical, high, medium and low risk findings) and remediation status (i.e. open, closed pending and extension, if any) are established and gaps are fully addressed in a timely manner.
- (xiii) Network and Application Penetration Testing ("PT") should be conducted annually, particularly for internet facing systems. The scope, results (i.e. number of critical, high, medium and low risk findings) and remediation status (i.e. open, closed pending and extension, if any) are established and gaps are

fully addressed in a timely manner.

- (xiv) Secured code review should be conducted before on-boarding new application. The scope, results (i.e. number of critical, high, medium and low risk findings) and remediation status (i.e. open, closed pending and extension, if any) are established and gaps are fully addressed.

(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) Incident Response Plan establishes and documents specific procedures that govern responses to security incidents (physical or system security). The roles and responsibilities of staff involved in responding to security incidents are clearly defined.
- (ii) Security response procedures are reviewed and tested annually and the Incident Response Plan 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 must be 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 the OSP performs regular system vulnerability assessment and penetration testing on environments with FIs' customer information.

1. Vulnerability Assessments

- (i) The OSP should continually monitor for emergent security exploits, and perform regular vulnerability assessments of its IT systems against common and emergent threats.

	(ii) As vulnerability assessments would only enable the OSP to identify security deficiencies in its IT systems at a particular point in time, OSP should institute a robust regime of prompt system patching and hardening, as well as adopt secure software coding practice.
2. Penetration Testing	<p>(i) The OSP should perform penetration testing at least annually on its internet facing systems.</p> <p>(ii) As penetration testing would only enable the OSP to identify security deficiencies in its IT systems at a particular point in time, the OSP should institute a robust regime of prompt system patching and hardening, as well as adopt secure software coding practice</p>
3. Timely Remediation	(i) The OSP should establish a process to effectively remediate issues identified from the vulnerability assessments and penetration testing a timely manner.

(i) Technology Refresh Management

These controls provide reasonable assurance that the OSP maintains up-to-date software and hardware components used in the production and disaster recovery environment.

- | | |
|--|---|
| 1. Timely refresh of IT systems and software of the production and disaster recovery supporting FIs | <p>(i) To facilitate the tracking of IT resources, the OSP should maintain an up-to-date inventory of software and hardware components used in the production and disaster recovery environment (supporting FIs) of which includes all relevant associated warranty and other supporting contracts related to the software and hardware components.</p> <p>(ii) The OSP should actively manage its IT systems and software (supporting FIs) so that outdated and unsupported systems which significantly increase its exposure to security risks are replaced on a timely basis. The OSP should pay close attention to the products' end-of-support ("EOS") date as it is common for vendors to cease the provision of patches, including those relating to security vulnerabilities that are uncovered after the products' EOS date.</p> <p>(iii) The OSP should establish a technology refresh plan to ensure that systems and software are replaced timely manner. OSP should conduct a risk assessment for systems approaching EOS dates to assess the risks of continued usage and establish effective risk mitigation controls where necessary.</p> |
|--|---|

III. SERVICE CONTROLS

(a) Setting-up of New Clients/Processes

These controls provide reasonable assurance that client contracting procedures within the OSP 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, renegotiating or renewing an outsourcing arrangement, the OSP is to provide 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 should include:
 - a. experience and competence to implement and support the outsourcing arrangements over the contracted period
 - b. financial strength and resources
 - c. corporate governance, business reputation and culture, compliance, complaints and outstanding or potential litigation
 - d. security and internal controls, audit coverage, reporting and monitoring environment
 - e. risk management framework and capabilities, including in technology risk management and business continuity management in respect of the outsourcing arrangements
 - f. arrangements for disaster recovery provisioning should be tracked and recorded
 - 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. track record and ability to comply 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. Service Level Agreements ("SLA").
- (iii) OSP's SLA with FIs should clearly include the following:
 - a. the scope of the outsourcing arrangements
 - b. the performance, operational, internal control and risk management standards
 - c. confidentiality and security (i.e. roles and responsibility, liability for losses in the event of breach of security/confidentiality), including a written undertaking to protect, isolate and

- d. 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. the process and procedures are in place to adequately monitor the controls in place
- f. notification of adverse developments or breach of legal and regulatory requirements
- g. dispute resolution (i.e. protocol for resolving disputes and continuation of contracted service during disputes as well as the jurisdiction and rules under which disputes are to be settled)
- h. default termination and early exit by all parties.
Note: FIs have right to terminate the SLA in the event of default, ownership change, insolvency, change of security or serious deterioration of service quality
- i. sub-contracting (i.e. restrictions on sub-contracting, and clauses governing confidentiality of data)
- j. FIs' contractual power 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 that indemnify and hold MAS, their officers, agents and employees harmless from any liability, loss or damage to the OSP and its sub-contractors arising out of any action taken to access and inspect the OSP or its sub-contractors pursuant to the outsourcing agreement
- o. 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 programs and source codes
- p. provisions for the OSP to implement of security policies, procedures and controls that are at least as stringent as the FIs'
- q. provisions to ensure that audit is completed for any new application/system prior implementation that will address FIs' information asset protection interests. The audit should

at least cover areas like system development & implementation life cycle adherence, the relevant documentation supporting each cycle phase, business user (including client where applicable) involvement and sign-off obtained on testing and penetration test outcome for application/ system and compliance with pre-agreed security policies with FIs.

- r. Provisions to sub-contracting of material outsourcing arrangements to be subjected to prior approval of the FIs and any applicable laws.

2. OSP's processes are set up and administered in accordance with FIs agreements/instructions.

- (i) Controls should be agreed by the FIs. The nature of these controls is appropriate for the nature and materiality of the outsourcing arrangements.
- (ii) Operating procedures are documented, kept current 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 the FIs' standard operating procedures (SOP) agreements/ 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 should be rectified promptly. All breaches and incidents are escalated as per the SLA.
- (ii) Controls for reconciliation, error prevention, and error correction mechanisms such as "Maker & Checker" should be in place for key processes.
- (iii) A Management Information report should be generated as per the agreed procedure which would identify

status of the task performed. KPIs need to be monitored as per the agreed procedure.

- (iv) For any exceptions noted, root cause analysis should be undertaken and where appropriate, remedial actions should be implemented to prevent recurrence.

3. **Services are processed in stages by independent parties such that there is segregation of duties from inception to completion**

- (i) Appropriate segregation of duties should be implemented for transaction processing as access should be based upon need to know.
- (ii) Access to record, post and authorise transactions or services are restricted. Only authorised users should have access to update customer service records.

4. **Sample Control for Data Entry Services**
Data entry procedures are performed in an accurate and timely manner.

- (i) The mail receiving clerk data stamps mails and client information as it is received. Each mail is logged in a tracking sheet.
- (ii) Mails and client information are sent to the relevant business department and recorded.
- (iii) Service Supervisor reviews and approves, and initials the data entry record as evidences of review.

5. **Sample Controls for Debt Collection Services**
Collections and monies received are posted to customer accounts in an accurate and timely manner

- (i) Documented collection processing procedures are in place to guide personnel in the debt collection process.
- (ii) Debt collection information is scanned into a document imaging application for archiving and retrieval of information.
- (iii) Debt collection information received from client is balanced in total to the check, wire or amount received.
- (iv) Debt collection information entered in the system is reviewed by the Service Supervisor before final posting.

6. **Sample Controls for Physical & Electronic Statement Printing Services**
Customer Statements are

- (i) Documented statement printing procedures are in place to guide plan administrators in statement printing process.
- (ii) A statement schedule outlines when statements are required to be printed and mailed for each customer.

**printed accurately and sent
timely to participants**

- (iii) Service Staff compare system reports to ensure that statement include the correct balance information.
- (iv) A log of the number of statements printed is created by the Service Staff and reviewed by the Service Supervisor to ensure that the correct number of statements was printed.

(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 & 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 to be stored in appropriate mediums where level of storage/ backups are determined based on the classification of data. For information/ records held in electronic storage media (including cloud based storage services), the OSP is to ensure appropriate levels of data/ record segregation exist to prevent co-mingling of data.

Procedures on Retention Management of Information/ Records/ Data are to be in place. These procedures should clearly state retention guidelines and they should be based on the classification of information held and applicable law.
- (iii) Procedures on Destruction of Information/Records/Data by the OSP are to be in place. These procedures should clearly state the destruction process and they should be based on the classification of information held.
- (iv) For terminated arrangements, the OSP is to provide the FIs with the relevant reports/documentation and evidence that demonstrates that all forms of data/records/information (both electronic and physical) held have been destroyed.

(d) Safeguarding Assets

These controls provide reasonable assurance that physically held assets of the OSP are safeguarded from loss, misappropriation and unauthorised use.

1. Physically held assets are safeguarded from loss, misappropriation and unauthorised use

- (i) Physical access to the operational OSP's office/facilities is restricted to authorised personnel. The entry to office/ facilities is through an automated proximity access card entry control system.
- (ii) A security system is authored to restrict access to the office/facilities after normal business hours. Access must be 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. Annual inventory of assets are performed. There should be procedures to manage any outdated systems and software.
- (iv) Proper tracking and verifying of asset movement should be in place.
- (v) Access rights are reviewed in accordance with relevant policies. Access rights for personnel that no longer require access must be removed immediately.

(e) Service Reporting and Monitoring.

These controls provide reasonable assurance that OSP's engagement with (1) its FI clients and (2) outsourced activities with its sub-contractors (that handles material outsourcing and FIs' customer information) are properly managed.

1. Outsourced activities are properly managed and monitored

- (i) Establish a structure and define ongoing governance process (including SLA and KPIs) to manage and deliver its services.
- (ii) Establish trainings to ensure its relevant staff and sub-contractors understand the FIs' requirements.
- (iii) The SLA with its FI clients and the sub-contractors clearly defines the performance monitoring (i.e.

includes performance measures and indicators such as system uptime) and reporting requirements. Achievements of key performance indicators (KPIs) and key risk indicators (KRIs) are tracked and monitored. The OSP arranges regular meetings with its FI clients and the sub-contractors to discuss its performance.

- (iv) Establish service recovery procedures and reporting of lapses relating to the agreed service standards, including processes ensuring regular exchange of information and communication of critical issues. The OSP meets its FI clients and sub-contractors to discuss issues periodically. Corrective actions and plans are prepared and agreed with FI clients and sub-contractors if performance does not meet expected service levels.
- (v) Conduct periodic review, at least on an annual basis on its sub-contractors. The review includes the internal risk management, management of information and deficiency or breach in the agreed service standards.

Due diligence on its sub-contractors is performed on an annual basis. This includes:

- a. reviewing of internal controls report, where available
 - b. confirming that the sub-contractors have appropriate IT security policies and procedures in place
 - c. reviewing of relevant aspects outlined under MAS Guidelines and Notices relevant to the outsourced services and as agreed with the FIs.
- (vi) Ensure that an independent control audit and/or expert assessment of its services are conducted at least every 12 months. The scope of the audits and/or expert assessment includes the security and control environment and incident management process. A copy of the audit report should be made known to the FIs as soon as it is available.

At least once every 12 months to engage an independent auditor to perform a control audit and provide the control audit report on its sub-contractors' compliance with the internal controls standards stipulated by the OSP and the respective FIs.

DEFINITIONS

In these Guidelines, unless the context otherwise requires:

“customer” means –

- (a) the customers of the financial institutions;
in relation to any trustee for a collective investment scheme authorised under section 286 of the Securities and Futures Act (Cap. 289), that is approved under that Act, the managers of and participants of the collective investment scheme;
- (b) in relation to an approved exchange, recognised market operator incorporated in Singapore, approved clearing house, recognised clearing house incorporated in Singapore, and licensed trade repository under the Securities and Futures Act, a person who may participate in one or more of the services provided by such entities; or
- (c) in relation to a licensed trust company under the Trust Companies Act (Cap. 336), a trust for which the trust company provides trust business services and includes the settlor and any beneficiary under the trust;

“customer information” means –

- (a) the information related to the customers of the financial institutions;
- (b) in relation to a licensed trust company, —protected information as defined in section 49 of the Trust Companies Act;
- (c) in relation to an approved exchange, recognised market operator incorporated in Singapore, approved clearing house and recognised clearing house incorporated in Singapore, —user information as defined in section 2 of the Securities and Futures Act;
- (d) in relation to a licensed trade repository, —user information and —transaction information as defined in section 2 of the Securities and Futures Act; or
- (e) in the case of any other financial institutions, information held by the financial institutions that relates to their customers and these include customers’ accounts, particulars, transaction details and dealings with the financial institutions;

“commercial banks” means – banks in Singapore licensed by MAS.

“financial institution” means - any bank licensed under the Banking Act (Cap. 19), any merchant bank approved under the Monetary Authority of Singapore Act (Cap 186), any finance company licensed under the Finance Companies Act (Cap. 108) or Capital Markets Services (CMS) licensee licensed under the Securities and Futures Act (Cap. 289) (SFA).

“material outsourcing arrangement” - refer to the definitions stated in the MAS Guidelines on Outsourcing.

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

“outsourcing arrangement” means - an arrangement in which an OSP provides the financial institution with a service that may currently or potentially be performed by the financial institution itself and which includes the following characteristics:

(a) the financial institution is dependent on the service on an ongoing basis but such service excludes services that involve the provision of a finished product (e.g. insurance policies); and

(b) the service is integral to the provision of a financial service by the financial institution or the service is provided to the market by the OSP in the name of the financial institution;

“service provider” or “outsourced service provider” means - any party which provides a service to the financial institution operating in Singapore;

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