

Third Party Trust

Manage your outsourcing arrangements

Who's keeping your promises?

October 2014

Issue 1

Service Providers version



Contents

	<i>Page</i>
<i><u>MAS Outsourcing Guidelines and Notice</u></i>	4
<i><u>Implications of Notice</u></i>	6
<i><u>MAS Outsourcing Guidelines</u></i>	18
<i><u>Competitive Intelligence</u></i>	37
<i><u>Appendix</u></i>	40

***“An ecosystem of trust
needs to exist between you
and any stakeholder or
partner who is making and
keeping promises on your
behalf”***

**Marco Amitrano
Global Assurance Markets Leader**

MAS

Outsourcing Notices and Guidelines

(consultation 09/2014)



Outsourcing Guidelines and Notice

The new MAS Outsourcing Guidelines and Notice have been enhanced to help financial institutions' to prevent their risk management, internal control, business conduct or reputation from being compromised or weakened by their outsourcing arrangement

- MAS released Outsourcing Guidelines and Notice for consultation in September 2014
- The notice will impact
 - All Financial Institutions (FIs) (See Appendix for definitions)
 - Includes all material outsourcing agreements
 - Potentially any existing arrangements where customer information may not be segregated or identified. Though this concept around protect in also linked to the Technology Risk Management (TRM) Guidelines and Notice

Non compliance to the Notice can result in:

- **Financial penalties**
- **Reputational damage**
- **Revocation of licence to operate in Singapore**

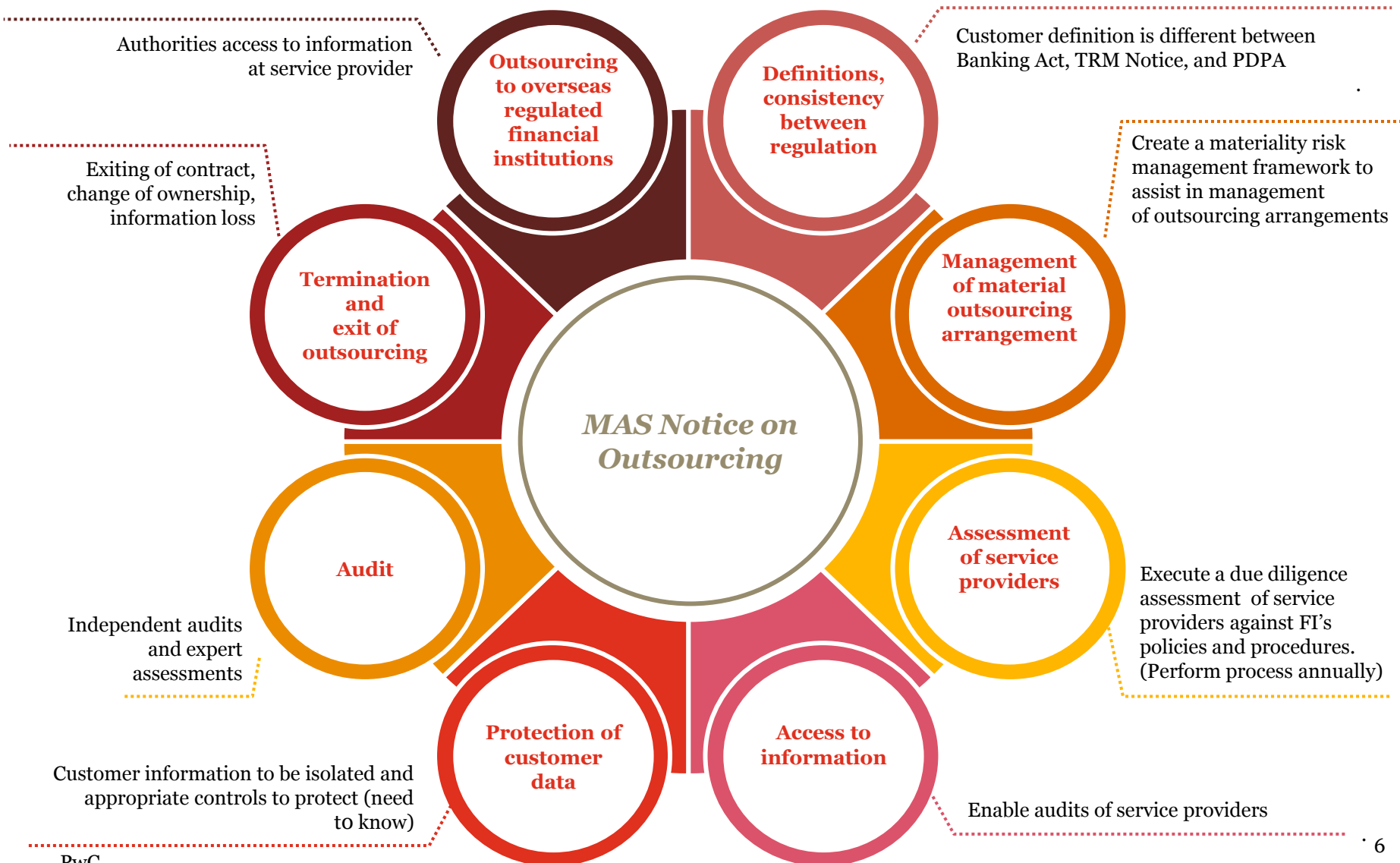
The Meaning of “material outsourcing arrangement”

*Outsourcing arrangement where:

- A failure or security breach of service potentially have **significant impact** on **business operations, reputation or profitability**; or prevent compliance with applicable laws and regulations,
- or
- Which involves customer information and, in the event of any unauthorized access or disclosure, loss or theft of customer information, may have **significant impact an your customers**;
- Which a **service provider** provides the institution with a service that may currently or potentially be performed by the institution itself and which includes the following characteristics:
 - (i) the institution is dependent on the service on an ongoing basis but such service excludes services that involve the provision of a finished product; and
 - (ii) the service is integral to the provision of a financial service by the institution or the service is provided to the market by the service provider in the name of the institution;

*Extracted from MAS Consultation Paper on Notice on Outsourcing

What are the implications of the Notice ?



With the new Outsourcing Notice Eight grouped areas that impact your business were identified

1. Definitions

*2. Management
of material
outsourcing
arrangements*

*3. Assessment of
service
providers*

*4. Access to
information*

*5. Protection of
customer data*

6. Audit

*7. Termination
and exit of
outsourcing*

*8. Outsourcing
to overseas
regulated
financial
institutions*

1**2****3****4****5****6****7****8**

Clarifications

“Will the new Outsourcing Notice supersede the Notice 634 ?”

Banking Act & Notice 634

When outsourcing any operational function to a service provider such that the outsourced function will be performed by the service provider outside Singapore and disclosure of customer information (as defined in section 40A of the Banking Act) to the service provider is involved, all banks in Singapore relying on the exception provided in paragraph 3 of Part II of the Third Schedule of the Banking Act are required to comply with the Conditions set out in the Appendix to this Notice.

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Definitions and Clarifications

“The Notice has definitions and are legally binding requirement for FI’s”

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

Presented as a full notice

Which act takes precedence? Banking Act, Notice 634, MAS TRM, PDPA?

Contains **8 detailed section of requirements**

Attempts to cover **material** outsourcing agreements (see material definition) **instead of all** outsourcing agreement involving customer information.

Newly defines terminology used by introducing definitions for words such as “customer”, “customer information”, “outsourcing arrangement”, “sub-contracting”, etc.

Definitions need to be consistent against MAS TRM, Banking Secrecy, PDPA and MAS Outsourcing

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Management of material outsourcing arrangements

Service
Providers: Need
to know the
criteria to be in
business

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

New requirement to demonstrate at **minimum**

- A. policies and processes to identify outsourcing agreement
- B. a risk management framework, systems, policies and processes to **assess, control and monitor its outsourcing arrangements** with respect to compliance to laws, rules, regulations, notices and directives applicable to the institution

Enhance policies and processes to identify all material outsourcing arrangements

Have a risk management framework to assess, control and monitor outsourcing arrangements to remain compliant notwithstanding outsourcing arrangements

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Management of material outsourcing arrangements

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

New requirement to demonstrate at
minimum

- A. maintenance of a **central register** of all material outsourcing arrangements.
- B. Steps and documentation taken upon request

Maintain a central register of all material outsourcing arrangements. Refine your current practices for adequate recording of your outsourcing arrangements

Retain documentary evidence demonstrating compliance to the notice

Establish good communication procedures between the board and the committee

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Assessment of service providers

Service
Providers: Visits
are now a
requirement by
law

Service
Providers:
Consider how
to prevent
domino effect

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

New detailed **requirements** extend the due diligence obligation to now **necessitate risk assessment processes**.

- Perform a due diligence undertaken during the assessment process as part of the monitoring and control processes of its outsourcing arrangements.
- Findings from due diligence should also be considered in determining the audit scope

The capability of assessing suppliers' governance, security, internal controls and the **safeguarding of confidentiality, integrity and availability** of information.

An institution should conduct onsite visits to the service provider by personnel who possess the requisite knowledge and skills to conduct the assessment, which includes physical and IT security controls

An **annual re-assessment** is now **required**.

An institution needs to assess employees of a service provider and perform the assessment on annual basis

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Access to information

Service Providers: To consider legal and business implications of indemnification

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

Extended requirement to include outsourcing agreements **provisions** to:

A. Allow the institution, **authority or any agent appointed by the Authority**, auditors rights to audit, access and inspect the service provider **and its sub-contractors** records, transactions, information stored at or processed by the service provider and its sub-contractors, reports and findings made internally or externally.

B. Indemnify and hold the Authority, its officers, agents and employees harmless from any liability, loss or damage to the service provider and its sub-contractors arising out of any action taken to access and inspect the service provider or its sub-contractors pursuant to the outsourcing agreement.

The right to audit the service provider
To indemnify the authority “Regulator’ or it’s Agents against any legal action if loss or damage occurs

Need to encourage the use of SSAE3402 report to reduce operations cost. To achieve this need:
Financial arrangement in place
Amend clause (5.9.6, Guidelines) to allow 3rd party review

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Protection of customer data

Service Providers: How to “isolate” each institution’s customer information?

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

- The notion of deposit customer information is now **removed**.
- **Requirement** to include **outsourcing agreements provisions has been extended** to
 - A. protect the confidentiality of customer information.
 - B. isolate** and clearly identify the customer information, institution’s documents, records, and assets.
 - C. Limit access to information by the employees of the service provider **and its sub-contractors** on a need and duties obligation basis.
 - D. Restriction of information disclosure by the service provider, **its sub-contractors and their employees** to any other party unless required to do so by law;
 - E. Notify** the institution as soon as practicable **prior to information disclosure**.
 - F. Any information disclosed shall be used by the institution strictly for the purpose for which it was disclosed.

- An institution shall require the service provider to isolate and clearly identify the institution’s customer information, documents, records, and assets to protect the confidentiality of the information.
- An institution shall only disclose customer information to the service provider (need to know)
- Immediate notification upon breach/loss of information

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Audit

Service Providers:
Ensure sub-contractors would pass audit.

Consultation Paper on Notice Outsourcing (Sept 2014)

- **Refined** requirement, audits should now be conducted by independent auditor and/or expert assessments based on the nature and extent of risk and impact to the institution from the outsourcing arrangements
- **New** - the elapse time between audits could now be up to 3 years.
- **New** – the **scope** of the audits **now includes** the service providers' and its **sub-contractors**
- **New** – the **sub-contractors** also **need to fulfill MAS' Guidelines** on Outsourcing **and compliance with the Notice** in relation to the outsourcing arrangement and provide a copy of their reports

What does this means to you

- Independent audit/expert assessment to be performed at least every 3 years (previously only stipulated as 'periodically' may be performed and prepared by the institution's internal or external auditors, or by agents appointed by the institution
- The scope includes service provider and sub-contractors

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Termination and exit of outsourcing

Service
Providers: How
to prove that
records have
been removed.

Consultation Paper on Notice Outsourcing (Sept 2014)

- Previous 2004 conditions are **kept**
- **Requirements** to have ability to terminate outsourcing agreement are **now extended** to include **events where**
 - A. the institution is **prevented from conducting any audits** or obtaining any report and finding made on the service provider;
 - B. the institution is prevented from assessing the service provider's compliance with the outsourcing agreement;
 - C. the institution is directed by the Authority to terminate the outsourcing arrangement as the service provider has failed to comply with all applicable laws and regulations.

What does this means to you

Upon the termination of an outsourcing agreement, an institution shall ensure that all documents, records of transactions and information previously given to the service provider are removed from the possession of the service provider or deleted, destroyed or rendered unusable.

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

1

2

3

4

5

6

7

8

Outsourcing to overseas regulated financial institutions

Consultation Paper on Notice Outsourcing (Sept 2014)

What does this means to you

Maintained requirement where for overseas regulated service provider institution a written confirmation is to be given to the authority to the effect that :

- A. The Authority and any independent auditors appointed by the Authority are allowed access by the supervisory authority to the institution's documents, records of transactions, information previously given to, stored or processed by the service provider
- B. Rights is granted to inspect the control environment within the service provider reporting any findings to the Authority
- C. The access is restricted to any customer information by supervisory authority unless access to the information is required for the sole purpose of carrying out its supervisory functions the Authority needs to be given prior written notification whenever access to information is granted
- D. It is prohibited under its laws from disclosing the Information to any other person, or it undertakes to safeguard the confidentiality of the Information and not disclose the Information to any other person

The institution must acquire written consent from the regulated service provider and give that to the supervisory authority before any disclosure.

Legend: This is the first introduction of a Notice in respect to Outsourcing. The requirements in the Notice are all new.

MAS

Outsourcing Notices and Guidelines

(consultation 09/2014)

Highlights for Service Providers



Challenges

Highlights for Service Providers

- Challenge of having multiple frameworks and requirements – what can be done to streamline / standardise ?
- Yearly due diligence – potential significant disruption to business from domino effect. Is it possible to smooth this out?
- Multiple audits – operational challenge. Preference for single SSAE 3402 audits?
- Indemnity clause – how to make it fairer?
- How to isolate data – is it even feasible?
- Termination requirements – may need process change
- Ensure sub-contractor comply
- Overseas operations have new compliance requirements
- Employees' fit and proper criteria – may affect existing staff and future recruitment. Are they too perceptive?
- Higher barrier for new entrants
- More difficult for institutions to outsource to overseas

MAS Outsourcing Guidelines

1.

Definitions

2.

Applicability

3.

*Engagement
with MAS on
outsourcing*

4.

*Responsibility
of Board and
Management*

5.

*Evaluation
of Risks*

6.

*Assessment
of Service
Providers*

7.

*Outsourcing
Agreement*

8.

*Confidentiality
and Security*

9.

*Business
Continuity
Management*

10.

*Monitoring and
Control of
Outstanding
Arrangements*

11.

*Audit and
Inspection*

1

2

3

4

5

6

7

8

9

10

11

Definitions

Key Requirements

- Definition of 'institution' has changed to be now defined as 'any financial institution as defined in section 27A of the Monetary Authority of Singapore Act (Cap. 186)
- Guidelines to assess the quality of its risk management systems. MAS is particularly interested in material outsourcing which, if disrupted, has the potential to significantly impact an institution's business operations, reputation or profitability and which may have systemic implications.

What you need to consider

Guidelines now define:

- Customer
- Customer information
- Material outsourcing arrangement
- Outsourcing arrangement

Further clarifies 'Material outsourcing' as 'which, if disrupted:

- significantly impact an institution's business operations
- Reputation
- Profitability and which may have systemic implications

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Applicability of Guidelines

Key Requirements

- An institution should conduct a self-assessment of all existing outsourcing arrangements
- Notify MAS in writing within two months
- Rectify the deficiencies identified in the self-assessment no later than six
- Mitigate the risks in the interim
- Annex 4 provides a template for an institution to maintain a register of its outsourcing arrangements which is to be submitted to MAS, upon request

What you need to consider

- Requirement for remediation of issues arising from self assessment has changed from 1 year to 6 months
- New template for outsourcing register provided

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Engagement with MAS on outsourcing

Key Requirements

- Notify MAS before it commits to the commencement of any material outsourcing arrangement or amends arrangement
- Observance of these Guidelines

MAS may require an institution to modify, make alternative arrangements or re-integrate an outsourced service:

- (a) An institution fails, or is unable to demonstrate a understanding of the nature and extent of risks
- (b) An institution fails or is unable to implement adequate measures to address the risks in a and timely manner;
- (c) Adverse developments
- (d) MAS' supervisory powers over the institution and ability to carry out MAS' supervisory functions in respect of the institution's services are hindered; or
- (e) The confidentiality of its customer information cannot be assured.

What you need to consider

Requirement to notify MAS has changed from 'when it is planning or has entered' to before commitment to the contract

Additional requirements to modify, make alternative arrangements or re-integrate an outsourced service when

- (a) Understand the risk and remediate in a timely manner
- (e) Protect customer information

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Engagement with MAS on outsourcing

Key Requirements

- Notify MAS as soon as possible of any adverse development or breach of legal and regulatory requirements
 - Newly regulated or acquisition should
 - Conduct a self-assessment of all existing or newly acquired outsourcing arrangements and inform MAS within two months
 - Rectify the deficiencies identified in the self-assessment no later than six months
 - Mitigate risks
- In supervising an institution, assess the quality of its board and senior management oversight and governance

What you need to consider

- New requirement for organisations which have recently come under the regulation of MAS to now comply with the guidelines
- MAS intends to review implementation of the guidelines and assess the quality of the board and senior management

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Responsibility of Board and Management

Key Requirements

What you need to consider

The board and senior management of an institution retain ultimate responsibility for the effective management of risks arising from outsourcing.

The board, or a committee delegated by it, is responsible for:

- (a) approving a framework to evaluate the risks and materiality
- (b) setting a suitable risk appetite
- (c) laying down appropriate approval authorities and limits
- (d) assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope and complexity of the outsourcing arrangements;
- (e) ensuring that senior management establishes appropriate governance structures and processes risk management,
- (f) undertaking regular reviews

- More detail around the need for the board and management to ensure an 'institution wide view' of risk management
- Requirement for Materiality Risk Framework
- Responsibility and accountability is with the senior management and board.

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Responsibility of Board and Management

Key Requirements

What you need to consider

Where the board delegates its responsibility to a committee, senior management is responsible for:

- (a) evaluating the materiality and risks from all existing and prospective outsourcing arrangements, based on the framework approved by the board
- (b) developing sound and prudent outsourcing policies and procedures
- (c) reviewing regularly the effectiveness of, and appropriately adjusting, policies, standards and procedures to reflect changes in the institution's overall risk profile and risk environment;
- (d) monitoring and maintaining effective control of all risks from its material outsourcing arrangements on an institution-wide basis;
- (e) ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested;
- (f) ensuring that there is independent review and audit for compliance with set policies and procedures;
- (g) ensuring appropriate and timely remedial actions are taken to address audit findings; and
- (h) communicating information pertaining to risks from its material outsourcing arrangements to the board in a timely manner.

Evaluate, develop, review, monitor, contingency plans, independent review, remediate in timely manner, communicate

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Evaluation of Risks

Key Requirements

The institution should establish a framework for risk evaluation which should include the following steps:

- (a) identification of the role of its outsourcing arrangements in the overall business strategy and objectives of the institution, and its interaction with corporate strategic goals
- (b) comprehensive due diligence on the nature, scope and complexity of the outsourcing arrangement, to identify the key risks and risk mitigation strategies
- (c) assessment of the service provider and its sub-contractors in the outsourcing arrangement
- (d) analysis of the impact of the arrangement on the overall risk profile of the institution, and whether there are adequate internal expertise and resources to mitigate the risks identified
- (e) analysis of the institution's as well as the institution's group aggregate exposure to the outsourcing arrangement, to manage concentration risks in outsourcing to a service provider
- (f) analysis of risk-return on the potential benefits of outsourcing against the vulnerabilities that may arise

What you need to consider

- Risk Management framework
- Due Diligence on the nature and scope
- Assessment of Service provider and Sub-contractors
- Analysis of arrangement on the overall risk profile
- Risk benefit analysis

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Assessment of Service Providers

Key Requirements

An institution should address all relevant aspects of the service provider. Including its capability to employ a high standard of care.

The due diligence should also take into consideration qualitative and quantitative aspects of financial, operational and reputation factors including the level of ethical and professional standards held by the service provider, and the service provider's ability to comply with its obligations under the outsourcing arrangement. Compatibility, performance, and internal controls should be emphasized in the assessment. Onsite visits to the service provider, and where possible, independent reviews and market feedback on the service provider, should also be used by the institution to supplement its findings. Onsite visits should be conducted by persons who possess the requisite knowledge and skills to conduct the assessment, which includes physical and IT security controls.

What you need to consider

- Evaluate the service provider; including ability to perform high standards of care
- Perform due diligence

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Assessment of Service Providers

Key Requirements

The due diligence should involve an evaluation of all available information about the service provider. Information to be evaluated include the service provider's on an annual basis:

- (a) experience and competence to implement and support the outsourcing arrangement over the contracted period;
- (b) financial strength and resources (the due diligence should be similar to a credit assessment of the viability of the service provider based on reviews of business strategy and goals, audited financial statements, the strength of commitment of major equity sponsors and ability to service commitments even under adverse conditions);
- (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 management⁷ and business continuity management⁸ in respect of the outsourcing arrangement;
- (f) disaster recovery arrangements made by the service provider and track record of its disaster recovery service provider if outsourcing service provider is responsible for such provisions with the outsourcing arrangement;
- (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 service provider operates, and other events) that may impact service performance; and
- (j) its track record and ability to comply with applicable laws and regulations.

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Outsourcing Agreement

Key Requirements

An institution should ensure that every outsourcing agreement addresses the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages. It should at the very least, have provisions to address all the following aspects of outsourcing:

- (a) scope of the outsourcing arrangement;
- (b) performance, operational, internal control and risk management standards;
- (c) confidentiality and security¹¹;
- (d) business continuity management¹²;
- (e) monitoring and control¹³;
- (f) audit and inspection¹⁴;
- (g) Notification of adverse developments
- (h) Dispute resolution
- (i) Default termination and early exit
- (j) Sub-contracting
- (k) Applicable laws

What you need to consider

A robust contract between the institution and service provider (including sub-contractor)

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Confidentiality and Security

Key Requirements

An institution should be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. An institution should take the following steps to ensure that the confidentiality of customer information is addressed:

(a) Address, agree and document the respective responsibilities of the various parties in the outsourcing arrangement to ensure the **adequacy and effectiveness** of security policies and practices, including the circumstances under which each party has the right to change security requirements. It should also address the issue of the **party liable** for losses in the event of a breach of security or confidentiality and the service provider's obligation to inform the institution;

(b) Address issues of **access** and **disclosure** of customer information provided to the service provider having regard to the institution's obligations under relevant laws and regulations.

Customer information should be **used** by the service provider and its staff strictly for the purpose of the contracted service. Any unauthorized disclosure of the institution's customer information to any other party should be prohibited;

(c) Disclose customer information to the service provider only on a **need-to-know** basis and ensure that the amount of information disclosed is commensurate with the requirements of the situation;

(d) Ensure the service provider is able **to isolate and clearly identify the institution's customer** information, documents, records, and assets to protect the confidentiality of the information, particularly where multi-tenancy arrangements are present at the service provider. An institution should also ensure that the service provider takes technical, personnel and organizational measures in order to maintain the confidentiality of customer information between its various customers; and

(e) Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning or obtaining periodic expert reports on confidentiality and security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose breaches of confidentiality in relation to customer information.

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Business Continuity Management

Key Requirements

An institution should ensure that its business continuity is not compromised by any outsourcing arrangement, in particular, of the operation of its critical systems as stipulated under the Technology Risk Management Notice. An institution should adopt the sound practices and standards contained in the Business Continuity Management (BCM) Guidelines issued by MAS, in evaluating the impact of outsourcing on its risk profile and for effective BCM on an ongoing basis.

For assurance on the functionality and effectiveness of its BCP plan, an institution should design and carry out regular, complete and meaningful testing of its plans that commensurate with the nature, scope and complexity of the outsourcing arrangement, including risks arising from interdependencies on the institution. For tests to be complete and meaningful, the institution should involve the service provider in the validation of its BCP and assessment of the awareness and preparedness of its own staff. Similarly, the institution should take part in its service providers' BCP and disaster recovery exercises.

What you need to consider

- Critical Systems from a BCM should not be compromised due to Outsourcing
- Regular testing
- BCM should be based on worst case scenarios

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Business Continuity Management

Key Requirements

The institution should base its business continuity considerations and requirements on worst-case scenarios.

Some examples of these scenarios are unavailability of service provider due to unexpected termination of the outsourcing or liquidation of the service provider, wide-area outage disruptions that result in collateral impact on both the institution and the service provider. Where the interdependency on an institution in the financial system is high¹⁸, the institution should maintain a higher state of business continuity preparedness. The identification of viable alternatives for resuming operations without incurring prohibitive costs is also essential to mitigate interdependency risk.

What you need to consider

- Critical Systems from a BCM should not be compromised due to Outsourcing
- Regular testing
- BCM should be based on worst case scenarios

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Monitoring and Control of Outsourcing Arrangements

Key Requirements

An institution should put in place all the following measures for effective monitoring and control of any material outsourcing arrangement:

- (a) A register of all material outsourcing arrangements that is readily accessible for review by the board and senior management of the institution.
- (b) Multi-disciplinary outsourcing management groups with members from different risk and internal control functions including legal, compliance and finance.
- (c) Establishment of management control groups to monitor and control the outsourced service on an ongoing basis
- (d) Establishment of service recovery procedures and reporting of lapses relating to the agreed service standards by the service provider;

What you need to consider

- Implement a material outsourcing register
- Outsourcing group needs to have personal with multiple skills (technical/legal/risk/compliance)
- Regular service delivery monitoring via validated reports:- confidentiality, security adequacy, compliance, security vulnerability management.
- Establishment of service recovery procedures and reporting of lapses relating to the agreed service standards by the service provider
- Periodic reviews, at least on an annual basis, of outsourcing arrangements.

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Monitoring and Control of Outsourcing Arrangements

Key Requirements

An institution should put in place all the following measures for effective monitoring and control of any material outsourcing arrangement:

(e) Periodic reviews, at least on an annual basis, of outsourcing arrangements.

(g) Pre - and post- implementation reviews of new outsourcing arrangements or when amendments are made to the outsourcing arrangements.

(f) Reporting policies and procedures. Reports on the monitoring and control activities of the institution should be prepared or reviewed by its senior management and provided to its board for information.

The institution should ensure that monitoring metrics and performance data specific to the institution are available for reporting, and not aggregated with metrics or data belonging to other customers of the service provider. The institution should also ensure that any adverse development arising in any outsourcing arrangement is brought to the attention of the senior management of the institution and service

What you need to consider

- Implement a material outsourcing register
- Outsourcing group needs to have personal with multiple skills (technical/legal/risk/compliance)
- Regular service delivery monitoring via validated reports:- confidentiality, security adequacy, compliance, security vulnerability management.
- Establishment of service recovery procedures and reporting of lapses relating to the agreed service standards by the service provider
- Periodic reviews, at least on an annual basis, of outsourcing arrangements.

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Audit and Inspection

Key Requirements

What you need to consider

An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives

An institution should include in all its outsourcing agreements clauses that:

- (a) allow the institution to conduct audits on the service provider and its sub-contractors, whether by its internal or external auditors, or by agents appointed by the institution
- (b) allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the institution
- (c) indemnify and hold MAS, its officers, agents and employees harmless from any liability, loss or damage to the service provider and its sub-contractors arising out of any action taken to access and inspect the service provider or its sub-contractors pursuant to the outsourcing agreement.

- Right to independently audit
- Indemnify MAS or any other party that is requested to assess the service provider
- Service provider to comply as soon as possible
- Maximum period between audits

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Audit and Inspection

Key Requirements

The outsourcing agreement should also include clauses that require the service provider to comply, as soon as possible.

An institution should ensure that independent audits and/or expert assessments of all its outsourcing arrangements are conducted.

The independent audit and/or expert assessment and reports on the service provider and its sub-contractors may be performed and prepared by the institution's internal or external auditors, or by agents appointed by the institution.

What you need to consider

- Right to independently audit
- Indemnify MAS
- Service provider to comply as soon as possible
- Maximum period between audits

Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

1

2

3

4

5

6

7

8

9

10

11

Audit and Inspection

Key Requirements

What you need to consider

Significant issues and concerns should be brought to the attention of the senior management of the institution and service provider, or to its board, where warranted, on a timely basis.

Copies of audit reports should be submitted by the institution to MAS. An institution should also, upon request, provide MAS with other reports or information on the institution and service provider that is related to the outsourcing arrangement.

The engagement of a service provider in a foreign country, or the engagement whereby the outsourced function is performed in a foreign country, exposes an institution to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the institution. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the institution. In its risk management of such outsourcing arrangements, an institution should take into account, with due diligence and on a continuous basis:

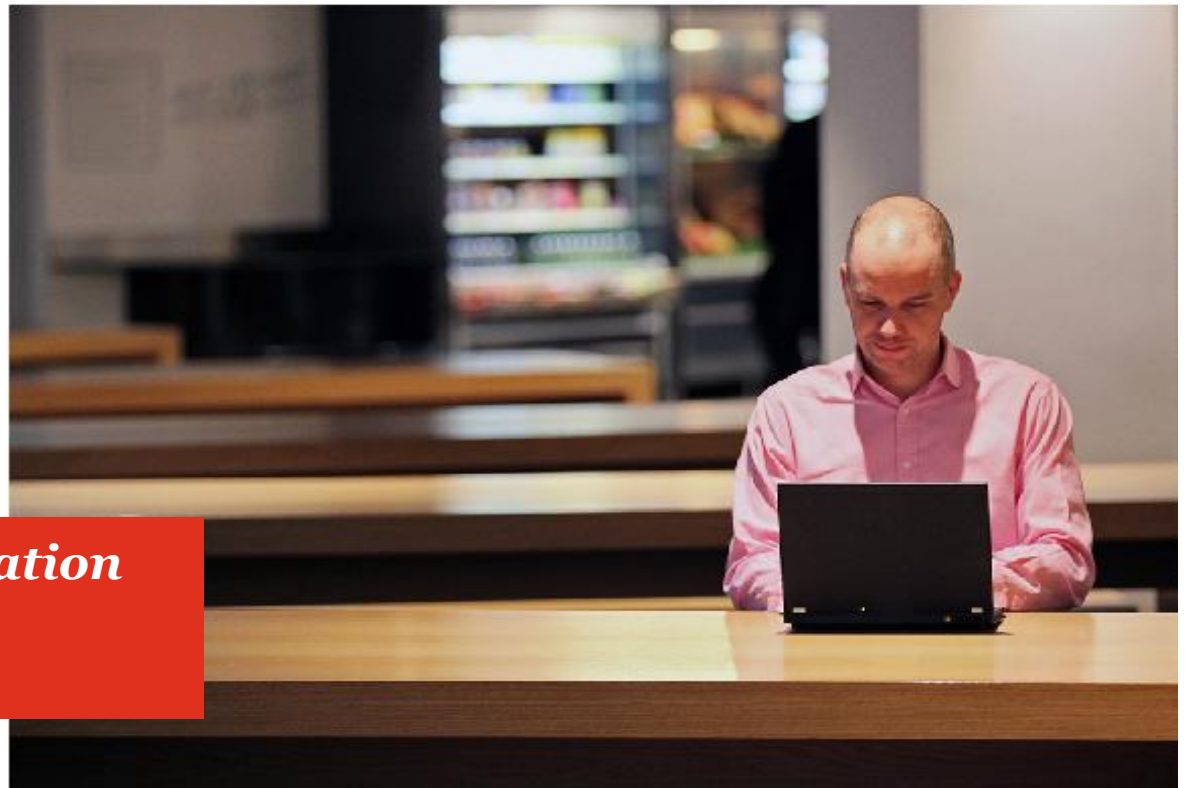
- (a) government policies;
- (b) political, social, economic conditions;
- (c) legal and regulatory developments in the foreign country; and
- (d) the institution's ability to effectively monitor the service provider

- Senior management need to beware of significant issues
- Copies of Audit reports made available to MAS
- Be aware of the risks when outsourcing to other countries

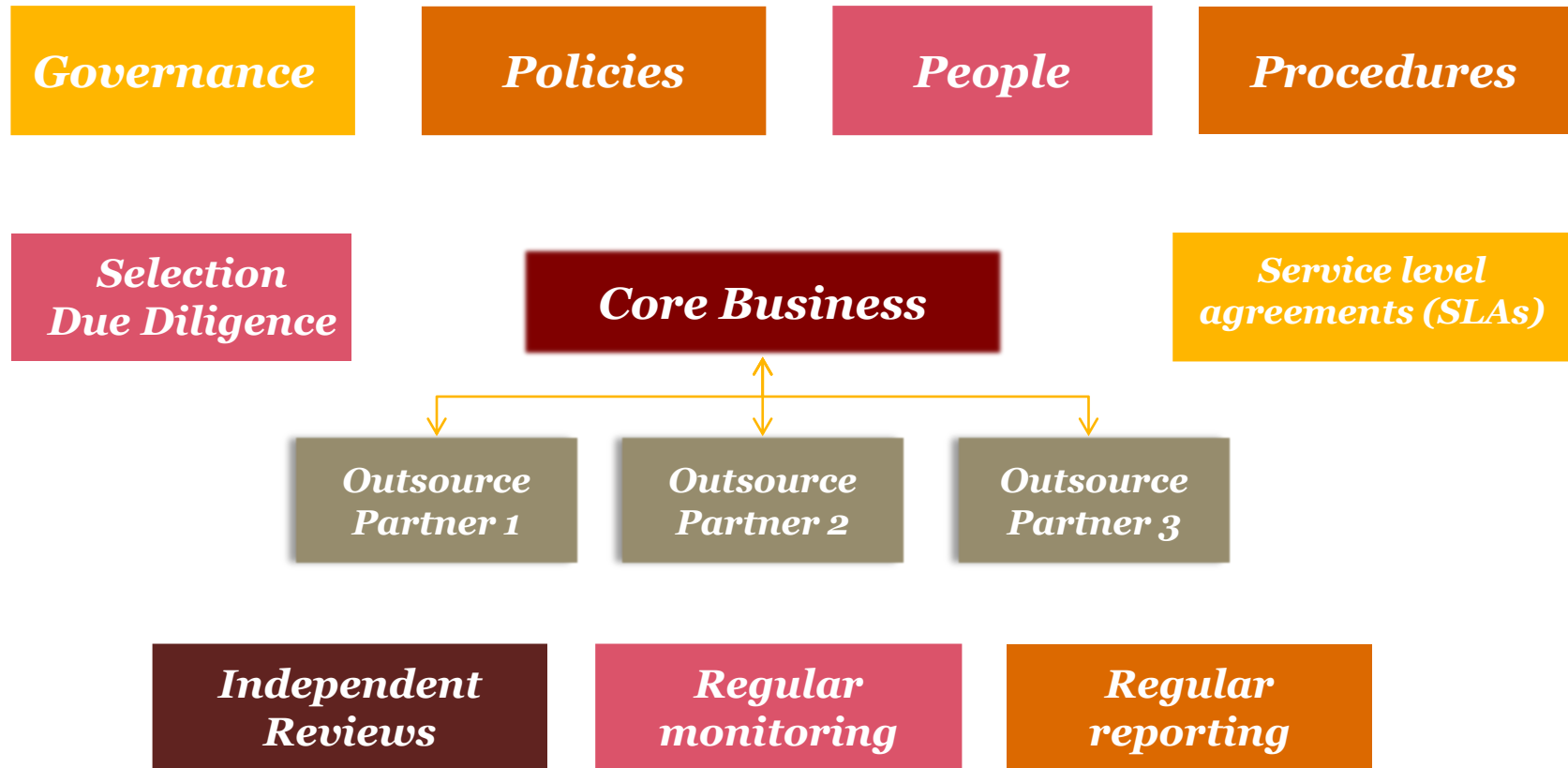
Legend: The shaded requirements represent the new. The non-shaded represents changes to previous Outsourcing Guidelines.

Competitive Intelligence

*Our observation
of industry
practices*



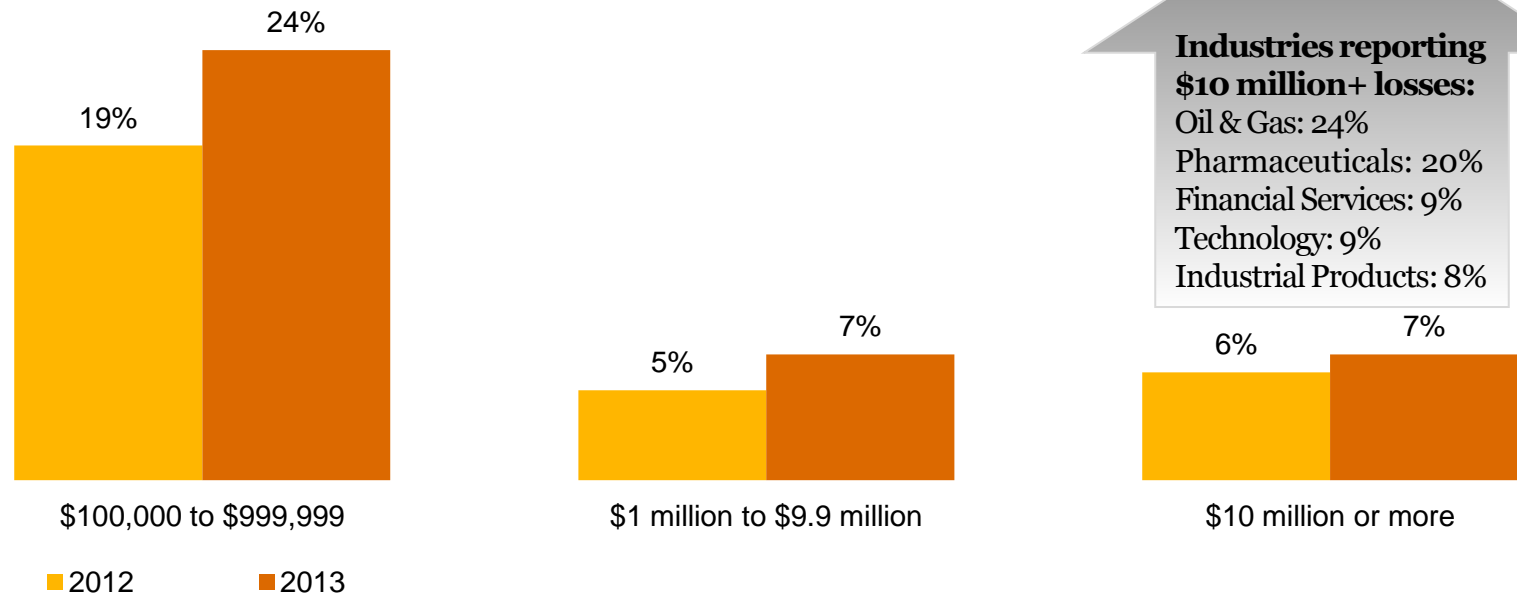
In a Nutshell – Areas of focus



The financial costs of incidents are rising, particularly among organisations reporting high dollar-value impact.

Average losses are up 18% over last year, which is not surprising given the costs and complexity of responding to security incidents. Big liabilities are increasing faster than smaller losses: Respondents reporting losses of \$10 million-plus is up 51% from 2011.

Financial losses of \$100,000 or more



Question 22A: "Estimated total financial losses as a result of all security incidents" Global Information Security Survey

Appendix: Useful Resources



Useful Resources

The MAS Notice on Outsourcing

http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Consultation%20Papers/ConsultationPaper_Notice%20on%20Outsourcing.pdf

MAS Guidelines on Outsourcing

http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Consultation%20Papers/ConsultationPaper_Guidelines%20on%20Outsourcing.pdf

Shine a brighter light on your business ecosystem

Mark Jansen

+65 8100 7123
mark.jansen@sg.pwc.com

Tan Shong Ye

+65 9820 3623
shong.ye.tan@sg.pwc.com

Chan Hiang Tiak

+65 9763 3190
hiang.tiak.chan@sg.pwc.com

Manish Chawda

+65 9180 1882
manish.chawda@sg.pwc.com

This presentation has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PricewaterhouseCoopers Limited. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Limited which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.