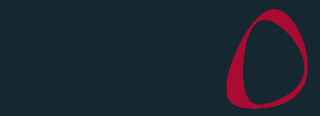
MAS Technology Risk Management Guidelines and Notice

12 November 2013

Rosemary Lee

Counsel, Pinsent Masons MPillay LLP



Pinsent Masons MPillay

Outline

- Recent incidents and MAS' response
- Internet Banking and Technology Risk Management (**IBTRM**) Guidelines
- Technology Risk Management (**TRM**) Guidelines and Notice
- Preparing for compliance
- Q&A

UOB Reported Outages

- 2 incidents between 2004 and 2006
- Duration: several days / unknown
- Services affected:
  - ATM
  - NETS facilities
  - Internet banking

DBS Outage 2010

- Duration: 7 hours
- Services affected:
  - ATM
  - Mobile banking
  - Internet banking
  - Credit and debit card
  - NETS

“MAS takes a serious view of this incident. We expect all financial institutions to put in place a robust technology risk management framework that will ensure the reliability, resiliency and speedy recoverability of the institution's IT systems and infrastructure, whether outsourced or in-house.”

Ms Teo Swee Lian, Deputy Managing Director, Financial Supervision, MAS (on the DBS Bank outage)

MAS' Response

- DBS failed to put in place a robust technology risk management framework.
- DBS failed to exercise sufficient oversight of the maintenance, functional and operational practices and controls of IBM.
- DBS should "diversify and reduce its material outsourcing risks".
- DBS should review outsourcing vendors' processes and functions to ensure maintenance and support teams are up to scratch.

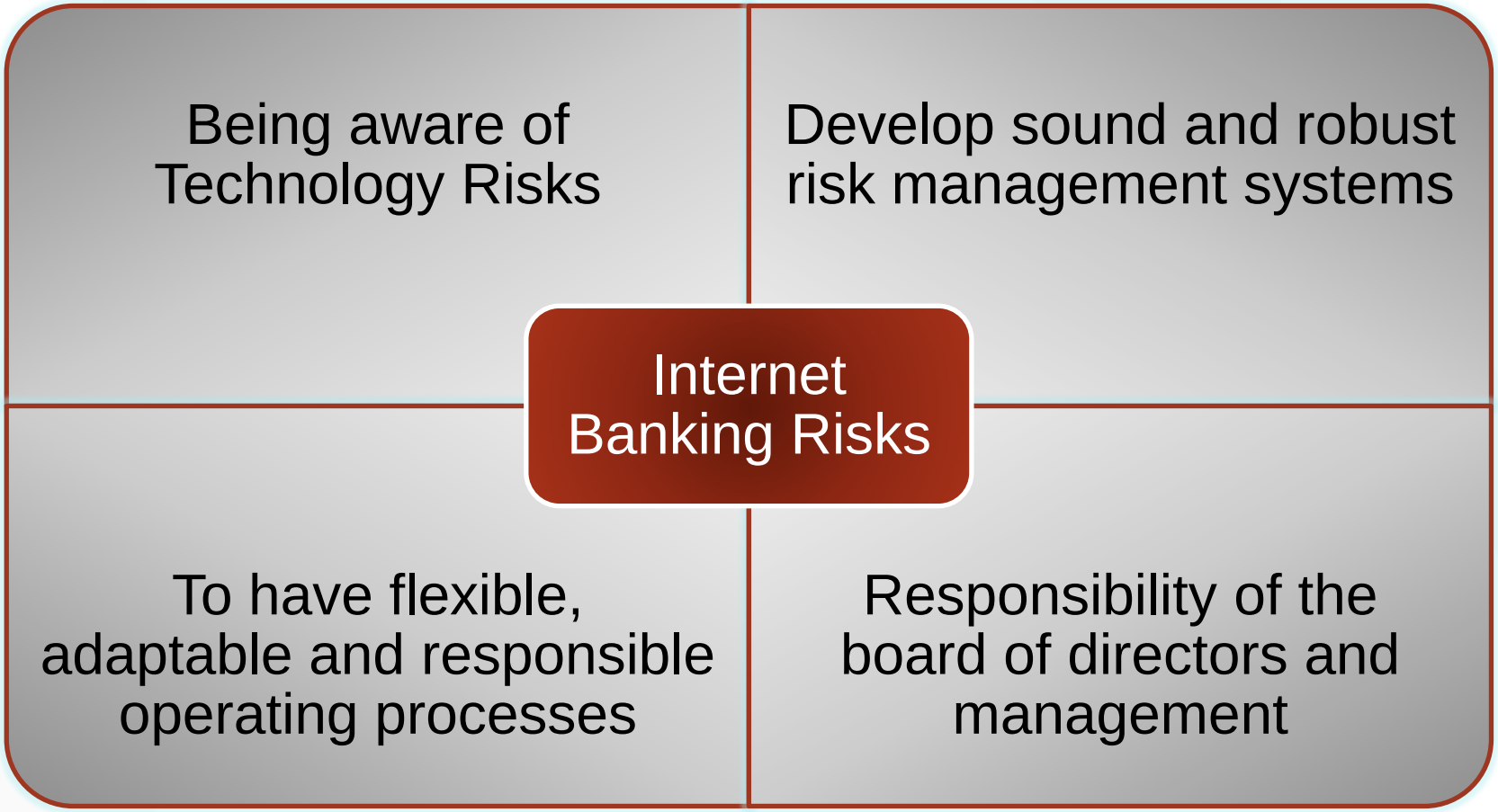
OCBC Outage 2011

- Duration: 4 hours
- Services affected:
  - ATM
  - Mobile banking
  - Internet banking
- MAS' response: "(OCBC) did not implement sufficient measures to address single point failure in its system and network infrastructure. OCBC Bank had therefore failed to observe the Security Practices set out in the MAS IBTRM Guidelines."

“MAS expects financial institutions to be responsible and accountable in managing and controlling technology risks as well as implementing measures to ensure the resilience of their IT systems and infrastructure.”

Mr Lee Boon Ngiap, Assistant Managing Director, Banking and Insurance, MAS (on the OCBC Bank outage)

IBTRM Guidelines



IBTRM Guidelines

Identify, classify and assess relevant risks

Develop a documented plan containing policies, practices and procedures to address and control these risks

Implement and regularly test the plan

Monitor risks and the effectiveness of the plan regularly

Update the plan periodically to take into account changes in technology, legal requirements and business environment

TRM Guidelines and Notice – Timeline

TRM Guidelines and Notice – What is an FI?

• Approved exchanges	• Banks
• Designated clearing houses	• Finance companies
• Holders of CMS licence	• Local credit or charge card licensees
• Recognised market operators	• MAS approved money brokers
• Trustee of an SFA authorised CIS	• MAS approved merchant banks
• Licensed financial advisors	• Holders of remittance licence
• Licensed insurers (other than captive insurers and marine mutual insurers)	• Operators and settlement institutions of designated payment systems
• Registered insurance brokers	• Licensed trust companies

Other Jurisdictions

Hong Kong

- **Guidance Note on Management of Security Risks in Electronic Banking Services** issued in July 2000 and updated in August 2011.

South Korea

- The Financial Services Commission announced on 25 June 2013 that it will adopt a revised set of **Regulations on Delegations of Information Processing and IT Facilities of Financial Companies**.

China

- China Banking Regulatory Commission published the **Commercial Bank Information Technology Risk Management Guidance** on 3 March 2009. This replaces the old “Banking Financial Service Organisations Information System Risk Management Guidance”.

TRM Guidelines – Overview (1)

Update of IBTRM Guidelines

Consolidation of existing circulars

- Information Reliability, Resiliency and Recoverability (2010)
- Technology Risk Management (2009)
- End-Point Security and Data Protection (2009)

Includes all IT systems

- IBTRM Guidelines applied only to Internet banking

Applies to all financial institutions (“FI”)

- IBTRM Guidelines only applied to banks

TRM Guidelines – Overview (2)

Not legally binding but FI's degree of observance will be a consideration in the risk assessment of the FI by the MAS

Addresses existing and emerging trends

- **Data centres**
- **Mobile online services**
- **Payment card security**
- **Cyber attacks**
- **Consumer protection and education**

TRM Guidelines – Key Areas (1)

- Greater oversight by the Board and Senior Management
- Technology Risk Management Framework
- Managing IT outsourcing risk
- Acquisition and development of information systems
- IT service management

TRM Guidelines – Key Areas (2)

- Systems reliability, resiliency and recoverability
- Operational infrastructure security management
- Enhanced data centre protection and controls
- Mobile online services
- Payment card security (ATM, credit and debit card)

COMPLIANCE CHECKLIST
FOR
TECHNOLOGY RISK MANAGEMENT GUIDELINES

Name of Financial Institution _____

Date Completed _____

Name of Respondent _____

Designation / Title _____

Contact Number _____

Email Address _____

Name of Reviewer _____

Designation / Title _____

Contact Number _____

Email Address _____

Instructions

1. This compliance checklist should be completed each year by senior officers who have direct knowledge of the financial institution's information systems and operations. The information provided in this checklist should be reviewed by their superiors.

TRM Notice - “Critical System”

A system, the failure of which will cause significant disruption to the FI’s operations or materially impact a FI’s service to its customers, such as a system which:

(a) processes transactions that are time-critical; or

(b) provides essential services to customers

TRM Notice - “Relevant Incident”

A system malfunction or IT security incident, which has a severe and widespread impact on the FI’s operations or materially impacts the FI’s services to its customers.

TRM Notice – Obligations (1)

Before incident/outages

- Put in place a framework and process to identify critical systems,
- Make all reasonable effort to maintain high availability for critical systems
- Establish a Recovery Time Objective (RTO) of not more than 4 hours from the time of the incident/outage for each critical system
- Validate and document RTO at least once every 12 months

During incident/outages

- Report incidents/outages within 1 hour from time of discovery
- Ensure maximum unscheduled downtime for each critical system does not exceed a total of 4 hours within any period of 12 months

TRM Notice – Obligations (2)

After incident/outages

- Submit a root-cause and impact analysis report (IT Incident Report) within 14 days of the incident/outage.

Implementation of IT controls

- Protection of customer information from unauthorised access or disclosure.

TRM Notice – Penalties (1)

Financial Institution	Legislation	Penalties
Finance Companies	Finance Companies Act	**For companies/directors/managers** • Fine not exceeding $20,000; and/or • Imprisonment not exceeding 3 years
Banks	Banking Act	**For companies** • Fine not exceeding $100,000; and • A further fine of up to $10,000 a day for continuing offences
Merchant Banks	Monetary Authority of Singapore Act	**For companies** • Fine not exceeding $20,000; and • A further fine of S$2,000 a day for continuing offences

TRM Notice – Penalties (2)

Financial Institution	Legislation	Penalties
Insurance Brokers and Insurance Companies	Insurance Act	**For directors/managers** • Fine not exceeding $50,000 or imprisonment not exceeding 2 years; and • A further fine of up to $5,000 per day for continuing offences **For companies** • Fine not exceeding $100,000; and • A further fine of up to S$10,000 per day for continuing offences
Credit Card or Charge Card Licensee	Banking Act	**For companies** • Fine not exceeding $25,000; and • A further fine of up to $2,500 a day for continuing offences

TRM Notice – Penalties (3)

Financial Institution	Legislation	Penalties
Approved Exchanges, Recognised market operators and Designated Clearing Houses	Securities and Futures Act	**For directors/managers** • Fine not exceeding $100,000; and/or • Imprisonment not exceeding 2 years **For companies** • Fine not exceeding $150,000; and • A further fine of $15,000 per day for continuing offences
Holders of CMS License and Trustee of a CIS	Securities and Futures Act	**For directors/managers** Fine not exceeding $100,000; and/or • Imprisonment not exceeding 2 years **For companies** • Fine not exceeding $50,000; and • A further fine of $5,000 per day for continuing offences

TRM Notice – Penalties (4)

Financial Institution	Legislation	Penalties
Remittance Licensees	Money-changing and Remittance Businesses Act	**For companies/directors/managers** • Fine not exceeding $25,000 and/or imprisonment not exceeding 12 months; and • A further fine of $2,500 per day for continuing offences
Operators and Settlement Institutions of Designated Payment Systems	Payment Systems (Oversight) Act	**For companies** • Fine not exceeding $150,000; and • A further fine of $15,000 for continuing offences **For directors/managers** • Fine not exceeding $100,000 and/or imprisonment not exceeding 2 years

Preparing for Compliance

Is compliance required?

- Are you an FI?
- Do you have critical systems?

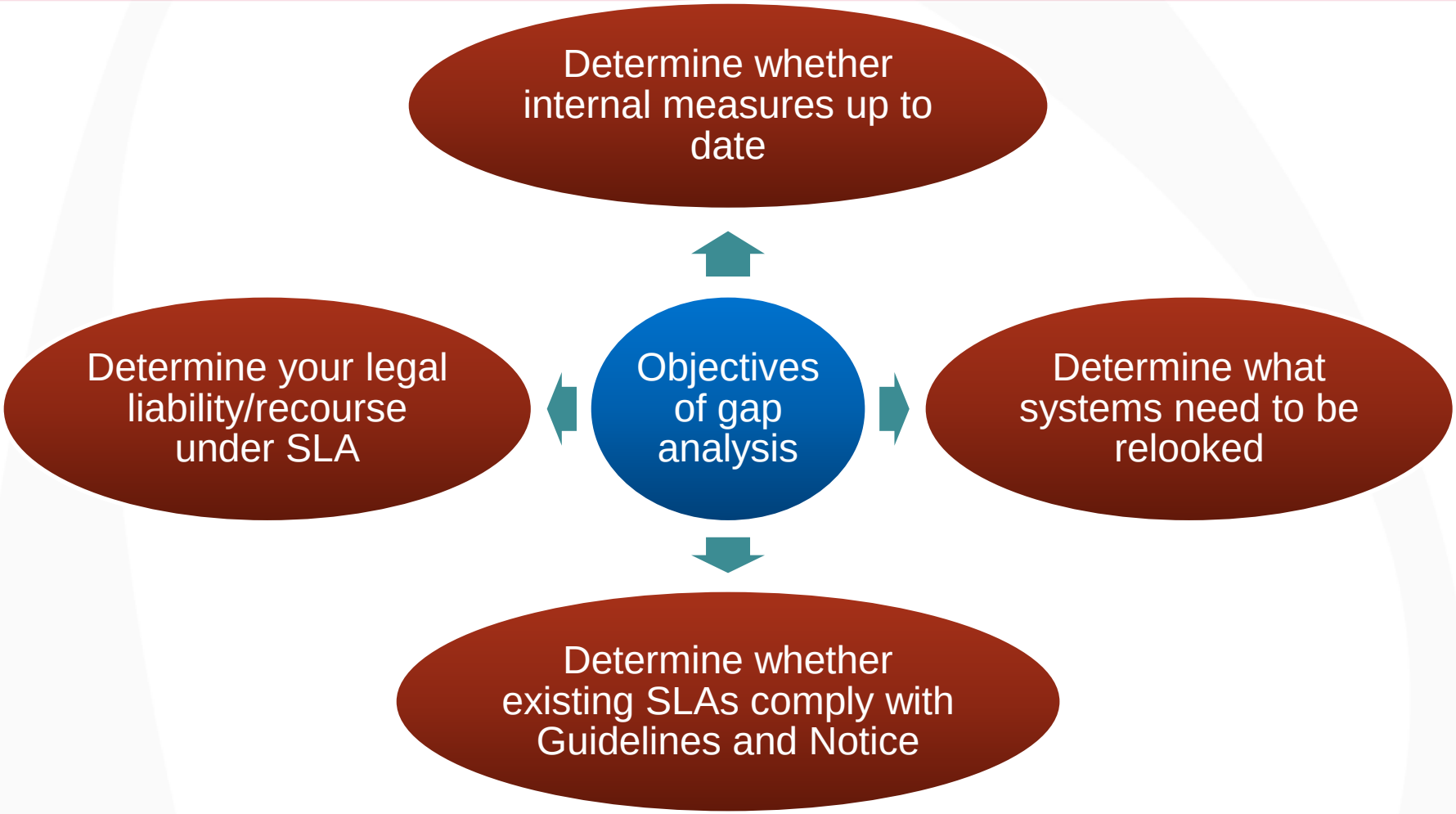
Gap analysis

- Identify existing framework and policies
- Compare with TRM Notice and Guidelines

Action

- Plug gaps through internal resources or engage external assistance

Preparing for Compliance – Gap Analysis



Preparing for Compliance – Action Steps

Create checklist of: • IT related matters which board and senior management must oversee • due diligence for service providers • mandatory contractual terms with service providers
Establish incident preparedness and response team
Establish proper escalation procedures
Critical review and assessment of current systems to ascertain capability to comply with TRM Notice before 1 July 2014
Create action plan for timely compliance
Review existing agreements and SLA with service providers to determine the need to renegotiate to include terms to facilitate compliance
Negotiate for terms to facilitate compliance to be included in future contracts

Q&A

Contact Us

Bryan Tan
bryan.tan@pinsentmasons.com
6305 8490

Rosemary Lee
rosemary.lee@pinsentmasons.com
6305 0912

Pinsent Masons MPillay

For a full list of our locations around the globe please visit our websites:

www.pinsentmasonsmpillay.com

www.Out-Law.com