Technology Risk Management

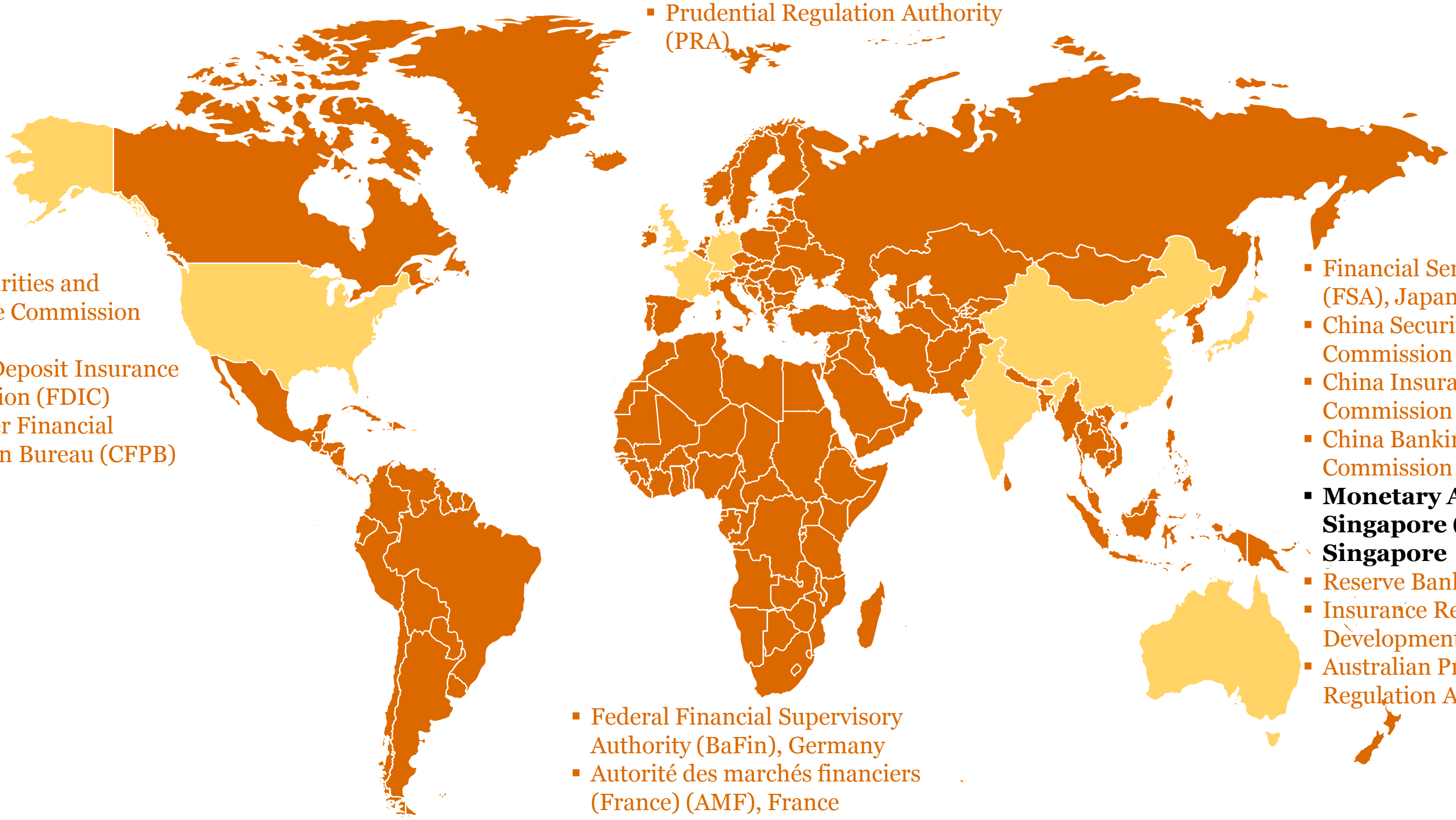
July 2013

Issue 1

Managing technology risk is now a business priority

Global Regulatory Technology Risk Requirements

Regulatory technology risk requirements landscape have changed over the past 3 years



- Financial Conduct Authority (FCA)
- Prudential Regulation Authority (PRA)

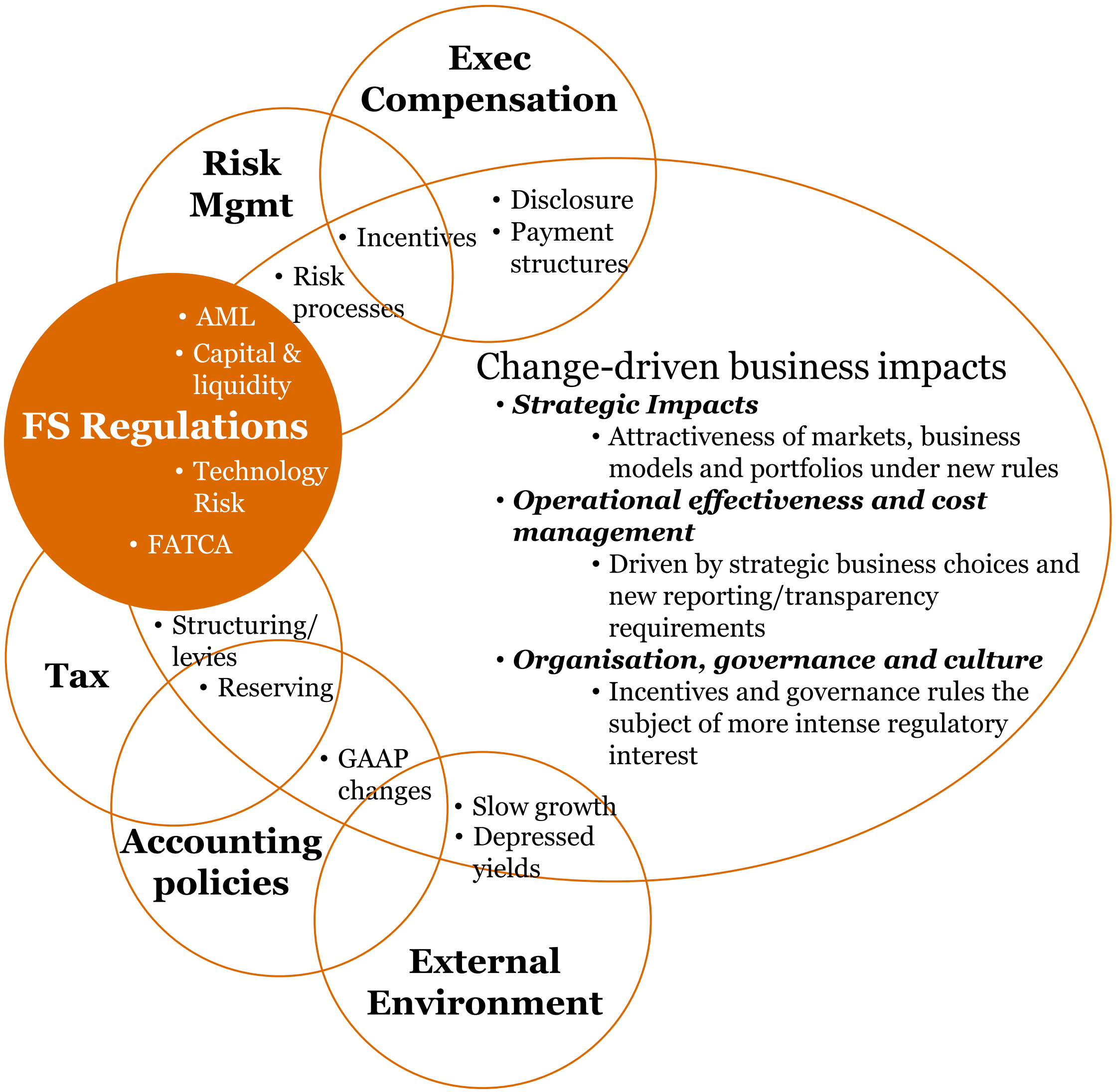
- U.S. Securities and Exchange Commission (SEC)
- Federal Deposit Insurance Corporation (FDIC)
- Consumer Financial Protection Bureau (CFPB)

- Federal Financial Supervisory Authority (BaFin), Germany
- Autorité des marchés financiers (France) (AMF), France
- Swiss Financial Market Supervisory Authority, Switzerland

- Financial Services Agency (FSA), Japan
- China Securities Regulatory Commission (CSRC)
- China Insurance Regulatory Commission (CIRC)
- China Banking Regulatory Commission (CBRC)
- **Monetary Authority of Singapore (MAS), Singapore**
- Reserve Bank of India (RBI)
- Insurance Regulatory and Development Authority (IRDA)
- Australian Prudential Regulation Authority (APRA)

Impact of regulation: Overview

The interplay of new technology risk regulation with other market changes is driving wide-ranging business impacts



Change-driven business impacts

- ***Strategic Impacts***
  - Attractiveness of markets, business models and portfolios under new rules
- ***Operational effectiveness and cost management***
  - Driven by strategic business choices and new reporting/transparency requirements
- ***Organisation, governance and culture***
  - Incentives and governance rules the subject of more intense regulatory interest

MAS Technology Risk Management Notices and Guidelines

The new MAS Technology Risk Management Guidelines (TRMG) have been enhanced to help financial institutions' improve oversight of technology risk management and security practices.

Technology Risk Management Notice and Guidelines

- The Notice and Guidelines were issued on 21 June 2013.
- Notice will be effective on 1 July 2014.
- All 12 notices tied to the Singapore Act and Laws will impact:
  - All Financial Institutions (FIs) (See Appendix for definitions)
  - Includes all IT systems

Non compliance to the Notice can result in:

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

What are the implications of the Notice ?

A FI shall put in place a framework and process to identify critical systems	1	Perform a Business Impact Analysis to identify Critical Systems
Recovery Time Objective (RTO) of ≤ 4 hours for critical systems	2	Test your Disaster Recovery (DR) Plans are robust
A FI shall implement IT controls to protect customer information from unauthorised access or disclosure	3	Encrypt customer data to protect
High availability for critical systems ≤ 4 hours of unscheduled downtime	4	Active: Active infrastructure
Inform MAS of major security incidents, systems malfunction within 60 minutes and submit root cause with 14 days	5	Real time monitoring and reporting procedures

With the new TRM Notice and Guidelines, six grouped areas that impact your business were identified

1
Notice

2
System Availability, Incident and Capacity Management

3
Operational Infrastructure Security and Access Management

4
Development and Change Management

5
Mobile Online Services

6
Others

Notice

Consultation Paper	TRMG 2013
Single Notice	Each type of FI (banks, insurance company, brokers, etc.) is issued one Notice, but the contents is the same.
No Definitions	Redefinition of following terms: ▪ Critical system: Failure of which will cause significant disruption into the operations of the FI or materially impact the FI's service to its customers ▪ System malfunction: failure of any of the FI's critical systems ▪ Relevant incident: System malfunction or IT security incident, which has a severe and widespread impact on the FI's operations or materially impacts the FI's service to its customers
Notification to MAS within 30 minutes for all IT Security Incidents	Notification: no later than 1 hour upon discovery of a relevant incident. Upon discovery refers to after the FIs have ascertained the nature and magnitude of an IT incident meets the criteria set out in the Notice.
Submission of root cause analysis within one month	Root cause analysis changed to: submit within 14 days of discovery. Can request for extension.

"The Notice has clear definitions and are legally binding requirement for FI's"

System Availability, Incident and Capacity Management

Consultation Paper	TRMG 2013
Achieve near zero system downtime for critical systems	Achieve high availability for critical systems.
Public announcement of major incidents should be made in a timely manner	This requirement was removed. Expectation BCP will address this matter.
Conduct quarterly trend analysis	Removal of quarterly trend analysis.
No Requirements	FI should inform MAS as soon as possible in the event that a critical system has failed over to its disaster recovery system.

System Availability, Incident and Capacity Management

Consultation Paper	TRMG 2013
No requirement to encrypt USB disks.	Encrypt USB disks containing sensitive or confidential information before transporting to off-site for storage. The encrypting of sensitive information should be performed on all mediums that are transported off-site.
No requirement for timeframe of review.	Evaluate the recovery plan and incident response procedures at least annually.
No detailed requirements	New requirements: • FI to ensure that indicators such as performance, capacity and utilisation are monitored and reviewed. • FI should establish monitoring processes and implement appropriate thresholds to provide sufficient time for the FI to plan and determine additional resources to meet operational and business requirements effectively.

Operational Infrastructure Security and Access Management

Consultation Paper	TRMG 2013
Implement 2FA for privileged users	Implement strong authentication mechanisms for privileged users.
Quarterly Vulnerability Assessment requirement	Frequency of vulnerability assessment is removed. Expectation to perform annual penetration test is still required.

“Strong authentication on customer and transactional processing”

Development and Change Management

Consultation Paper	TRMG 2013
Only allowed production environment to be connected to the Internet	Non-production environment is now allowed to connect to the internet provided a risk assessment has been performed and appropriate controls are in place.

> ***“Non-production environments can connect to the internet”***

Mobile Online Services

Consultation Paper	TRMG 2013
Transaction-signing for high-risks / high-value transactions	Online financial systems servicing institutional investors, can use alternate controls, if assessed to be equivalent or better than using token-based mechanisms to authorise transaction.
Magnetic stripes were not allowed	If, for interoperability reasons, transactions could only be effected by using information from the magnetic stripe on a card, the FI should ensure that adequate controls are implemented to manage these transactions.

"Magnetic stripes are allowed"

Others

Consultation Paper	TRMG 2013
Archival of cryptographic key	The requirement that cryptographic keys should only be used for a single purpose, and archival of keys has been removed. Expectation a Key Management policy should cover lifecycle of keys.
Reliability and resiliency	Requirement to implement mirrored / parity redundancy for RAID (Redundant Array of Independent Disk), as well as allocation and configuration for hot spares removed.
Requirement for IT Audit to validate and verify issues raised by MAS inspection	Removal of IT audit (IA) requirement. Expectation that IT Audit will review MAS findings. It is good practice for IA to be aware of relevant issues and consider as part of their risk universe.

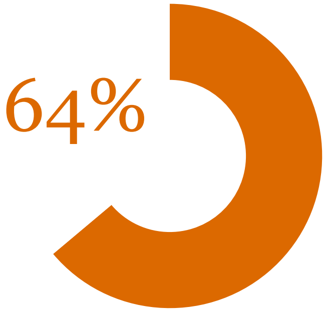
"More areas to focus on"

Others

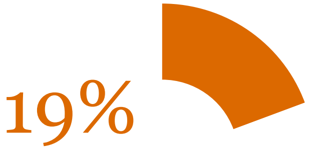
Consultation Paper	TRMG 2013
Requirement for clearing browser cache after online session did not exist	Added one pre-caution that FI should advise the customer to adopt "clear browser cache after the online session“. Expectation this be part of customer awareness.
Onsite visit to Data centres, or service providers should be performed	Removed, good practice would verify data centres and services providers are compliant to IT Outsourcing requirements and MAS TRM guidelines.
Verify the authenticity and integrity of the mobile apps	Removed; but transaction-signing should be implemented for authorising transactions.
PIN should be changed regularly	Added "or when there is any suspicion that it has been compromised or impaired.

"More areas to focus on"

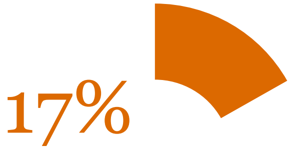
Summary of Gap Analysis between IBTRM (Internet Banking and Technology Risk Management) and the new TRM Notice and Guidelines



New and Enhanced Requirements



No Change in Requirements



Clarifications and Statements Update

Applicable to all financial institutions and include all IT systems (inclusive internet).

System Availability and Incident Management – Impact and Costs

Action Required	Impact			
	Framework	Processes	Systems	Cost
Define critical systems	●	●		L
Critical Systems need to have high availability with ≤ 4 hours of unscheduled downtime	●	●	●	H
Mechanism to monitor downtime		●	May be	M-H
Develop and implement Recovery Plan for Critical Systems (RTO) of ≤ 4 hours. Test & validate annually	●	●	●	H
Develop and implement incident handling process to achieve 1 hr response upon discovery of "relevant incident"	●	●	●	H
Develop and capacity management process	●	●	May be	M-H

Dependency and complexity in involving 3rd party service providers

Legend: L – Low; M – Medium; H- High

Technology Risk Management Guideline vs. IBTRM v3- Themes

1
Technology Risk Management Framework, Roles of Senior Mgmt & Board

2
Enhanced Data Centre Requirements

3
Mobile Online Services

4
Operational Infrastructure Security Management

5
System Availability and Infrastructure Management

6
Others

Technology Risk Management Framework and Role of Senior Management and the Board

Key Requirements	What you need to consider
• Senior management involvement in the IT decision-making process • Implementation of a robust risk management framework • Effective risk register be maintained and risks to be assessed and treated • Implementation of a employee screening process and annual security awareness training	• How is senior management involved in IT decision making and risk management? • Is there an effective governance in place to ensure the board can make informed decisions? • Is there a formalised IT risk management framework in place? • Do employee screening processes include the third parties?

Enhanced Data Centre Requirements

Key Requirements	What you need to consider
• Data centre security should include physical: security guards, card access systems, mantraps and bollards etc.	• Define your data centres and classify the critical systems in scope • The TVRA needs cover all possible scenarios

"A robust Threat and Vulnerability Risk Assessment (TVRA) should be performed on critical systems and data centres"

Mobile Online Services

Key Requirements	What you need to consider
• A security strategy that included the MAS requirements • Identification of fraud scenarios and payment card fraud counter measures on mobile devices • Sensitive data should be encrypted • Customers should be educated on security	• Does your current security strategy encompass mobile banking applications? • Does current risk assessment consider mobile banking fraud, mobile-application? • What is sensitive data? Is information other than authentication-specific information encrypted on the local device?

Operational Infrastructure Security Management

Key Requirements	What you need to consider
• Inventory of software and hardware components and end of support/life (EOS/L) • Baseline standards for security configurations • A robust patch management process • Real-time monitoring of security events • Detection of unauthorised changes to critical systems	• An asset management database that includes critical systems that can be monitored • File and system integrity monitoring • How does your current patch management process classify patches? Do you have a patch management strategy that works? • How are you monitoring your database configuration changes and privileged access?

System Availability and Infrastructure Management

Key Requirements	What you need to consider
• Redundancies for single points of failures (Cross-border) • Recovery time objective (RTO) and recovery point objective (RPO) • Recovery plan and testing • Incident response procedures • Problem management process (root-cause analysis)	• Are you looking at an Active /Active, or Active/Passive service to meet these guidelines and the Notice. (n+1) • Have all critical systems and network components (on and offshore) been included? • Do you have a dedicated CERT and a defined plan for security and major incidents? • How and who will manage the public announcements and disclosure?

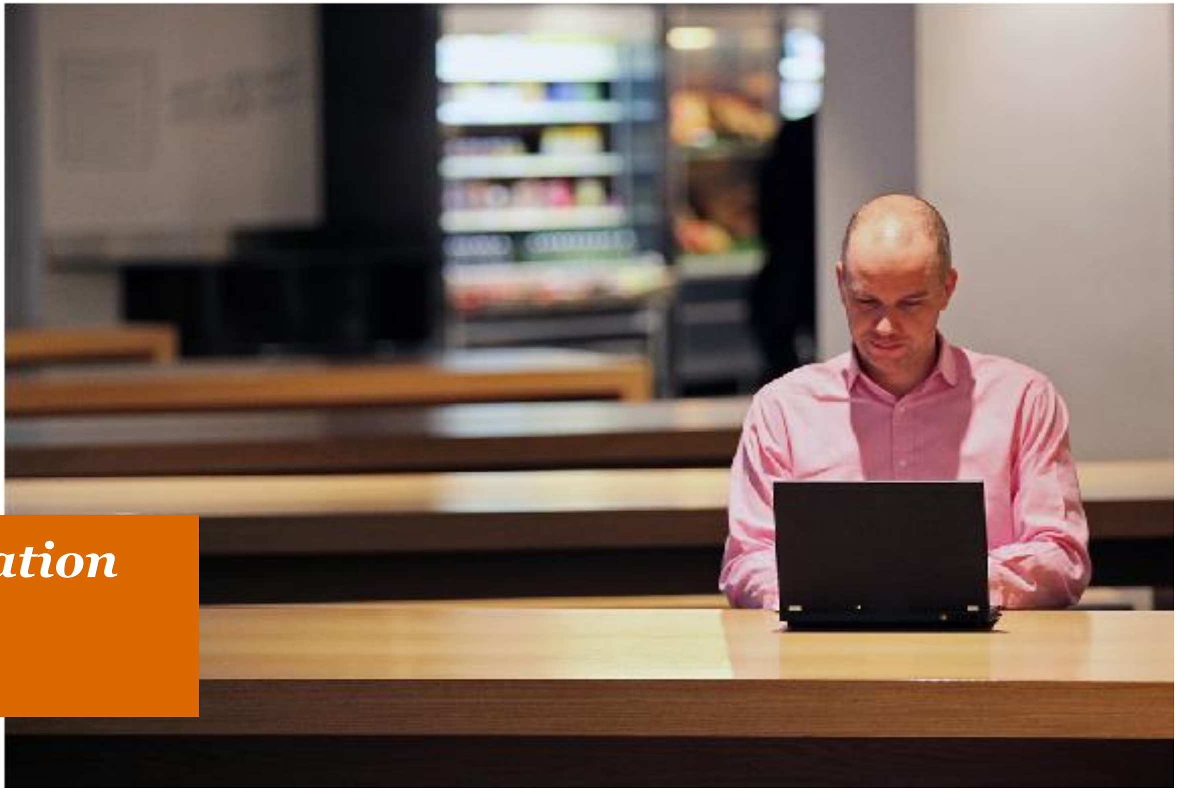
Others - ITSM (Information Technology Service Management) & Acquisition and Development of Information Systems

Key Requirements	What you need to consider
• A robust IT service management framework should be implemented • Problem management trend analysis • A project management framework should be used and established • End user applications should be developed inline with best practices	• Is there a problem management process in place? Are you using Information Technology Infrastructure Library (ITIL)? • How and are you reviewing projects and procurements of systems against the needs of the business post implementation? • Is a cost benefit analysis and business case developed for all system changes? • Do you know what end user tools/spreadsheets/ macros are critical to your business? What was the methodology used to develop these tools?

Others – Payment Card Security

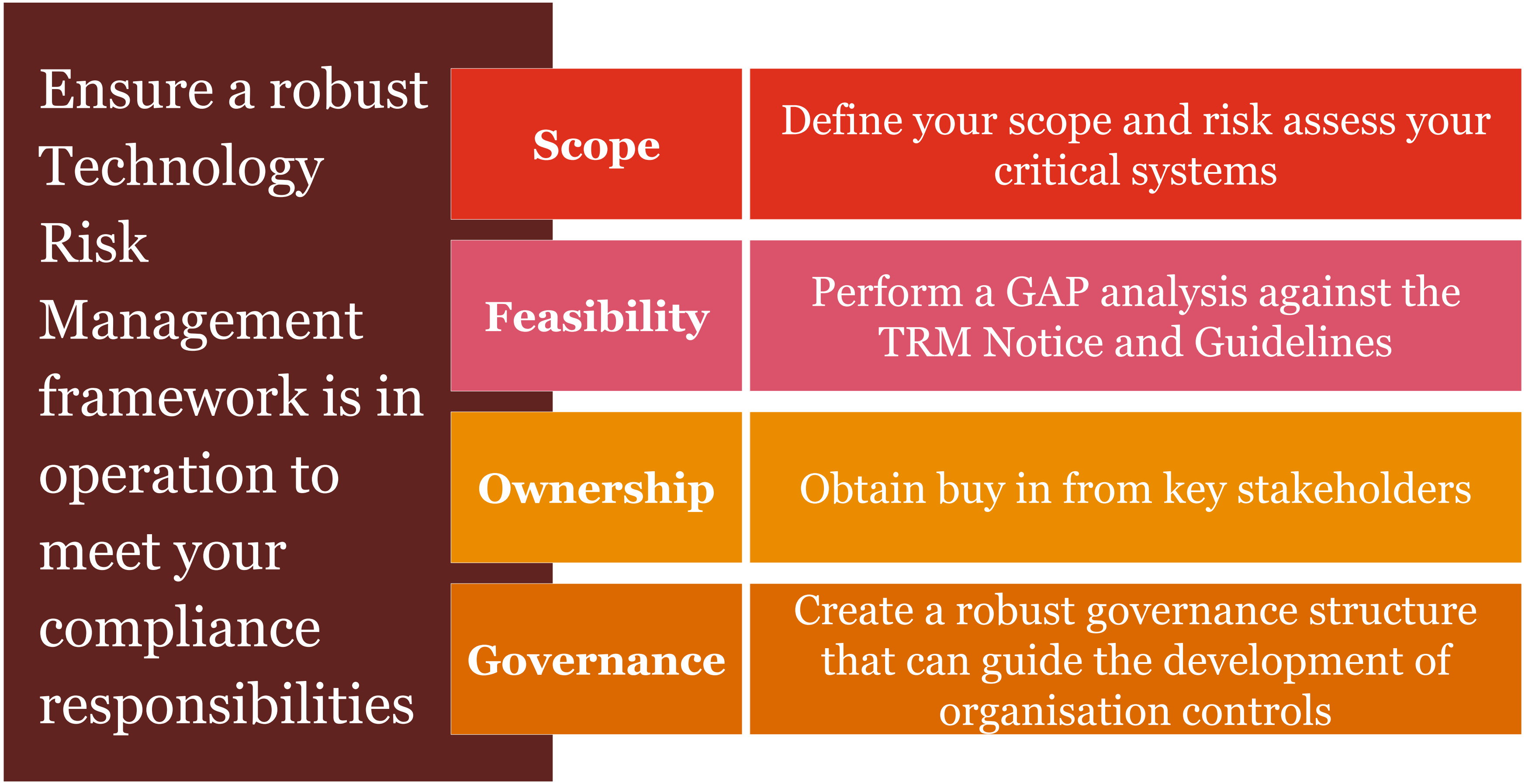
Key Requirements	What you need to consider
• Sensitive payment card data should be encrypted • Secure chips should be deployed to store sensitive payment card • FIs should only allow online transaction authorisation • Implementation of Fraud Detection Systems (FDS) with behavioural scoring	• Where is your payment card data stored? and is the data encrypted when stored and during processing? • Is a FDS in place that uses behavioural scoring?

Competitive intelligence



Our observation of industry practices

What you should consider



Ensure a robust Technology Risk Management framework is in operation to meet your compliance responsibilities

Scope

Define your scope and risk assess your critical systems

Feasibility

Perform a GAP analysis against the TRM Notice and Guidelines

Ownership

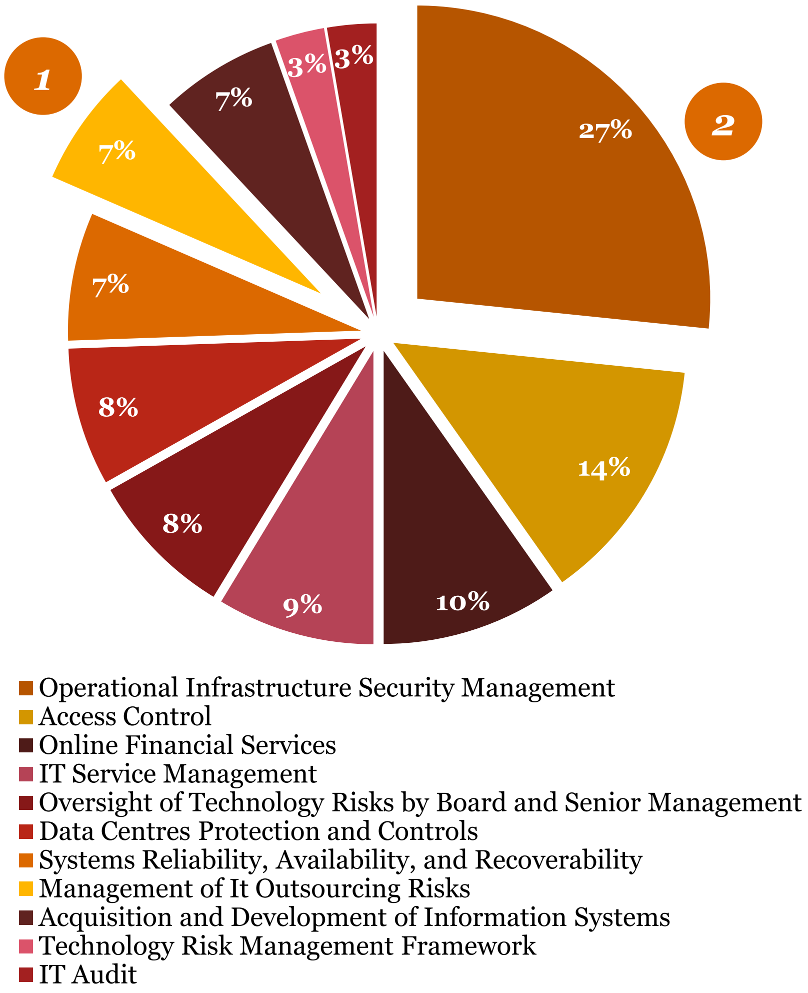
Obtain buy in from key stakeholders

Governance

Create a robust governance structure that can guide the development of organisation controls

Banking benchmarking of issues

Reported Issues by Domain



1

The single most popular issue:

Management of IT Outsourcing Risks, representing 7% of issues reported

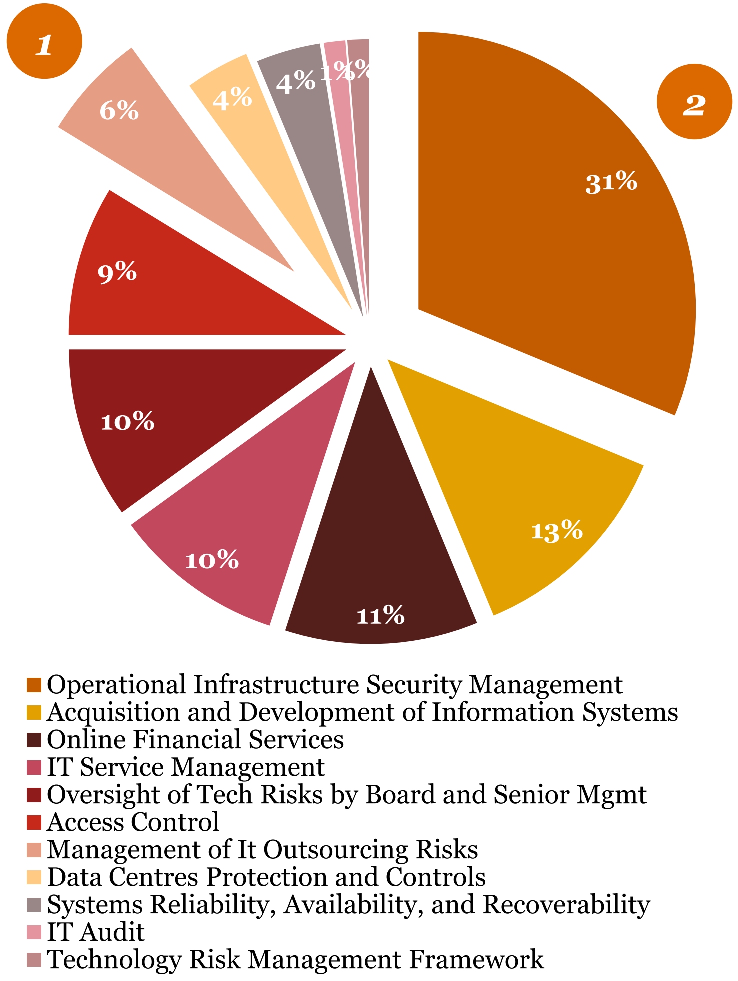
2

Highest number of issues:

Operational Infrastructure Security Management, representing 27% of issues reported

Insurance benchmarking of issues

Reported Issues by Domain



1

The single most popular issue:

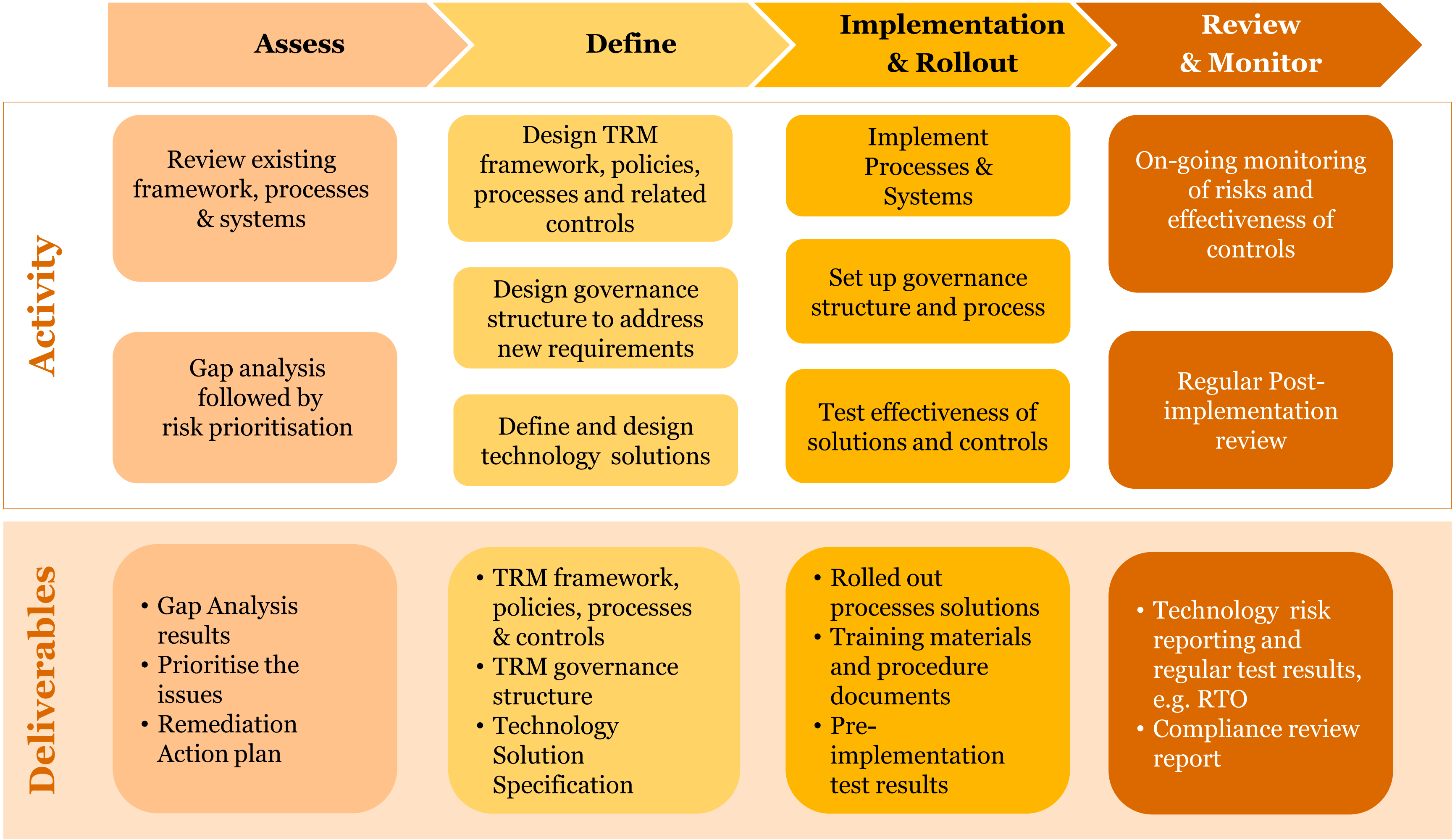
Management of IT Outsourcing Risks, representing 6% of issues reported

2

Highest number of issues:

Operational Infrastructure Security Management, representing 31% of issues reported

PwC’s 4-Step MAS TRM Compliance program



	Assess	Define	Implementation & Rollout	Review & Monitor
Activity	Review existing framework, processes & systems Gap analysis followed by risk prioritisation	Design TRM framework, policies, processes and related controls Design governance structure to address new requirements Define and design technology solutions	Implement Processes & Systems Set up governance structure and process Test effectiveness of solutions and controls	On-going monitoring of risks and effectiveness of controls Regular Post-implementation review
Deliverables	• Gap Analysis results • Prioritise the issues • Remediation Action plan	• TRM framework, policies, processes & controls • TRM governance structure • Technology Solution Specification	• Rolled out processes solutions • Training materials and procedure documents • Pre-implementation test results	• Technology risk reporting and regular test results, e.g. RTO • Compliance review report

Appendix: Case Studies

Case Studies – Onshore banking

Issue

The MAS completed its inspection of Technology and issued a report containing a number of findings.

1. Risk Management of process around critical systems
2. Adhering to 4 hours RTO

Action

PwC were engaged to facilitate the remediation effort:

- understanding the current production environment/ architecture for all critical applications and the business lines supported by those applications
- engaging stakeholders from business, IT, technology risk and operational risks in risk assessment workshops
- identify critical information and technology assets residing in each application and analyse possible consequences that bank may face
- review the design effectiveness of internal controls in place
- assess residual risks and facilitate the discussion with stakeholders on treatment plans if required

Impact

- Assisted all stakeholders to understand their information assets and technology risks.
- Insights on regulations helped the bank making cost-effective decisions
- Strong focus on adherence to budgeted spend has been observed when defining systems that require RTO of 4 hours
- Enabled the bank to report to MAS that it has completed its first round of assessments in a timely manner
- Provided an efficient approach that enables the bank to capture and address risks in a uniform manner

Case Studies – Offshore banking

Issue

The Global bank engaged PwC to perform an assessment to evaluate their Global stance on Technology polices, procedures and controls adherence to APAC regulators, with over 72 issues for Singapore.

Action

To address these , issues, a MAS program was initiated and PwC were engaged to facilitate the remediation effort:

- understanding the current prescriptive changes that can processed for a quick wins
- engaging stakeholders from business, to develop multiple plans to find cost effective solution to especially with global data centre's hosting critical systems for Singapore

Impact

The MAS program provides a great opportunity to make policy changes and innovate with cost effect solutions already used elsewhere in the bank:

- PwC have developed a framework to adhere to future regulatory requirements
- Developed innovate solutions with the banks staff to save cost and become compliant

Appendix: Useful Resources

Useful Resources

The MAS TRM Notice:

http://www.mas.gov.sg/regulations-and-financial-stability/regulations-guidance-and-licensing.aspx?sc_p=2&sc_y=&sc_type=&sc_q=

Useful documents:

- Instructions on Incident Notification and Reporting to MAS
- Incident Report Template
- FAQs – Notice on Technology Risk ManagementGuidelines
- MAS TRM Guidelines

The documents above can be found by following the link below.
http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Technology-Risk.aspx

Definition of Financial Institution

Financial institution has the same meaning as in section 27A(6) of Monetary Authority of Singapore Act (Cap.186).

(a) any bank licensed under the Banking Act (Cap. 19);

(b) any finance company licensed under the Finance Companies Act (Cap. 108);

(c) any person that is approved as a financial institution under section 28; [13/2007 wef 30/06/2007]

(d) any money-changer licensed to conduct money-changing business, or any remitter licensed to conduct remittance business, under the Money-changing and Remittance Businesses Act (Cap. 187);

(e) any insurer registered or regulated under the Insurance Act (Cap. 142);

(f) any insurance intermediary registered or regulated under the Insurance Act;

(g) any licensed financial adviser under the Financial Advisers Act (Cap. 110);

(h) any approved holding company, securities exchange, futures exchange, recognised market operator, designated clearing house or holder of a capital markets services license under the Securities and Futures Act (Cap. 289);

(i) any trustee for a collective investment scheme authorised under section 286 of the Securities and Futures Act, that is approved under that Act;

(j) any trustee-manager of a business trust that is registered under the Business Trusts Act (Cap. 31A);

(k) any licensed trust company under the Trust Companies Act (Cap. 336);

(ka) any holder of a stored value facility under the Payment Systems (Oversight) Act (Cap. 222A); and [42/2007 wef 01/11/2007]

(l) any other person licensed, approved, registered or regulated by the Authority under any written law,

but does not include such person or class of persons as the Authority may, by regulations made under this section, prescribe.

Focus on risk, compliance will follow

Contact us

Tan Shong Ye	shong.ye.tan@sg.pwc.com +65 6236 3262
Mark Jansen	mark.jansen@sg.pwc.com +65 6236 7388
Manish Chawda	manish.chawda@sg.pwc.com +65 6236 7447

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.