New Requirements for Financial Services Industry

Monetary Authority of Singapore
Technology Risk Management
Guidelines & Notices

New Requirements for Financial Services Industry

Mark Ames
Director, Seminar Program
ISACA Singapore
MAS Supervisory Framework

**Supervisory Objectives**
- stable *financial system*;
- safe and sound financial intermediaries;
- safe and efficient *financial infrastructure*;
- fair, efficient and transparent organised markets;
- transparent and fair-dealing intermediaries and offerors; and
- well-informed and *empowered consumers*.

**Impact Assessment**
- Impact on Singapore financial environment if the FI experiences ‘distress’

**Risk Assessment**
- Risk that a financial institution will not meet *supervisory objectives*

**Issues of Supervisory Concern**

**Supervisory Intensity**

**Specific Supervisory Plan**
- ‘Supervisory Requirements’

**Technology Risk Management Guidelines**
From IBTRM to TRM++

MAS TRM Guidelines (recommended best practice)

- Extended from on-line banking services to:
  - All banking financial services
  - Financial advisors and fund managers,
  - Trust companies
  - Money changers
  - Remittance agents and money brokers
  - Insurance providers and brokers
  - Payment systems operators

In effect from 21 June 2013

New Mandatory Requirements- ‘Notices’

- Identify ‘critical systems’
  - High level of reliability, availability, and recoverability of critical IT systems;
- Protect customer information
  - from unauthorised access or disclosure.
- Mandatory Reporting
  - Outages, Security Breaches

These take effect from 1 July 2014
Notices – Identify Critical Systems

• a system, the failure of which will:
  • cause significant **disruption to operations**, or
  • materially **impact service to customers**,

• a system which—
  • (a) processes **transactions that are time critical**; or
  • (b) provides **essential services** to customers;

Organisations are required to **establish a framework and process to identify critical systems** as defined in the Notice and maintain a list of critical systems, if any.

By 1 July 2014
Notices – Unscheduled Outages

• Apply to identified Critical Systems

• Establish a recovery time objective ("RTO") of not more than 4 hours for each critical system.
  • The RTO is the duration of time, from the point of disruption, within which a system must be restored.

• Ensure that maximum unscheduled downtime for each critical system does not exceed a total of 4 hours within any period of 12 months.

• Indications are that MAS expects no more than 4 cumulative hours annually of incidents that result in
  • severe and widespread impact on operations, or
  • material impact on service to customers

• Effective from 1 July 2013.
Notices - Mandatory Reporting

• Unscheduled outages of ‘critical systems’
  • causing significant disruption of services to customers
• Security Incidents
  • Critical Systems
    • hacking, intrusion or denial of service attack
  • All Systems
    • compromise of customer information

• Must be Reported within one hour ‘of discovery’
• Root-cause and impact analysis report within 14 days

Must notify MAS within 1 hour upon the discovery of a system malfunction or IT security incident regardless of when the malfunction or incident occurs.

From 1 July 2014
MAS TRM Guidelines

• Principles and best practice standards focussing on:
  a. Robust technology risk management framework;
  b. System security, reliability, resiliency, and recoverability; and
  c. Strong authentication to protect customer data, transactions and systems.

• Guidelines are *not* legally binding:
  - the degree of observance with the spirit of the Guidelines is *an area of consideration* in the risk assessment of the FI by MAS
MAS TRM expectations

• All financial institutions will address key areas of concern
  • Risk Management
  • Outsourcing
  • Online Services
  • Payment Cards
  • System Acquisition & Development
  • Service Management & Continuity Planning
  • Infrastructure & Data Centre Security
  • Audit, Oversight & Governance

• With special emphasis on:
  • Protecting Customer Information
  • Cryptographic Functions
  • Access Control and Privileged Access
COBIT 5 and TRM

Evaluate, Direct, & Monitor

- Governance Framework
- Deliver Benefits
- Manage Risk
- Optimise Resources
- Stakeholder Transparency

Align, Plan, & Organise

- Management Framework
- Service Management
- Risk Management
- Security Management

Build, Acquire, & Implement

- Project Management
- Requirements Definition
- Build Management
- Change Management
- Asset Management

Deliver, Service, & Support

- Operations Management
- Service Management
- Incident Management
- Continuity Management
- Manage Security Services

Enterprise IT Management Processes

Adapted from COBIT® 5, figure 16. © 2012 ISACA.
Protecting Customer Information

• **Encrypt** customer personal, account and transaction data:
  • stored and processed in systems. (9.0.2)
  • stored in all types of endpoint devices (9.1.3).
  • exchanged with external parties (9.1.5)
  • stored on IT systems, servers and databases (9.1.6)
  • on backup tapes and disks, including USB disks (8.4.4)
  • in storage and transmission within mobile online services and payments. (12.2.4)

Priority!

You should now be identifying gaps and planning remediation as a priority
Protecting Customer Information

- Encrypt customer personal, account and transaction data:
  - stored and processed in systems. (9.0.2)
  - stored in all types of endpoint devices (9.1.3).
  - exchanged with external parties (9.1.5)
  - stored on IT systems, servers and databases (9.1.6)
  - on backup tapes and disks, including USB disks (8.4.4)
  - in storage and transmission within mobile online services and payments. (12.2.4)

Don’t forget the PDPA!
Comes into force in parallel with TRM
Legally binding with penalties for non-compliance

You must know and document where and how you hold Customer personal information

Consolidate customer personal information

You should now be identifying gaps and planning remediation as a priority
Cryptographic Functions

- **Verify** cryptographic implementations
- Use only cryptographic modules based on **authoritative standards** and reputable protocols.
- **Review** cryptographic algorithms and crypto-key configurations for deficiencies and loopholes.
- **Thoroughly assess** ciphers, key sizes, key exchange control protocols, hashing functions and random number generators.
- **Rigorously test:**
  - all **cryptographic operations** (encryption, decryption, hashing, signing) and
  - **key management procedures** (generation, distribution, installation, renewal, revocation and expiry)

Ensure you have access to required expertise
Access Control and Privileged Access

- apply stringent selection criteria and thorough screening
- controls and security practices are unchanged from IBTRM:

  a. Implement strong authentication mechanisms such as two-factor authentication for privileged users;
  b. Institute strong controls over remote access by privileged users;
  c. Restrict the number of privileged users;
  d. Grant privileged access on a “need-to-have” basis;
  e. Maintain audit logging of system activities performed by privileged users;
  f. Disallow privileged users from accessing systems logs in which their activities are being captured;
  g. Review privileged users’ activities on a timely basis;
  h. Prohibit sharing of privileged accounts;
  i. Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and
  j. Protect backup data from unauthorised access.

Enact in policies, standards and procedures. Document controls.
TRM Risk Management Framework

• Establish a technology risk management framework to manage technology risks in a systematic and consistent manner.
  a. Roles and responsibilities in managing technology risks;
  b. Identification and prioritisation of information system assets;
  c. Identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities;
  d. Implementation of appropriate practices and controls to mitigate risks; and
  e. Periodic update and monitoring of risk assessment to include changes in systems, environmental or operating conditions that would affect risk analysis.

• New requirements
  • maintain a risk register
  • develop IT risk metrics and quantify potential impacts and consequences of risks across the business and operations.
TRM Risk Management Framework

- **Risk Measurement:**
  * Likelihood/Probability (of something happening) X
  * Consequences/Impact (of loss or disruption of service)

Example:
Likelihood of Credit Card Management system failing
(based on previous experience and experience in other organisations)
Is once in two years. Annual probability =50%

Impact – average outage two hours:
Lost revenue = $200
Recovery cost = $6,500
Customer complaints = 30 > $100 per complaint to resolve = $3,000
Total Impact = $9,700

**Annualised Risk** = .50 X $9,700 = $4,850

Document accountabilities, processes and actions.
TRM – IT Outsourcing Risks

• Directors and Senior Management are liable
  • For understanding risks and exercising due diligence in entering outsourcing arrangements

• Regulators (e.g. MAS) must have access
  • to outsourced systems and facilities.

• Maintain security of operations

• Thorough Contingency and Recovery Planning
  • Including failure of outsourcing firm

• ‘Cloud Computing’
  • Keep customer data and information assets separate
  • Contractual arrangements to remove/ retrieve data
  • Recovery capability (RTO) consistent with business and regulatory requirements

Apply the same ‘Risk Appetite’ and controls.
TRM – System Development & Acquisition

- All Applications:
  - Apply appropriate security controls based on the type and complexity of services provided.

- Project Management Framework
  - project risk assessment,
  - risk classification,
  - critical success factors
  - Full documentation standards
  - Oversight and monitoring

- Specify Security Requirements
  - access control
  - authentication
  - transaction authorisation
  - data integrity
  - system activity logging
  - audit trails
  - security event tracking
  - exception handling

Develop a standard ‘Controls Library’.
TRM – System Development & Acquisition 2

• Testing
  • Full testing methodology including regression testing
  • Penetration and vulnerability testing
  • Separate environments.

• Source Code Review – Identify:
  • security vulnerabilities and deficiencies,
  • mistakes in system design or functionality

• End User Applications
  • Identify important end-user applications – spreadsheets, macros, scripts, etc
  • Include in recovery and support plans
  • Apply similar reviews as for large applications

Vendors and partners must also comply: Inform them and put in contracts.
TRM – Service Management & Continuity

• Change Management & Migration
  • Fully documented framework including staged approvals and assessment of risks
  • Fall back/roll back planning
  • Synchronisation with backup and recovery environments

• Incident & Problem Management
  • Refer to requirements in Notices regarding Security Incidents
    • Reporting and analysis of ‘Major’ incidents
  • Fully documented framework including
    • Classification of severity – especially for security incidents
    • Escalation and response plans
    • action plan to address public relations issues
  • Establish a computer emergency response team
    • comprising staff within the FI with necessary technical and operational skills to handle major incidents.

Comply with Notices on Incident Reporting as a priority.
TRM – Data Security

Infrastructure Security

• Asset classification and protection
  • Identify important data
  • Implement appropriate controls
  • Protect sensitive information
  • Encrypt sensitive information
    • At end points, in transmission, stored on corporate systems

• Social media, cloud-based storage, and webmail
  • Don’t use to store or communicate sensitive information
  • Prevent and detect the use of such services

Review your communications with customers.
TRM – Technology Management
Infrastructure Security

• System Inventories
  • Hardware, software, and support agreements
  • Production and DR
  • Comprehensive and current

• Security Configuration Management
  • Define & document security settings; regularly review & verify

• Unsupported (Unsupportable) Systems
  • Replace them!
  • Have refresh and life-cycle plans and planning process

Start planning now to create or update
• detailed system inventories,
• configuration standards, and
• refresh plans.
TRM – Network Security
Infrastructure Security

• Configuration Standards
  • Regularly monitor for compliance

• Anti-Virus 🕷️
  • Comprehensive malware detection, prevention, & removal is better!

• Firewalls and IDS
  • At perimeter and to segregate internal trusted networks

• Secure WLANs

• Vulnerability and Penetration Testing
  • Don’t rely on automated tools
  • Demonstrate remediation planning

• Patch Management
  • Change management!

• Security Monitoring
  • real-time monitoring of security events for critical systems

Document your own internal standards supported by risk assessments.
TRM – Data Centre Security

• A digest of current data centre security standards:

  ISO 27001  SAS 70  ETSI
  TIA-942  COBIT 5  European Telecommunication
  Standardization Institute

• Threat Vulnerability Risk Assessment (TVRA) is central
• Monitor Service Providers
• Physical, Logical, and Environmental Controls

Ensure your data centres and service provider data centres meet current international standards

ISACA®
TRM – Online Services

- Manage higher risks associated with on-line services.
- Repeated emphasis on:
  - Security Strategy
  - Data Security
  - Security Requirements
  - Customer Education
  - Security Monitoring
  - Physical and logical access security
  - Two factor authentication
  - Transaction signing
  - Equivalent controls for mobile services
  - Implementation of Cryptography (App C)
  - DDoS countermeasures (App D)
  - Minimise exposure to cyber attacks (App E)

Online services are a key focus and priority for MAS – Make it your focus, too.
TRM – Payment Cards

Applies to card issuers and kiosk operators
Banks, American Express, SAM, AXS, etc.

• Cards and Transactions
  • Chip cards are mandatory
  • Activation controls
  • OTP for CNP
  • Fraud monitoring
  • ‘Deviant’ transactions

• ATMs and Kiosks
  a. Anti-skimming controls
  b. Detection and notification systems
  c. Tamper-resistant keypads
  d. Prevent shoulder surfing
  e. Video surveillance.

Complying with PCI-DSS will address many other MAS TRM areas of concern.
TRM – Internal Audit

- Independent and Objective IT Audit Function
  - Or other governance and oversight structures
- Comprehensive Audit Scope
  - Scope should encompass TRM areas of coverage
- Annual IT Audit Plan
  - Priority on high risk areas
- Track and Monitor IT Audit Issues
  - Fund and support remediation programs

Integrate internal audit with other GRC activities to demonstrate that you can and will meet ‘supervisory objectives’.
TRM – Appendices

A: SYSTEMS SECURITY TESTING AND SOURCE CODE REVIEW
B: STORAGE SYSTEM RESILIENCY
C: CRYPTOGRAPHY
D: DISTRIBUTED DENIAL-OF-SERVICE PROTECTION
E: SECURITY MEASURES FOR ONLINE SYSTEMS
F: CUSTOMER PROTECTION AND EDUCATION

The devil is in the detail:
These specify key details of MAS ‘supervisory objectives’.
COBIT 5 and TRM

Evaluate, Direct, & Monitor

- Governance Framework
- Deliver Benefits
- Manage Risk
- Optimise Resources
- Stakeholder Transparency

Align, Plan, & Organise

- Management Framework
- Service Management
- Risk Management
- Security Management

Build, Acquire, & Implement

- Project Management
- Requirements Definition
- Build Management
- Change Management
- Asset Management

Deliver, Service, & Support

- Operations Management
- Service Management
- Incident Management
- Continuity Management
- Manage Security Services

Enterprise IT Management Processes

Adapted from COBIT® 5, figure 16. © 2012 ISACA.
COBIT 5 and Risk Framework

Two Perspectives on Risk

Risk Function Perspective
- The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

Risk Management Perspective
- The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

MAS Technology Risk Management Guidelines

MAS Supervisory Objectives
THANK YOU

Mark Ames, CISA, CISM, CRISC
Director Seminar Program
ISACA Singapore
program.seminar@isaca.org.sg