GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Implementing and Auditing CIS Controls (Security 566)"
at http://www.giac.org/registration/gccc

Practical Considerations on IT Outsourcing Implementation under the Monetary Authority of Singapore's Technology Risk Management Guidelines

GIAC (GCCC) Gold Certification

Author: Andre Shori, AShori@mastersprogram.sans.edu

Advisor: Dr. Stephen Northcutt

Accepted: 1 July 2016

Abstract

Singapore ranks third overall in the Global Financial Centres Index. The Monetary Authority of Singapore (MAS), Singapore's central bank, has helped to achieve this success through guidance and regulation of the financial industry including how to conduct themselves in a secure and reliable manner. The Technology Risk Management Guidelines (TRM) are both a cyber philosophy and a set of regulatory requirements for financial institutions to address existing and emerging technological risks. However, successful implementation of TRM can be challenging from a practical standpoint for today's Cybersecurity Managers. TRM's Management of IT Outsourcing Risk is a key focus area which encompasses many of the principles and requirements promoted throughout the Guideline. By utilizing threat based, hierarchical measures such as those advocated by the Centre of Internet Security, Cybersecurity Managers can adhere to the Spirit of the Guidelines while implementing effective operational cybersecurity and safe Vendor integration.

1. Introduction

In 2016 the Global Financial Centres Index honored Singapore with Asia's top spot, globally trailing only London and New York as a financial center. The Monetary Authority of Singapore (MAS), Singapore's central bank, has helped to achieve this success through guidance and regulation of the financial industry including how to conduct themselves in a secure and reliable manner. The Technology Risk Management (TRM) Guidelines (*Technology Risk Management*, 2013)[i] are regulatory requirements for financial institutions such as Banks or Insurance companies to address existing and emerging technological risks associated with a wide variety of areas such as Mobile Payment, IT Service Management and more.

1.1 TRM Components

Effective 1 July 2014, MAS expanded their Technology Risk Management legislation of Banks to include all licensed financial institutions (FI) in Singapore and consolidated these into one single repository. FIs now covered under TRM include such sectors as Commercial and Merchant Banks, Financial Advisors, Insurers, Brokers, Finance Companies, Credit Cards and Payment Systems (NETS, mobile wallets). Although termed principally as a "guideline" and not a standard, it would be a mistake to conclude that TRM is a stand-alone best practice document. TRM enforcement primarily entails four key MAS regulatory instruments in its distribution: Notices, Guidelines, Circulars, and Acts (*Regulatory Instruments Issued by MAS*, 2012)[ii]. Acts denote Statutory Laws passed by the Singapore Parliament (such as the Banking Act) and are the umbrella structure under which TRM operates. Similarly, Notices or Directions are the detailed specific instructions to FIs to ensure compliance and are likewise legally binding. Violators of any of these are subject to substantial penalties incurred including fines, civil or criminal prosecution or FI license revocation. In contrast, Guidelines are, at first glance, "non-legal, best practice standards" and Circulars are privately or publicly published documents and also have no legal effect in and of itself.

Cybersecurity Managers (CM) must understand that TRM is MAS's current major legal, technological and advisory upgrade. Despite being labeled "non-legal", CMs should take TRM in its entirety. TRM exists to ensure that "reliability, availability and recoverability of critical IT systems" is preserved and "safeguarding and protection of customer information from

unauthorized access or disclosure" is maintained (*Technology Risk Management*, 2013)[i]. FIs must be to be ready to demonstrate to MAS that all possible attention is paid to addressing TRM fundamental principles. MAS may require additional measures to be taken by an institution, or MAS itself may take any appropriate supervisory actions it deems necessary if not satisfied with an FI's observance of the TRM. CMs would do well to keep in mind that when a breach or outage occurs or for audit purposes, MAS will use TRM as part of the overall risk assessment of the FI.

It is essential that CMs understand that TRM is presented as a holistic philosophy and practical guideline, backed by Acts of Parliament. All MAS licensees must give it due consideration or risk punitive measures as outlined here. TRM is not presented as a legally required compliance checklist, and CMs should be clear that implementation of TRM is for more than legal requirements. TRM is a guideline to all FIs, cleverly written to give some flexibility and autonomy in choosing the methods and techniques to achieve TRM's primary goals.

While TRM provides cyber philosophy, practical implementation strategy dictates utilizing a hierarchical and threat based, consensus security control. Measures such as the Centre for Internet Security's Controls for Effective Cyber Defence (Controls) can be tweaked by CMs for effective TRM deployments. A mapping of the CIS controls (v6.0f) to TRM, which may prove useful, can be requested at info@enclavesecurity.com, and a mapping of the Controls as outlined in this paper related to outsourcing are delineated in Appendix A.

1.2 Management of IT Outsourcing Risks

TRM consists of 14 primary subsections, each covering cybersecurity areas such as IT Service Management, Data Centre Protection and Controls, Access Controls and more. The Guidelines encompasses a variety of fields too diverse to adequately cover the entire influence it has on Enterprise-wide cybersecurity controls within this paper.

By tactically focusing on the Management of IT Outsourcing Risks, this document:

1. Allows examination of most of the key areas and principles that TRM advocates because most TRM subsections are touched on when entering into an outsourcing arrangement; and

2. Serves as a repository and unified advisory for CM's pre, during and post implementation of Outsourced arrangements.

1.3 Provisos

1. This paper assumes the reader has a working knowledge of the Centre for Internet Security's Critical Security Controls for Effective Cyber Defence (Critical Controls) (Center for Internet Security Critical Security Controls for Effective Cyber Defense, n.d.)[iii]. Detailed discussions of the Controls is outside the scope of this paper and is covered in other papers. SANS Institute has an excellent Whitepaper (*Heitala*, 2013)[iv] detailing the Controls and their implementation, and readers are strongly encouraged to read that first if the Controls are new to them;
2. In the course of the discussion on the impact of TRM on an FI's cyber defense strategies, it is also assumed that FIs already incorporate the 20 Controls and other related ancillary disciplines including Critical Governance Controls;
3. Unless otherwise specifically mentioned, in this paper the term "CM" references the office of the Senior Management or Board level appointee that leads the organization's cybersecurity efforts such as a CISO and his or her staff.

2. Outsourcing Arrangements: Definition and Significance

MAS does recognize the importance of Vendor relationships and technologically focused products and services provided to FIs as part of their overall business strategies (such as lower cost of operations, greater competitiveness or increased efficiency) and the associated risks of these arrangements. In a consultation paper titled "Guidelines on Outsourcing" (*Guidelines on Outsourcing*, 2014)[v], MAS identified rising prominence and costs related to cybersecurity incidents as areas of immediate concern. Engaging in any outsourcing relationship with a Vendor brings with it increased reputation, compliance, and operational risk complications, particularly those arising from failure by Vendors in providing the service or product, security breaches or inability to comply with legal and regulatory requirements.

MAS provides clear definitions of what they define constitute an outsourcing relationship. MAS states "an outsourcing agreement [is] a written agreement setting out the contractual terms and conditions governing relationships, functions, obligations, responsibilities,

rights and expectations of the contracting parties in an outsourcing arrangement." Such outsourcing arrangements are "arrangement[s] in which a service provider provides the institution with a service that may currently or potentially be performed by the institution itself" (*Guidelines on Outsourcing*, 2014)[v]. TRM also extends retroactively to existing outsourcing contracts and subjects these to the same requirements as outlined in section 5 of TRM.

Per MAS, outsourcing relationships include the following characteristics:

a. "the institution is dependent on the service on an ongoing basis, but such service excludes services that involve the provision of a finished product (e.g. insurance policies)" (*Guidelines on Outsourcing*, 2014)[v]; and
b. "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" (*Guidelines on Outsourcing*, 2014)[v].

MAS also includes service providers (including subcontractors) located outside of Singapore, so long as they provide products or services impacting Singapore operations or customers.

Examples of outsourced relationships include IT systems management and maintenance, middle or back office operations, BCP/DRP, Cloud, Investment Management, Policy Issuance, Claims Administration, general HR functions, Data Archival services and so on. Services exempt from TRM jurisdiction are general operations such as Postal, Telecommunications (Phone, not Internet-based), Utilities, Insurance Policy Sales Agents or Legal engagement.

It is, therefore, essential that FIs adopt sound and responsive risk management frameworks for all outsourcing arrangements. MAS places the responsibility for scrutiny, and careful implementation of these solutions squarely on the Board of Directors and proper explanation of this vetting must be documented and presented upon request.

2.1 Critical Systems

FIs must also be able to demonstrate that higher regimes of security and protection exist for infrastructure components deemed critical in nature. MAS defines a "Critical System" as "[any] system, the failure of which will cause significant disruption to the operations of the FI or

materially impact the FI's service to its customers". These include "systems which process transactions that are time critical, or provide essential services to customers" (*Response to Feedback Received – Consultation Paper on the Notice on Technology Risk Management*, 2012)[vi]. Some MAS-provided examples of "Critical Systems" include Automated Teller Machine (ATM) systems, online banking systems, and systems which support payment *(Frequently Asked Questions: Notice on Technology Risk Management, n.d.)*[vii]. FIs must identify and classify all systems contained in their IT infrastructure (Controls One – Inventory of Authorized and Unauthorized Devices and Control Two – Inventory of Authorized and Unauthorized Software) to maintain and suitably protect them including those in which an outsourcing arrangement could have potential impact.

2.2 Material Outsourcing Arrangements

MAS defines two different types of outsourcing arrangements. Any outsourcing arrangement which, in the event of a service failure or security breach, has the potential to:

a. materially impact an institution's business operations, reputation or profitability or adversely affect an institution's ability to manage risk and comply with applicable laws and regulations; or
b. which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may materially impact an institution's customers;

is defined by MAS as a "Material Outsourcing Arrangement" (*Draft Notice on Outsourcing*, 2014)[viii]. CMs should note that any outsourcing arrangement that could impact a critical system or personally identifiable information (PII) is certain to be categorized as a Material Outsourcing Arrangement. All Material Outsourcing Arrangements must be reported to MAS before commencement, generally in the form of a detailed questionnaire justifying the necessity and nature of the partnership. MAS treats these relationships seriously, and CMs should expect the greatest amount of scrutiny on these types of outsourced relationships.

3. Due Diligence

The FI's Board of Directors ("the Board") and its CMs are held directly accountable for the oversight of technology risks and cybersecurity. Before the onset of any outsourcing arrangement, Sections 5.1.1 - 5.1.10 of TRM mandates adequate due diligence, and close examination of the ramifications of any outsourcing arrangements be conducted. It is critical for the Board and Senior Management to demonstrate that they understand the full impact and potential consequences of outsourcing. Through a program of Executive Sponsorship, the Board must develop Information Assurance Charters with Roles and Responsibilities defined, establish appropriate steering committees and create a schedule of Board of Director briefings. The Board is also responsible for ensuring "an appropriate accountability structure and organisational risk culture is in place to support effective implementation of the organisation's Cyber resilience programme." (Ho, 2015) [ix].

FIs need to plan, manage and deploy any outsourcing into their infrastructure in such a manner as to not weaken or compromise internal controls. The FI's Board must formally endorse IT cybersecurity strategies and risk tolerances while ensuring that enough management focus, expertise, and resources are brought to bear. An extensive security risk assessment must be made by the FI's CMs and presented for Board approval. One benefit of such close examination is these CMs will gain a deeper understanding of actual maintenance and operational costs of outsourcing arrangements. This analysis may also help the Board in making an informed build or buy decision before entering into contracts with Vendors.

3.1 Cybersecurity Training

To help gain Board level approvals and to assist the Board in obtaining a deeper understanding of additional cybersecurity risks in an outsource arrangement, adequate cybersecurity education must be provided. The Board must be able to demonstrate sufficient familiarity with Information Technology and cyber risk, acquired through Board level training programs (Control 17 – Security Skills Assessment and Appropriate Training to Fill Gaps). The goal of any such program should be to "help equip the Board with the requisite knowledge to exercise its oversight function competently and appraise the adequacy and effectiveness of the FI's overall cyber resilience programme" (Ho, 2015) [viii]. Board level training must be prioritized

within the organization because Board level decisions and backing are keys to an effective cybersecurity policy. This training must be tailored to the FI's Business and Infrastructure, and adapted to the current cybersecurity knowledge levels of the individual Board members.

3.2 Additional Regulations

TRM is not the be-all, end-all for technological risk regulation impacting FIs and their Vendors. Other regulations are still enforceable and in some cases, may override or complement TRM. For example, where a Vendor is engaged to supply ATM hardware or Credit Card payment, PCIDSS would apply. In all types of systems that incorporate Personally Identifiable Information (PII) of the FI's customers, the Personal Data Protection Act 2012 (PDPA) (*Personal Data Protection Act Overview*, 2016)[x] also applies. All other underlying statutes and laws are applicable and unless accompanied by specific language in another Act or detailed in a TRM notice, are not superseded by TRM. FIs must understand the full gamut of all legal implications and relevant statutes when engaging a Vendor. It is recommended that Legal Counsel be engaged to ensure that all impacts are discovered, examined and incorporated. MAS views Vendors and their "parent" FIs as single entities. As the licensee, the responsibility then falls to the FI to ensure that Vendors also follow all pertinent legal statutes. No longer will a catch-all one paragraph stating "[Vendor] will be responsible for ensuring that all applicable legally binding statutes are adhered to in the provision of [service]" be sufficient.

4. Alignment with Operational Cybersecurity Frameworks

Vendors need to be aware right from the get-go that they are subject to audit both individually and/or together with the FI. All Vendors are also subject to the same practices and principles that govern the FI and is auditable as part of the same ecosystem. Section 5.1.3 of TRM indicates that all contractual agreements with Vendors must include clauses that recognize the authority of MAS to perform assessments on the service provider itself. This Vendor availability for audit holds especially true when the product or service provided is a Material Outsourcing Arrangement. Before entering into any outsourced contract with a Vendor, FIs must strive to work closely with Vendors to ensure that they understand all legal requirements incurred as a result of this arrangement.

Consultation partners such as PWC suggest the creation of a separate risk-based framework for outsourcing arrangements and create service metrics, KPI's and reporting for outsourced arrangements (PWC, 2013)[xii]. It should be noted however that in the spirit of TRM, MAS does not appear to place a high amount of differentiation between the products and services of an outsourced partner and the primary goods and services of the FI.

MAS, in fact, requires that all Vendors undergo the same vetting that the FI's infrastructure undergoes. TRM section 5.1.4 clearly states that engaging a Vendor must result in the same level of internal controls as the FI especially in regards to data confidentiality and security (Control 13 – Data Protection and Control 14 – Controlled Access Based on the Need to Know). Therefore an improved goal would be the full integration of the Vendors day to day performance into the FI's controls.

CMs must track Vendor KPI's and SLA's as part of their service metrics and include these in Security Dashboards or reporting tools to the Board. If possible, Vendors should also provide logs compliant with Security Content Automation Protocol (SCAP) (Control Six – Maintenance, Monitoring, and Analysis of Audit Logs).

4.1 Business Continuity & Disaster Recovery Planning

All Vendors must be included in Business Continuity or Disaster Recovery Planning (BCP/DRP), and BCP/DRP plans must take into account factors unique to these arrangements. Vendor Roles and Responsibilities must be clearly established, documented and included in all incident handling processes. Additionally, Vendor specific contact information must be made available for use during an incident.

These plans must be updated regularly (recommended annually at a minimum, more often for Material Outsourcing Arrangements) and tabletop exercises conducted that include Vendor participation as part of routine scenario testing. Vendor participation is mandatory under TRM, and Vendors involvement in such exercises must be clearly defined in the outsourcing contract and included as part of the Vendors performance metrics and SLA's.

TRM mandates the recovery time objective to restore any Critical System to its last known good state as four hours. The maximum total unscheduled downtime in a 12 month period

cannot exceed a total of four hours. FIs must also ensure that MAS's (challenging) incident reporting requirements are met, specifically that:

1. FIs are required to notify MAS no later than one hour after an incident is discovered; and
2. Root cause analysis (utilizing their incident report template) must be submitted to MAS within 14 days from the discovery of the relevant incident (*Technology Risk Management Guidelines*, 2016)[i].

Vendor's contribution and performance during BCP/DRP exercises must be assessed, documented, and reported at the Board level as part of the FI's technological and infrastructure health.

MAS may also assess a Vendor directly to ensure support capabilities during incidents such that there is minimal impact to FI operations. These expectations must be established and included as a standard clause in all outsourcing contracts.

CMs must ensure that tight integration between Vendor's data backup schema and the FI's BCP/DRP strategy exists (Control 10 - Data Recovery Capability). Either party may assume full responsibility or better yet, a coordinated and complementary backup system between both companies be put in place. Regular testing of the backup media and data restoration must be included in BCP/DRP planning and testing.

TRM also dictates that FI's BCP/DRP plans contain contingencies that include "worst case scenario" testing. If a Vendor is unable to recover from a service disruption, viable alternatives must be available for Vendor replacement such that any downtime is minimized. These alternate arrangements must be in place at all times and maintained as a standby.

All BCP/DRP measures must be documented and available on demand at all times for TRM reporting, incident root cause analysis and part of an annual audit.

4.2 Data Loss Prevention

Data, particularly that which contains private and confidential information, is classified by MAS as one of the core principle items warranting special care and protection. Under Section 5.1.4 of the TRM, MAS reminds CMs to "employ a high standard of care and diligence…to

protect the confidentiality and security of its sensitive or confidential information…" (*Technology Risk Management Guidelines*, 2016)[i]. Based on classification levels defined by identified data owners, all restricted information must be encrypted whenever transmitted over less-trusted networks (such as between Vendors and FI's networks). Depending on the exact nature of the outsourced relationship, a high level of trust may be necessitated. CMs must ensure that Vendors are provided only necessary data access to deliver their functions in a safe and secure manner (Control 14 – Controlled Access Based on the Need to Know and Control 18 – Application Software Security). Wherever practical, ACL's, network segmentation, Database hardening, and VLANs must be utilized, and all sensitive information must be encrypted whether during transit, at rest or while stored. DLP solutions must be used to ensure that no unauthorized or unrecorded data exfiltration takes place.

4.3 Cloud Computing

MAS has made it clear that Cloud Computing warrants additional scrutiny and risk management due to additional Cloud specific characteristics. MAS places particular attention to Cloud Computing and devotes an entire section (Section 5.2) of TRM to this area. As part of due diligence on Cloud service Vendors, an FI's Board and Senior Management must demonstrate a thorough understanding of all Cloud computing's additional risk attributes. TRM section 5.2.2 details these to include "platform multi-tenancy, data commingling, data integrity, data sovereignty, data confidentiality, data loss prevention, availability and recoverability and data offshoring" (*Technology Risk Management Guidelines*, 2016)[i]. Cloud architecture also includes Software as a Service (SAAS), Platform as a Service (PAAS) or Infrastructure as a Service (IAAS). These may be deployed in a public, private or hybrid service model.

Cloud Vendors will need to work with their FIs to furnish information of its activities including an appropriate inventory of devices they utilize and secure (Control One – Inventory of Authorized and Unauthorized Devices; Control Two – Inventory of Authorized and Unauthorized Software; and Control Three – Secure Configuration for Hardware and Software). Vendors must also demonstrate their ability to limit access to Cloud Administration (Control Five – Controlled Use of Administrative Privileges) and their DLP and Data Recovery Capability (Control 10 - Data Recovery Capability and Control 14 – Controlled Access Based

on the Need to Know). Continuous Online Vulnerability Scanning must be performed and documented (Control Four).

When utilizing SAAS, CMs and the Vendor must also demonstrate that regular Application Code Reviews are performed, and Patch Management is contractually integrated with the FI's change management system. (Control 18 – Application Software Security).

Cloud services and platforms are online and frequently Internet-based therefore, attention must be made to the Secure Configuration for Network Devices (Control 11) of Vendors and FI's respective ISP's.

FI's CMs and their Board must be able to demonstrate to MAS prior to commencement of such an arrangement, that all risk mitigation including Cloud specific risk characteristics and infrastructure has been discussed, prepared for and in place. For FIs that already have existing cloud-based solutions or relationships, these contracts and operations will need to be re-evaluated for TRM readiness. As with all outsourced arrangements, in the case of a Material Outsourcing Arrangement, MAS requires written notification before commencement.

4.4 Cyber Hygiene and Cybersecurity Control

Vendors must be assessed to ensure good cyber hygiene practices and be able to provide evidence of such to the FI and MAS (such as summary results of internal audits or logs to be integrated into the FI's Security Information and Event Management system (SIEM)). Access to FI's infrastructure should be limited and controlled as much as possible and 2FA utilized wherever possible (Control Five – Controlled Use of Administrative Privileges). Dedicated terminals with limited functionality for Vendor access to these systems should be deployed.

Dedicated Workstations, Servers, Mobile Devices or any Access Points (AP's) must be locked down and not used for general web browsing or email access. Any systems Vendors introduce into the FI's network must meet secure configuration standards (Control Three – Secure Configurations for Hardware and Software and Control Seven – Email and Web Browser Protection). If such access is required, then the Vendor must follow security standards defined by the FI. Anti-virus, anti-spyware, host, and network-based firewalls, IDS, and IPS functionality should be standard on all Vendor supplied equipment (Control 8 - Malware Defenses) and must be contractually required on all Vendor's equipment.

CMs must understand and fully realize the implications of Vendor supplied services and products on network boundaries (Control 12 - Boundary Defence). Vendor supplied devices may represent a new boundary for the FI and must be integrated into the FI's overall network defense strategy. Deployments that include Mobile Applications may result in situations where boundaries may become fluid and transient. CMs must take demonstrable and documented approved measures to ensure the sanctity of network boundaries.

Vendors systems must also be included in ongoing vulnerability assessments and penetration testing (Control 20- Penetration Testing and Red Team Exercises) and as outlined in Section 9.4 of the TRM.

4.5 Outsourcing Relationship Termination

CMs should keep in mind that all good things must come to an end. MAS mandates that FIs prepare for and execute appropriate security measures when outsourcing contracts are terminated. Under TRM section 5.2.4, in the event of an outsourcing arrangement ending due to its natural conclusion or prematurely, the FI is obligated to "promptly remove or destroy data stored at the service providers systems and backups" (*Technology Risk Management Guidelines*, 2016)[i]. Control 13 – Data Protection and Control 14 – Controlled Access Based on the Need to Know are helpful in ensuring a practical means to achieve this.

As a best practice, CMs should also ensure that all Vendor access to their infrastructure and operations are terminated (Control Five – Controlled Use of Administrative Privilege and Control 16 – Account Monitoring) and that proper verification of this is performed, documented and signed off by Senior Management and the Board.

5. TRM Improvement

As demonstrated in this paper, guidelines like TRM provide insight into areas of top concern and what the Regulatory Agency want FI CMs to focus on. TRM takes things a step further by placing the responsibility of solid cybersecurity practices under the direct ownership and personal liability of FIs' top leadership i.e. the CEO. MAS allows the flexibility to create their cybersecurity plans and procedures by having chosen to utilize a guideline instead of a compliance document, so long as the FIs can address MAS's top-level priorities. However, TRM

is also a legal framework inasmuch as it is a best practice document and this has further implications as a result. MAS has the legal right to audit any of its licensees' operations and to penalize organizations and individuals or revoke the FIs license if deemed to be not meeting MAS principles.

It must be noted that this paper is in no way a criticism of the entire TRM. TRM is an absolute step in the right direction, and this article has explored cybersecurity governance and operational best practices that are encompassed within it. However, failure to meet TRM can have severe repercussions for FIs, but meeting TRM standards is not an easy task for CMs and Boards to accomplish due to a current lack of clarity and available information.

5.1 Measurements

TRM is full of general assertions such as "[t]he board and senior management should fully understand risks associated with IT outsourcing" or "IT Outsourcing should not result in weakening or degradation of the FI's internal controls..". Especially large blanket statements such as the one under section 4.0.1, "[a] technology risk management framework should be established to manage technology risks in a systematic and consistent manner…" (*Technology Risk Management*, 2013)[i] do point the way but do not provide sufficient clarity on how FIs are to accomplish this. While these are all great directions for CMs to head towards, more clarity to aid CMs or the Board in establishing how to measure when this has been achieved to MAS standards would be helpful.

In the event of a breach, MAS has made it clear that the TRM will be used as a benchmark and FIs will be measured against it. So how then do CMs implement their security operations and guidelines, such that they can demonstrate to MAS that they have addressed TRM and made every effort to ensure the best possible safe and secure operational technical environment? In practice, under current conditions, this is almost impossible to do effectively. In general, there are five essential elements (*5 Essential Elements of Corporate Compliance*, 2012)[xi] when creating corporate policy and TRM does help by addressing four off these quite clearly - Leadership, Risk Assessment, Training, and Oversight. However in areas of Standards and Control, TRM is currently vague and arbitrary.

As an illustrative example, suppose an FI decides to use a common Cloud-based Vendor application such as Office365 to standardize its back office applications and lower its operating costs. Microsoft is highly unlikely to allow a MAS auditor to run a vulnerability scan against its source code. Section 5.1.3 of the TRM is clear that engagement of any service providers must not hinder MAS's ability to examine said service provider's systems. Therefore under TRM, this may constitute a violation, and the FI could be penalized if an incident involving Office365 occurs. MAS Auditors may accept proof of review by competent/reputable security assessors and attestation of secure coding practices, but again, this is at their discretion.

More clarification is needed on what criteria FIs must use to decide if a Vendor's products or services are deemed "safe and secure." It would be helpful if there were a preferred Vendor list or a Global Certification Process accepted and recognized by MAS such as ISO 27034, 27001 or perhaps through the establishment of a Singapore Government standard (similar to NIST in the US). Further clarification and information from MAS would be helpful for CMs to help vet Vendors under TRM.

More information dissemination and clarification by MAS would be helpful in ensuring that their licensees can achieve their expectations. In the event of a breach, MAS will take a very dim view of anything that it deems to have not met their guideline. Without TRM weightings and thresholds, FIs are forced to set their own measurements and tolerances and hope that MAS will find them acceptable upon review (reactive approach).

5.2 Incident Repositories

TRM also mandates that all incidents be reported in a timely manner, however rarely is any information about reported incidents shared publicly. If Offence informs Defence, it is helpful to provide a repository of lessons learned or root cause analysis documentation that FIs can utilize to learn and improve their security (proactive approach). A sanitized publication or online repository would prove beneficial to everyone (within and outside Singapore's borders) in improving cybersecurity through knowledge sharing.

5.3 Audit

MAS has also been auditing FIs for TRM compliance since 2015 but does not share the results of its audits. Furthermore, a formal audit standard does not appear to exist for FIs to refer to gain clearer insight into how to achieve a measurable level of care. As mentioned before, TRM is not meant to be a compliance only document where FIs work down a checklist but it is a set of papers whose compliance means understanding and embracing the "spirit of TRM." FIs need to have a more practical and specific notion of what that is when implementing security plans. The alternate, making it up as they go along, would seem less useful.

More guidance is also needed if Auditors are expected to score FI's cybersecurity performance uniformly. Auditors need to know where to focus their attention and help develop with the FI, a prioritized plan on what areas to improve first (severity ranking of Audit findings for example). Arbitrary scoring and opinions by Auditors can lead to imbalances and improper focus, and a weightings or scoring system would be helpful to Auditors and Auditees alike.

5.4 Changing Landscapes

In the two years since the release of TRM, MAS has not issued any revisions. Cybersecurity topography is constantly evolving, and MAS has been relatively quiet about new threats and opportunities that changes in technology have represented. Vendors and their products and services constantly evolve and will continue to add impact to risk landscapes. IoT, BYOD, Detection vs. Prevention, and most recently ransomware are just some examples of new topics and strategies that are not explicitly addressed but must be included by CMs intent on ensuring the best possible security posture of their organizations. MAS should issue more timely circulars addressing major security topics or perhaps a recurrent newsletter of some sort.

5.5 TRM Timeline

CMs must also consider what constitutes an adequate timeline for TRM implementation within their organizations. Given that rolling out effective, practical security controls takes time, and that many of the FIs began their TRM forays only in mid-2014, CMs need a basic understanding of what is MAS's timeline for TRM "compliance". Hopefully, MAS realizes that

effective cybersecurity is a journey and not a one-time exercise, and will work with their licensees to ensure that effective cybersecurity is achieved over time.

6. Conclusion

Guidelines such as TRM aid in the provision of a safe, secure and reliable financial environment and will continue to be an integral part of national cybersecurity policies in Singapore. An essential element of this strategy continues to be consistent vigilance by all FIs with major focuses on cyber defense, Data protection and IT infrastructure resilience.

TRM can be highly subjective and at present, whether an FI has successfully achieved TRM's embodied philosophy is still open to case-by-case interpretation. MAS should close this gap by providing more guidance and clarification through the establishment of more efficient communication channels such as forums, newsletters, more circulars to FIs. These should culminate in the publication of a new updated, and more precise TRM Guideline for FIs to observe.

CMs must incorporate TRM philosophy in their enterprise while understanding the evolving and dynamic threat landscape. As demonstrated, deploying an effective TRM enabled strategy can be a challenging task for CMs to succeed at. Utilizing methods and strategies such as those contained in the Controls enable a more pragmatic and focused approach to organizational cyber defense, and CMs would do well to apply these in their cyber protection strategies.

An efficient and secure approach to TRM requires extending implementation strategies to include practical considerations, effective measurements and performance metrics. These are not always defined clearly in TRM and must be supplemented with experience, intelligence, planning, and the right tools to ensure that FIs are safe, secure and well-defended institutions that customers can feel confident placing their funds with.

References

[i] *Technology Risk Management Guidelines*. (2016). Retrieved from Monetary Authority of Singapore website: http://www.mas.gov.sg/~/media/MAS/Regulations and Financial Stability/Regulatory and Supervisory Framework/Risk Management/TRM Guidelines 21 June 2013.pdf

[ii] *Regulatory Instruments Issued by MAS*. (2012). Retrieved from Monetary Authority of Singapore website: http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/regulatory-instruments-issued-by-mas.aspx

[iii] *The Center for Internet Security Critical Security Controls for Effective Cyber Defense*. (n.d.). Retrieved from The Center for Internet Security website: https://www.cisecurity.org/critical-controls/download.cfm?f=CSC-MASTER-VER%206.0%20CIS%20Critical%20Security%20Controls%2010.15.2015

[iv] Heitala, J. D. (2013). *Implementing the Critical Security Controls*. Retrieved from SANS Institute website: https://www.sans.org/reading-room/whitepapers/analyst/implementing-critical-security-controls-35125

[v] *Guidelines on Outsourcing*. (2014). Retrieved from Monetary Authority of Singapore website: http://www.mas.gov.sg/~/media/MAS/News and Publications/Consultation Papers/ConsultationPaper_Guidelines on Outsourcing.pdf

Andre Shori, AShori@mastersprogram.sans.edu

[vi] *Response to Feedback Received – Consultation Paper on the Notice On Technology Risk Management*. (2012). Retrieved from Monetary Authority of Singapore website: http://www.MAS.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/Response%20to%20Consultation%20Paper_TRM%20Notice.pdf

[vii] *Frequently Asked Questions: Notice on Technology Risk Management*. (n.d.). Retrieved from Monetary Authority of Singapore website: http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/FAQs_Notice%20on%20TRM.pdf

[viii] *Draft Notice on Outsourcing*. (2014). Retrieved from Monetary Authority of Singapore website: http://www.MAS.gov.sg/~/media/MAS/News%20and%20Publications/Consultation%20Papers/ConsultationPaper_Notice%20on%20Outsourcing.pdf

[ix] Ho, H. S. (2015). *Technology Risk and Cyber Security Training for Board*. Retrieved from Monetary Authority of Singapore website: http://www.MAS.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRS%20Circulars/Circular%20TR03%202015%20%20Technology%20Risk%20and%20Cyber%20Security%20Training%20For%20Boa.pdf

[x] *Personal Data Protection Act Overview*. (2016). Retrieved from Personal Data Protection Commission Singapore website: https://www.pdpc.gov.sg/legislation-and-guidelines

[xi] *5 Essential Elements of Corporate Compliance*. (2012). Retrieved from Baker & McKenzie website: http://www.bakermckenzie.com/files/Uploads/Documents/NorthAmerica/DoingBusinessGuide/NewYork/br_elementscorporatecompliance.pdf

[xii] PWC. (2013, July). Technology Risk Management. Retrieved from https://www.pwc.com/sg/en/financial-services/assets/techriskmanagement201307.pdf

Appendix A

2.1 Critial Systems	Control 1 - Inventory of Authorized and Unauthorized Devices	Control 2 - Inventory of Authorized and Unauthorized Software		
3.1 Cybersecurity Training	Control 17 – Security Skills Assessment and Appropriate Training to Fill Gaps			
4. Alignment with Operational Cybersecurity Frameworks	Control 13 – Data Protection	Control 14 – Controlled Access Based on the Need to Know	Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs	
4.1 Business Continuity & Disaster Recovery Planning	Control 10 – Data Recovery Capability			
4.2 Data Loss Prevention	Control 14 – Controlled Access Based on the Need to Know	Control 18 – Application Software Security		
4.3 Cloud Computing	Control 1 – Inventory of Authorized and Unauthorized Devices	Control 2 – Inventory of Authorized and Unauthorized Software	Control 3 – Secure Configuration for Hardware and Software	Control 4 - Continuous Online Vulnerability Scanning
	Control 5 – Controlled Use of Administrative Privileges	Control 10 - Data Recovery Capability	Control 11 - Secure Configuration for Network Devices	Control 14 – Controlled Access Based on the Need to Know

	Control 18 – Application Software Security			
4.4 Cyber Hygiene and Cybersecurity Control	Control 3 – Secure Configurations for Hardware and Software	Control 5 – Controlled Use of Administrative Privileges	Control 7 – Email and Web Browser Protection	Control 8 - Malware Defenses
	Control 12 - Boundary Defence).	Control 20 - Penetration Testing and Red Team Exercises		
4.5 Outsourcing Relationship Termination	Control 5 – Controlled Use of Administrative Privilege	Control 13 – Data Protection	Control 14 - Controlled Access Based on the Need to Know	Control 16 – Account Monitoring