RMiT

2019



IntelliSecure Insights:
Bank Negara Malaysia
Risk Management in Technology

Introduction

Do you have a robust Technology Risk Management framework?

Issues and challenges arising from implementing the new Bank Negara Malaysia Risk Management in Technology Policy.

The Bank Negara Malaysia ("BNM") released the Risk Management in Technology on that will be ineffective from 1 June 2019.

The new policy represents requirements to help financial institutions better manage technology-related risks and enhance technology resiliency.

IntelliSecure has reviewed these Standards and Guidelines and summarised the key points to consider in the this "Insight" document.

What are the technology challenges?

The last five years have seen an increase in reliance on technology to meet business demands. Concerns related to risks associated with using technology are highlighted on a daily basis in the media. Regulatory bodies have been forced to intervene and guide Financial Institutions to protect themselves and their customer information. As such, The Bank Negara Malaysia ("BNM") has released a Risk Management in Technology ("RMiT") policy containing Standards and Guidelines for any financial institution operating in Malaysia.

The RMiT policy creates a significant challenge for financial institutions. The Standards and Guidelines not only impacts technology aspects but also influences the operational processes and people elements of the business.

The RMiT Standards and Guidelines offer a number of best practices tactically, but implementation will consume a considerable amount of time, effort and cost, especially for the larger financial institutions.

The RMiT Standards and Guidelines has seen many financial institutions rethink their operational business strategy in Malaysia. Some of the more common concerns are:

- The cost of implementing controls against revenue
- The sum of fines that could be imposed due to non-compliance to the Standards and Guidelines
- The reputational damage of non-compliance
- Senior executives held accountable, with supervisory and administrative actions taken against them

Who is impacted?

The Standards and Guidelines issued under the relevant provisions of the respective Act applicable for financial institutions, including assets managers, banks, brokers, credit card or charge card licensees, financial advisors, finance companies, insurance companies and operators and settlement institutions of designated payment systems and REIT managers.

Key Points

What are the issues?

The issues are not only linked to adhering to the RMiT Standards and Guidelines but also to understanding what the impact of implementing or not implementing them means to the financial institution and how the Standard and Guidelines will change their operational model; thus, they question a financial institution's business strategy and raise further concerns.

- The prescriptive nature of the new RMiT Standards and Guideline
- The stringent notifications for incidents and conducting e-banking, internet insurance and internet Takaful services
- Implementing an effective Cyber Risk Management Framework, that can give you a cyber security posture at all times
- Enforcing service providers and third parties to comply with the requirements
- Use of Two-Factor Authentication (2FA) across critical services and customer transactions

Key Requirements

1. A financial institution must ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres.
2. A financial institution must ensure each critical system is designed for high availability and must not exceed cumulative unplanned downtime of more than 4 hours on a rolling 12-month basis and a maximum of 90 minutes downtime per incident.
3. A financial institution must immediately notify the Bank of any cyber incidents affecting the institution. Upon completion of an investigation, the financial institution is also required to submit a report on the incident as specified in ORION[7].
4. The financial institution should implement Technology risk management framework (TRMF) and Cyber resilience framework (CRF).
5. The Chairman of the Board is required to attest on the financial institution's ability to execute the strategic and business plans, risk management processes, resources to support Takaful and adequate controls to protect the banks' systems and services.

How can IntelliSecure help?

We have a dedicated team with over 80 years of experience that has helped many clients achieve compliance with strict Technology Risk regulatory requirements. Our pragmatic approach will focus on delivering an outcome that meets the project objective while aligned with your goals.

Contact us

Manish Chawda
Founder
(SG) +65 91801882
(MY) +60 392125439
manish@intellisecure.co

About IntelliSecure

IntelliSecure is a specialist cyber security and regulatory consultancy focused on helping organisations understand their current exposure to digital risk. Our solutions include cyber security consultancy, security technology, and compliance.

This publication 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. Nia Pte Ltd does not accept any liability, responsibility or duty of care for any consequence of you or anyone else acting or refraining to act, in reliance on the information in this publication or for any decision based on it. © 2024 Nia Pte Ltd. All rights reserved. IntelliSecure and the Nia logo are registered trademarks of Nia Pte Ltd.