PRAGMATIC TECHNOLOGY RISK MANAGEMENT (PTRM)

CYBERSECURITY IN QUALITY MANAGEMENT

KNOWLEDGE SHARING

10 September 2021

PRAGMATIC Technology Risk Management

Pragmatic Technology Risk Management

Pragmatic Technology Risk Management, PTRM in short, is a sole proprietorship registered by Albert Siow Chun Siung in March 2019, to provide technology risk management related advisory/assurance services to Malaysian, Singaporean and Thai clients with affordable engagement fee and in-depth experience as of Albert Siow's 15 years practicing in the technology risk management industry.

By the literal meaning of the word "pragmatic", PTRM intends to provide advisory to the client with pragmatism in mind, where the client would be able to achieve maximum control enhancement and risk mitigation with given minimal change and investment. Service value are provided with the objectives as below:

- **Regulatory Requirements Compliance**
- **Easy to Learn and Implement**
- **Aligned to Client Risk Management Framework**
- **Little or Minimal Monetary Investment**
- **Maximize Operation Effectiveness**
- **Effective Risk Mitigation**

PRAGMATIC
Technology Risk Management

ALBERT SIOW

Mobile: +60122502677
Email: albert@PTRM.asia

Principal Consultant

Albert has 14 years experience providing IT consultation services to local and foreign clients. He started his career in 2006 as IT security engineer in Kent, UK, serving 2012 Olympic Games Committee, Lloyd bank, KPMG Europe etc. He came back to Malaysia in 2008 and served Digi, Public Bank, HongLeong Bank, Digi, AirAsia in local IT security consulting firm. He joined Deloitte in 2011 and became the manager in Deloitte SEA services providing services to member firms in Deloitte Enterprise Risk Services South East Asia. Prior to establish PTRM, he was the head of department for Mazars: Technology and Security advisory division, providing technology risk advisory services to Mazars Asia & Pacific region member firms in China, HongKong, Thailand, Cambodia, Singapore, Australia and India on 2014 - 2019. He has assisted Basis Bay and Bridge Datacentre (formerly CSF Group) obtaining ISO 27001 certifications.

Qualifications

- Certified Information System Security Professional (CISSP) – exam passed in 2012
- Certified in Governance of Enterprise IT (CGEIT) – exam passed in 2014
- Cisco Certified Intrusion Prevention System Specialist 2012
- Certified Information System Auditor (CISA) 2010
- Certified Cisco Network Associate: Security (CCNA: Security) 2006
- Microsoft Certified System Engineer (MCSE) 2008
- Microsoft Certified System Administrator (MCSA) 2008
- Certified Ethical Hacker (CEH) 2008
- Master of Science in Distributed Systems and Networks, University of Hertfordshire, UK 2005
- Bachelor of Science in Software Engineering, The Nottingham Trent University, UK 2004

PRAGMATIC
Technology Risk Management

TABLE OF CONTENTS

PRAGMATIC Technology Risk Management

01 Technology Risk Management

TECHNOLOGY RISK MANAGEMENT

- Technology risk, or information technology risk, is the **potential for any technology failure to disrupt a business**.
- Companies face many types of technology risks, such as information security incidents, cyberattacks, password theft, service outages, and more.
- Every type of technology risk has the potential to cause financial, reputational, regulatory, and/or strategic risk. As such, it's critical to have an effective technology risk management strategy in place to anticipate potential problems.
- Information Security: C I A

TECHNOLOGY RISK MANAGEMENT

Risk Management's Role in Technology Risk

- Risk management includes the strategies, processes, systems, and people aimed at **effectively managing potential technology risks**.
- Essentially, the goal of cybersecurity risk management is to **identify potential technology risks before they occur** and have a plan to address those technology risks. Risk management looks at the **internal and external technology risks** that could have a negative effect on a company.
- Risk management teams define their technology risk management plans by identifying and analyzing technology risks, managing the technology risks by implementing their strategies, and forming contingency plans.

TECHNOLOGY RISK MANAGEMENT

Some Typical Technology Risks

- Sensitive Information Leakage
- Critical Data not Backed Up
- Virus/Malware attack
- Cybersecurity attack
- Physical Attack
- Natural Disaster
- Compliance and Regulatory Punishment
- Insider Sabotage; and more…

TECHNOLOGY RISK MANAGEMENT

Your Technology Risk Exposure = Your Reliance on Technology

NOT Total Worth of your Technology Infrastructure !!

1 simple question: **How good is your business without internet connection?**

TECHNOLOGY RISK MANAGEMENT

The Ultimate Goal of Technology Risk Management:

02 Common Information Security Weakness in Malaysia

COMMON INFORMATION SECURITY WEAKNESS

1. No technology risk assessment
2. IT SOP not documented => Business continuity issue
3. Lack of information IT security training
4. No incident response plan for information security
5. IT team is not trained for security solution
6. No password enforcement
7. No internal assessment/audit on information security posture
8. Vendors automatically understand our information security requirements

COMMON INFORMATION SECURITY MINDSET

1. It would never happen on my business
2. No information in my business is critical.
3. Poor information security awareness among the staff
4. Pirated is as good as licensed software
5. My data will never get lost.
6. Everyone in my company is trustworthy!
7. All information in my business is critical.
8. The cloud handle everything for me.

03 Simple TRM in 4 steps

SIMPLE TRM IN 4 STEPS

PRAGMATIC Technology Risk Management

SIMPLE TRM IN 4 STEPS

Step 1: Risk Identification

- Threat vs Risk
- Be creative
- Think out of the box
- Longer list = More Comprehensive Coverage
- Sample risks:
  - Natural Disaster
  - Virus/Malware
  - Incomplete Data Backup
  - Power Failure
  - Regulatory Compliance
  - Poor awareness among staff
  - Poor awareness among vendors
  - Unauthorized Access
  - Weak IT Infrastructure Protection
  - Ransomware
  - Poor Internet Connection
  - IED/VIED/Terrorist Attack

SIMPLE TRM IN 4 STEPS

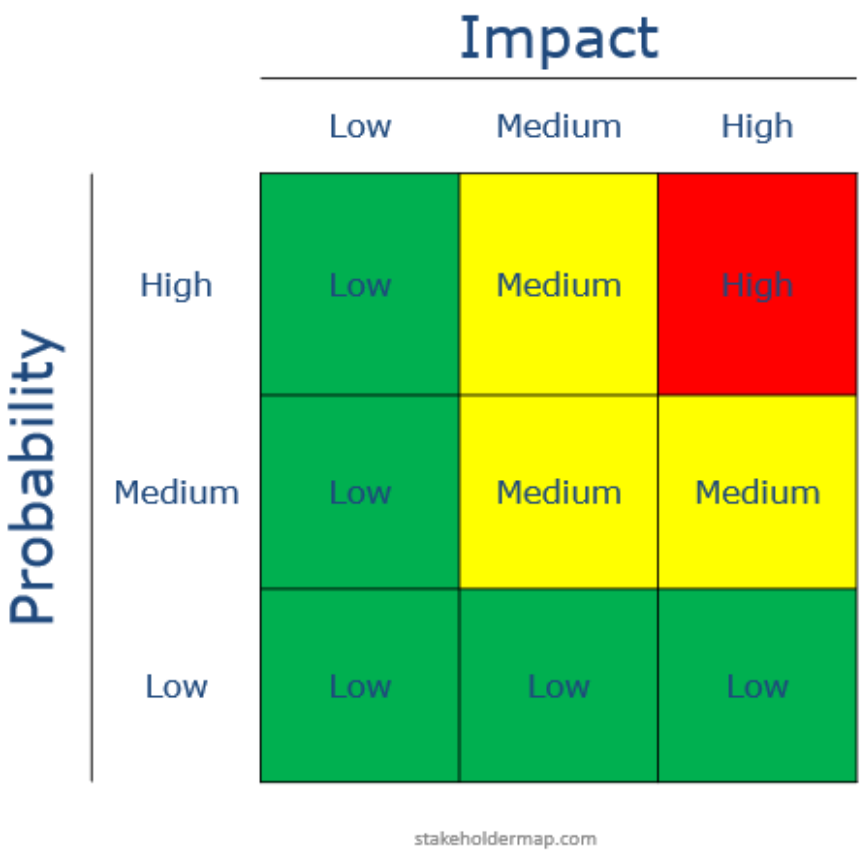
Step 2: Critical Asset/Information Identification

- What are the most critical asset and information in your business?
- Don’t be greedy while your pocket is not ready!
- It is PERFECTLY OK to start with small coverage.
- Who is the asset/information/process owner?

SIMPLE TRM IN 4 STEPS

Step 3: Establish Risk Matrix

- Measurable
- Quantitative vs Qualitative
- Risk rating for all risks
- Impact vs Probability



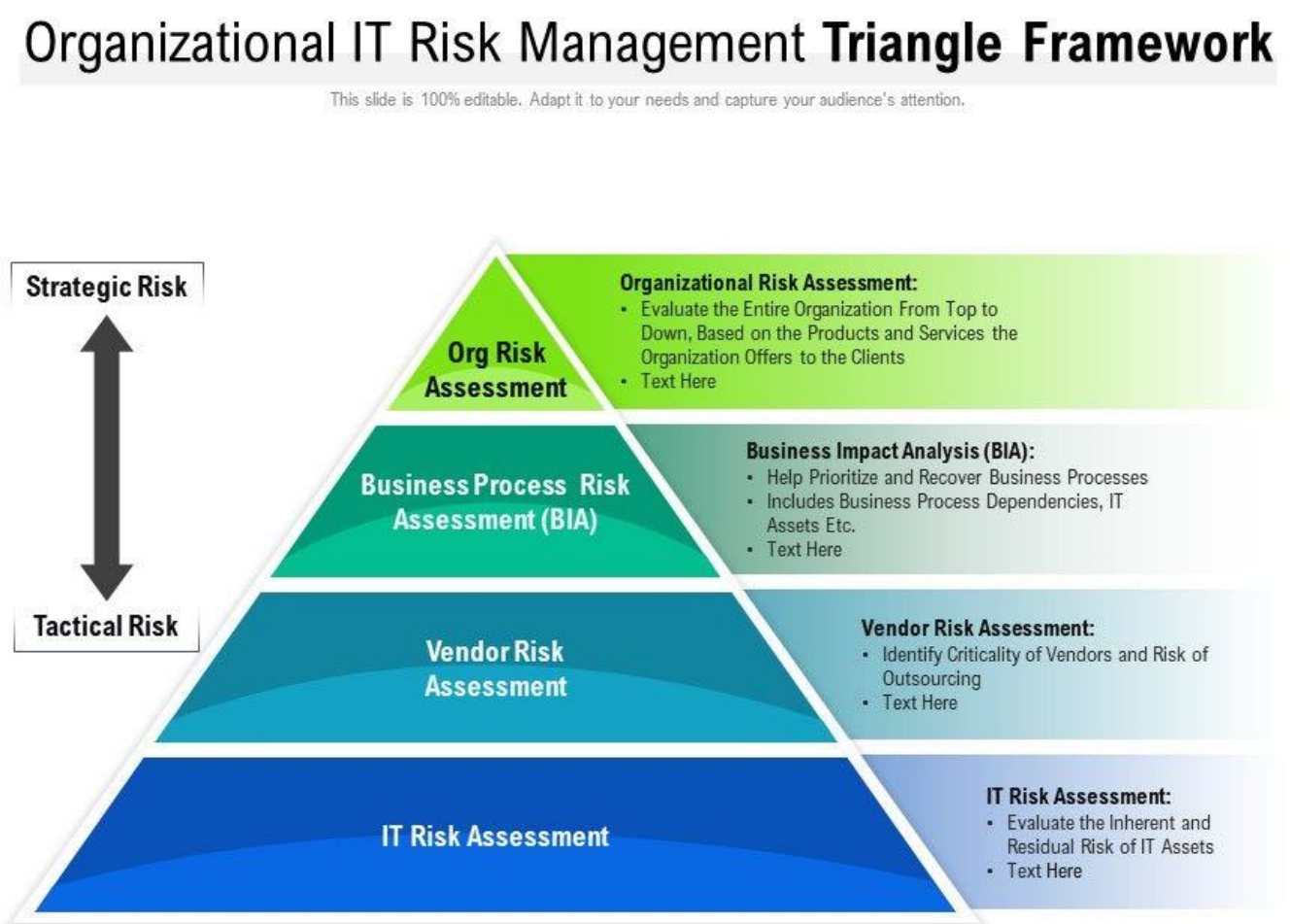
PRAGMATIC Technology Risk Management

SIMPLE TRM IN 4 STEPS

Step 4: Risk Assessment

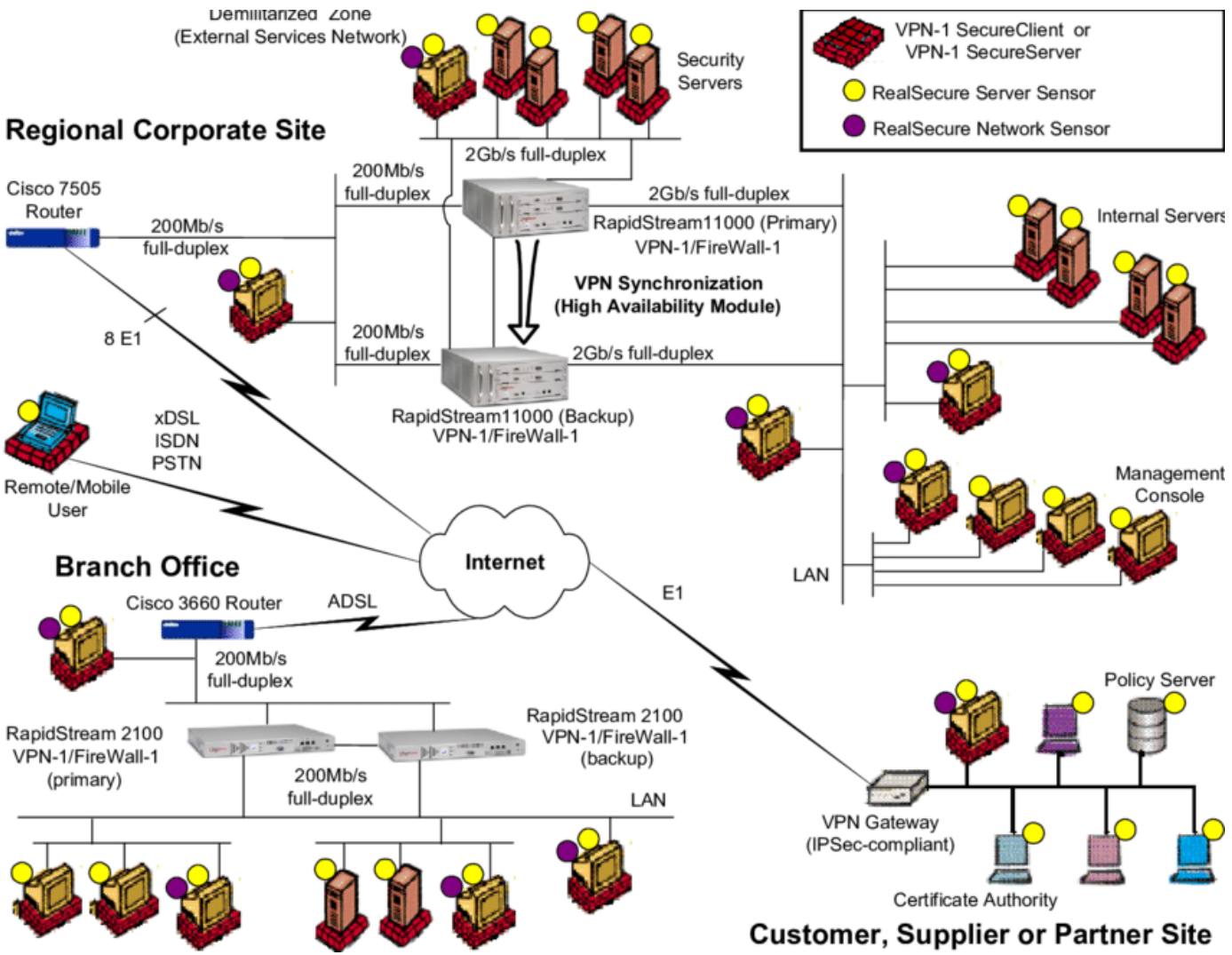
- Higher Risk = Higher Priority
- Implementation belongs to Asset/Information/Process owner (Accountability!)
- Roll up Risk Treatment Plan
- What is **Expected Outcome/Effective Implementation**? How to measure?

SIMPLE TRM IN 4 STEPS

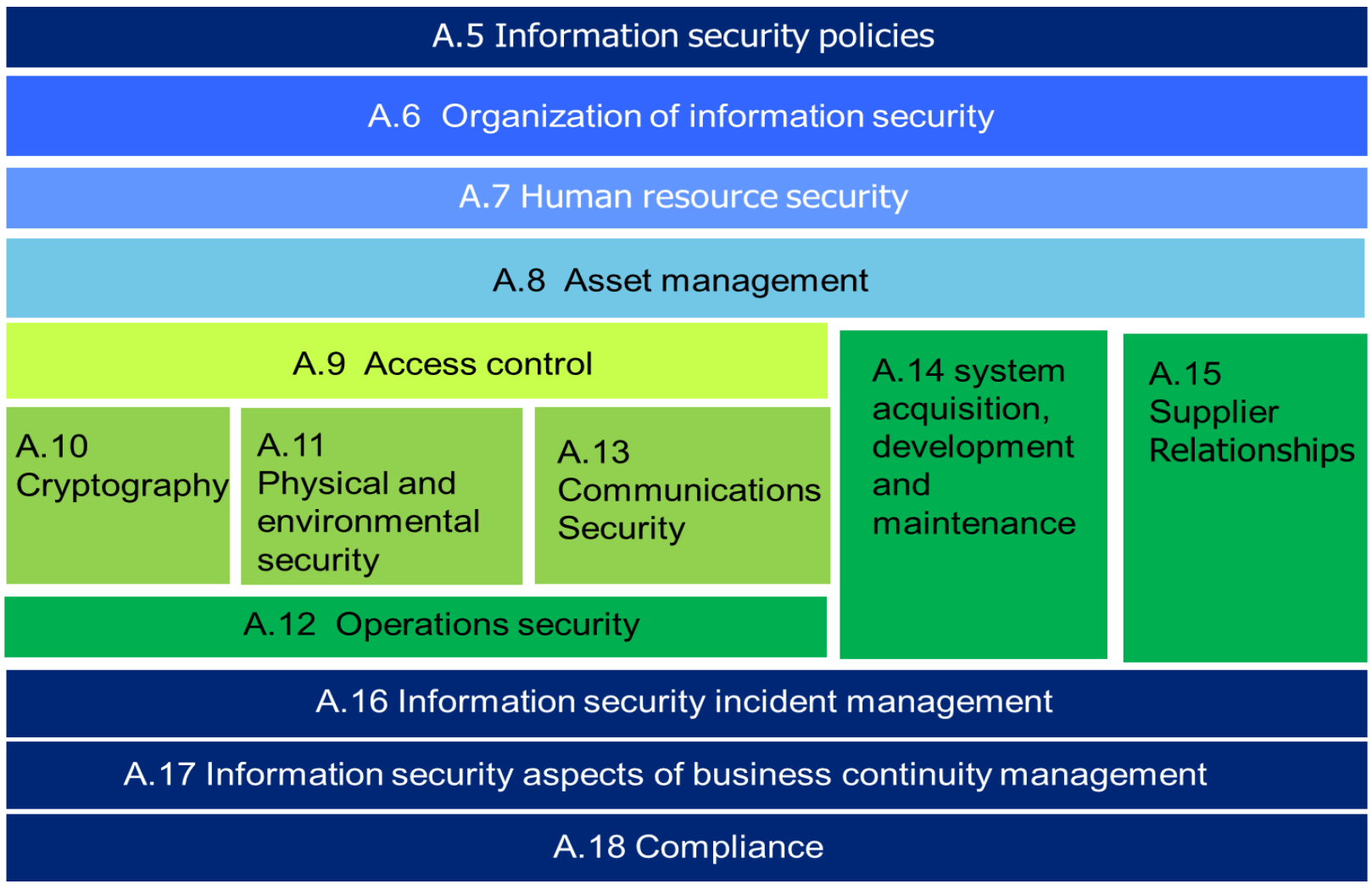


SIMPLE TRM IN 4 STEPS

WHAT CAN GO WRONG?



ISO 27001 ISMS ANNEX A CONTROLS



PRAGMATIC Technology Risk Management

04 Simple Information Security Tips

SIMPLE INFORMATION SECURITY TIPS

- You outsource the process, you don’t outsource the risk!
- Never trust, always verify.
- Password Complexity + Password History = Good Password
- Ask yourself regularly: Do you have all risks covered?
- When is your last IT security awareness training for your business?
- Encrypt the information whenever possible
- When you are in doubt, DON’T RESPOND.

CONTACT

Pragmatic Technology Risk Management (PTRM)
27, Jalan Perdana 2/18, Pandan Perdana
55300 Kuala Lumpur
Malaysia
Tel : +6012- 2502677
Email: albert@ptrm.asia

https://ptrm.asia

PRAGMATIC
Technology Risk Management