Asia-Pacific
Economic Cooperation

APEC
Guidebook on SME Digital Resilience

APEC Small and Medium Enterprise Working Group (SMEWG)
July 2017

CONTENT

01 Foreword

As the most crucial forum for multi-lateral economic cooperation and dialogue in the Asia-Pacific region, APEC houses 21 member economies whose total population reaches approximately 2.6 billion and whose combined global trade represents almost 50% of that of the international community. This shows just how far-reaching APEC's impact on economic development can be on a global scale. Of the 21 APEC member economies, Chinese Taipei has been an active one, who, over the past years, has built strong cross-border partnerships and public-private partnerships (PPP) through its participation in the Small and Medium Enterprises Ministerial Meeting (SMEMM) and Small and Medium Enterprises Working Group (SMEWG). Over the years, Chinese Taipei's contributions in promoting business continuity planning (BCP) for SMEs, developing innovative entrepreneurship, and creating a quality environment for businesses to grow have all been recognized by APEC as significant achievements, which effectively increased the international visibility of Chinese Taipei.

Chinese Taipei first proposed the initiative for the establishment of the APEC SME Crisis Management Center in 2010 to assist SMEs respond swiftly to the negative impact of the global financial crisis of the time. When the devastating disasters that soon followed in Japan, Thailand, and New Zealand disconnected industry supply chains,

Chinese Taipei decided to transform the crisis management center in 2011 and proposed the 4-year project “Improving Natural Disaster Resilience of APEC SMEs to Facilitate Trade and Investment” in the first APEC Senior Officials' Meeting (SOM) in an effort to aid SMEs in their business continuity planning and stabilize global supply chains. Collaboration was also sought with crisis management professionals and BCP experts based in the Asia-Pacific region, the joint effort of which culminated in the publication of the Guidebook on SME Business Continuity Planning, available in 7 languages and promoted in many Asia-Pacific economies.

In recent years, the rapid development of technology and mobile internet has been altering traditional business models and industry links at an accelerated pace. Estimates by market research company eMarketer indicate that retail e-commerce sales will increase from 8.6% in 2016 to 12.8% in 2019, and that online sales by global buyers and internet users will increase from 26.4% and 53.4% respectively to 32.8% and 57.6%.

It appears that the Asia-Pacific region has become the world's largest digital economic market (accounting for 33% globally), providing SMEs with tremendous business opportunities and job openings. (eMarketer, 2015) To survive and thrive in the digital economy, digital transformation and the innovative online-to-offline (O2O) business model are something that SMEs cannot afford to neglect. Digital transformation and the O2O business model are the key components underpinning the economic prosperity and growth in the Asia-Pacific region and will shape and drive the development of innovative new businesses and SMEs. However, digital transformation in traditional businesses will also bring about concerns regarding digital security, to which special attention must be paid.

The term "digital resilience", therefore, refers to the capabilities of SMEs to respond to and recover from digital crises such as Internet security threats and cyber-attacks. Statistics by PwC in 2014 show that 60% of SMEs had experience with security threats and the financial loss caused by a security incident averaged between US$ 100,000 and US$ 180,000. The lack of digital capabilities and security awareness makes SMEs a sweet spot for cyber-attacks and can lead to global value and supply chain disconnections, which has the potential to cost the world up to US$ 3 trillion as of 2020. (McKinsey, 2015)

Most SMEs without crisis response experience or capabilities often find themselves in a quandary and are at a loss as to who to turn to for help in the event of a digital attack. Even when they manage to implement some form of internal measures, the results of their chosen remedies usually do not materialize quickly enough to be effective. Post-crisis recovery is a race against time. How should SMEs prepare themselves for this challenging task?

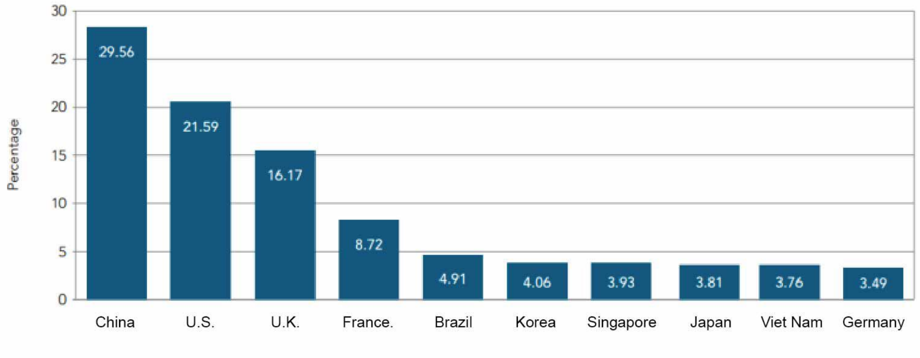
With the same dedication, as previously made to the APEC Accelerator Network (AAN) and the four-year BCP project, Chinese Taipei conducted a cross-border collaboration in 2017 with experts from the fields of digital security and business continuity planning such as Trend Micro and Belfor and gave birth to the APEC SME O2O Expert Network. Relevant experts based in the Asia-Pacific region are invited to draft and review this guidebook in the hopes of providing SMEs in the region with some tools to strengthen their digital competitiveness and resilience so as to enable quality growth in the digital era.

02 Introduction

The advent of the digital economy and the age of the Internet of Things (IOT) has made the promotion of SMEs growth and internationalization a vital mission. Thus it has become a key direction for Chinese Taipei and APEC to assist small and medium enterprises (SMEs) in the Asia-Pacific region to utilize the innovative Online-to-Offline (O2O) business model to participate in the new regional and global blue seas created by the digital economy while strengthening their digital competitiveness and resilience.

However, the digital economy is a double-edged sword. As it generates opportunities for businesses, it also brings challenges. The Global Risks 2016 Report by the World Economic Forum points out that internet crimes create over US$ 445 billion of financial loss globally every year (approximately NT$14 trillion, 435billion and 800 million). The Third Quarter, 2016 State of the Internet Report by Akamai shows that many of the top 10 source countries for DDoS attacks (to disrupt or shut down websites, services or networks) were APEC member economies. This means that while APEC member economies transform themselves digitally, they have also become easy targets of cyber-attacks.

Top 10 Source Countries for DDoS Attacks, Q3 2016

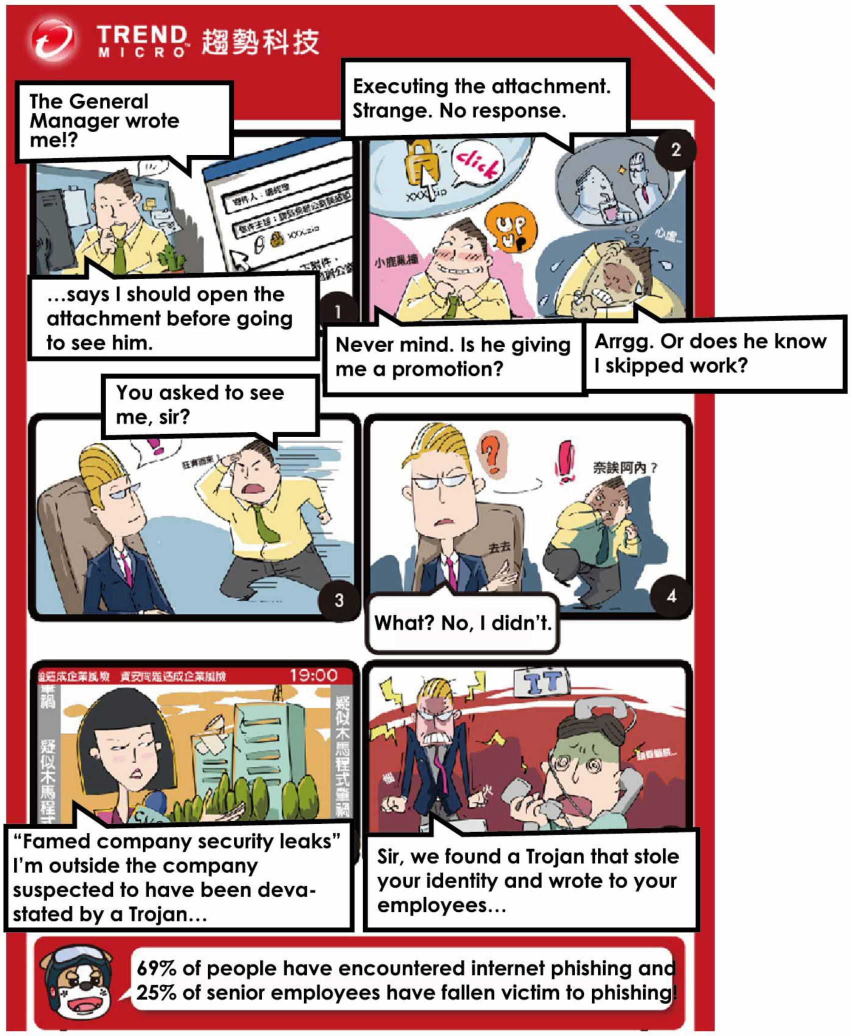


Yet fast-paced technology revolutions have given birth to more than one type of cyber-attacks. In addition to DDoS, business email compromise (BEC) is also a common form of fraud where the criminals send out false financial requests in the name of the company's supplier, executive, chief financial officer, lawyer, etc. Statistics by the Criminal Investigation Bureau (CIB), National Policy Agency show that there were 42 cases of BEC scams in 2016 and most cases suffered losses no less than millions of NT dollars. There were also 8 recorded cases of foreign enterprises who fell prey of BEC and requested help from local police because the payments were directed here. The most well-known case of them – also with the highest amount – was made public by the CIB on November 2, 2016 in a news release titled "Female bank clerk stops NT$150 million fraud, publicly commended by CIB director-general." In the scam, a female accountant surnamed Chen working at a Hong Kong investment company received a business email from the CEO the previous Tuesday. The email said, "I'm the CEO. I am currently working on an important asset merger project.

Please send US$4.8 million to the designated account immediately. The transaction is to be kept confidential…" Without any double, she instantly remitted US$4.8 million (approximately NT$153 million and 600 thousand) to the designated Taishin Bank account in Chinese Taipei.

Fortunately, the transaction was intercepted before too late, saving the company a tremendous financial loss.

Digital security company Trend Micro also regularly shares cases of digital threats with its clients and the general public to raise awareness on internet security.

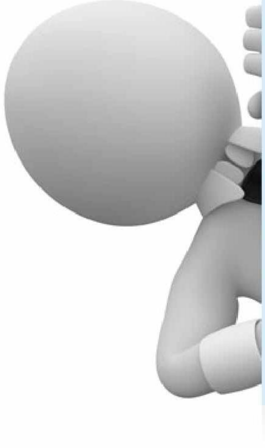

TREND MICRO 趨勢科技
The General Manager wrote me!?
...says I should open the attachment before going to see him.
1
Executing the attachment. Strange. No response.
2
Never mind. Is he giving me a promotion?
Arrgg. Or does he know I skipped work?
You asked to see me, sir?
3
4
What? No, I didn't.
"Famed company security leaks" I'm outside the company suspected to have been devastated by a Trojan...
19:00
Sir, we found a Trojan that stole your identity and wrote to your employees...
IT
69% of people have encountered internet phishing and 25% of senior employees have fallen victim to phishing!

It is evident that in the age of digital economy, digital resilience cannot be overlooked. Once a company is compromised, it may suffer various degrees of harm, from financial loss to business reputation damage to even losing the business entirely.

For this reason, the guidebook is written to help SMEs understand how to react to malicious business competition and information threats to help them remain competitive and digitally secured.

The steps outlined in the guidebook are referenced from “ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements” and its Annex A. This international standard on information security management systems (ISMS) is applicable to all organizations worldwide. Risk management steps and methods are referenced from “ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.” However, in consideration of the relatively limited resources of SMEs, the steps are designed to reflect the reality of SMEs while keeping the spirit of the ISO standards. This moderation and streamlining allow resource-sensitive SMEs an equal chance to put in place a sound ISMS to fortify the defense capabilities of SMEs against cyber security threats.

This guidebook introduces 11 steps on ISMS in an easy-to-understand way, taking the readers on a trip to explore the realm of ISMS while providing a good grasp of the spirit of the international ISMS standard ISO 27001.



Step 1: Understanding your ISMS requirements and forming an ISMS team
Gaining a full picture of the company by taking a look at applicable legal and market requirements as well as the company’s internal management

Step 2: Determining ISMS policies and objectives
Formulating ISMS policies and finalizing implementation objectives

Step 3: Listing and categorizing information assets

Taking stock of information assets related to information security and categorize them

Step 4: Identifying and evaluating information asset risk

Conducting risk identification and risk evaluation on the information asset

Step 5: Assessing information asset risk

Assessing risks associated with the information assets and identifying high-risk ones

Step 6: Producing a risk treatment plan

Determining risk treatment options for high-risk information assets as revealed by the risk assessment results

Step 7: Selecting ISMS controls

Selecting and implementing effective information security controls to minimize risks as per the risk treatment plan

Step 8: Establishing a business continuity plan

Business continuity planning is the best protection any company can have against crises

Step 9: Responding to and reporting information security incidents

Appropriate reporting of and responses to information security incidents are necessary

Step 10: How to determine the effectiveness of your ISMS

Determining the effectiveness of your ISMS controls through regular reviews and conformance to international standards

Step 11: Continuous ISMS improvement and problem follow-up

The 11 steps are underpinned by the PDCA cycle **(Plan-Do-Check-Act)** to progressively improve ISMS effectiveness in SMEs. While each step constitutes a PDCA cycle, the 11 steps together form a larger PDCA cycle. The relation between the 11 steps and the PDCA cycle is illustrated below:

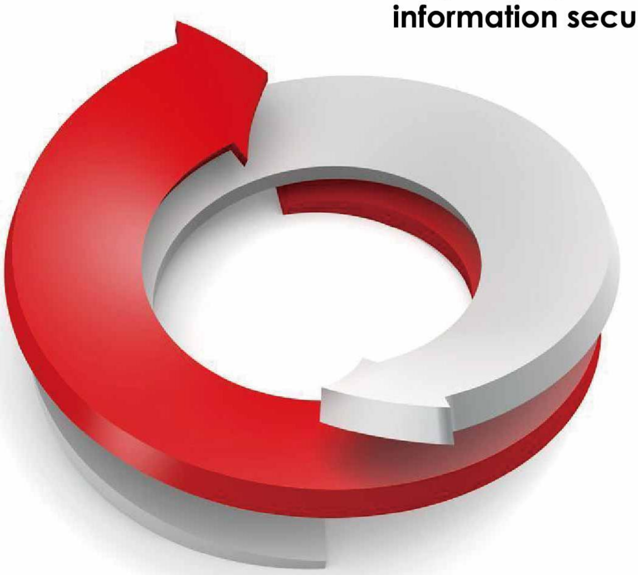
Plan

1. **Understanding your ISMS requirements and forming an ISMS team**

2. **Determining ISMS policies and objectives**

Do

3. **Listing and categorizing information assets**
4. **Identifying and evaluating information asset risk**
5. **Assessing information asset risk**
7. **Selecting ISMS controls**
8. **Establishing a business continuity plan**
9. **Responding to and reporting information security incidents**



Act

6. **Producing a risk treatment plan**

11. **Continuous ISMS improvement and problem follow-up**

Check

10. **How to determine the effectiveness of your ISMS**

Figure 1: PDCA Cycle

03 Steps

Step 01 Understanding your ISMS requirements and forming an ISMS team

Before establishing and implementing an ISMS, you first need to understand the information security issues and requirements of your company. You can begin by exploring the following three areas.

❶ Clarifying legal or regulatory requirements and contractual obligations

Firstly, you need to clarify what local legal or regulatory requirements there are that are applicable to your company. Once you have compiled all the legal and regulatory requirements, you will have a clear picture of the legal restrictions of your company and will be less prone to violations.

In addition, you will also need to gain a good grasp of the requirements on information security specified in contracts to which the company is bound. These may be contracts made between the company and its clients or suppliers. Some of the contracts contain confidentiality requirements or require delivered information to be kept in confidence. These requirements must be clarified and complied. During and/or after the implementation of the contracts, proper information security measures must be put in place.

❷ Understanding internal and external issues

When it comes to ISMS issues, you need to know both the internal and external issues facing the company. Internal issues may relate to the company's vision and objectives and the requirements and expectations of the highest-level management for the company. In terms of external issues, you need to consider the position of the company in the industry and whether security management issues will lower the company's competitiveness.

❸ Stakeholders' requirements and expectations for security issues

This can also be viewed from two angles, internal and external stakeholders. Internal stakeholders may include directors of the board, managers of all levels and employees. External stakeholders may include government agencies, fire departments, police departments, business partners, business competitors, etc. These stakeholders' requirements and expectations for the company's security management issues should all be taken into account.

❹ Forming an ISMS team

After understanding your ISMS issues, requirements, and expectations, you will need to organization an ISMS team to take charge of ISMS affairs and promote and implement ISMS controls. To do so, first you will need to designate someone to lead the team. This person is normally called the Chief Information Security Officer (CISO). The company's highest-level management will need to authorize the CISO to conduct cross-department coordination and gain access to the resources necessary for ISMS promotion and implementation, including human resources. Next, you will need to build the ISMS team. It is suggested to select team members through department nominations as this will make future ISMS control implementation across the company much easier.

Step 02 Determining ISMS policies and objectives

A policy is the highest guiding principle of any mission. Before implementing your ISMS, you need to formulate an ISMS policy that reflects the internal and external issues, requirements and expectations as detailed in step 1. An ISMS policy can not only point out a clear direction for your ISMS but also demonstrate to the general public your aspiration in promoting information security management.

Once your ISMS policy is in place, you can begin to draft your ISMS objectives that are in line with the policy. You may use the SMART principle to set your ISMS objectives to ensure their effectiveness. The SMART principle:

Specific
Measurable
Achievable
Realistic
Time-related

Table 1: SMART Principle for Objective Setting

In addition to using the SMART principle to determine your ISMS objectives, regular monitoring and reviews are also necessary during ISMS implementation to keep you updated on the ongoing outcomes of your ISMS relative to the objectives. After your ISMS is implemented, you need to look at the final results against the objectives, list corrective actions to take to meet the objectives, and set or adjust the objectives for the next round based on the implementation results of the corrective actions.

Step 03

Listing and categorizing information assets

Step 3 to step 6 delve into risk management, which is a pivotal aspect of your ISMS.

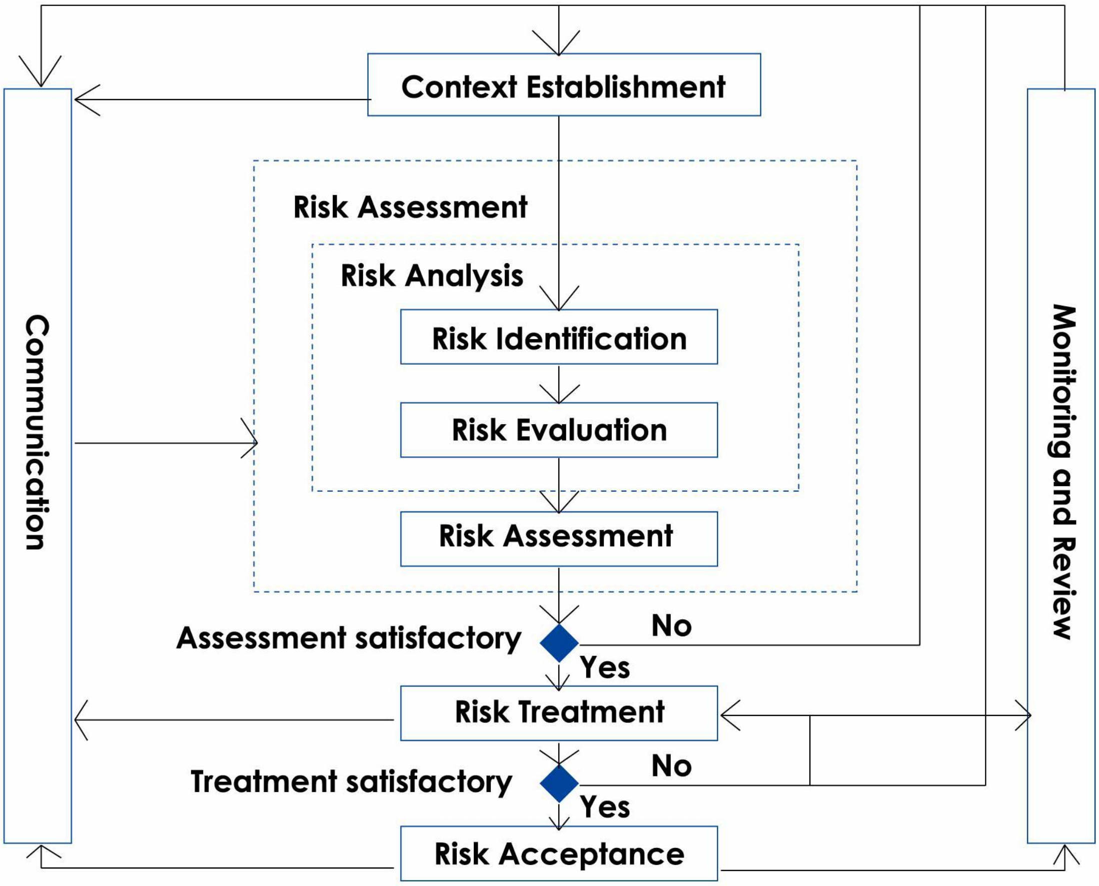


Figure 2: Risk Management Process

ISMS issues concern judgement on and protection against risk. To address an ISMS issue means to try to steer clear of risk and avoid the damage that it may cause. To manage risk, you first need to identify risk. To identify risk, you first need to understand what assets you have that are related to information processing and application.

Asset Identification and Information Processing and Application

It takes many items (assets) to make information processing and application possible. These items are called "information assets". We first need to know what information assets the company has that enable the processing and application of information. Then we need to list the information assets and categorize them properly.
Common information assets in a company include physical space, power and air-conditioning, documents and contracts, computers/internet equipment, administrative and operational processes, etc. Even people involved in information processing are considered an information asset.

Step 04 Identifying and evaluating information asset risk

After taking stock of the company's information assets, we can then identify and evaluate the risk of each information asset. To identify the risk of an information asset, you can ask yourself the following three questions:

1. What are the tangible and intangible value of the information asset?
2. What external threats may this information asset face?
3. What vulnerabilities may this information asset have in terms of internal management?

Once the risks of all information assets are evaluated, you can use the evaluation results to calculate their risk scores, which will then be used to determine treatment priorities.

There are a number of ways to evaluate risk:

- **Qualitative evaluation: evaluating risk in an intuitive and subjective manner.**

Likelihood Risk Impact	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Medium
Low	Medium	Medium	Low

Table 2: Qualitative Risk Matrix

In an intuitive and subjective way, you may determine the level (high, medium or low) of the impact and likelihood of the threats and vulnerabilities associated with an information asset, and then check against the Qualitative Risk Matrix to determine the risk level of the information asset.

- **Quantitative evaluation: Evaluating risk using quantifiable numbers**

As a concept, the risk level of an information asset is positively correlated with its impact and likelihood, which are derived from your assessment of the threats and vulnerabilities of the information asset. Quantitatively, the risk value of an information asset can be expressed in the following equation:

Risk value = value x likelihood x impact

Hence, to obtain the risk value of an information asset, you first need to assess and assign quantifiable values to the value of the information asset, and to the impact and likelihood of the threats and vulnerabilities associated with the information asset.

Step 05

Assessing information asset risk

In the previous step, the risk evaluation provides you with a comprehensive list of risk values associated with your information assets. Some risk values may be high and some may be low. Now, we need to check the risk values using risk assessment and acceptance principles to determine which information assets need to be treated first to reduce their risk values. To do so, we need to consider the available resources of the company to decide on a risk value threshold. Only information assets with a risk value above the threshold will be treated. These above-threshold values are also called acceptable risk values. Information assets with acceptable risk values will need to be included in a risk treatment plan, which will be detailed in the next step. You can determine your risk value threshold based on the number of risks you have and your available human resources, budget and time.

Step 06

Producing a risk treatment plan

Once your risk value threshold is confirmed, all information assets with risk values equal to or above the threshold must be included in your risk treatment plan. In addition to basic information fields such as person-in-charge and expected due dates, your risk treatment plan should also specify what the risk treatment is treating - is it targeting the threats, mitigating vulnerabilities or lowering impact (asset value loss) - and how much the risk value will be reduced. When this is done, you may then calculate residue-risk values by using the equation above and see if the residue-risk values are now below the threshold

There are four common options to risk treatment:

- Risk mitigation: using controls to lower risk values so that the residue-risk values can fall under the risk threshold.
- Risk acceptance: accepting the risk and not taking any action.
- Risk avoidance: steering clear of activities or situations that may cause specific risks.
- Risk transfer: transferring the risk to a difference place that can be best

You may choose yours risk treatment options based on your available resources.

Step 07 Selecting ISMS controls

nformation security is designed to protect information against threats by implementing appropriate controls that allow businesses to continue operation, minimize potential losses, and maximize business opportunities.

There is no end to information security protection and companies can’t afford to invest unlimited resources to its ISMS. Therefore, you should determine your risk treatment plan and prioritize your treatment items based on your risk assessment results and available resources.

This step will look at some controls for different treatment items to reduce or eliminate the risk of threats and vulnerabilities from both management and technical angles.

Want controls should you use? The following may provide some guidance:

Ⓐ Human resource security

Ensuring that employees or contractors understand and fulfill their information security responsibilities before, during and after employment. For example: holding regular staff training on information security.

Ⓑ Asset management

Offering proper protection to information assets by avoiding unauthorized disclosure, modification, removal or destruction.

Ⓒ Access control

This may include

(a)User access and management: controls on the registration, termination and access permission of employee accounts, management and review of accounts with special access, etc.

(b)Access control management of systems and applications.

Ⓓ Physical and environment security

(a)Protection of secure areas: for example, prohibition to eat and/or drink in the equipment room, cautious use of electrical sockets in the equipment room.

(b)Equipment: preventing the loss, damage, theft and hacking of information assets.

Ⓔ Operations security

(a)Setting correct and safe system operation steps.

(b)Protection from Malware: for example, installing anti-virus software on every computer.

(c)Backup: regular backups of important systems.

(d)Preservation and protection of important system logs.

(e)Restricting the installation of unauthorized software on company computers by employees.

F **Communications security**

(a)Network security management: networks should be managed and controlled to protect information systems and applications.
(b)Information transmission: additional protection should be given to confidential information, such as encryption.

Step 08 Establishing a business continuity plan

Is your company prepared for a disaster? If not, your company is likely to suffer grave losses during disaster and negative incidents. As a countermeasure, business continuity planning (BCP) is one of the best protections you can have against crises.

The Small and Medium Enterprise Administration introduced 10 simple steps in its Guidebook on SME Business Continuity Planning that takes the readers on a journey to explore ISO 22301, an international standard on BCP, and help companies build their own BCPs. The guidebook is available for download online:

- **http://www.moeasmea.gov.tw/ct.asp?xItem=11453&ctNode=473&mp=2 (English)**

- **http://www.tami.org.tw/sp1/bulletin/government/government_1030514.pdf (Chinese)**

Step 1 Determine BCP Purpose, Scope and Team
Step 2 Prioritized Activities and Recovery Time Objective
Step 3 What Do You Need to Resume Key Activities?
Step 4 Risk Assessment- Know Your Disaster Scenarios
Step 5 Do Not Forget Pre-Disaster Protection and Mitigation
Step 6 Emergency Response to Disaster
Step 7 BC Strategies to Early Resumption
Step 8 Be Financially Prepared
Step 9 Exercise Makes Your Plan Functional
Step 10 Ongoing Review and Improvement

Step 09 Responding to and reporting information security incidents

It is vital to recognize that security incidents are unavoidable. Yet, security incidents continue to bring chaos among people, disabling them from containing the damage swiftly. It is important to know how to respond to information incidents that may lead to system disruption. This way, you can reduce the impact on your business operation, minimize the damage caused, monitor the incident effectively and learn from the experience.

Continuously implementing the PDCA cycle allows you to effectively reinforce your information security defense.

As information security incidents usually happen without warning, you should have in place a set of useful measures to quickly resort to when an information security incident occurs.

In addition to internal controls, you can also contact Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC)
(http: // www.cert.org.tw) for assistance.

Step 10 How to determine the effectiveness of your ISMS

After you have put so much effort into information asset identification, risk assessment, risk treatment and BCP, it is time to check whether what you have done is correct and whether the controls are effective.

You can check the effectiveness of your ISMS from two angles:

❶ **Technical:**
Common technical methods include: Information security health checks, vulnerability scanning, penetration testing, etc. Usually, these are done by having information security experts visiting your company to conduct information security tests and simulate attacks. This allows the experts to produce a diagnosis for your ISMS that points out blind spots of your ISMS team and draws attention to security loopholes.

❷ **Non-technical:**
You may review your ISMS through regular internal and external audits to ensure that your information security is protected according to plan. Of course, if you would like to take your ISMS to the next level, you can consider applying for ISO 27001 certification to ensure that your ISMS is fully developed and internationally recognized.

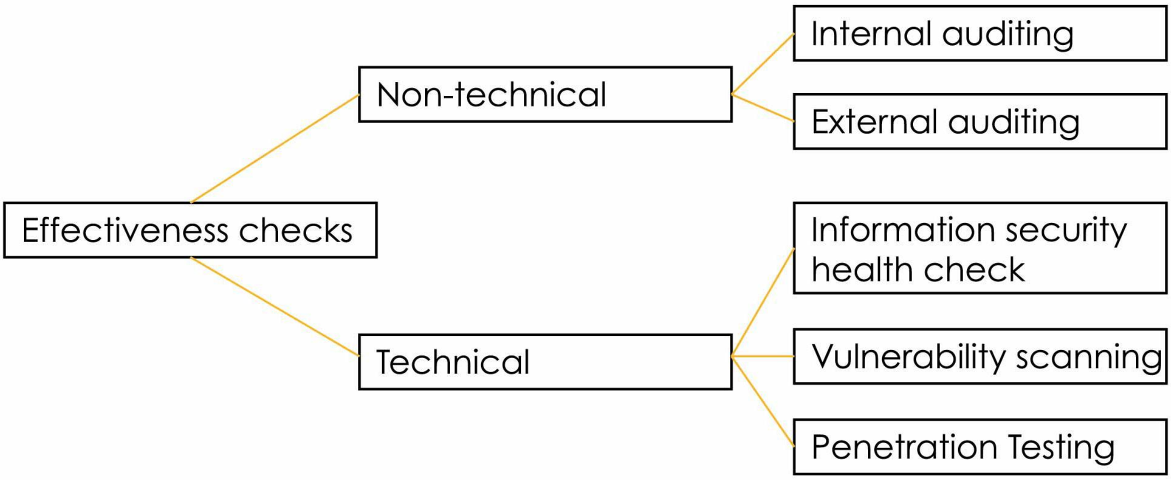


Figure 3: Types of ISMS effectiveness checks

Step 11

Continuous ISMS improvement and problem follow-up

Continuous improvement is vital to maintaining your ISMS. In your daily maintenance of the ISMS, you may find problems during regular checks, in information security incidents or as you conduct step 10. In this case, you should seek to understand the causes and look for appropriate and effective solutions. These solutions must be followed up on to ensure effective and correct implementation.

04 Checklist

Self-Assessment Checklist for SMEs

#	Question	Step	Answer		
			No	Partly yes	Yes
1	Has your company clarified relevant legal or regulatory requirements and contractual obligations?	1	0	2	4
2	Has your company understood both the internal and external ISMS issues concerning the company?	1	0	2	4
3	Has your company clarified stakeholders' requirements and expectations for information security?	1	0	2	4
4	Has your company selected an ISMS leader and formed an ISMS team?	1	0	2	4
5	Does everyone in the company have a clear understanding of the company's ISMS policy?	2	0	2	4
6	Are there specific and measurable objectives for your company's ISMS?	2	0	2	4
7	Are there regular reviews on the implementation results of the company's ISMS policy and objectives?	2	0	2	4
8	Has your company produced an information asset categorization plan at the early stage of risk management?	3	0	2	4
9	After having a categorization plan, has your company taken stock of its information assets and put them in their respective categories?	3	0	2	4

10	After taking stock of the company’s information assets, has your company assessed asset values, external threats and internal vulnerabilities based on asset characteristics?	4	0	2	4
11	Has your company used both qualitative and quantitative analyses in risk assessment?	4	0	2	4
12	Has your company determined which information assets are high-risk based on the risk assessment results?	5	0	2	4
13	Has your company created a risk treatment plan for high-risk information assets that reflects the company’s usable resources?	6	0	2	4
14	After producing the risk treatment plan, has your company selected and implemented controls?	7	0	2	4
15	Has your company formulated a business continuity plan that takes into account possible disasters for the company?	8	0	2	4
16	While information security incidents are unavoidable, has your company designed a reporting process for effective management and damage containment?	9	0	2	4
17	Has your company conducted non-technical ISMS effectiveness checks?	10	0	2	4
18	Has your company conducted technical ISMS effectiveness checks?	10	0	2	4
	Total Score				

What is the ISMS in your company like?	Total Score
Your company's ISMS is not effective enough. Your company is vulnerable to information security threats and the loss that they may bring.	< 24
Your company has begun to notice the importance of ISMS but the effort remains insufficient. You are suggested to continue to strengthen your ISMS.	≧ 24 < 48
Your company is rather protected in terms of information security; however, this is no guarantee that information security threats won't happen. You are suggested to continuously improve your ISMS based on regular risk assessment results and seek to achieve higher standards.	≧ 48

Appendix: Easy Tools for Information Security and Information Security Organizations

Easy Tools for Information Security
1. **Removing threats from contaminated computers** http://esupport.trendmicro.com/solution/zh-tw/1097458.aspx
2. **/URL safety checks** https://global.sitesafety.trendmicro.com/index.php https://www.google.com/transparencyreport/safebrowsing/diagnostic/?hl=zh-TW http://www.urlvoid.com/ https://www.virustotal.com/
3. **File virus checks** https://www.virustotal.com/
Information Security Organizations/Companies
1. **Taiwan Computer Emergency Response Team / Coordination Center** http://www.twcert.org.tw
2. **National Information and Communication Security Center** https://www.ncert.nat.gov.tw/
3. **165 National Anti-fraud Hotline** http://165.gov.tw/index.aspx
4. **Taiwan Cloud Security Alliance** https:// www.twcsa.org/
5. **Trend Micro** http://www.trendmicro.tw/tw/index.html
6. **HiNet Internet Security** http://hisecure.hinet.net/secureinfo/hotnews.php
7. **OWASP** https://www.owasp.org/index.php/Main_Page
8. **FIRST (Forum of Incident Response and Security Teams)** https://www.first.org/
9. **APCERT (Asia Pacific Computer Emergency Response Team)** http://www.apcert.org/

Note

Note

Note

主辦單位
Host

經濟部中小企業處
SMALL AND MEDIUM ENTERPRISE ADMINISTRATION,
MINISTRY OF ECONOMIC AFFAIRS

合作夥伴
Partner

TREND MICRO 趨勢科技

執行單位
Organizer

台灣經濟研究院
Taiwan Institute of Economic Research

APEC Project: SME 01 2016A

Produced by

APEC SME Crisis Management Center
5F, No. 16-8, Dehuei St., Jhongshan District, Taipei 10461,
Chinese Taipei
Tel: (886)-2-2586-5000 #548 Fax: (886)-2-2599-3713

Small and Medium Enterprise Administration, Ministry of Economic Affairs, Chinese Taipei
3F, No. 95, Sec 2, Roosevelt Rd., Taipei 100, Chinese Taipei
Tel: (886)-2-2366-2237 Fax: (886)-2--2367-7484

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#217-SM-03.1.