



如何使用「香港社福界 - 資訊科技保安實務指南」

分享「資訊科技保安審計先導計劃」的觀察及經驗

20 / 01 / 2022

Sean Tam

Billy Ho



如何使用「香港社福界 - 資訊科技保安實務指南」



IT Security Practice Guide

- To develop one (1) IT Security Practice Guide for all NGOs



One(1) for “Large NGOs”



One(1) for “Medium NGOs”



One(1) for “Small NGOs”



1 for all NGOs

- 3 security levels for different protection requirements

Elementary

Intermediate

Advanced

17 Security Domains

1. IT Security Governance
2. Password Control and Authentication
3. Websites and Web Applications
4. Data Management
5. Computer Networks Security
6. Email Security
7. Cloud Computing Security
8. Physical Security
9. Mobile Security
10. Remote Access/Work from Home
11. Security Risk Assessment and Audit
12. Insider Threats
13. Vendor Management
14. Awareness and Training
15. Incident Response
16. Business Continuity Management
17. Log Management and Monitoring

3 Security Level

Elementary

The basic good practices

Intermediate

More good practices will be covered

Advanced

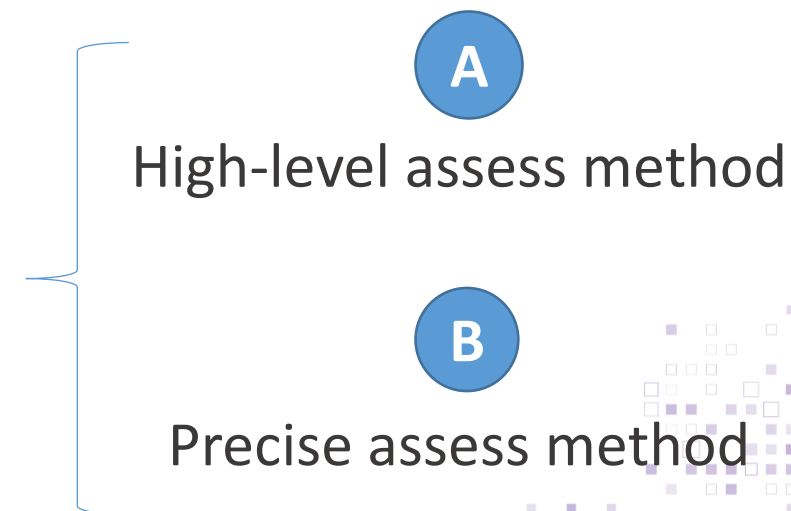
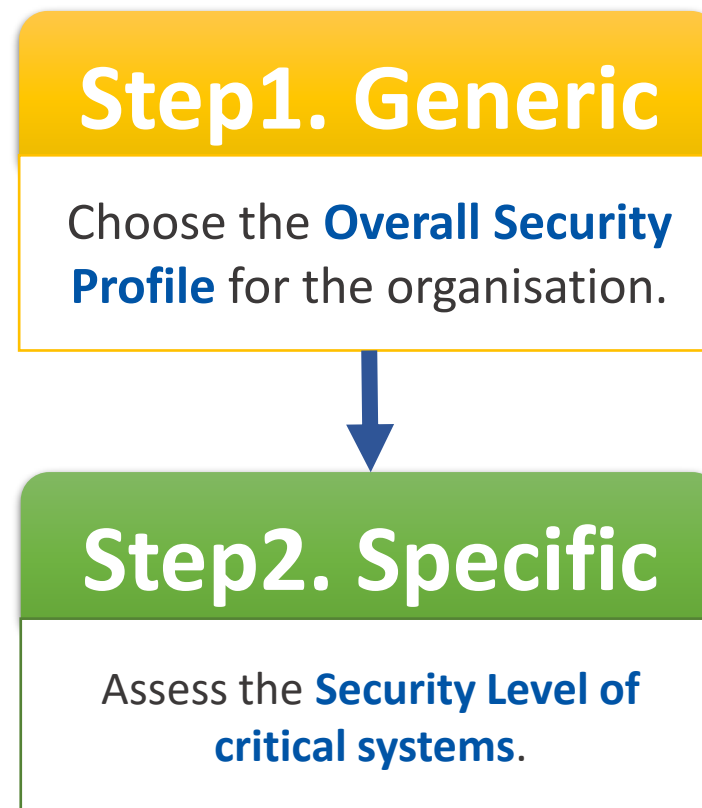
The comprehensive good practices will be covered

3 Security Level

Remote Access/Work from Home				
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Access to your home computer's desktop and mobile devices should at least be password protected, and the password should be strong one.	✓	✓	✓
2	Update your personal devices antivirus solution with an updated signature and update your software and operating systems.		✓	✓
3	Encrypt devices and other media that contain sensitive personal information. Includes laptops, tablets, smartphones, removable drives, and cloud storage solutions. Disk encryption or folder encryption also helps protect information on stolen or compromised computers.			✓



How can NGO choose the protection requirements?





Current State



Target State

Step1. Generic

Choose the **Overall Security Profile** for the organisation.

Basic

Advanced

Intermediate

Elementary



A Progressive Model

High-level assess method

Elementary

NGO should adopt the requirements of elementary security level to **all assets**.

Intermediate

NGO should adopt the requirements of intermediate security level to **the assets which contain valuable and sensitive information**.

Advanced

NGO should adopt the requirements of advanced security level to **the high-risk assets, such as public internet facing, cloud platform, aged applications**.

Step2. Specific

Assess the **Security Level of critical systems.**

Precise assess method

NGO can use **IT Asset valuation template** to assess the security requirement of their systems accurately.

Basic Information			IT Asset Attribute						Risk Component & Security Score (automatically determined)			
Asset No.	Asset Information	Location	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Patches (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
WAS-001	WebApp Internet Facing, Cross NGOs	NGO DC-001	High	Sensitive	Before Launch	Outdated	Backup	Own & Partners	High	Very High	High	13
WAS-002	WebApp Backend system (Confidential)	NGO DC-002	High	Confidential	Before Launch	Outdated	Backup	Own	High	Very High	Low	11
WAS-003	Website for Public	Public Cloud (Azure)	High	Public	Before Launch	Outdated	Backup	Public	High	Medium	Medium	10
SYS-001	WebApp for NGO & Public Users	Public Cloud (Azure)	High	Restricted	Before Launch	Outdated	Backup	Own & Public	High	High	Very High	13
SYS-002	WebApp for Internal users	On-premises	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
SYS-003	WebApp Internal (Sensitive)	On-premises	Medium	Sensitive	Before Launch	Outdated	Backup	Own	High	High	Low	10
Mobile-001	Mobile App Internal	Out Door	Medium	Restricted	Before Launch	Outdated	Not Available	Own	High	Medium	Medium	10
NGO-Data	NGO Proprietary Info.	NGO	Medium	Sensitive	Before Launch	Outdated	Backup	Own	High	High	Low	10

The system can be **one device (one IP address)** [more specific] or **a set of devices in a system** [more general].

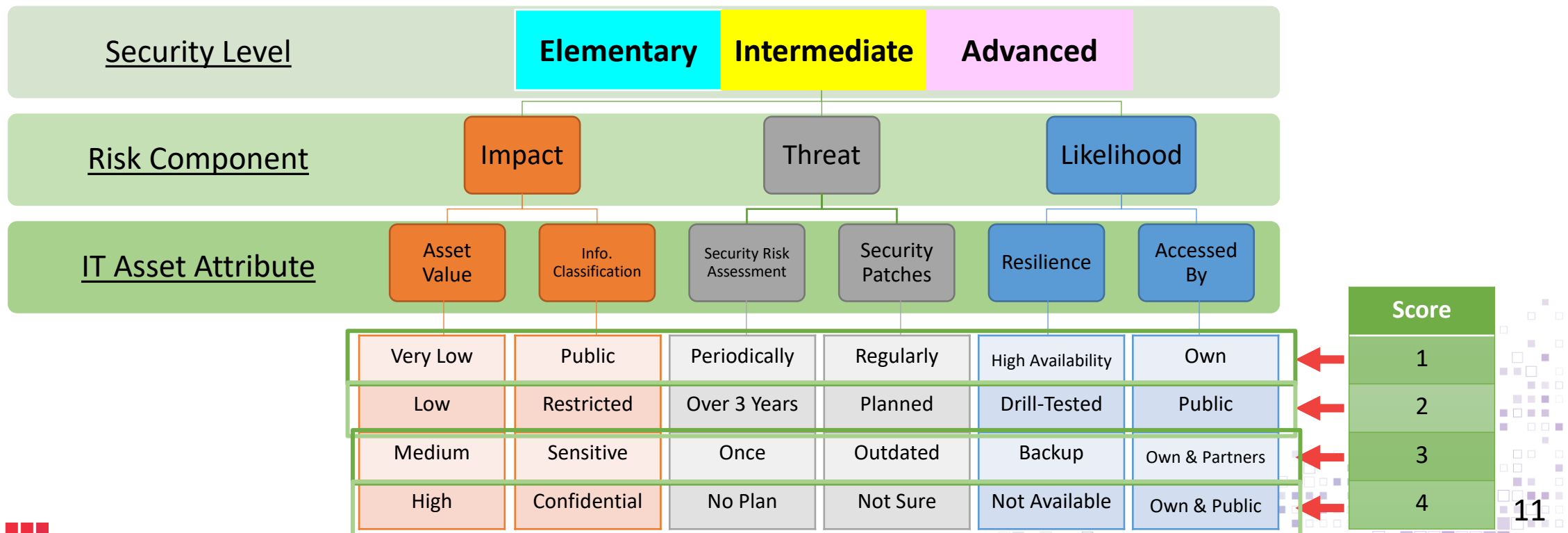
Step2. Specific

Assess the **Security Level**
of critical systems.

Precise assess method

Based on the 6 attributes of IT assets to determine 3 measures of risk component : “ Impact”, “Threat” and “Likelihood”.

Figure out 3 security level: “Elementary”, “Intermediate”, and “Advanced”



Step2. Specific

Assess the **Security Level** of critical systems.

Risk Component and Security Level

Risk Component

Asset Value	Impact Score: Asset & Classification			
	1	2	3	4
	2	3	4	5
	3	4	5	6
	4	5	6	7
	1	2	3	4
Information Classification				

Impact Level = Asset Value and Information Classification

Update	Threat Score: Update & Risk Assessment			
	1	2	3	4
	2	3	4	5
	3	4	5	6
	4	5	6	7
	1	2	3	4
Security Risk Assessment				

Threat Level = Security Risk Assessment and System Update

Resilience	Probability Score: Resilience & Accessed by			
	1	2	3	4
	2	3	4	5
	3	4	5	6
	4	5	6	7
	1	2	3	4
Accessed By				

Likelihood Level = Accessed By and Resilience

Security Level

Security Level	Impact + Threat + Likelihood
Elementary	Security Score: 3 ~ 7
Intermediate	Security Score: 8 ~ 11
Advanced	Security Score: 12 ~ 15



The IT Asset valuation template will **automatically** determine the Risk Component and Security Level

IT Asset Valuation List Template

										Risk Component & Security Score (automatically determined)			
Basic Information			IT Asset Attribute										
1	Asset No.	Asset Information	Location	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Patches (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
2	WAS-001	WebApp Internet Facing, Cross NGOs	NGO DC-001	High	Sensitive	Before Launch	Outdated	Backup	Own & Partners	High	Very High	High	13
3	WAS-002	WebApp Backend system (Confidential)	NGO DC-002	High	Confidential	Before Launch	Outdated	Backup	Own	High	Very High	Low	11
4	WAS-003	Website for Public	Public Cloud (Azure)	High	Public	Before Launch	Outdated	Backup	Public	High	Medium	Medium	10
5	SYS-001	WebApp for NGO & Public Users	Public Cloud (Azure)	High	Restricted	Before Launch	Outdated	Backup	Own & Public	High	High	Very High	13
6	SYS-002	WebApp for Internal users	On-premises	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
7	SYS-003	WebApp Internal (Sensitive)	On-premises	Medium	Sensitive	Before Launch	Outdated	Backup	Own	High	High	Low	10
8	Mobile-001	Mobile App for Internal	Out Door	Medium	Restricted	Before Launch	Outdated	Not Available	Own	High	Medium	Medium	10
9	NGO-Data	NGO Proprietary Info.	NGO	Medium	Sensitive	Before Launch	Outdated	Backup	Own	High	High	Low	10
10	NGOs-Data	NGO Shared Info.	G-Suite-Google	Medium	Sensitive	Before Launch	Planned	Not Available	Own	Medium	High	Medium	10
11	NGO-Data-X	NGO Internal Data	On-premises	High	Restricted	No Plan	Outdated	Backup	Own	Very High	High	Low	11
12	NGO-Data-XX	NGO Sensitive Data	On-premises	Medium	Sensitive	Before Launch	Outdated	Backup	Own	High	High	Low	10
13	WEB-001	NGO Main Site	Cloud	Medium	Sensitive	Before Launch	Planned	Not Available	Public	Medium	High	High	11
14	WEB-002	NGO Intranet	On-premises	Medium	Restricted	No Plan	Planned	Backup	Own	High	Medium	Low	9
15	XFW-0001	10.10.1.1 / 225.128.1.1	HQ-DC-01	High	Confidential	Before Launch	Outdated	Not Available	Own	High	Very High	Medium	12
16	HRS-1002	227.12.27.5	HRM-Azure-Cloud	Medium	Restricted	Occasional	Planned	Backup	Own	Low	Medium	Low	7
17	FIN-1001	226.50.1.10	IMS-Azure-Cloud	Medium	Sensitive	Occasional	Planned	Backup	Own	Low	High	Low	8
18	NGO-APP-001	NGO Application	HQ-DC-01	Medium	Restricted	Before Launch	Outdated	Not Available	Own	High	Medium	Medium	10
19	IFS-HQ-DC-OA-01	10.10.20.100	HQ-DC-01	Medium	Restricted	No Plan	Outdated	Not Available	Own	Very High	Medium	Medium	11
20	IFS-HQ-DC-CASE-01	10.10.20.101	HQ-DC-01	Medium	Restricted	No Plan	Outdated	Not Available	Own	Very High	Medium	Medium	11
21	WEB-HQ-DC-01	10.10.1.10/225.128.1.2	Cloud AWS	Medium	Restricted	Before Launch	Planned	Not Available	Public	Medium	Medium	High	10
22	IDB-HQ-DC-01	10.10.5.5	HQ-DC-01	High	Sensitive	Occasional	Outdated	Backup	Own	Medium	Very High	Low	10
23	IDB-HQ-DC-02	10.10.5.6	HQ-DC-01	High	Restricted	Before Launch	Outdated	Backup	Own & Partners	High	High	High	12
24	Financial Data	NGO Financial Data	HQ-DC-01	Medium	Sensitive	Occasional	Planned	Backup	Own	Low	High	Low	8
25	HR Data	NGO HR Data	HQ-DC-01	Medium	Restricted	Occasional	Planned	Backup	Own	Low	Medium	Low	7
26	NGO Broad Data	NGO Broad Data	HQ-DC-01	Medium	Confidential	Occasional	Planned	Backup	Own	Low	Very High	Low	9
27	Guest-WIFI	NGO Guest WIFI	HQ Main Hall	Very Low	Public	No Plan	Not Sure	Not Available	Public	Very High	Very Low	High	10



Asset Value

Info. Classification

Security Risk Assessment

Security Patches

Resilience

Accessed By

Asset Value

The primary assets:

[more specific]

one device (one IP address)

[more general]

a set of devices in a system

Level	Score	Description
Very Low	1	Require little effort or cost to recover, no impact to the organization.
Low	2	Cost of recovery acceptable, causing slight inconvenience or some embarrassment.
Medium	3	Moderate resources or effort to recover, financial and reputation loss are noticeable.
High	4	Significant financial or great effort to recover, loss of key asset or capability required carrying out services.

	A	B	F	G	H	I	J	K	L	M	N	O
	Asset No	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
1												
2	WAS-001	WebApp Internet Facing, Cr	High	Sensitive	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
3	WAS-002	WebApp Backend system (C	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
4	WAS-003	Website for Public	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
5	SYS-001	WebApp for NGO & Public U	High	Restricted	Once	Outdated	Backup	Own & Public	High	High	Very High	13
6	SYS-002	WebApp for Internal users	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
7	SYS-003	WebApp Internal (Sensitive)	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10
8	Mobile-001	Mobile App for Internal	Medium	Restricted	Once	Outdated	Not Available	Own	High	Medium	Medium	10
9	NGO-Data	NGO Proprietary Info.	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10

Asset
ValueInfo.
ClassificationSecurity
Risk
AssessmentSecurity
Patches

Resilience

Accessed
By

Information Classification (Confidentiality)

Level	Score	Description
Public	1	Information that are not sensitive and there is no issue with release to the general public i.e. organization website.
Restricted	2	Information only to be accessed internally or with third parties that have signed a non-disclosure agreement i.e. organisation email, policies, and procedures etc.
Sensitive	3	Information only to be accessed by the specified group i.e. organization financial information, clients' sensitive information.
Confidential	4	Information which, if disclosed to unauthorized persons (internal/external) could cause material harm to the organization i.e. information that could result in the loss of competitive advantage or reputation.

	A	B	F	G	H	I	J	K	L	M	N	O
	Asset No	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
1												
2	WAS-001	WebApp Internet Facing, Cro	High	Sensitive	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
3	WAS-002	WebApp Backend system (Co	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
4	WAS-003	Website for Public	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
5	SYS-001	WebApp for NGO & Public Us	High	Restricted	Once	Outdated	Backup	Own & Public	High	High	Very High	13
6	SYS-002	WebApp for Internal users	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
7	SYS-003	WebApp Internal (Sensitive)	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10
8	Mobile-001	Mobile App for Internal	Medium	Restricted	Once	Outdated	Not Available	Own	High	Medium	Medium	10
9	NGO-Data	NGO Proprietary Info.	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10

Asset
ValueInfo.
ClassificationSecurity
Risk
AssessmentSecurity
Patches

Resilience

Accessed
By

Security Risk Assessment

Score	Security Risk Assessment
1	Periodically
2	Over 3 Years
3	Once
4	No Plan

	A	B	F	G	H	I	J	K	L	M	N	O
	Asset No	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
1	WAS-001	WebApp Internet Facing, Cro	High	Sensitive	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
2	WAS-002	WebApp Backend system (Co	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
3	WAS-003	Website for Public	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
4	SYS-001	WebApp for NGO & Public Us	High	Restricted	Once	Outdated	Backup	Own & Public	High	High	Very High	13
5	SYS-002	WebApp for Internal users	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
6	SYS-003	WebApp Internal (Sensitive)	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10
7	Mobile-001	Mobile App for Internal	Medium	Restricted	Once	Outdated	Not Available	Own	High	Medium	Medium	10
8	NGO-Data	NGO Proprietary Info.	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10

Asset
ValueInfo.
ClassificationSecurity
Risk
AssessmentSecurity
Patches

Resilience

Accessed
By

System Update (Integrity)

Rate	System Patches Update
1	Regularly
2	Planned
3	Outdated
4	Not Sure

	A	B	F	G	H	I	J	K	L	M	N	O
	Asset No	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
1												
2	WAS-001	WebApp Internet Facing, Cro	High	Sensitive	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
3	WAS-002	WebApp Backend system (Co	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
4	WAS-003	Website for Public	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
5	SYS-001	WebApp for NGO & Public Us	High	Restricted	Once	Outdated	Backup	Own & Public	High	High	Very High	13
6	SYS-002	WebApp for Internal users	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
7	SYS-003	WebApp Internal (Sensitive)	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10
8	Mobile-001	Mobile App for Internal	Medium	Restricted	Once	Outdated	Not Available	Own	High	Medium	Medium	10
9	NGO-Data	NGO Proprietary Info.	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10

Asset
ValueInfo.
ClassificationSecurity
Risk
AssessmentSecurity
Patches

Resilience

Accessed
By

Resilience (Availability)

Rate	System Resilience
1	High Availability
2	Drill Tested
3	Backup
4	Not Available

	A	B	F	G	H	I	J	K	L	M	N	O
	Asset No	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
1												
2	WAS-001	WebApp Internet Facing, Cro	High	Sensitive	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
3	WAS-002	WebApp Backend system (Co	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
4	WAS-003	Website for Public	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
5	SYS-001	WebApp for NGO & Public Us	High	Restricted	Once	Outdated	Backup	Own & Public	High	High	Very High	13
6	SYS-002	WebApp for Internal users	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
7	SYS-003	WebApp Internal (Sensitive)	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10
8	Mobile-001	Mobile App for Internal	Medium	Restricted	Once	Outdated	Not Available	Own	High	Medium	Medium	10
9	NGO-Data	NGO Proprietary Info.	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10



Asset
Value

Info.
Classification

Security
Risk
Assessment

Security
Patches

Resilience

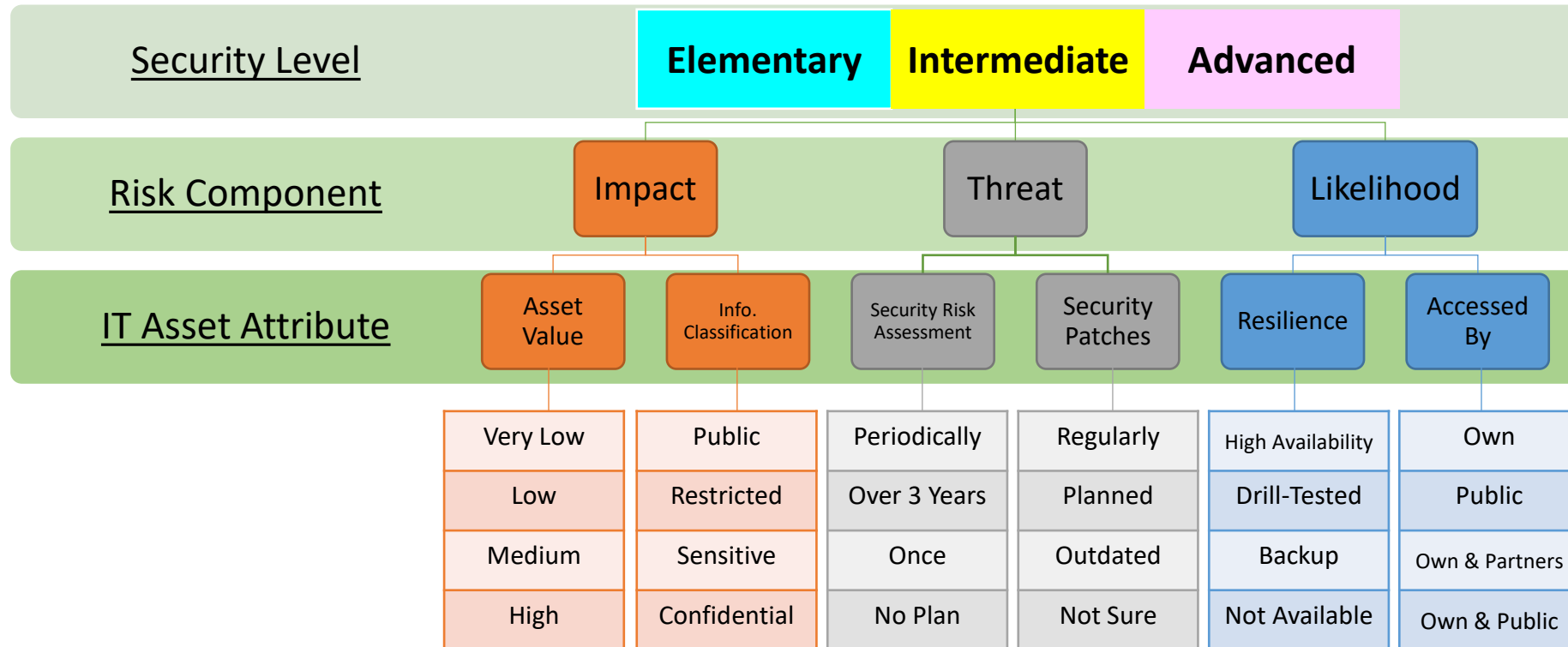
Accessed
By

Accessed By Whom

Level	Rate	Description
Own	1	Organisation internal access only.
Public	2	Open for public access
Own & Partners	3	Grant access to NGO, affiliated NGOs and/or third parties organisations.
Own & Public	4	Allow NGO and registered persons access with limited authority i.e. NGO membership portal.

	A	B	F	G	H	I	J	K	L	M	N	O
	Asset No	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Threat Level	Consequence (Impact)	Probability (Likelihood)	Security Score
1												
2	WAS-001	WebApp Internet Facing, Cro	High	Sensitive	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
3	WAS-002	WebApp Backend system (Co	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
4	WAS-003	Website for Public	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
5	SYS-001	WebApp for NGO & Public Us	High	Restricted	Once	Outdated	Backup	Own & Public	High	High	Very High	13
6	SYS-002	WebApp for Internal users	Medium	Restricted	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
7	SYS-003	WebApp Internal (Sensitive)	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10
8	Mobile-001	Mobile App for Internal	Medium	Restricted	Once	Outdated	Not Available	Own	High	Medium	Medium	10
9	NGO-Data	NGO Proprietary Info.	Medium	Sensitive	Once	Outdated	Backup	Own	High	High	Low	10

Precise assess method



Example

Step 3. The IT Asset Valuation List will **automatically** determine the Risk Component and Security Level

Basic Information		
Asset No.	Asset Info.	Location
1	Internal Database	On-premises

Step 1. Fill in the basic information in IT Asset Valuation List

Step 2. Fill in the IT Asset Attributes in IT Asset Valuation List

IT Asset Attribute					
Asset Value	Info. Classification	Security Risk Assessment	System Patches	Accessed By	Resilience
High	Confidential	No Plan	Outdated	Own	Backup

Risk Component & Security Score			
Impact	Threat Level	Likelihood	Security Score
Very High	Very High	Low	12

Database Security				
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Access to the database must be securely controlled.	✓	✓	✓
2	Whether your database server is on-premise or in a cloud data centre, it must be located within a secure, climate-controlled environment.	✓	✓	✓
3	Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky.		✓	✓
4	All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.		✓	✓
5	Always use the latest version of the database management software and apply all patches as soon as they are issued.			✓
6	Secure Data at Rest: Encrypt personal data stored in a database, in particular data which has a higher risk of harm to or which would adversely impact the relevant individuals in the event that it is compromised. • Encrypt storage (i.e.: Bitlocker, Databases (TDE) etc.) • Encrypt passwords and other configuration settings Secure Data in Transit: Enable database encryption services: • Enable network level encryption protocols • Virtual Private Network (SSL / IPSec)			✓
7	Log all unauthorised and anomalous database activities, so that these activities can be tracked and analysed.			✓

Step 4. Based on the security levels, follow the corresponding security recommendations on each covered area.

Checklists and Templates

- IT Asset Valuation List Template
- Security Incident Response Form and Records (Template)
- Vendor Risk Assessment Checklist
- Security Audit Checklist Template
- Seven Habits of Cyber
- Security Risk Assessment Guidelines

Security Incident Response Report Form

INCIDENT IDENTIFICATION INFORMATION	
Date and Time of Notification: ..	
Incident Detector's Information: ..	
Name: ..	Date and Time Detected: ..
Title: ..	Location: ..
Phone/Contact Info: ..	System or Application: ..
INCIDENT SUMMARY	
Type of Incident Detected: ..	
<input type="checkbox"/> Denial of Service	<input type="checkbox"/> Malicious Code
<input type="checkbox"/> Unauthorized Access	<input type="checkbox"/> Unauthorized Use
<input type="checkbox"/> Unplanned Downtime	<input type="checkbox"/> Other ..
Description of Incident: ..	

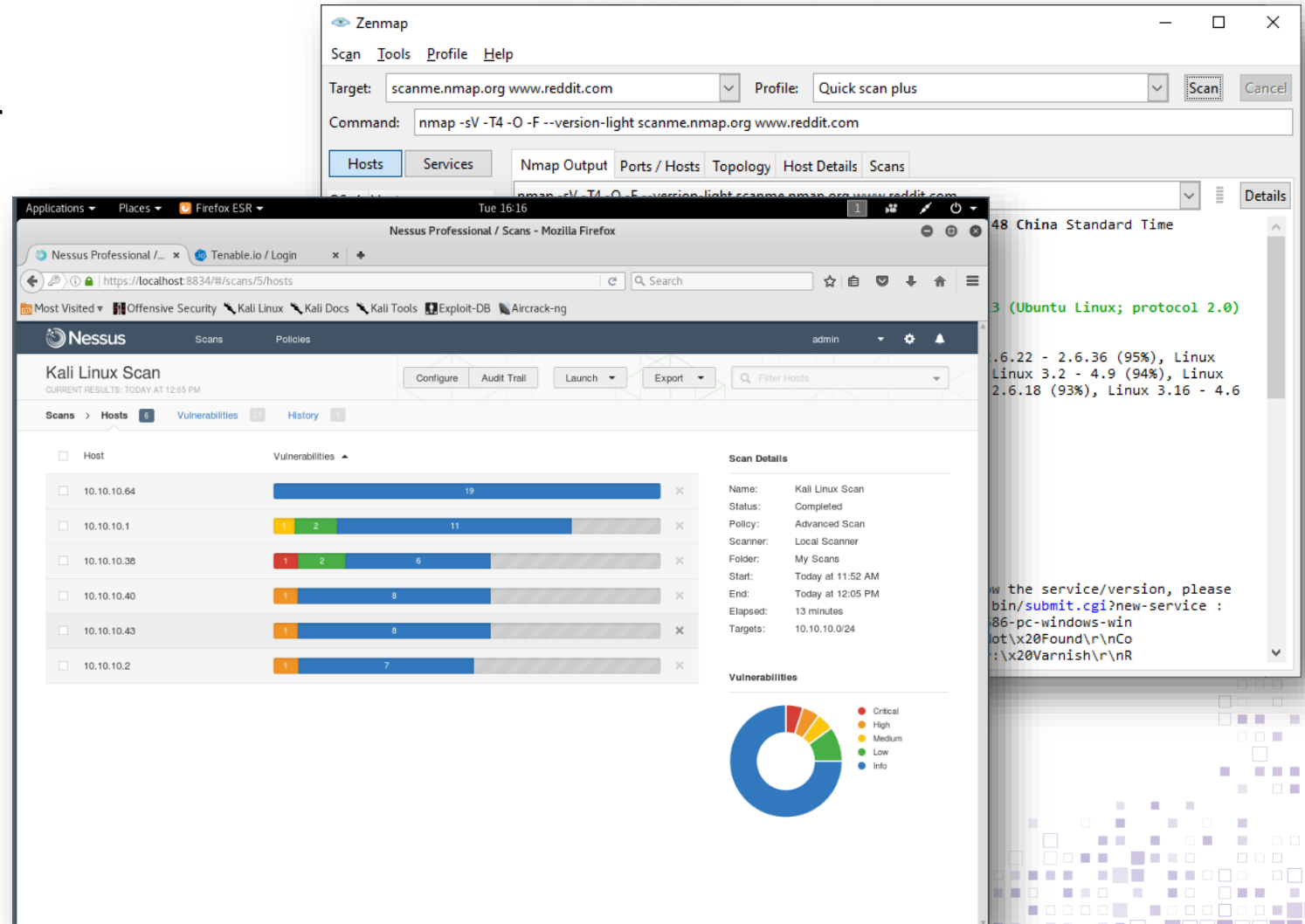
Seven Habits of Cyber Security for NGOs

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
1. Security Policy and Security Management	Security Policy is an important document in an organization. It dictates security requirements and attitude of senior management with respect to cybersecurity risk management. Senior management should setup a mechanism to maintain and disseminate the requirements of security policy to staff in a regularly basis.	<input type="checkbox"/> Staff should be given a chance to read through the security policy, understand security requirements of the organization and acknowledge to conform when they onboard. <input type="checkbox"/> The policy should be put in somewhere the staff can refer to easily. <input type="checkbox"/> Policy should be updated and let the staff to re-acknowledge the policy regularly.	<input type="checkbox"/> My organization does not have a security policy <input type="checkbox"/> My organization has a security policy <input type="checkbox"/> The security policy can be easily accessed by staff <input type="checkbox"/> Staff needed to acknowledge the security policy when they onboard <input type="checkbox"/> Staff needed to re-acknowledge the security policy regularly

Registry changes by malware.

Security Risk Assessment Tools

- WinAudit
- NMap/Zenmap Security Scanner
- Nessus Essentials
- OWASP Zed Attack Proxy (ZAP)
- Kali Linux
- Logging Made Easy
- VeraCrypt



分享「資訊科技保安審計先導計劃」的觀察及經驗


Case Sharing : NGO

- ❖ Lack of Cyber Security Awareness & Knowledge
- ❖ No IT Staff / Over Reliance on Service Providers
- ❖ Cyber Security Incident Happened Before
- ❖ Difficulty in Quantifying Cyber Risks



Before.. 25

NGO Sector Is Vulnerable....

An illustration of a person in a red shirt and black pants sitting at a white desk, working on a laptop. The background is a light blue circle containing various security-related icons: a red shield with a white exclamation mark, a blue folder with a red padlock, a blue folder with a red circle and a white exclamation mark, and a blue folder with a red circle and a white exclamation mark. Dotted lines connect the person to the icons.

Only **20%** of NGOs have a policy in place to address cyberattacks.

Source: NTEN

59% of NGOs do not provide any cybersecurity training to staff on a regular basis

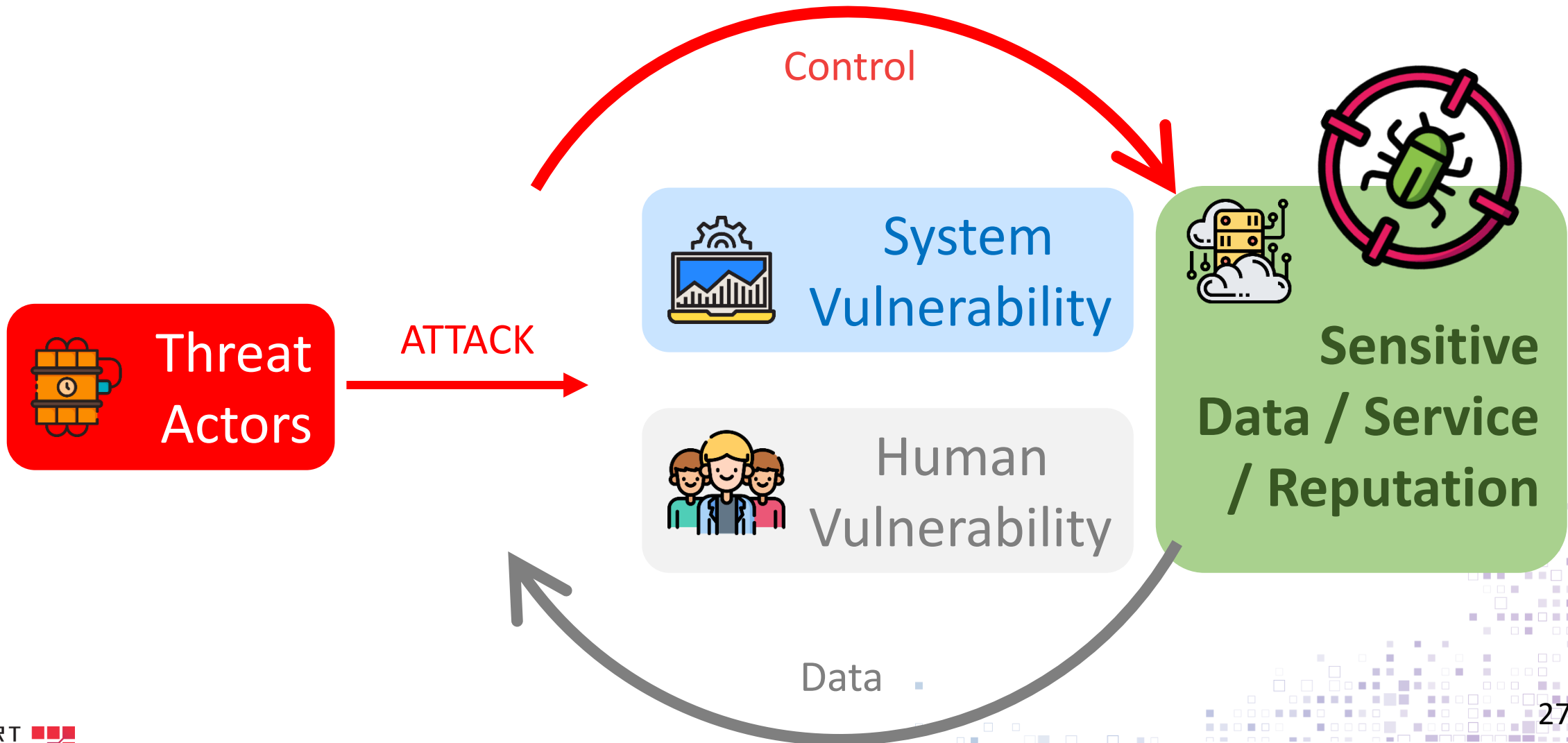
Source: NTEN

More than **70%** of NGOs have **NOT** run even one vulnerability assessment to evaluate their potential risk exposure.

Source: CohnReznick

Copyright © 2021 HKPC All rights reserved

Cyber Attack





System Vulnerability

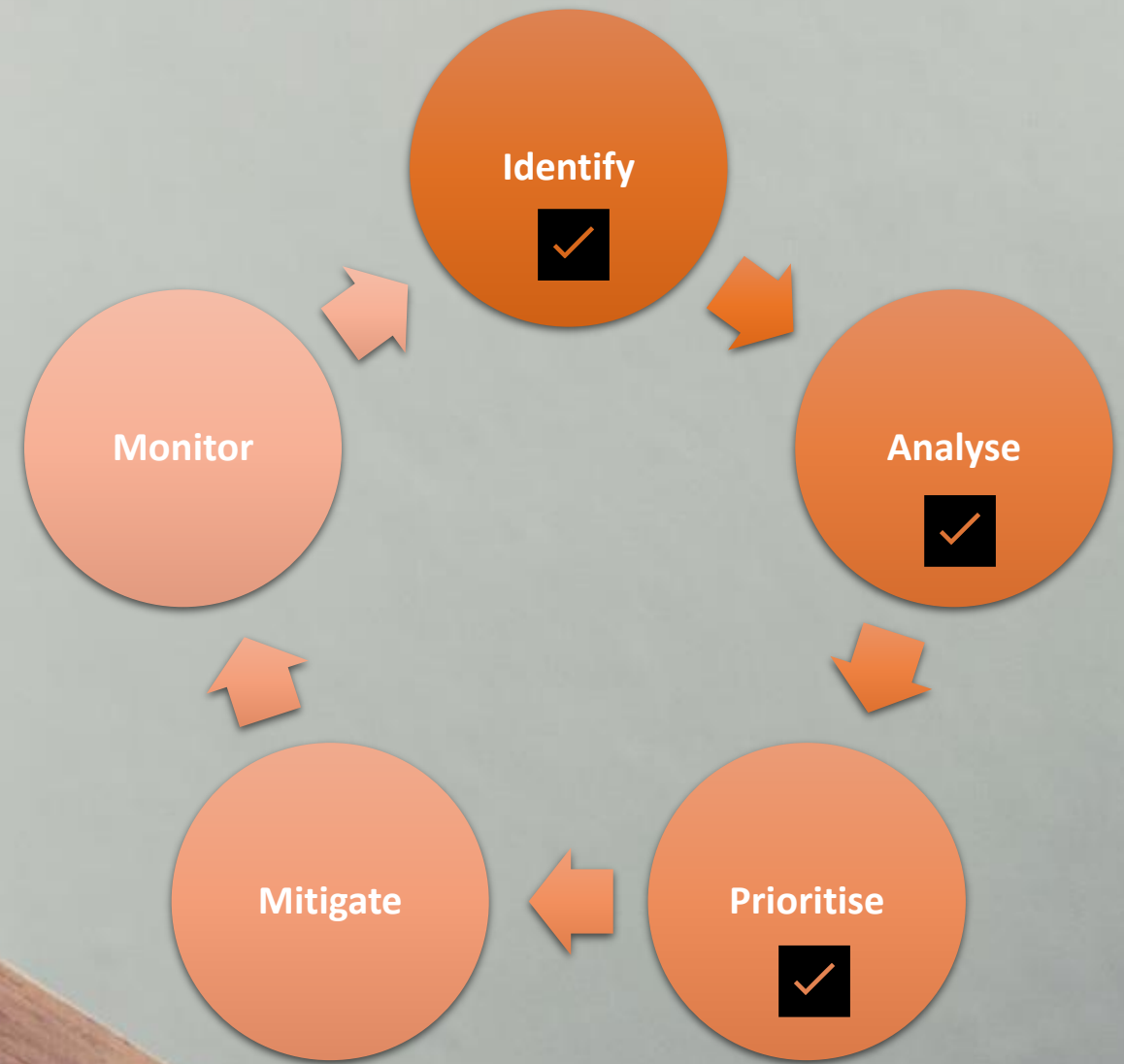
- Unpatched System/Software
- Misconfiguration
- Missing/Poor Encryption
- Bugs
- ...



Human Vulnerability

- Malicious Insider
- Careless Staff
- Staff vulnerable to social engineering
- Weak Passwords
- ...

Risk Management





Knowing Your Risks is not only the first step
to cyber security...
It is an important step also!



After..

Case Sharing : NGO

- ❖ **Improved Management & Staff's Cyber Security Awareness**
- ❖ **Identified the Weakness and Vulnerability on the Systems and Operation Workflow**
- ❖ **Better Understand Cyber Risks and Corresponding Mitigation Actions**

Thank you!

IT Security Portal

<https://itsecurity.hkcss.org.hk/>

HKCERT

<https://www.hkcert.org/>

HOTLINE: **8105 6060**

Sean Tam

Email: seantam@hkpc.org

Phone: **2788 5857**

Billy Ho

Email: billyho@hkpc.org

Phone: **2788 5779**