



IT Security Practice Guide for the Social Welfare Sector in Hong Kong

Version 1.0

April 2021

The contents of this document are prepared by Hong Kong Productivity Council (HKPC), appointed by The Hong Kong Council of Social Service (HKCSS) as Information Technology Security Consultant. The copyright of this document is owned by HKCSS. The purpose of this document is to improve the IT security of the Social Welfare Sector in Hong Kong. This document shall not be used or reproduced wholly or partially without prior and explicit consent of HKCSS.

Distribution

Copy No.	Holder
1	Hong Kong Productivity Council (HKPC)
2	Information Technology Resource Centre (ITRC) of the Hong Kong Council of Social Service (HKCSS)

Version History

Ver. No.	Ver. Date	Description	Filename
0.1	Sep 2020	First Draft	IT Security Practice Guide for the Social Welfare Sector v0.1 (20200918)
0.2	Dec 2020	Revised draft version based on comments from PSC members and Pilot NGOs	IT Security Practice Guide for the Social Welfare Sector v0.2 (20201214)
1.0	April 2021	Official Version	IT Security Practice Guide for the Social Welfare Sector v1.0 (20210416)

Prepared By: Consultancy Team Endorsed By: _____
Hong Kong Productivity Council

Date: April 2021 Date: _____

TABLE OF CONTENTS

Preface	6
1. Introduction	7
2. NGO IT Security Overview	9
3. The Audience	10
4. Stakeholder of Security Domain	11
5. IT Security Practices Framework	12
6. IT Asset Valuation	13
6.1. Security Profile [Elementary, Intermediate, Advanced]	13
6.2. IT Asset Valuation Template Content.....	15
7. IT Security Practices for NGO	20
7.1. IT Security Governance	20
7.2. Password Control and Authentication.....	33
7.3. Websites and Web Applications	37
7.4. Data Management	40
7.5. Computer Networks Security	45
7.6. Email Security	47
7.7. Cloud Computing Security.....	49
7.8. Physical Security	56
7.9. Mobile Security	58
7.10. Remote Access/Work from Home	62
7.11. Security Risk Assessment and Audit	64
7.12. Insider Threats.....	66
7.13. Vendor Management	69
7.14. Awareness and Training.....	71
7.15. Incident Response Management.....	72
7.16. Business Continuity Management.....	75
7.17. Log Management and Monitoring.....	78
8. Checklists and Templates	80
8.1. IT Asset Valuation List Template	80
8.2. Security Incident Response Form and Records (Template).....	81
8.3. Vendor Risk Assessment Checklist.....	83
8.4. Security Audit Checklist Template	84
8.5. Seven Habits of Cyber Security	85
8.6. Security Risk Assessment Guidelines	86
9. Security Risk Assessment Tools	87
9.1. WinAudit.....	87
9.2. NMap/Zenmap Security Scanner	88
9.3. Nessus Essentials.....	89
9.4. OWASP Zed Attack Proxy (ZAP)	90
9.5. Kali Linux	91
9.6. Logging Made Easy (LME)	92
9.7. VeraCrypt.....	93
Appendix A - References	94
Appendix B - Glossary	95
Appendix C - Acronyms	99

Tables Reference

<i>Table 1: IT Security Practices Sections</i>	11
<i>Table 2: Six Formal Information Valuation Models</i>	13
<i>Table 3: IT Asset Valuation Template Content</i>	17
<i>Table 4: Impact Level = Asset Value and Information Classification (Confidentiality)</i>	17
<i>Table 5: Threat Level = Security Risk Assessment and System Update (Integrity)</i>	17
<i>Table 6: Likelihood Level = Accessed By and Resilience (Availability)</i>	17
<i>Table 7: IT Asset Attributes and Risk Components</i>	18
<i>Table 8: IT Asset Protection Security Level</i>	19
<i>Table 9: Benchmarking Example</i>	19
<i>Table 10: Policies and Procedures</i>	23
<i>Table 11: Asset management</i>	25
<i>Table 12: Recommended Information Classification Mapping</i>	26
<i>Table 13: Information Classification Definition</i>	27
<i>Table 14: Information Classification</i>	27
<i>Table 15: Asset Matrix Handling Example</i>	28
<i>Table 16: Information Handling</i>	29
<i>Table 17: Configuration Management</i>	31
<i>Table 18: Support and Competence</i>	32
<i>Table 19: Traditional Password Control</i>	34
<i>Table 20: NIST Suggested Password Control</i>	36
<i>Table 21: Authentication</i>	37
<i>Table 22: Websites and Web Applications</i>	39
<i>Table 23: Data Security</i>	40
<i>Table 24: Database Security</i>	41
<i>Table 25: Personally Identifiable Information Protection</i>	44
<i>Table 26: Computer Network Security</i>	46
<i>Table 27: Email Security</i>	48
<i>Table 28: AWS Shared Responsibility Model for Security in the Cloud</i>	49
<i>Table 29: Azure Shared Responsibility Model for Security in the Cloud</i>	49
<i>Table 30: Cloud Computing Security</i>	53
<i>Table 31: Avoid Cloud Vendor Lock-In</i>	55
<i>Table 32: Physical Security</i>	57
<i>Table 33: Mobile Device Security</i>	59
<i>Table 34: Portable Device Security</i>	61
<i>Table 35: Remote Access/Work from Home</i>	63
<i>Table 36: Security Risk Assessment and Audit</i>	65
<i>Table 37: Insider Threats</i>	68
<i>Table 38: Vendor management</i>	70
<i>Table 39: Awareness and Training</i>	71
<i>Table 40: Incident Response Management</i>	74
<i>Table 41: Business Continuity Management</i>	77
<i>Table 42: Log Management and Monitoring</i>	79
<i>Table 43: Glossary</i>	98
<i>Table 44: Common Abbreviations</i>	100

Figures Reference

Figure 1: Policies, Standards, Procedures and Guidelines Hierarchy 21
Figure 2: The Asset Management Process Workflow 25
Figure 3: The Configuration and Change Management Process Workflow 31
Figure 4: BitLocker Drive Encryption – Control Panel 60
Figure 5: NIST SP800-61r2 Incident Response Life Cycle..... 72
Figure 6: Business Continuity Management Tasks..... 77
Figure 7: Cyber Security Monitoring..... 79
Figure 8: Umbrella View of SIEM 79
Figure 9: IT Asset Valuation Template (Templates) 80
Figure 10: Security Incident Reporting Form (Template) 81
Figure 11: Security Incident Reporting Records (Template)..... 82
Figure 12: Vendor Risk Assessment Management Record (Template)..... 83
Figure 13: NGO IT Audit Checklist (Template)..... 84
Figure 14: Seven Habits of Cyber Security..... 85
Figure 15: Security Risk Assessment Guidelines 86
Figure 16: WinAudit Asset Audit Tool 87
Figure 17: Nmap Network Scanner 88
Figure 18: Nessus Vulnerability Scanner 89
Figure 19: Zed Attack Proxy OWASP 90
Figure 20: Kali Linux..... 91
Figure 21: Logging Made Easy 92
Figure 22: VeraCrypt..... 93

Preface

The formidable developments in Information Technology (IT) and the Internet have revolutionised the way we live and work. Alongside the undeniable benefits that computerisation introduces in modern society, it also introduces vulnerabilities, so the cyberspace's security should be a significant concern of all stakeholders.

Non-Government Organisations (NGOs)' primary goal is to exist to serve specific goals, work towards a mission, and focus efforts on obtaining funding and reducing costs. Ownership, management, and staff all work towards these goals, as their entire incentive structure is built on them.

NGOs rely on the use of information technology for both their operations and strategic applications. In a sense, they are no different from any small, medium or large-scale enterprise regarding IT. Many NGOs in the social welfare sector may process sensitive information and personally identifiable information (PII). Keeping information confidential and free from integrity and privacy challenges as well as ensuring their systems are available are important to an NGO. They need to ensure they are protecting themselves, staff, data and systems against cyber security threats.

NGOs typically focus on providing IT to support their operations and services. Cyber security for an NGO will only receive more attention after an extensive or damaging security incident. Most corporate organisations are considered mature in managing information security; but NGOs in Hong Kong are still far behind in their quest towards that desired maturity level. Some tasks can be carried out within the social welfare NGO in order to achieve reasonable control in the area of information security.

The common IT security weaknesses in NGOs are:

- Lack of IT expertise and information security expertise
- Resources and priority
- Lack of compliance and regulation
- Security awareness

1. Introduction

In recognition of the importance of proactive information security management to maintain stability and integrity of NGOs, and the protection of the stakeholders' interests, this IT Security Practice Guide (this Guide) sets forth a voluntary risk-based cyber security approach – a set of industry standards and best practices to help NGOs of the social welfare sector in Hong Kong.

This Guide herein generally aims to strengthen NGOs' ability to customise and quantify adjustments to their cyber security programs using cost-effective security controls and risk management techniques. For small NGOs, this can help to understand how to provide basic security for computer systems and networks, raise security awareness within the organisation, and protect sensitive information as a social service organisation. For large NGOs, this provides a cost-effective approach to securing computer systems based on business needs of the organisation, without placing additional regulatory requirements on the business.

Keys in this Guide include:

- A sound governance framework with strong leadership is essential to strengthen organisation-wide cyber security. Board-level and senior management-level engagement are critical to the success of NGOs' cyber security controls, along with a clear chain of accountability.
- A well-trained staff with good security awareness can serve as the first line of defence against cyber-attacks. Effective training can reduce the likelihood of a successful attack by providing well-intentioned staff with the knowledge to avoid becoming inadvertent attack vectors (for example, by unintentionally downloading malware).
- The level of sophistication of technical controls employed by an individual NGO is highly contingent on their situation. While smaller NGOs may not be positioned to implement the included controls in their entirety, these strategies can serve a critical benchmarking function to support an understanding of vulnerabilities relative to industry standards.
- NGOs often use third-party vendors for IT services such as Cloud Computing Services and Application Development/Support, which may require vendor access to sensitive information. NGOs should manage cyber security risk exposures that arise from these relationships by exercising strong due diligence and developing clear operation and verification policies.

This Guide is general in nature, and the contents may not be applicable in all situations. This Guide is intended to function as a living document and will continue to be updated and improved as the industry provides feedback on implementation. Lessons learned from the early distribution of this framework to NGOs will be integrated into future versions. It can ensure that the document continues to meet NGOs' needs in an environment of dynamic threats and innovative solutions.

When NGOs refer to this Guide, they need to make reasonable judgments based on factors such as their own situation, existing procedures, resources, information and system environment. The Hong Kong Council of Social Service (HKCSS) will not be held responsible for any problems arising during the adoption of this Guide or failing to meet the security requirements in this Guide.

What's in this Guide

Chapter 1 An introduction to the idea and purpose of this Guide.

Chapter 2 Give an overview on why IT Security is important on NGOs everyday operations, and how this guide could help them develop into IT resilient organisations.

Chapter 3 Lists the target reader of this Guide .

Chapter 4 Directs different stakeholders to corresponding sections of Chapter 7, so for understanding the good practices described in the seventeen (17) IT Security domains.

Chapter 5 Provides basic references for readers in understanding the IT Security Practices Framework.

Chapter 6 Introduces the concept of security profiles and demonstrate the use of IT Valuation Template for IT security risk assessment.

Chapter 7 Illustrates good practices for each of the IT Security domain, and the corresponding security level that a particular security practice suitable for.

Chapter 8 Recommended IT checklist and template.

Chapter 9 Recommended security risk assessment for IT security team.

2. NGO IT Security Overview

In the past, cyber security and privacy were often low on the list of NGO priorities. However, times are changing; the stakes for NGOs are increasingly high. Breaches, compromised data, and cyberattacks can put vulnerable beneficiaries at risk, disrupt NGO operations and services, expose NGOs to liability, and tarnish the reputation NGOs have so painstakingly built.

As a result, NGOs are now paying attention. Yet many NGOs are still unsure how to move forward. They often do not know how best to develop cyber security or data protection strategies that meet the evolving needs and challenges of today's online environment. Even when strategies are put in place, execution is inconsistent. NGOs often lack the budget, staffing resources, or management time needed to implement cyber security and privacy protections effectively, making their job far harder than for commercial or public sector organisations.

To minimise this risk, NGOs should develop strategies to incorporate the concept of resilience the ability to withstand natural, manmade, and cyber threats. Specifically, they should work to ensure both the security and privacy of their IT systems to reduce the chance of exposing their beneficiaries, staff, or donors to online attacks. To start, organisations need to ask themselves two fundamental questions:

1. Does the organisation have the capacity to protect its staff and beneficiaries from malicious cyber attacks?
2. Is the organisation ready to meet increasingly stringent data privacy standards and understand the serious penalties for compliance failure that nations and donors continue to demand?

Cyber security is not hard; it is merely complex. The challenge is to accomplish these and other related tasks in a complete and comprehensive manner while facilitating the essential operating functions of a successful business.

Cyber security is not only an IT problem, but it is also an enterprise-wide problem that requires an interdisciplinary approach, and a comprehensive governance commitment to ensure that all aspects of the business are aligned to support effective cyber security practices.

Ideally, NGO should regularly evaluate their IT security as part of a larger review of all production systems. The idea is to make sure the tech gear and processes are not out of step with the business strategy.

This Guide is designed to assist NGOs tackle the cyber security challenges and help them develop into IT resilient organisations. It identifies key cyber security and data protection challenges for NGOs, and outlines possible first steps NGOs can take to bolster cyber security and protect data.

3. The Audience

This Guide gives the guidelines for senior management, information security professionals, information and communication technology management to develop and implement their own IT security good practices and guidelines.

NGO staff who may benefit from a review of the security controls in this Guide include:

- Individuals who have access to systems, include general users;
- Individuals with information system, security, and/or risk management and oversight responsibilities (e.g. chief information officers, senior information security officers, information system managers, information security managers);
- Individuals with information system development responsibilities (e.g. program managers, system designers and developers, information security engineers, systems integrators);
- Individuals with information security implementation and operational responsibilities (e.g. mission/business owners, information system owners, information owners/stewards, system administrators, information system security officers); and
- Individuals with information security assessment and monitoring responsibilities (e.g. auditors, system evaluators, assessors, independent verifiers/validators, analysts, information system owners).

4. Stakeholder of Security Domain

Although everyone in the organisation plays their part to defend against the cyberattacks, each security area should have its key cyber security stakeholder(s). This Guide provided good practices on 17 security domains. Below are the recommended stakeholders of each security domain. The stakeholder is advised to study the related domains or assign the related employees to follow the corresponding good practices, in order to manage cyber risk in all security domains.

#	Security Domain	Stakeholder(s)	
		Management.	IT / Security
7.1	IT Security Governance		
	7.1.1 IT Security Policies and Procedures	✓	
	7.1.2 Asset Management and Maintenance	✓	
	7.1.3 Information Classification	✓	
	7.1.4 Information Handling	✓	
	7.1.5 Configuration Management	✓	✓
	7.1.6 Support and Competence	✓	✓
7.2	Password Control and Authentication		
	7.2.1 Traditional Password Control	✓	✓
	7.2.2 New Password Control Approach Recommending by NIST	✓	✓
	7.2.3 Authentication		✓
7.3	Websites and Web Applications		✓
7.4	Data Management		
	7.4.1 Data Security		✓
	7.4.2 Database Security		✓
	7.4.3 Sensitive and Personal Data Protection	✓	✓
7.5	Computer Networks Security		✓
7.6	Email Security	✓	✓
7.7	Cloud Computing Security		
	7.7.1 Cloud Computing and Data Security	✓	✓
	7.7.2 Avoid Cloud Vendor Lock-In	✓	✓
7.8	Physical Security	✓	✓
7.9	Mobile Security		
	7.9.1 Mobile Devices Security	✓	✓
	7.9.2 Portable Storage Security	✓	✓
7.10	Remote Access/Work from Home	✓	✓
7.11	Security Risk Assessment and Audit	✓	✓
7.12	Insider Threats	✓	✓
7.13	Vendor Management	✓	
7.14	Awareness and Training	✓	✓
7.15	Incident Response	✓	✓
7.16	Business Continuity Management	✓	✓
7.17	Log Management and Monitoring	✓	✓

Table 1: IT Security Domains

5. IT Security Practices Framework

This Guide aims to provide practical suggestions to NGOs better prepare themselves to protect their organisations against cyber security threats.

Readers should note that this Guide is not intended to be an exhaustive policy on IT security and data protection. It describes common practices and suggestions which may not be relevant or appropriate in every case.

Each NGO needs to examine its operations in detail and decide on the most reasonable and appropriate security measures for itself. NGOs may wish to seek professional advice and services regarding Information Technology (IT) security, where necessary.

The following documents, principles, and best practices constitute foundational references:

- The ISO 27001¹ standard offers a set of best-practice controls that can be applied to organisation based on the risks organisation face and implemented in a structured manner in order to achieve externally assessed and certified compliance.
- The National Institute of Standards and Technology (NIST) CSF² provides a comprehensive and programmatic approach so that any organisation can adapt to best suit their needs. The Standard can also be extended by integrating with a number of other standards and frameworks, including the NIST (Cybersecurity Framework) and NIST RMF³ (Risk Management Framework).
- This NISTIR uses the Framework for Improving Critical Infrastructure Cybersecurity (CSF) as a template for organising cyber security risk management processes and procedures. The Fundamentals of Small Business Information Security⁴ NISTIR 7621r1 - NIST
- The Personal Data (Privacy) Amendment Ordinance 2012 (the "PDPO") is applicable to both the private and the public sectors. It is technology-neutral and principle-based. The Data Protection Principles ("DPPs" or "DPP"), outline how data users should collect, handle and use personal data, complemented by other provisions imposing further compliance requirements.⁵

100_____

¹ ISO/IEC 27001:2013 Information Security Management System (ISMS)

<https://www.iso.org/standard/54534.html>

² National Institute of Standards and Technology (Cybersecurity Framework), NIST (CSF) version 1.1

<https://www.nist.gov/cyberframework>

³ NIST Cyber Security Risk Management Framework version 1.1

<https://www.nist.gov/cyberframework/risk-management-framework>

⁴ NIST Small Business Information Security: The Fundamentals (NISTIR 7621)

<https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final>

⁵ Security and Privacy Controls for Code of Practice, Hong Kong – PDPO Cap 486., PCPD

https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

6. IT Asset Valuation

6.1. Security Profile [Elementary, Intermediate, Advanced]⁶

In order to understand system security, we must first understand what are the risks may affect the systems. The purpose of this Guide is to provide guidance on common IT security considerations and best practices to NGOs on the management and technical perspective.

The organisations may consider the following criteria to valuing their information assets (example: server, system, application, data etc.).

Six Formal Information Valuation Models			
Foundational Measures		Financial Measures	
Focused on improving information management discipline		Focused on improving information's economic benefits	
Intrinsic Value	How correct, complete and exclusive is this asset/data? <i>E.g. research data, in high quality, with significant sample size and brining insight</i>	Cost Value	What would it cost if lost this asset/data? <i>E.g. the costs of system recovery and re-inputting data</i> <i>The costs of remedial actions and legal liabilities in case of data leakage or system breakdown</i>
Business Value	How good and relevant is this asset/data for specific purposes? <i>E.g. Donors' bank account information for recurrent donation</i>	Market Value	What good could get from selling this asset/data?
Performance Value	How does this asset/data affect key business drivers? <i>E.g. Service statistics for on-going service development</i>	Economic Value	How does this asset/data contribute to our bottom line?

Table 2: Six Formal Information Valuation Models

100 _____

⁶8.1 IT Asset Valuation Template

We recommended each NGO shall choose a security profile - **Elementary**, **Intermediate** or **Advanced** profile. We assumed that the **Elementary** profile is the default good practices to the NGOs. The NGO should adopt requirements of the related security level.

The Elementary profile is the baseline measures that most NGOs should implement to their systems whilst NGOs may adopt **Intermediate** profile measures if they deem that their system needs extra protections. As for **Advanced** profile measures, they should be implemented on sensitive and vital systems, of which breaches to them can lead to serious consequences.

An NGO with **Elementary** profile may choose to adopt a higher security level (**Intermediate** or **Advanced**) measures for certain critical systems. However, it does not change its basic profile. The NGO can even set the higher-level profile as their target profile and develop a plan to enhance their security level.

Sometimes NGO may want to know what their system's security level if they have to meet the **Intermediate** or even **Advanced** level. The IT Asset valuation template may help to give a handy way to manipulate. Organisation may find details information about the IT asset valuation on Section 6.2.

The IT asset valuation template will require organisation input the IT asset information with the selection level of these six attributes i.e.: "Asset Value", "Information Classification", "Security Risk Assessment", "System Update", "Resilience" and "Accessed by" to calculate the security level.

Asset valuation is a tool that an NGO can use to assess the security requirement of a system. A system can be one device (e.g.: server or database) or a set of devices in a system (e.g.: server farm/on cloud).

6.2. IT Asset Valuation Template Content

Understanding the value of corporate assets is fundamental to cyber security risk management. The correct level of security can be applied only when the true value is known.

This Guide will use the **IT Asset Valuation Template**⁷ to determine an information asset value. The template was designed for NGOs to fill in asset information and security requirements in determining the risk level and the protection requirements.

The IT Asset Valuation template is self-explanatory. User may input information assets narratives such as Asset No, Asset information, Description, Reference, Location on these columns in free format.

User inputs IT Asset attributes into column F to column K, then IT Asset Valuation Template will generate the level of Threat, Impact, and Likelihood based on the user input values, as in Table 2: IT Asset Attributes and Risk Components.

Finally, the IT Asset Valuation template will derive a security protection in “Elementary”, “Intermediate”, and “Advanced” security level.

IT Asset Valuation Template Content (Risk Based)				
#	Column Name	Description	Input Value	Category
A	Asset No	The information asset number.	Free format	Asset Narrative
B	Asset Info.	Brief asset information such as asset tag, internal/external IP address etc.	Free format	
C	Description	Describe the details of the information asset. Information asset can have many different forms such as servers, data, paper documents etc.	Free format	
D	Reference	An information asset reference such as serial or license number, expiry date.	Free format	
E	Location	Where the information asset is running or stored.	Free format	
F	*Asset Value	Asset value may measure either in Qualitative or Quantitative.	Very Low, Low, Medium, High	Attribute Rating
G	*Info. Classification (Confidentiality)	The Information Classification / Confidentiality level of the information technology asset.	Public, Internal, Restricted, Confidential	

100_____

⁷ 8.1 IT Asset Valuation Template

H	*Security Risk Assessment	Any information security risk assessment has been performed on the system	Periodically, Over 3 Years, Once, No Plan,	
I	*System Patches (Integrity)	Any security patches or OS upgrade has been performed/Integrity level of the information asset	Regularly, Planned, Outdated, Not Sure,	
J	*Resilience (Availability)	The system resilience/availability level of the information asset (e.g.: Backup, Drill Tested, High Availability etc.)	High Availability, Drill-Tested, Backup, Not Available	
K	*Accessed By	Which entities and organisations may access	Own, Public, Own & Partners Own & Public	
L	Consequence (Impact)	The Consequence/Impact level of overall harm or loss that could occur as a result of the exploitation of security vulnerability. (Sum of the “ Asset Value ” and “ Info. Classification ” score)	Very High High, Medium Low, Very Low	
M	Threat Level	The assessed threat level of the information asset. (Sum of the “ Security Risk Assessment ” and “ System Patches ” score)	Very High High, Medium Low, Very Low	
N	Probability (Likelihood)	The Probability/Likelihood that the threat will exploit the vulnerability of the information asset. (Sum of the “ Accessed By ” and “ Resilience ” score)	Very High High, Medium Low, Very Low	
O	Security Score	The sum of overall risk level of the IT asset based on its attributes.	3 ~ 15	Security Score
P	Elementary Security Level (3 ~ 7)	The NGO should implement technical and/or administrative security controls rated at elementary level for those systems.	3 ~ 7	Security Level
Q	Intermediate Security Level (8 ~ 11)	The NGO should implement technical and/or administrative security controls rated at intermediate levels for those systems.	8 ~ 11	

R	Advanced Security Level (12 ~ 15)	The NGO should implement technical and/or administrative security controls rated at advanced levels for those systems.	12 ~ 15	
* Information Asset Attribute				

Table 3: IT Asset Valuation Template Content

		Impact Score: Asset & Classification			
Asset Value	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8
		1	2	3	4
		Information Classification			

Table 4: Impact Level = Asset Value and Information Classification (Confidentiality)

		Threat Score: Update & Risk Assessment			
Update	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8
		1	2	3	4
		Security Risk Assessment			

Table 5: Threat Level = Security Risk Assessment and System Update (Integrity)

		Probability Score: Resilience & Accessed by			
Resilience	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8
		1	2	3	4
		Accessed By			

Table 6: Likelihood Level = Accessed By and Resilience (Availability)

Column	IT Asset Attribute (1 ~ 4 Levels)	Risk Component
F	*Asset Value	Impact = Asset Value & Info. Classification
G	*Info. Classification (Confidentiality)	
H	*Security Risk Assessment (SRA)	Threat = Security Risk Assessment & System Patches
I	*System Patches (Integrity)	
J	*Resilience (Availability)	Likelihood = Resilience & Accessed by whom
K	*Accessed By	

Table 7: IT Asset Attributes and Risk Components

Determine Adequate Security Level			
Security Level	Threat, Impact, Likelihood	Definition	Colour Code
Elementary	Security Score 3 ~ 7	<p>Most NGOs should adopt these good practices as the baseline controls in the information security protection requirements. This security level believes that it can make the most of limited resources especially for small NGOs.</p> <p>For example, for small organisations, they may often lack any specific IT support and the skills gap can go much deeper than just security. In these situations, recommended to follow the Elementary good practices.</p>	✓
Intermediate	Security Score 8 ~ 11	<p>Not all information technology assets and data in the organisation must be protected in the same way.</p> <p>Adopt the Intermediate level may help the NGO to prioritise their risks and enhance the information security level with adequate resources.</p>	✓
Advances	Security Score 12 ~ 15	<p>The more advanced the technology implemented in the NGO doesn't means the more secure they are. When the NGO has more products/services in play and offers, the more security threats may expose.</p> <p>In addition, insider threat is one of the largest problems in cyber security, representing a massive share of attacks and financial/reputation damages.</p>	✓

		Under this situation, the NGO may think about security in a more holistic way. Recommended the NGO adopt this level of security good practices.	
--	--	---	--

Table 8: IT Asset Protection Security Level

The following table illustrates three different scenarios.

Attribute	Range	NGO & Public Web Services		Cross NGOs Web Services		NGO Internal Web Services	
		Weight	#	Weight	#	Weight	#
Asset Value	1 ~ 4	High	4	High	4	High	4
Information Classification	1 ~ 4	Internal	2	Restricted	3	Confidential	4
Security Risk Assessment	1 ~ 4	Once	3	Once	3	Once	3
System Update	1 ~ 4	Outdated	3	Outdated	3	Outdated	3
Resilience	1 ~ 4	Backup	3	Backup	3	Backup	3
Accessed By	1 ~ 4	Own & Public	4	Own & Partners	3	Own	1
>> Consequence (Impact)	1 ~ 5	High	4	Very High	5	Very High	5
>> Threat Level	1 ~ 5	High	4	High	4	High	4
>> Probability (Likelihood)	1 ~ 5	Very High	5	High	4	Low	2
Benchmarking Score		Advanced	13	Advanced	13	Intermediate	11

Table 9: Benchmarking Example

7. IT Security Practices for NGO

7.1. IT Security Governance

Information Security Governance is crucial for any business as it not only allows for budgeting for both capacity and new technologies, but it also helps to prepare for times of disaster. Negligence in the area of Information Security Governance can result in board members, directors or partners being held responsible for breaches, damage to reputation or even financial loss. Information Security Governance Framework helps to outline goals, standards or frameworks for an NGO to achieve.

In order to mitigate the risk of cyber-attacks, an NGO must implement strong processes and good cyber security governance. For example, maintaining an audit trail can show unusual frequent access to a particular file at odd hours, and therefore alert an NGO to look into the situation further.

IT security governance encompasses the processes by which organisations are directed, controlled and held to account. It includes the authority, accountability, leadership, direction and control exercised in an organisation. Greatness can be achieved when good governance principles and practices are applied throughout the whole organisation and that's why governance is important.

IT Governance including the following domains:

- IT Security Policies and Procedures
- Asset Management and Maintenance
- Information Classification
- Information Handling
- Configuration Management
- Support and Competence

7.1.1 IT Security Policies and Procedures

Information Technology Security Policies (ITSP) is a set of rules enacted by an organisation to ensure that all users within the organisation’s domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organisation stretches its authority.

An ITSP is governing the protection of information, which is one of the many assets a corporation needs to protect. The organisation is working off a common understanding of the expectations and a common understanding of terms.

Proper information security documentation is comprised of five main parts:

- (1) Policy that establishes management’s intent
- (2) Control Objective that identifies the condition that should be met
- (3) Standards that provides quantifiable requirements to be met
- (4) Procedures that establish how tasks must be performed
- (5) Guidelines are recommended, but not mandatory

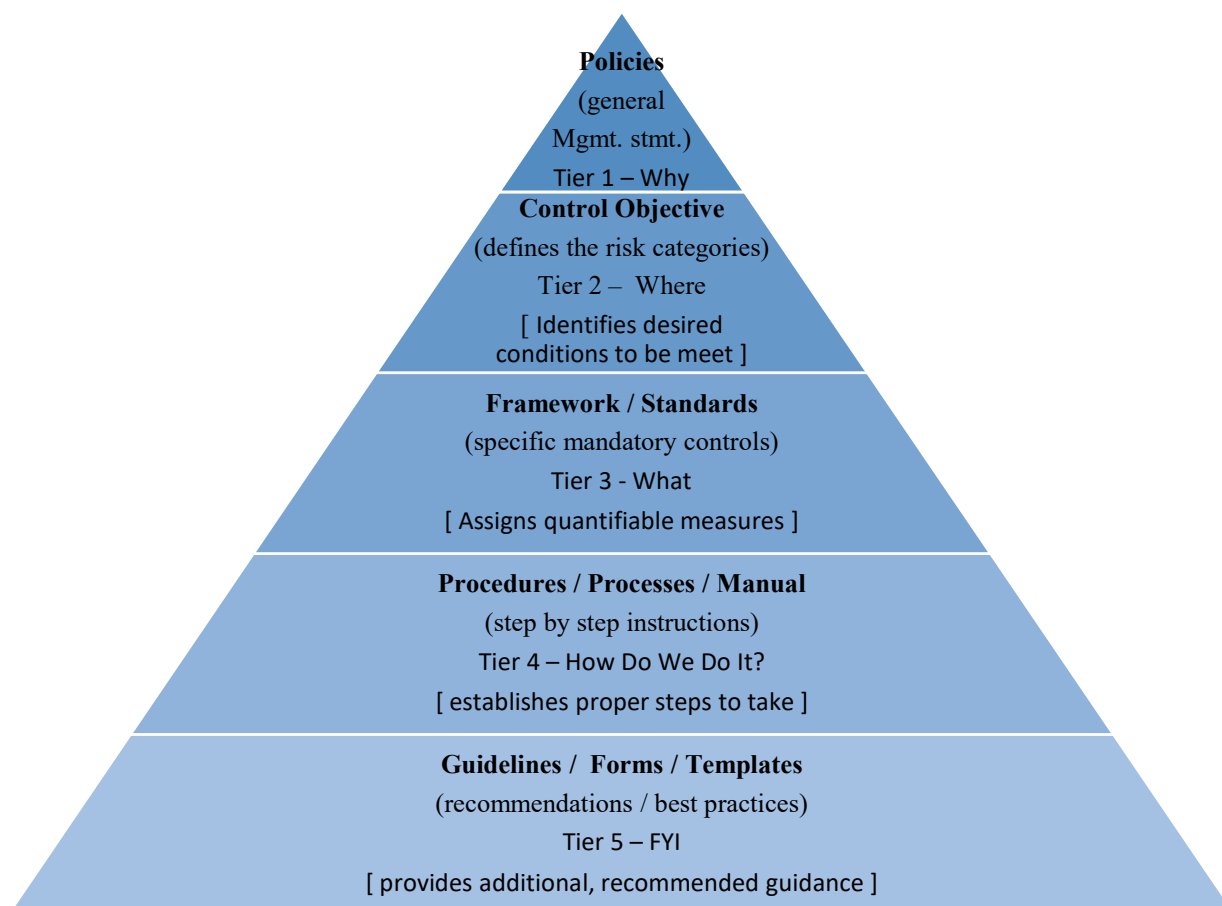


Figure 1: Policies, Standards, Procedures and Guidelines Hierarchy

The scope of a company's IT security documentation should apply to all employees, contractors, sub-contractors, and third-party contracted by the organisation to handle, process, transmit, store, or dispose of data.

Policies and Procedures		Stakeholder(s): Management		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Establish and enforce IT Security Policies and relevant procedures.	✓	✓	✓
2	IT Security Policy should include requirements created by: <ul style="list-style-type: none"> • Business strategy • Organisation governance and accountability of security function • Security and privacy coverage of organisation and related third parties who provide service to the organisation • Management responsibility to develop a culture of security and business continuity • Business unit's responsibility to assess and protect the security and privacy impact of their systems and apply relevant measures • Disciplinary process of employees when there is negligence and abuse • Regulations, legislation and contracts • The current and projected information security threat environment. 	✓	✓	✓
3	The information security policy should contain statements concerning: <ul style="list-style-type: none"> • Definition of information security, objectives and principles to guide all activities relating to information security • Assignment of general and specific responsibilities for information security management to defined roles • Processes for handling deviations and exceptions. 	✓	✓	✓
4	Policies are short and to the point in conveying principles that guide activity within the organisation.	✓	✓	✓
5	An IT Security Policy should have conciseness, readability, actionability, enforceability, and flexibility.	✓	✓	✓
6	Management approval for the revised policy should be obtained.	✓	✓	✓

7	The information security policy should be supported by topic-specific policies such as: a) Access control b) Information classification and handling c) Physical and environmental security d) End user-oriented topics such as: • acceptable use of assets • clear desk and clear screen • information transfer • mobile devices and teleworking • restrictions on software installations and use e) Backup f) Information transfer g) Protection from malware h) Management of technical vulnerabilities i) Cryptographic controls j) Communications security k) Privacy and protection of personally identifiable information l) Supplier relationships m) Regulatory compliance	✓	✓	✓
8	Security policies and procedures should be accessible to all employees.	✓	✓	✓
9	Employees at all levels shall read and accept the security policies to discern how they should act in the best interest of the organisation.	✓	✓	✓
10	NGO should adhere to legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met.	✓	✓	✓
11	NGO should keep such policies and procedures reviewed and updated periodically.		✓	✓
12	Defined management responsibilities to ensure that security is applied throughout an individual's employment within the organisation.		✓	✓
13	Applicable information from organisational privacy policies should be included in cyber security workforce training and awareness activities.		✓	✓
14	Established a formal disciplinary process for employee who have committed a security breach.		✓	✓
15	Evaluate and enforce compliance and regulatory obligations. This means understanding and implementing, where necessary, compliance and regulatory obligations relating to cyber security that apply directly in the NGO.		✓	✓

Table 10: Policies and Procedures

7.1.2 Asset Management and Maintenance

The IT infrastructure in an NGO will typically consist of various hardware and software components such as software applications, network equipment and server hardware. Inventory of assets helps ensure that effective protection takes place and identify lost assets.

Information assets include hardware, software, data and services. They must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance. Periodic review of the inventory shall be conducted to ensure that the assets are properly owned, kept and maintained. The point of developing an asset inventory is that organisation know which classified information have in their possession, and who is responsible for it (i.e., who is the owner).

Asset Management and Maintenance		Stakeholder(s): Management		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Have an accurate list of IT asset and keep it updated. An organisation should identify all assets and document the importance of these assets.	✓	✓	✓
2	All hardware and software (operating systems, middleware, applications etc.) must be recorded.	✓	✓	✓
3	Regularly update operating systems, firmware, middleware and applications.	✓	✓	✓
4	Ensure that security patches are applied in a timely manner as recommended by the supplier of the IT product commensurate with the criticality of the IT system.	✓	✓	✓
5	Ensure that hardware and software maintenance and upgrades of IT systems are routinely scheduled and carried out by competent persons, and that impacted security controls are still functioning properly following maintenance or repair actions.	✓	✓	✓
6	Conduct an inventory of all Internet access points for the information system and all interconnections with partner networks (suppliers, sales partners, etc.).		✓	✓
7	Perform audits to ensure the correct registration of IT Assets; compare the registration with reality annually.		✓	✓
8	Identify which assets need securing, as well as the threats and risks to them.		✓	✓
9	The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value.		✓	✓

10	NGO should have a labelling system to ensure IT Assets are labelled with the assigned unique asset tag that will enable positive identification during the asset’s lifecycle.		✓	✓
11	Keep an exhaustive inventory of privileged accounts and ensure this is updated.		✓	✓
12	Make use of automated mechanisms such as monitoring application that detect the presence of unauthorised user-installed software within the IT system and notify those responsible upon such detection.			✓

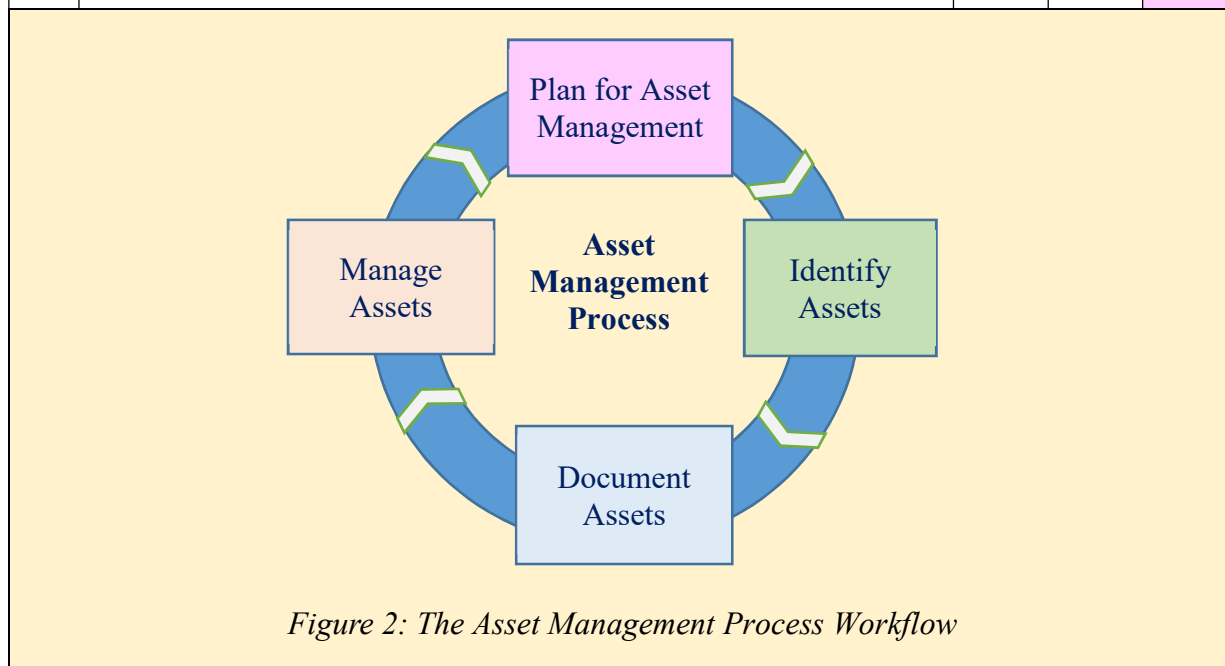


Figure 2: The Asset Management Process Workflow

Table 11: Asset management and Maintenance

Related Tool(s):

8.1 IT Asset Valuation List Template

9.1 WINAUDIT

7.1.3 Information Classification

Security standards such as ISO 27001 recommend that information should be classified and labelled according to its sensitivity. Each Information asset category will be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the organisation classification scheme.

However; NGO implementing a uniform information security classification system across the NGO may not practical. It is, however, recommended that confidential documents, folders, files, email messages etc. should be labelled accordingly.

Good practice says that information classification should be done via the following process:

1. Entering the asset in the inventory
2. Classification of information
3. Information labelling
4. Information handling

Information Classification		Stakeholder(s): Management																	
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A															
1	<p>The level of protection in the scheme should be assessed by analysing Confidentiality, Integrity and Availability and any other requirements for the information considered.</p> <p>Classified information can be in different forms and types of media, e.g.:</p> <ul style="list-style-type: none"> a) electronic documents b) information systems / databases c) paper documents d) storage media (e.g., disks, USB drives, etc.) e) information transmitted verbally email 	✓	✓	✓															
2	<p>Suggested mapping the classification level with the following table for the organisations' information classification is less than 4 level.</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>4 Level</th> <th>3 Level</th> <th>2 Level</th> </tr> </thead> <tbody> <tr> <td>Public</td> <td>Public</td> <td>Public</td> </tr> <tr> <td>Internal</td> <td>Internal</td> <td>Confidential</td> </tr> <tr> <td>Restricted</td> <td>Confidential</td> <td>Confidential</td> </tr> <tr> <td>Confidential</td> <td>Confidential</td> <td>Confidential</td> </tr> </tbody> </table> <p><i>Table 12: Recommended Information Classification Mapping</i></p>	4 Level	3 Level	2 Level	Public	Public	Public	Internal	Internal	Confidential	Restricted	Confidential	Confidential	Confidential	Confidential	Confidential	✓	✓	✓
4 Level	3 Level	2 Level																	
Public	Public	Public																	
Internal	Internal	Confidential																	
Restricted	Confidential	Confidential																	
Confidential	Confidential	Confidential																	
3	The information classification scheme should be aligned to the access control policy	✓	✓	✓															
4	The classification scheme should include conventions for classification and criteria for review of the classification over time.	✓	✓	✓															

5	<p>Define the level of classification criteria (see example below):</p> <ul style="list-style-type: none"> Confidential (top confidentiality level) Restricted (medium confidentiality level) Internal (lowest level of confidentiality) Public (everyone can see the information) <table border="1" data-bbox="276 394 1121 1644"> <thead> <tr> <th colspan="3" data-bbox="276 394 1121 432">Information Classification Example</th> </tr> </thead> <tbody> <tr> <td data-bbox="276 432 320 725">1</td> <td data-bbox="320 432 517 725">Public</td> <td data-bbox="517 432 1121 725"> <p>The information assets which do not have any confidentiality requirement and / or can be disseminated to the general public belong to this category.</p> <p><i>Example: annual financial report of the organisation and information displayed on the organisation's website</i></p> </td> </tr> <tr> <td data-bbox="276 725 320 1019">2</td> <td data-bbox="320 725 517 1019">Internal</td> <td data-bbox="517 725 1121 1019"> <p>The information assets which can be distributed within all offices of the organisation, business partners, or contractors belong to this category.</p> <p><i>Example: office orders and internal circulars, inter-office memorandum, internal policies and procedures</i></p> </td> </tr> <tr> <td data-bbox="276 1019 320 1391">3</td> <td data-bbox="320 1019 517 1391">Restricted</td> <td data-bbox="517 1019 1121 1391"> <p>The information assets that contain data pertaining to the needs of a specific department/section/unit, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned unit, project, or business process only.</p> <p><i>Example: client personal and sensitive information files</i></p> </td> </tr> <tr> <td data-bbox="276 1391 320 1644">4</td> <td data-bbox="320 1391 517 1644">Confidential</td> <td data-bbox="517 1391 1121 1644"> <p>The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets.</p> <p><i>Example: personnel medical files and work injury cases</i></p> </td> </tr> </tbody> </table> <p data-bbox="395 1653 1007 1686"><i>Table 13: Information Classification Definition</i></p>	Information Classification Example			1	Public	<p>The information assets which do not have any confidentiality requirement and / or can be disseminated to the general public belong to this category.</p> <p><i>Example: annual financial report of the organisation and information displayed on the organisation's website</i></p>	2	Internal	<p>The information assets which can be distributed within all offices of the organisation, business partners, or contractors belong to this category.</p> <p><i>Example: office orders and internal circulars, inter-office memorandum, internal policies and procedures</i></p>	3	Restricted	<p>The information assets that contain data pertaining to the needs of a specific department/section/unit, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned unit, project, or business process only.</p> <p><i>Example: client personal and sensitive information files</i></p>	4	Confidential	<p>The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets.</p> <p><i>Example: personnel medical files and work injury cases</i></p>	✓	✓	✓
Information Classification Example																			
1	Public	<p>The information assets which do not have any confidentiality requirement and / or can be disseminated to the general public belong to this category.</p> <p><i>Example: annual financial report of the organisation and information displayed on the organisation's website</i></p>																	
2	Internal	<p>The information assets which can be distributed within all offices of the organisation, business partners, or contractors belong to this category.</p> <p><i>Example: office orders and internal circulars, inter-office memorandum, internal policies and procedures</i></p>																	
3	Restricted	<p>The information assets that contain data pertaining to the needs of a specific department/section/unit, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned unit, project, or business process only.</p> <p><i>Example: client personal and sensitive information files</i></p>																	
4	Confidential	<p>The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets.</p> <p><i>Example: personnel medical files and work injury cases</i></p>																	
6	Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their lifecycle.	✓	✓	✓															

Table 14: Information Classification

7.1.4 Information Handling

Identify information that must be protected and ensure that responsibility for doing so is assigned. This should be done systematically by NGO, groups and individual members of staff as applicable.

Information Handling		Stakeholder(s): Management																																					
		E	I	A																																			
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A																																			
1	Ensure that those with responsibility for secure handling of information are offered training, guidance and support.	✓	✓	✓																																			
2	Ensure that both the information owners and those responsible for handling that information, where different, have the same understanding of the security requirements, expectations and limitations.	✓	✓	✓																																			
3	Ensure that information is managed continuously until it is destroyed, or until that responsibility is transferred to another organisation.	✓	✓	✓																																			
4	Once organisation classify the information, then organisation need to label it appropriately. Labelling of information is usually the responsibility of the asset owner.	✓	✓	✓																																			
5	For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction should be defined. This should also include the procedures for chain of custody and logging of any security relevant event.		✓	✓																																			
<table border="1"> <thead> <tr> <th></th> <th>Public</th> <th>Internal</th> <th>Restricted</th> <th>Confidential</th> </tr> </thead> <tbody> <tr> <td>NGO Publish Doc.</td> <td>✓</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Electronic documents</td> <td>✓</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Information systems</td> <td></td> <td>✓</td> <td>✓</td> <td></td> </tr> <tr> <td>Storage media</td> <td></td> <td>✓</td> <td>✓</td> <td></td> </tr> <tr> <td>Verbally transmitted information</td> <td></td> <td>✓</td> <td>✓</td> <td></td> </tr> <tr> <td>Email</td> <td></td> <td>✓</td> <td>✓</td> <td>✓</td> </tr> </tbody> </table> <p><i>Table 15: Asset Matrix Handling Example</i></p>			Public	Internal	Restricted	Confidential	NGO Publish Doc.	✓	✓			Electronic documents	✓	✓			Information systems		✓	✓		Storage media		✓	✓		Verbally transmitted information		✓	✓		Email		✓	✓	✓		✓	✓
	Public	Internal	Restricted	Confidential																																			
NGO Publish Doc.	✓	✓																																					
Electronic documents	✓	✓																																					
Information systems		✓	✓																																				
Storage media		✓	✓																																				
Verbally transmitted information		✓	✓																																				
Email		✓	✓	✓																																			
6	Agreements with other organisations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organisations.		✓	✓																																			

7	Monitor and Maintain - Periodically review and refine the information classification and handling procedure and make changes if necessary.		✓	✓
---	--	--	---	---

Table 16: Information Handling

7.1.5 Configuration Management

Management of configuration change is a systematic way to handle changes within an organisation to effectively deal with the change and to capitalize on possible opportunities. It involves adapting to the change, controlling the change, and affecting new change.

Configuration Management		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Have a configuration plan (tasks, timeline, responsibilities, authorities, budget, resources, needed information, etc.)	✓	✓	✓
2	Develop a Change Management process which includes scope of change, objectives, impacts, justification, fall back option, risk assessment and approval authority. And change requests and reports should be documented.	✓	✓	✓
3	Engage project relevant persons as appropriate in the change process.	✓	✓	✓
4	Develop a communication plan that considers the appropriate people within the organisation (customers, external providers, interested parties, etc.) that may need to be informed.	✓	✓	✓
5	Implement the change - change coordination with relevant parties' activities with the goal of meeting the Change Management Objectives.	✓	✓	✓
7	Measure or determine the effectiveness of the change.	✓	✓	✓
8	Document the final change result (Success, Failure, Roll Back, Cancel etc.) for audit.		✓	✓
9	Lessons learned from failures and successful projects. Capturing and sharing undocumented knowledge and experience. The results of improvements in processes, products and services.		✓	✓
10	Train people - determine the necessary competence of person(s) doing work under its control that affects the performance and effectiveness of the quality management system.		✓	✓
10	Use a cross functional team to review the plan to provide feedback related to the plan and associated risks.			✓

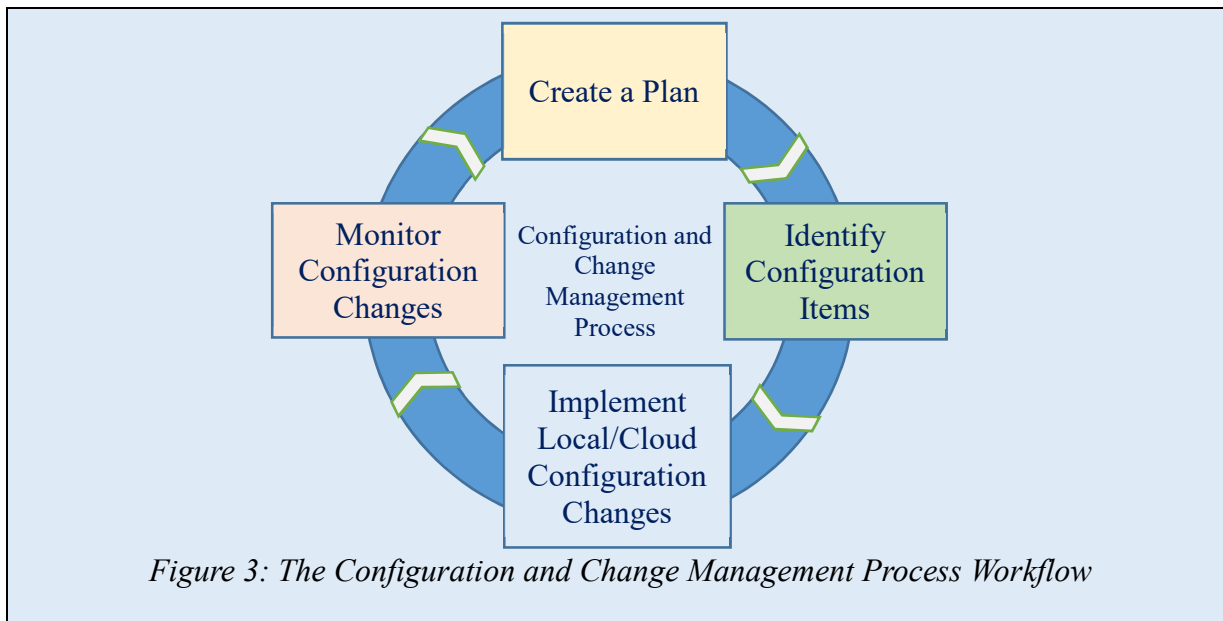


Table 17: Configuration Management

Related Tool(s):

- 8.3 Vendor Risk Assessment Checklist
- 8.5 Seven Habits of Cyber Security

7.1.6 Support and Competence

No organisation is immune to cybercrime, meaning that all need to make IT security a top priority. Successful IT security professionals need more than technical skills. To truly advance in the field, these experts should be strategists, communicators, lifelong learners.

Support and Competence		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Provision to fund information security management activities.	✓	✓	✓
2	The NGO shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	✓	✓	✓
3	Determine the necessary competence of person(s) doing work under its control that affects its information security performance.	✓	✓	✓
4	Ensure that these persons are competent on the basis of appropriate education, training, or experience.	✓	✓	✓
5	Visible support and commitment from all levels of management.	✓	✓	✓
6	Distribution of guidance on information security policy and standards to all managers, employees and other parties.	✓	✓	✓
7	Effective marketing of information security to all managers, employees, and other parties to achieve awareness.		✓	✓
8	Providing appropriate awareness, training, and education.		✓	✓
9	Retain appropriate documented information as evidence of competence.		✓	✓

Table 18: Support and Competence

7.2. Password Control and Authentication

The authentication, authorization, and passwords guide apply to any computing account on their computer resource, to the users of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication.

7.2.1 Traditional Password Control

Support and Competence		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Ensure authorised access at the IT level and ensure access enforcement mechanisms are employed at all levels of the IT layer to increase information security, including controlling remote access where outside users connect into the IT systems through external networks.	✓	✓	✓
2	Inform users that passwords should not be recorded on paper (handwritten or otherwise) and attached to computers or other equipment, or shared between users.	✓	✓	✓
3	Determine a suitable authentication method (whether single-factor or multi-factor) for accessing personal data based on the risk of damage to the relevant individuals in the event of a data breach.	✓	✓	✓
4	Ensure that strong passwords used for authentication, such as have a length of at least eight (8) or more characters, contain at least one alphabetic character, one numeric character, both lowercase and uppercase characters. Also, encourage users not to use passwords that can be easily deduced, such as their birth dates or names.	✓	✓	✓
5	Ensure that users change default or system-generated passwords to strong passwords at the earliest possible opportunity.	✓	✓	✓
6	Determine a suitable maximum number of attempts to be allowed for a user to authenticate his or her identity. Implement account lockout when the maximum number of attempts is reached, to prevent dictionary or brute-force attacks.	✓	✓	✓
7	Ensure that users are required to change their passwords regularly. The frequency should be based on the risk of damage to the relevant individuals if the data is compromised.	✓	✓	✓
8	Discourage users from using the same password across different systems or applications, also disallow users from using a password that was used within the last three password changes.	✓	✓	✓
9	Assign unique and distinct user IDs to individual users.	✓	✓	✓

10	Ensure that when a password used for authentication is typed in, it is to be hidden under placeholder characters such as asterisks * or dots •.	✓	✓	✓
11	Ensure that passwords used for authentication are encrypted during transmission and encrypted or hashed in storage.	✓	✓	✓
12	Ensure that passwords used include special characters such as ‘!’, ‘&’ and so on.		✓	✓
13	Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognized by the industry as relevant and secure.		✓	✓

Table 19: Traditional Password Control

7.2.2 New Password Control Approach Recommending by NIST

When required users to create complex passwords, users often cope with frequently changed, complex passwords by storing them in an insecure manner (e.g. a sticky note on a computer monitor) and by meeting the requirements in weaker password that are more easily predictable (e.g. Password1-!).

The SP800-63B Digital Identity Guidelines (NIST SP800-63)⁸ work to combat this behaviour by essentially proposing the use of one long simple password that should only be changed when it is compromised. This password guidelines are to focus on making passwords easy to remember and hard to guess, no longer requiring password expirations, copy and paste functionality in password fields are allowed.

New Password Control Approach Recommending by NIST		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	<p>A longer password is usually better than a more random password as long as the password is at least 8-16 characters long. In fact, a long password that comprises only lower-case letters can be more beneficial than crafting just the right combination of alphanumeric gibberish.</p> <p>NIST SP800-63B Password Guidelines:</p> <ol style="list-style-type: none"> 1. Eight (8) character minimum when a human set it. 2. Six (6) character minimum when set by a system/service. 3. Support at least sixty-four (64) characters maximum length. 4. All ASCII characters (including space) should be supported. 5. Truncation of the password shall not be performed when processed. 6. Check chosen password with known password dictionaries. 7. Allow at least ten (10) password attempts before lockout. 8. No complexity requirements. 9. No password expiration period. 10. No password hints. 11. No knowledge-based authentication. (e.g. who was the user's best friend in high school?) 12. No SMS for 2FA. (use a one-time password token or from an app like Google or Microsoft Authenticator) 	✓	✓	✓
2	Make the Passwords User-Friendly: Passwords should be user-friendly and place the burden on the system whenever possible.		✓	✓

3	Do not impose other composition rules (e.g. mixtures of different character types) on passwords. Instead, encourage users to use passphrases that are long and alphanumeric in nature.		✓	✓
4	Do not require that memorized password be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise.		✓	✓
5	Require screening of new passwords against lists of commonly used or compromised passwords. Cross-check poor password choices: NIST recommends that users stay away from well-known or common passwords, like “Password-1,” “1q2w3e4r5t6y,” etc.			✓

Table 20: New Password Control Approach Recommending by NIST

7.2.3 Authentication

User authentication is the functionality that most information technology system's application shared.

The following are most common authentication solutions:

- A challenge and response: User ID and password (something you know)
- One-time Passwords (OTP): OTP technology is based on a shared secret that is stored on the authentication device and the authentication backend (something you have).
- Biometric authentication: Compares data for the person's characteristics to that person's biometric "template" to determine resemblance (something you are).

Authentication		Stakeholder(s): IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	For challenge and response systems: <ul style="list-style-type: none"> • System/Vendor's default credentials should be changed before launch. • Never use weak password for production systems. • Never storing passwords in plain text unless there is a strong protection mechanism implemented. • Do not use words right out of the dictionary. 	✓	✓	✓
2	Minimise privilege of user account.	✓	✓	✓
3	Never shared privileged accounts.	✓	✓	✓
4	Use groups for defining permissions.	✓	✓	✓
5	Don't use privileged accounts for day to day operations.		✓	✓
6	Use X.509 certificates or public key authentication systems.		✓	✓
7	For high-risk and sensitive applications use multi-factor authentication.		✓	✓
8	Password-less authentication: Consider using a 3rd party authentication – OpenID Connect ⁹ , OAuth2 ¹⁰ by Google/Facebook/Twitter.			✓

Table 21: Authentication

7.3. Websites and Web Applications

Websites and web applications are often used to communicate or provide services. Since websites and web applications ultimately connect into a database and the database may contain personal and confidential data, precautions must be taken by IT admin against common forms of malicious

100

⁹ OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 family of specifications

<https://openid.net/>

¹⁰ OAuth 2.0 is the industry-standard protocol for authorization

<https://oauth.net/2/>

activities on websites and web applications. An attack against an NGO's website can lead to denial-of-service (DoS) and data leaks.

Websites and Web Applications		Stakeholder(s): IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Limit consecutive failure login attempts – brute-force through a web UI should not be possible.	✓	✓	✓
2	Do not allow the bypassing of user authentication to access personal data or confidential data.	✓	✓	✓
3	Configure web servers to disallow the browsing of file directories (Disable Directory Listing feature).	✓	✓	✓
4	Ensure that files containing personal data or confidential data are not made available through a web application or web server. Even if the web link to such files is not published, it is still possible to discover and access these files.	✓	✓	✓
5	Perform validation of user input. All user input information shall be validated and sanitised before pass to backend database process. Validate input field length and content must be at server side.		✓	✓
6	Perform cookie data validation and URL validation to correspond with the session in use.		✓	✓
7	Set the session timeout to as minimum as possible value and avoid forever-lasting sessions. If the user closes their browser, their session should expire immediately.		✓	✓
8	Deleting all cookies and invalidating the session when the user logout the web application.		✓	✓
9	Mark cookie HttpOnly and set Secure flag to enforce all web traffic are ride on the browser's encryption channel.		✓	✓
10	Have a same site origin policy to restricts how a document or script loaded from one origin can interact with a resource from another origin. It helps isolate potentially malicious documents, reducing possible attack vectors.		✓	✓
11	Disallow framing (X-Frame-Options: DENY) to prevent Clickjacking attacks.		✓	✓
12	Implement Content Security Policy (CSP) to detect and mitigate Cross Site Scripting (XSS) and data injection attacks.		✓	✓

13	Redirect or Force HTTPS (sensitive information can leak through unprotected connection channel - HTTP) if possible.		✓	✓
14	Make sure the server uses only the secure protocol such as TLS 1.2 or latest secure cryptography algorithms.		✓	✓
15	Disable web server insecure ciphers such as MD5, RC4, SHA, DES, 3DES etc. according to the industrial best practices.		✓	✓
16	Don't leak information through error messages. Configure custom page for user request error responses.		✓	✓
17	Use CSRF protection (e.g. CSRF one-time tokens that are verified with each request). Use Built-In or existing CSRF Implementations for CSRF Protection Framework.		✓	✓
18	Minimum privilege of user accounts: Follow the application security best practices, as well as network security, which encourages to limit access to only need it.		✓	✓
19	Perform web application scanning and source code analysis in order to detect web vulnerabilities before production launch. Perform web application vulnerability scanning in every 2 years.			✓
20	Implement Web Application Firewall (WAF) such as ModSecurity ¹¹ to protect web applications against an attack such as SQL injection, Cross-site scripting and common web attacks.			✓

Table 22: Websites and Web Applications

100_____

¹¹ ModSecurity, TrustWave – Open Source Web-Application Firewall, supports Apache, Microsoft IIS, & Nginx
<https://www.modsecurity.org/>

7.4. Data Management

NGO should consider the types of data they store in file/database and how this data is accessed by their employees and clients (if access is provided to clients).

If personal data is stored in a file/database, NGO should consider the types of personal data to be stored and the risk of harm or adverse impact on the relevant individuals should their personal data be compromised in the event of a breach.

7.4.1 Data Security

Data Security		Stakeholder(s): IT Admin		
		E	I	A
Security Level: E = Elementary, I = Intermediate, A = Advanced				
1	Before implement any type of data security strategy, the organisation should take stock of where their most sensitive information is stored. Secure data at rest, beside website protected by a firewall, encrypt data at rest adding an additional layer of defence.	✓	✓	✓
2	When data is transmitted, ensure that the NGO's ICT systems protect the confidentiality and integrity of the transmitted data, for example, by implementing an encrypted communication channel.	✓	✓	✓
3	Create regular data backups based on the data backup procedure. Schedule a backup data restore drill test to confirm and verify information integrity and media reliability.	✓	✓	✓
4	Until the data or the electronic media containing the data is sanitised, protect the electronic media by placing it in secure storage such as locked cabinets or a controlled media library.	✓	✓	✓
5	Enable the "Encrypt" backup option, use cryptographic mechanisms to prevent unauthorized modification of data in storage. Sensitive files, as well as entire devices, should be encrypted.		✓	✓
6	Use data sanitisation techniques with strength and integrity, which are commensurate with the type and confidentiality of the information residing on the media, in order to remove information from the media such that the information cannot be retrieved or reconstructed.		✓	✓
7	Use software mechanisms to detect and log unauthorized changes to data in storage, and which will trigger audit alerts when such events occur.		✓	✓
8	Where law practices wish to outsource electronic data storage or plan to store electronic data in the cloud, due diligence must be carried out on the service provider and there should be a written outsourcing agreement in place, covering amongst other obligations, liability for breaches of data protection and confidentiality.			✓

Table 23: Data Security

7.4.2 Database Security

Databases are used to store information such that it can be easily accessed, managed and updated. Database software and management systems may have different security features.

Security concerns for internet-based attacks are some of the most persistent challenges to database security. NGOs must ensure their database security measures are strong enough to withstand these attacks such as SQL injection attacks.

There are three layers of database security:

- Database level occurs within the database itself, where the data live including data masking and encryption;
- Access level security focuses on controlling who is allowed to access certain data or systems containing it including access control lists and permissions;
- Perimeter level determines who can and cannot get into databases including firewalls and VPN.

Database Security		Stakeholder(s): IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Access to the database must be under authenticated and authorisation controls. Do not open database administration interface to the Internet.	✓	✓	✓
2	Whether the organisation database server is on-premise or in a cloud, 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 the system admin 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 latest patches as soon as they are available.			✓
6	Secure Data at Rest: Encrypt personal and sensitive 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. <ul style="list-style-type: none"> • Encrypt storage (i.e.: BitLocker, Databases (TDE) etc.) • Encrypt passwords and other configuration settings Secure Data in Transit: Enable encryption in data communication: <ul style="list-style-type: none"> • 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. Monitoring database operations with server-generated alerts.			✓

Table 24: Database Security

7.4.3 Sensitive and Personal Data Protection

How people collaborate is extremely important when working on documents that contain internal proprietary information, regulated information like personally identifiable information (PII) or financial details. The sensitive information and PII handling good practices document for NGOs reference.

Personal Data means information which relates to a living individual and can be used to identify that individual. It must also exist in a form which access to or processing of is practicable.

Data Subject is the individual who is the subject of the personal data.

Data User is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.

Data Processor is a person who processes personal data on behalf of another person (a data user), instead of for his/her own purpose(s).

Sensitive and Personal Data Protection		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Establishing PII handling procedure to protect privacy data or sensitive data includes: <ul style="list-style-type: none"> • Define information classification • Implement information classification labeling • Accessing sensitive information only what is necessary to complete a work-related duty or job • Disclosing PII only within and between authorised entities to conduct official business/services. 	✓	✓	✓
2	Disseminate the importance of personally identifiable information (PII) protection message to all employees and partners. <ul style="list-style-type: none"> • Apply appropriate protective measures to employee PII • Don't keep sensitive information longer than needed • Think privacy when handling PII and sensitive information • Treat PII data as if it were financial information 	✓	✓	✓
3	Instead of just limiting the types and amount of personal data to be collected, data users should also consider the best practice of not collecting any PII or should collect only the minimum PII.	✓	✓	✓

4	<p>Encryption protects organisation business from cybercriminals accessing sensitive data or employees making an unintended mistake with their data.</p> <p>Most commonly, organisations encrypt the following:</p> <ul style="list-style-type: none"> • Organisation intellectual property or proprietary data • Organisation financial reports • Personally Identifiable Information (PII) • Research and development data • Sensitive customer/client data • Upcoming product/service launch details 	✓	✓	✓
5	<p>NGO should take all practicable steps to ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use, including the consideration of:</p> <ul style="list-style-type: none"> • The kind of data and the harm that could result if any of those incidents should occur; • The physical location where the data is stored; • Any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; • Any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and • Any measures taken for ensuring the secure transmission of the data. 	✓	✓	✓
6	<p>Collection and Use of Personal Data through the Internet (website):</p> <ul style="list-style-type: none"> • Instead of showing a complex online form comprising both mandatory and optional fields, a two-part form should be used to clearly group mandatory and optional fields separately. This will also prompt data users to reconsider if they should avoid collecting the optional data 	✓	✓	✓
7	<p>Children are often identified as a vulnerable group who have special requirements in privacy protection, particularly in the context of online activities.</p> <p>Children are more inclined to follow instructions without questioning, less privacy-aware and less able to exercise caution when communicating online. Even if warnings are given, children are often unable to appreciate the full ramifications of over-disclosure or over-sharing of their personal data, and those warnings are invariably disregarded.</p> <ul style="list-style-type: none"> • Avoid open-type questions in online forms by which children may feel more inclined to over-supply information to data users; • “Just in time” reminders or warning messages may be adopted in the online form to alert children of the minimum amount of information they are expected to supply; and • When collecting information about third parties (such as 	✓	✓	✓

	parents or friends), children should be explicitly reminded that they need to consult and obtain consent from those people before providing their personal data.			
8	If a data user wants to change the use, explicit and voluntary consent given by the affected data subjects must be sought top management approval.	✓	✓	✓
9	Define PII incident reporting procedure <ul style="list-style-type: none"> When reporting a Privacy (PII) incident, provide as much detailed information as possible about what occurred, when did the incident occur and what information was compromised. Any paper documentation, webpage URL or system process information from the breached should be reported. Organisation will take appropriate action to mitigate the effects of the incident and report its findings as determined by the organisation and PCPD. 	✓	✓	✓
10	Security measures for storing, processing and transmitting personally identifiable information (PII) / sensitive information ¹² : <ul style="list-style-type: none"> Access to personally PII should be granted on need-to-know basis. Ensure implement stringent password policies (i.e. password length, complexity, etc.) Documents with sensitive information / PII must be labelled with appropriate security classification information. Remind users that they should keep their sensitive information / PII should be locked in a safe place, or if stored electronically, protected by passwords that they will remember. User process/access sensitive information should be logged and reviewed by IT / or responsible staff periodically. Sensitive information / PII must be shared should be encrypted or communicate via secure channels. Strong access control protection should be enforced when sensitive information / PII stored either in cabinet or file server. Network security access control such as firewall should be implemented for segregating internal network from the external network. PII should be removed / destroyed in a determined period when it is no longer necessary. 	✓	✓	✓

Table 25: Personally Identifiable Information Protection

7.5. Computer Networks Security

Wireless local area networks (commonly referred to as “WiFi networks”) are generally regarded as being more vulnerable, because a cyber attacker need not be physically connected to the relevant computer network in order to gain access.

Defences that can be used to improve the security of computer networks include:

- Firewalls; and Web proxies, anti-virus software and anti-spyware software.
- Intrusion prevention systems (“IPS”) – devices or software applications that monitor networks or system activities and prevent malicious activities or policy violations;
- Intrusion detection systems (“IDS”) – network security appliances that monitor network and system activities for malicious activities and which may raise alerts upon detecting unusual activities;
- Security devices that prevent the unauthorised transfer of data out of a computer network;

Computer Network Security		Stakeholder(s): IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Unless strictly necessary, disallow remote network administration.	✓	✓	✓
2	Restrict employees’ access to known malicious websites.	✓	✓	✓
3	Unless absolutely essential, IT contractors and third-party suppliers should not be given administrator-level access to the IT network or any other IT infrastructure.	✓	✓	✓
4	Equip networks with network defence devices or software.		✓	✓
5	Design and implement the internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type and so on, and implementing boundary protection with external networks.		✓	✓
6	Establish usage restrictions, configuration requirements, connection requirements, and implement guidelines for wireless access.		✓	✓
7	Apply secure connection technologies or protocols such as TLS to protect the transmission of electronic data and to protect the authenticity of communications sessions between web clients and web servers.		✓	✓
8	Prohibit direct connection from a private network to an external network (such as the internet) without the use of boundary protection devices such as routers and firewalls to mediate communications.		✓	✓

9	Disable access switches' unused network ports.			✓
10	<p>Organisation may implement mobile devices management (MDM) software solutions may help to protect the organisation mobile devices.</p> <p>There are free MDMs for Android devices: ManageEngine Mobile Device Manager¹³, Miradore¹⁴, Relution¹⁵, Flyve MDM¹⁶, Headwind¹⁷ etc.</p>			✓

Table 26: Computer Network Security

Related Tool(s):

8.5 Seven Habits of Cyber Security

9.2 NMap/Zenmap Network Scanner

100_____

¹³ ManageEngine Mobile Device Manager

<https://www.manageengine.com/mobile-device-management/free-mobile-device-management-software.html>

¹⁴ Miradore

<https://www.miradore.com/>

¹⁵ Relution

<https://relution.io/en/>

¹⁶ Flyve-MDM

<https://www.flyve-mdm.com/>

¹⁷ Headwind

<https://h-mdm.com/>

7.6. Email Security

An NGO like other types of businesses, rely heavily on emails to carry out their operation activities. Emails are susceptible to a wide range of threats and cyber attacks. Some of these attacks include Business Email Compromise (“BEC”), phishing and other forms of malicious software attacks.

Email Security		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Anti-malware application installed on the email servers and user workstation should be enabled to prevent spam emails from being sent to end users, or to reduce the number of spam emails being sent. Keep the software updated and perform scans regularly.	✓	✓	✓
2	If an email appears suspicious, verify the identity of the sender and the legitimacy of the email contents through an out-of-band method. For example, by: (i) performing a verification via telephone; or (ii) checking the sender’s actual email address or return email address. Do not merely rely on the displayed name of the email address. Do not click on, open or execute suspicious attachments. Should the user have any doubt, call IT help immediately.	✓	✓	✓
3	Do not click on unrecognised links. At first glance, a link may appear legitimate. The user can verify the actual link when the user hovers their mouse over the link embedded in the body of an email. If the displayed link address and the actual link address are different, do not click on the link.	✓	✓	✓
4	Encrypt or password protect attachments containing personal data that have a higher risk of adversely affecting the relevant individuals should the data be compromised. The password should be communicated separately. For encryption, review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure. For password protection, ensure that a strong password is used. Example: Encrypt with Microsoft O365 Message Encryption In an email message, choose Options, select Encrypt and pick the encryption that has the restrictions the organisation wants to enforce, such as Encrypt-Only or Do Not Forward.		✓	✓

5	Use two-step verification ¹⁸ with Microsoft account (O365 account), O365 E1 support free 2FA feature, E3 seems also supported ¹⁹ . Two-factor authentication (2FA) helps protect the user by making it more difficult for someone else to sign into the user's Microsoft account.		✓	✓
6	Implement Sender Policy Framework (SPF ^{20, 21}), Domain Keys Identified Mail (DKIM ^{22, 23}) and Domain-based Message Authentication, Reporting and Conformance ("DMARC ^{24, 25} ") email authentication methods and protocols.			✓

Table 27: Email Security

SPF, DKIM, and DMARC are current best-practice security frameworks for securing email in transit and maintaining the organisation domain reputation.

DKIM — Domain Keys Identified Mail: Yet another application of PKI, DKIM is a control that system admin can implement to detect tampering of mail content during transit through verification of hashes.

SPF — Sender Policy Framework: SPF is a control that can be implemented to allow only certain domains to send mail using the organisation domain name. Similar to DKIM, SPF also relies on DNS records as a backbone for its implementation.

DMARC — Domain Message Authentication, Reporting and Conformance: also implemented as a TXT DNS record allows mail servers to be configured with policies on how to handle mail authentication through one or both of the SPF and DKIM, along with specification on forwarding, dropping and quarantining mail. Basically, DMARC = DKIM + SPF + Additional Reporting and Policy creation/enforcement features.

100_____

¹⁸ Setup two-step verification with Microsoft account

<https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4>

¹⁹ Features and licenses for Azure AD Multi-Factor Authentication

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing>

²⁰ How Microsoft 365 uses Sender Policy Framework (SPF) to prevent spoofing - Microsoft

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing>

²¹ Help prevent email spoofing with SPF records – Google Workspace (former G-Suite)

<https://support.google.com/a/answer/33786>

²² Use DKIM to validate outbound email sent from your custom domain - Microsoft

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email>

²³ Set up DKIM to prevent email spoofing – Google Workspace (former G-Suite)

https://support.google.com/a/answer/174124?hl=en&ref_topic=7564555

²⁴ Use DMARC to validate email - Microsoft

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email>

²⁵ Manage suspicious emails with DMARC – Google Workspace (former G-Suite)

https://support.google.com/a/answer/2466563?hl=en&ref_topic=7562942

7.7. Cloud Computing Security

Cloud computing allows users to access software and IT resources from any physical location via the internet. Cloud security includes keeping data private and safe across online-based infrastructure, applications, and platforms.

Most cloud computing security risks are related to cloud data security. Whether a lack of visibility to data, inability to control data, or theft of data in the cloud, most issues come back to the data customers put in the cloud.

In every cloud service—from software-as-a-service (SaaS) like Microsoft Office 365, Google Apps, DropBox to infrastructure-as-a-service (IaaS) like Amazon Web Services (AWS), Google Compute Engine, Alibaba Cloud, and platform-as-a-service (PaaS) like Windows Azure, Wasabi, Soho Creator—the cloud computing customer is always responsible for protecting their data from security threats and controlling access to it. Cloud service providers (CSPs) treat cloud security issues and risks as a Shared Responsibility.

The following tables show the Shared Responsibility Model between the Cloud Service Providers (CSPs) and the Customers from AWS and Azure.

Customer is Responsible for Security “IN” the Cloud	Customer / User Data			
	Platform, Application, Identity & Access Management			
	Operating System, Network, & Firewall Configuration			
	Client-side Data Encryption & Data Integrity Authentication	Server-side Data Encryption (File System and / or Data)		Network Traffic Protection (Encryption / Integrity / Identity)
AWS is Responsible for Security “OF” the Cloud	Software			
	Compute	Storage	Database	Networking
	Hardware / AWS Global Infrastructure			
	Global Infrastructure	Regions		Edge Location
		Availability Zone		

Table 28: AWS Shared Responsibility Model for Security in the Cloud

Responsibility	SaaS	PaaS	IaaS	On-prem	Responsible
Information and data					Responsibility always retained by customer
Devices (Mobile and PCs)					
Accounts and identities					
Identity and directory infrastructure					Responsibility varies by service type
Applications					
Network controls					
Operating system					
Physical hosts					Responsibility transfer to cloud service provider
Physical network					
Physical datacenter					
	Microsoft		Customer		

Table 29: Azure Shared Responsibility Model for Security in the Cloud

7.7.1 Cloud Computing and Data Security

NGOs' that adopt cloud services should be aware of the security and compliance challenges that are unique to cloud services. NGO should assess if the cloud service provider's security level of protection offered is sufficient for the personal and confidential data being stored in the cloud.

Cloud Computing and Data Security		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Pay attention to the security risks of cloud computing: <ul style="list-style-type: none"> • Loss of Visibility • Compliance Violations • Lack of Cloud Security Strategy and Architecture • Insider Threats • Contractual Breaches • Insecure Application User Interface (API) Lock-in • Misconfiguration of Cloud Services • Cloud Vendor Lock-in 	✓	✓	✓
2	Be aware of which laws apply to any personal data stored in the cloud and the jurisdiction in which this data is stored. Related ordinance and regulation are: <ul style="list-style-type: none"> • The Personal Data (Privacy) Ordinance²⁶ (PDPO) (Cap. 486) (“the Ordinance”) – PCPD. • The General Data Protection Regulation (EU) (GDPR)²⁷ 	✓	✓	✓
3	Back up the organisation cloud data offline, whether it is in the cloud or not. <ul style="list-style-type: none"> • At least three current copies (known as the 3-2-1 rule), and one of those copies truly offline. • If the organisation have an online backup console, if possible, protect it with 2FA such as Azure Cloud²⁸ and Google Cloud²⁹. • Computers accessing backup and restore portals should be among the best protected in the organisation. • Test backups restoration regularly. 	✓	✓	✓
4	Securely manage the organisation data. When store data in the cloud, make sure that that data is properly protected. A cloud environment should support data encryption for data moving both to and from the cloud (i.e.: VPN).	✓	✓	✓

100

²⁶ The Personal Data (Privacy) Ordinance - PCPD

https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

²⁷ The General Data Protection Regulation (EU) 2016/679 (GDPR)

<https://gdpr-info.eu/>

²⁸ Features and licenses for Azure AD Multi-Factor Authentication

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing>

²⁹ Google 2-Step Verification

<https://www.google.com/landing/2step/index.html>

5	The organisation needs to establish cloud data deletion policies when the organisation will eventually leave the cloud service provider the organisation currently using (i.e.: to migrate to a new cloud provider or to switch back to an on-premise architecture) that safely removes sensitive information/data from organisation's system while maintaining compliance.	✓	✓	✓
6	Implement endpoint security to securing end-user devices, such as laptops, desktops, and mobile devices. Organisations need to protect endpoints to their organisation networks and for devices used to access their cloud accounts.	✓	✓	✓
7	Enacting access control and security clearance policies to manage the users that attempt to visit the organisation cloud environment. Organisation should assign specific rights and access policies to different users; to ensures that each NGO's employee can only view or manipulate the applications or data necessary for him or her to do their job.	✓	✓	✓
8	Provide training to employees on the cloud security practices. Sometimes, the biggest security threat to the organisation cloud technologies is the own organisation and its employees (insider). An organisation should take some time to train employees that will be using the cloud environment on the best security practices should be adopted.	✓	✓	✓
9	When employees leave your company, make sure they can no longer access your cloud storage, systems, data, customer information, and intellectual properties.	✓	✓	✓
10	Encryption is one of the best ways to secure your cloud computing system: <ul style="list-style-type: none"> • Communications encryption • Sensitive data encryption • Secure data at rest and end-to-end encryption of all data that is uploaded to the cloud. 		✓	✓
11	Best practices for cloud encryption involve the following steps: <ul style="list-style-type: none"> • Formulate a cloud encryption policy • Define what data needs encryption, and when • Identify where that data resides • Implement encryption solutions and key management 		✓	✓

12	<p>Implement security tools to protect and secure data in Cloud</p> <ul style="list-style-type: none"> • AWS³⁰ EC2 (Linux/Windows) / Azure³¹ (Linux/Windows) / Google Cloud³² <ul style="list-style-type: none"> - Disk Encryption - File/ Folders Encryption • AWS RDS / Azure MSSQL <ul style="list-style-type: none"> - Supports Transparent Data Encryption (TDE) • Google Cloud SQL <ul style="list-style-type: none"> - Google Cloud is encrypted at the storage level • AWS S3 <ul style="list-style-type: none"> - S3 default server-side encryption for an S3 bucket 		✓	✓
13	<p>Ensure that the cloud service provider is ISO certified for the relevant standards as necessary. Relevant standards may include ISO/IEC 27001:2013³³, ISO/IEC 27017:2015³⁴, ISO/IEC 27018:2019³⁵ or other recognized international standards. Obtain a copy of the certification for the organisation records if possible.</p>		✓	✓
14	<p>Protect all the NGO's cloud users' access with two-factor authentication to ensure that only authorized personnel can log in to the NGO's cloud apps and access that sensitive data.</p>		✓	✓
15	<p>Real-time monitoring and analysis of user activities to spot out suspicious activities in the cloud. To improve visibility, turn on security logging and monitoring to see unauthorized access attempts and other issues.</p>		✓	✓
16	<p>Perform routine penetration tests on a regular basis allows the organisation cloud admin to detect for any risk gaps that have appeared in cloud systems.</p>		✓	✓

100

³⁰ Amazon AWS Cloud Services<https://aws.amazon.com/>³¹ Microsoft Azure Cloud Services<https://azure.microsoft.com/en-us/>³² Google Cloud<https://cloud.google.com/>³³ ISO/IEC 27001:2013 specifies the requirements for establishing, maintaining and continually improving an information security management system within the context of an organisation.<https://www.iso.org/standard/54534.html>³⁴ ISO/IEC 27017:2015 provides guidelines for information security controls applicable to the provision and use of cloud services.<https://www.iso.org/standard/43757.html>³⁵ ISO/IEC 27018:2019 relates to the protection of personally identifiable information and provides guidance on ensuring that cloud service providers offer suitable information security controls to protect the privacy of client data.<https://www.iso.org/standard/76559.html>

17	Defense-in-depth is particularly important when securing cloud environments because it ensures that even if one control fails, other security features can keep the application, network, and data safe.			✓
18	If possible, negotiate that the organisation cloud service provider conducts on-going third-party audits and provides the organisation with reports on these audits.			✓

Table 30: Cloud Computing Security

7.7.2 Avoid Cloud Vendor Lock-In

Migrating to the cloud can bring a multitude of benefits to the organisation, such as increased agility, flexibility, and cost savings. Despite all of these positives, many organisations who are considering a move to the cloud have concerns. And one of the primary issues is vendor lock-in due to the lack of standardisation.

The issue with vendor lock-in is the difficulty in moving to another cloud service provider if something goes awry. There are four primary lock-in risks that you will take working with a single cloud provider. These include:

- Data transfer risk
- Application transfer risk
- Infrastructure transfer risk
- Human resource knowledge risk

Avoid Cloud Vendor Lock-In		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Due diligence <ul style="list-style-type: none"> • Evaluate cloud services carefully. • Determine the organisation goals of migrating to the cloud. • Assess the organisation current IT situation and current infrastructure and cost and resources levels. • Select the type of cloud environment needed – public, private, or hybrid? • Determine the specific cloud components necessary. 	✓	✓	✓
2	Maximise data portability: <ul style="list-style-type: none"> • Data backups • Ensure data can be moved easily 		✓	✓
3	Design the organisation application to be loosely coupled: <ul style="list-style-type: none"> • Applications should be built or migrated to be as flexible and loosely coupled as possible. • Business logic should not only be separated from the application logic but should be clearly defined and documented. 		✓	✓
4	Multi-cloud or hybrid cloud strategy: <ul style="list-style-type: none"> • A multi-cloud approach incorporates multiple cloud providers, reducing dependence on any single vendor. • In a hybrid cloud, some data will remain within an organisation's direct control, either in a private cloud or stored on-premises. 			✓

5	Implement DevOps tools and processes <ul style="list-style-type: none"> • DevOps tools like Kamatera³⁶ and Jenkins³⁷ are increasingly being implemented to maximize code portability. • Built application in container technology like Docker³⁸ and CoreOS³⁹ help isolate software from its environment and abstract dependencies away from the cloud provider. 			✓
6	Employ configuration management tools like Chef ⁴⁰ , Puppet ⁴¹ , and Juju ⁴² to help the cloud admin automate the configuration of the infrastructure on which the organisation apps run.			✓

Table 31: Avoid Cloud Vendor Lock-In

100

³⁶ Kamatera Express

<https://www.kamatera.com/express/compute/>

³⁷ Jenkins CDF, X, Tekton, Spinnaker

<https://www.jenkins.io/>

³⁸ Docker

<https://www.docker.com/>

³⁹ CoreOS

<https://coreos.com/>

⁴⁰ ChefDK

<https://download.chef.io/product/chefdk>

⁴¹ Puppet

<https://puppet.com/try-puppet/open-source-puppet/>

⁴² Juju

<https://juju.is/docs/clouds>

7.8. Physical Security

Physical security is the technologies and systems in place to protect the organisation workplace. Protecting confidential information, important data, assets, networks, equipment, premises facilities, and organisation's assets is what physical security is about.

If physical security is not maintained properly, all the safety measures will be useless once the attacker gets through by gaining physical access. Physical security is proving to be challenging than previous as there are more sensitive devices available (like USB drives, laptops, mobile devices, etc.) that enables the losing of data easy.

Physical Security		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Create a security culture to ensure that all staff take security seriously. Physical security should take into account the organisation's personnel, data, intellectual property and physical assets.	✓	✓	✓
2	Ensure the computer room only for authorised person access. Every computer and equipment inside the room should have an inventory number and should be labelled.	✓	✓	✓
3	Visitor management systems and access control are core elements of effective physical security.	✓	✓	✓
4	A video surveillance the computer room/data centre by CCTV. Show signage on the entrance can show individuals that they are on camera and should not consider criminal activity.	✓	✓	✓
5	Servers and storage devices with sensitive information are to be placed in a locked and dedicated computer room with controlled access.	✓	✓	✓
6	Make sure the storage media and sensitive files are locked in a locked closet, or a secure room.	✓	✓	✓
7	Organisation's data holding devices should be enabled access control protection feature such as password protection.	✓	✓	✓
8	Enable mobile device access control protection that prevent unauthorised person to access the device.	✓	✓	✓
9	Regularly back up the organisation's phone data, in case it gets lost.	✓	✓	✓
10	Install antivirus or an anti-malware product on the mobile phone if possible.	✓	✓	✓
11	Attach an anti-theft laptop cables to all users' laptop computer in a public place that could help protect the devices.		✓	✓

12	Sensitive information on media should be stored in a secure place protected from unintentional events like fire and from intentional events like theft or vandalism. It is advisable to keep the backup separate from the server.		✓	✓
13	Implement intrusion detectors, motion detectors and alarms inside the server room.			✓

Table 32: Physical Security

7.9. Mobile Security

The fast-maturing mobile devices (“MDs”) can perform many of the functions of the personal computers. Such devices include laptops, mobile phones, tablets, USB, and portable hard disk. These devices enable access to a wide range of applications with the additional benefit of being mobile.

Risks relating to securing mobile devices are categorized into five basic concerns:

- Lost and stolen devices
- Physical access
- The role of end user device ownership
- Always on with increased data access
- Lack of awareness

The risk introduced by mobile devices tends to be an expansion of the current risk landscape — rather than introducing completely new risks, it has the potential to amplify and increase certain risk.

7.9.1 Mobile Devices Security

Mobile devices security is a measure to protect against a wide range of threats that seek to violate your privacy and seek to take any other information stored on your phone. These attacks on mobile device are to take your private information such as bank information, login information, and your organisation data.

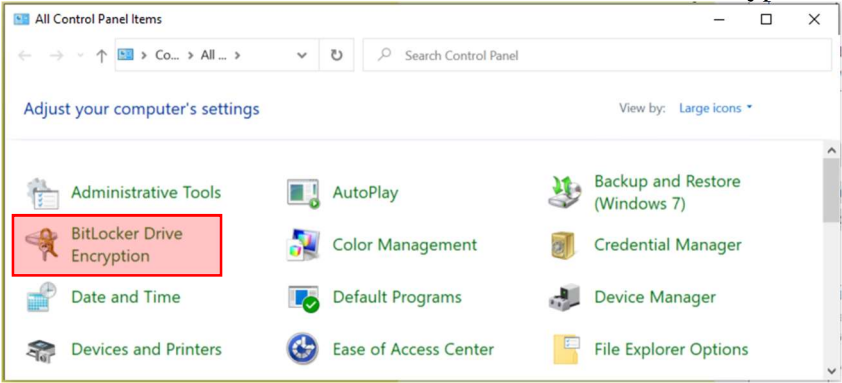
Mobile Devices Security		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Creating a flexible but enforceable policy to ensuring that it effectively limits risk to the organisation. <ul style="list-style-type: none"> • General security requirements for mobile devices • Authentication (passcode/PIN) requirements • Storage/transmission encryption requirements • Requirements to automatically wipe devices after a number of failed login attempts • Usage restrictions for mobile devices • Company liability • Rights to monitor, manage and wipe • Organisation specified supporting model • Leading practices for mobile data usage on international travel • Acceptable use (if different from the normal acceptable use policy) 	✓	✓	✓
2	Establish usage restrictions, configuration requirements, connection requirements and implementation guidance for NGO-controlled Mobile Devices such as Corporate Owned Personally Enabled (COPE) devices.	✓	✓	✓
3	Evaluate device usage scenarios and investigate leading practices to mitigate each risk scenario.	✓	✓	✓

4	Enforce industry standard security policies: whole-device encryption, PIN code, failed login attempt actions, remotely wiping, etc.	✓	✓	✓
5	Set a security baseline. Certify hardware/operating systems for enterprise use this baseline.	✓	✓	✓
6	Secure devices and apps, use mobile anti-malware programs to protect NGO issued and Bring Your Own Device (BYOD) mobile devices. * Please refer solutions in section 7.5 Computer Network Security Table #26.	✓	✓	✓
7	Only install authorised app.	✓	✓	✓
8	Review, monitor and revise policies regularly.	✓	✓	✓
9	Add mobile device risk to the organisation's awareness program.		✓	✓
10	Create a patch education process to encourage users to update their mobile devices.		✓	✓
11	In BYOD scenario, segment business environments and data from personal employee data as much as possible. Segmenting a network into logical operational areas with strict access control limits between each scope is a well-established security principle.		✓	✓
12	Involve stakeholders early through the formation of a mobility group.		✓	✓
13	Test and verify the security of the implementation.		✓	✓
14	Create and enforce an appropriate BYOD support and usage policy. * Please refer solutions in section 7.5 Computer Network Security Table #26.		✓	✓
15	Introduce more stringent authentication and access controls for critical business apps.			✓
16	Invest in a mobile device management (MDM) solution to enforce policies and monitor usage and access if possible. * Please refer solutions in section 7.5 Computer Network Security Table #26.			✓
17	Revamp existing support processes to include secure provisioning and deprovisioning (wipe) of devices, and an increased level of self-help. * Please refer solutions in section 7.5 Computer Network Security Table #26.			✓

Table 33: Mobile Device Security

7.9.2 Portable Storage Security

Portable Storage Media such as USB drives, flash memories devices, and portable hard drive that contain sensitive and confidential information should have reasonable measures to protect the confidentiality of the data. Portable devices might be used outside the organisation, connect to other computers and are prone to loss and theft.

Portable Storage		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Increasing threats of data breaches have led to portable storage devices that now have built-in security protocols (i.e. encrypted USB storage / encrypted portable hard drive etc.). By encrypting the files on your portable storage device are essentially need a long password to protect it.	✓	✓	✓
2	<p>To encrypt information on the USB storage devices and portable hard drives without encryption protection feature, Microsoft BitLocker-To-Go may one of the solutions.</p> <p>Turn on BitLocker-To-Go to Encrypt Files</p> <ol style="list-style-type: none"> 1. Connect your removable storage device or USB storage devices to your computer. 2. Go to “Control Panel” and select “BitLocker Drive Encryption”  <p><i>Figure 4: BitLocker Drive Encryption – Control Panel</i></p> <ol style="list-style-type: none"> 3. Select the removable storage drive you want to encrypt and then click “Turn on BitLocker”. 4. Choose how you want to encrypt the drive. 5. Select the encryption mode. 6. Follow the steps to complete the portable hard drive encryption. <p>The footnote URL ⁴³ is a detail of “Enable BitLocker Device Encryption” to encrypt data stored on portable hard drives.</p>		✓	✓

100_____

⁴³ Enforce drive encryption type on removable data drives - Microsoft.
<https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings#enforce-drive-encryption-type-on-removable-data-drives>

4	<p>Secure data at rest on USB storage and portable hard drives with third parties' tools:</p> <ul style="list-style-type: none"> • Encrypt entire storage devices on portable hard drive⁴⁴ <ul style="list-style-type: none"> - VeraCrypt is a multi-platform, freeware open source tool created to provide users with on-the-fly encryption include the ability to create virtual encrypted disks and mount them. • Encrypt individual files⁴⁵ <ul style="list-style-type: none"> - 7-zip is a free, open source multi-platform file archiving utility for compressing files (or file groups) into containers referred to as archives. 		✓	✓
---	---	--	---	---

Table 34: Portable Device Security

⁴⁴ Encrypt entire storage devices on portable hard drive

<https://www.veracrypt.fr/en/Home.html>

⁴⁵ 7Zip Encrypt individual files

<https://www.7-zip.org/>

7.10. Remote Access/Work from Home

Nowadays, more and more organisations are asking their employees to Work From Home (WFH). This presents several different cyber security challenges and risks for businesses whose day-to-day operations are usually office based.

Furthermore, as employees work in different environments their cyber risk profiles change, with some using a wider range of personal devices.

There are several common risks which many organisations will need to be manage including phishing attacks, loss of devices, using personal devices, and/or working in public spaces.

Remote Access/Work from Home		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Access with the user about their home computer's desktop and mobile devices should at least be password protected, and the password should be strong one (i.e. user's password must be at least 8 characters long).	✓	✓	✓
2	Use organisation provided services for e-mail, messaging, conferencing, and all other work if possible.	✓	✓	✓
3	Recommend the user clear their web browser history after use to avoid other users accessing sensitive information.	✓	✓	✓
4	Recommend the user disable auto-fill settings on their web browser.	✓	✓	✓
5	When using personal workstation to view sensitive information online, select the private browsing mode on the internet browser (Private browsing - Firefox, Incognito - Chrome, InPrivate - Edge)	✓	✓	✓
6	Keep the remote operating system and applications update. Enable the system and applications auto-update configuration.	✓	✓	✓
7	Recommend the WFH user update their personal devices antivirus solution with an updated signature and update the organisation software and operating systems.	✓	✓	✓
8	Recommend the WFH users secure their files, backup important files offline on external hard drive, or in the cloud. Make sure they store their paper files securely.		✓	✓
9	Provide WFH users with a multi-factor authentication to access the organisation office network with sensitive information.		✓	✓

10	Make sure the WFH users have access to organisation’s remote office or cloud infrastructure through an encrypted VPN Tunnel. Also provide guideline to secure their home Wi-Fi with encryption and strong password, in case VPN isn’t an option or if it fails for some reason.		✓	✓
11	Make sure WFH users’ backup their daily work offline on organisation’s cloud drive or encrypted USB media.		✓	✓

Table 35: Remote Access/Work from Home

7.11. Security Risk Assessment and Audit

Risk assessment programs help ensure that the greatest risks to the organisation are identified and addressed on a continuing basis. Security risk assessments help NGO discover the most critical gaps in their security posture, which in turn enables NGO to prioritize their security investments. Every NGO has its own unique risk profile. By identifying individual security gaps and the most likely threats, NGO can create a cyber security roadmap that strategically mitigates risk.

Security Risk Assessment and Audit		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	The assessment of risks to the organisation, considering the organisation's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.	✓	✓	✓
2	Areas of rationale for performing an NGO security risk assessment include: <ul style="list-style-type: none"> • Cost justification • Productivity • Senior management buy in • Communication 	✓	✓	✓
3	Security risk assessment requirements: <ul style="list-style-type: none"> • Project Scopes and Objectives • Constraints • Roles & Responsibilities of Stakeholders • Approach and Methodology • Project Size and Schedule • Data and Tools 	✓	✓	✓
4	Consider factors when perform risk analysis: <ul style="list-style-type: none"> • Asset Identification and Valuation • Threat Analysis • Vulnerability Analysis • Asset/Threat/Vulnerability Mapping • Impact and Likelihood Assessment • Risk Results Analysis • Compile security risk assessment report and follow-up plan 	✓	✓	✓
5	The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a NGO's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.	✓	✓	✓

6	Clearly defined segregation of duties. Ensure that the same personnel do not perform conflicting functions, for example, administrating security access controls as well as performing audit functions.		✓	✓
7	Ensure that audit information is protected from unauthorised access, modification and deletion, and is retained for administrative, auditors or other operational purposes, until such time that these records are no longer required.		✓	✓
8	Review and analyse IT systems and services audit records and logs regularly for indication of inappropriate or unusual activity and report the findings to those responsible for managing such events.			✓
9	Conduct a risk assessment, including the likelihood and severity of harm arising from unauthorised access, use, disclosure, disruption, modification or destruction of the IT systems and the information that stores, processes and transmits.			✓
10	Conduct periodic vulnerability scanning of the IT systems to detect outdated systems, missing patches, and security vulnerabilities in the IT systems and software applications that are used.			✓
11	Periodically carry out a security audit (suggest at least in two years) with an action plan, the implementation of which should be monitored at the highest level.			✓

Table 36: Security Risk Assessment and Audit

Related Tool(s):

- 8.6 Security Risk Assessment Guidelines
- 9.3 Nessus Essentials
- 9.4 OWASP Zed Attack Proxy (ZAP)
- 9.5 Kali Linux

7.12. Insider Threats

Insiders are individuals trusted to protect organisational secrets and intellectual property. The proliferation of sensitive data, excessive access to data, and lack of employee awareness all exacerbate the threat posed by insiders. Insider threats include fraud, intellectual property theft, espionage, and IT infrastructure damage.

The four types of insider threat can be defined according to their rationales and objectives:

1. The careless workers who mishandle data, break use policies and install unauthorised applications
 - Microsoft database leaked because of employee negligence⁴⁶
2. The inside agents who steal information on behalf of outsiders
 - Twitter users scammed because of phished employees⁴⁷
3. The Ex/disgruntled employees who seek to harm their organisation
 - Former Cisco employee purposely damaged cloud infrastructure⁴⁸
4. The malicious insiders who use existing privileges to steal information for personal gain
 - General Electric employees stole trade secrets to gain a business advantage⁴⁹

100

⁴⁶ Microsoft Security Shocker As 250 Million Customer Records Exposed Online

<https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=498a691f4d1b>

⁴⁷ 2020 Twitter bitcoin scam

https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam

⁴⁸ Ex-Cisco Engineer Pleads Guilty in Insider Threat Case

<https://www.bankinfosecurity.com/ex-cisco-engineer-pleads-guilty-in-insider-threat-case-a-14917>

⁴⁹ Investigation Into Theft of Intellectual Property from GE Leads to Two Guilty Pleas

<https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920>

As insider threats are a “people problem,” not an IT problem, it should include actions to deter, detect, and mitigate threats.

Insider threats		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	<p>Establish an information security policies and procedures</p> <ul style="list-style-type: none"> To develop a clear set of information security policies and procedures. The security policy should incorporate an insider threat program, which should be actionable, sustainable and seek measurable results. Developing a security culture with established policies and procedures to deter, detect, and mitigate those threats will minimize the frequency and impact of security incidents. Establish baselines on activities like work schedules and data transfers, determine what is outside the norm, and then identify individuals that deviate from the established boundaries. Educating employees by incorporating insider threat awareness into mandatory organisational training. Employees should receive training to understand insider threats, to identify the above risk indicators, and to report observed behavior appropriately. 	✓	✓	✓
2	<p>Establish Incident detection platforms</p> <ul style="list-style-type: none"> Implement user monitoring and data-loss protection mechanisms, this can alert security team to unauthorized data transfers. Log management and security information and event management (SIEM) assist with detection exception activities and the analysis that occurs in the aftermath of a security incident. 	✓	✓	✓
3	<p>Insider threats deterrence methods</p> <ul style="list-style-type: none"> All organisations should implement the least privilege principle, which is applicable to physical and cyber security. Establishing security policies and data encryption, should also include access controls. Individuals or third parties should not receive access to networks, data, or physical spaces unless it is necessary to perform their job function. With fewer people gaining access, fewer potential malicious actors or negligent employees will have the opportunity to compromise accounts. 	✓	✓	✓
4	<p>Authorised security personnel and regular employees should also observe the behavior of other employees. The identification of high-risk indicators is a key component to preventing insider threat issues.</p>		✓	✓

5	Security personnel can work with IT to implement technical restrictions, including prohibiting the use of USBs, external drives, or other device plug-ins, blocking unauthorized Internet downloads, and restricting access to certain downloads.		✓	✓
6	Take note that disgruntled employees seeking revenge or entitled employees looking for a competitive edge at a new employer may attempt to take data just prior to or at the point termination.		✓	✓
7	To prevent unauthorized data removal, HR/IT Department should restrict the employee's physical and IT access at termination, take ID badges, and escort the individual from the facility.		✓	✓
8	HR Department should coordinate with IT Department, organisations should monitor data flows prior to employee departure and remove the individual from email distribution lists.		✓	✓

Table 37: Insider Threats

7.13. Vendor Management

Choosing a supplier or service provider the organisation may need to go through a formal selection process. To make sure the vendor the organisation choose is the best one to provide the service or product the organisation needs, the following points may help the organisation select the right vendor for their business.

Vendor management		Stakeholder(s): Management		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	The organisation should identify and mandate information security controls to specifically address supplier access to the organisation's information in a policy.	✓	✓	✓
2	All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.	✓	✓	✓
3	Write a Request for Proposal (RFP) or Request for Quotation (RFQ) when the business requirements are defined and have a short list of vendors that NGO want to evaluate. RFP or RFQ should contain the following sections: <ul style="list-style-type: none"> • Submission details • Introduction and executive summary • Business overview and background • Detailed specifications • Assumptions and constraints • Terms and conditions • Selection criteria 	✓	✓	✓
4	The main objective of the proposal evaluation and vendor selection phase is to minimize human emotion and political positioning in order to arrive at a decision that is in the best interest of the company. The following factors should be considered when selecting a supplier: <ul style="list-style-type: none"> • Price • Quality of product or service • Client reference • Customer service • Clear communication • Ethics and integrity of the vendor • Professional employees • Recommendations from others 	✓	✓	✓

5	<p>NGO should create a list of the supplier's selection criteria that suppliers need to fulfil to be able to provide NGO with the items NGO need.</p> <p>The supplier selection criteria can include the following items:</p> <ul style="list-style-type: none"> • Lead times from receipt of the order to delivery • Service level agreement • Maintenance and support details • History records and references • Supplier performance • Quality assurance processes • Payment terms and conditions • Contactable references 	✓	✓	✓
6	The vendors management should Focus on total cost of ownership, not just initial cost.	✓	✓	✓
7	NGO should define the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access.	✓	✓	✓
8	NGO should define the types of obligations applicable to suppliers to protect the organisation's information.	✓	✓	✓
9	NGO should define the conditions under which information security requirements and controls will be documented in an agreement signed by both parties.	✓	✓	✓
10	NGO should monitor supplier's obligations to comply with the organisation's security requirements.	✓	✓	✓
11	NGO should define information security requirements to apply to ICT product or service acquisition in addition to the general information security requirements for supplier relationships.	✓	✓	✓
12	NGO should require that suppliers propagate appropriate ICT security practices throughout the supply chain if these products include components		✓	✓
13	NGO should implement a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements.		✓	✓
14	NGO should include the right to audit the supplier processes and controls related to the contract and agreement.		✓	✓

Table 38: Vendor management

Related Tool(s):

8.3 Vendor Risk Assessment Checklist

7.14. Awareness and Training

Security awareness training is a method of educating employees to the dangers of phishing or other online scams and should be a required component of every organisation. Security awareness programs help organisations achieve the goal of fewer security incidents.

An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees to minimize possible security risks.

There are several benefits of that show how it can help protect the organisation from hackers, thieves, and other bad actors.

- Training reduces staff errors.
- Training enhances security.
- An educated staff increases compliance.
- Training can help protect an NGO's reputation.

Awareness and Training		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Senior Management has a responsibility to develop a culture of security and business continuity awareness.	✓	✓	✓
2	All employees of the NGO should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.	✓	✓	✓
3	Reminded all users they are the last line of defence. Established a formal security incident reporting procedure for users to report security/threat incidents through appropriate management channels as quickly as possible.	✓	✓	✓
4	As part of initial awareness training for new employees and conduct of training regularly to keep employees educated of cyber security threats and security measures.	✓	✓	✓
5	Establishing the basics, which include: Anti-phishing tactics, Password security, Physical security, and Social engineering attacks		✓	✓
6	Service providers that provide cyber security related services for the organisation are informed about the organisation's applicable privacy policies			✓

Table 39: Awareness and Training

7.15. Incident Response Management

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Formal incident event reporting and escalation procedures should be in place.

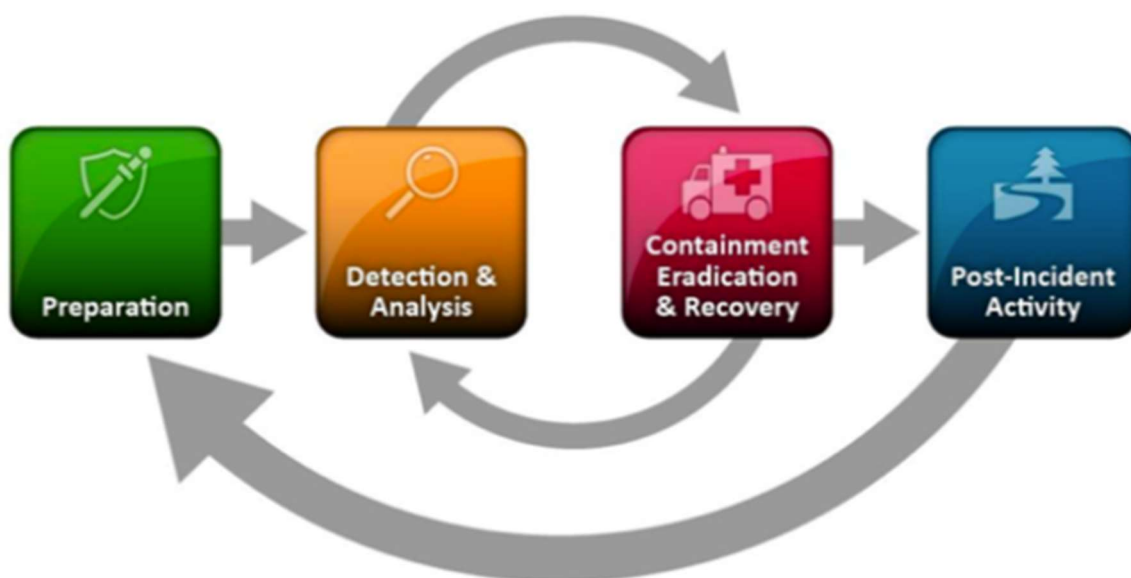


Figure 5: NIST SP800-61r2 Incident Response Life Cycle⁵⁰

All employees should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Incident Response Procedure

- Preparation - Protect assets with the appropriate safeguards.
- Detection - Detect intrusions, breaches, and unauthorized access.
- Containment Eradication - Respond to a potential cyber security event.
- Recovery - Recover from a cyber security event by restoring normal operations and services.
- Post-Incident Activity - A final review of what happened and the organisation incident response plan as well as steps to address any vulnerabilities in the systems, policies, or procedures.

100

⁵⁰ Computer Security Incident Handling Guide - NIST 800-61 revision 2
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Incident Response Management		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Define four tiers of responses can prepare for based on projected impact of outages, ranging from most to least severe: <ul style="list-style-type: none"> • Tier A: Systemic / life-threatening impact; • Tier B: Business critical impact; • Tier C: Operational impact; and • Tier D: Minimal impact 	✓	✓	✓
2	Creating an incident response policy, procedure, and plan. Review the policy, procedure, and plan annually. In the event of a data security incident, implement the established incident response model.	✓	✓	✓
3	Preparation <ul style="list-style-type: none"> • Implement the organisation response patterns where the event and data occur. • Assess impact and prioritize risks when incident occur. • Use human responses for unique, new, and sensitive incidents. • Automate where possible, build mechanisms that programmatically triage and respond to common situations. 	✓	✓	✓
5	Developing incident report template for incident handling and reporting.	✓	✓	✓
6	Setting guidelines for communicating with outside parties regarding incidents.	✓	✓	✓
7	Selecting an incident response team structure and staffing model.	✓	✓	✓
8	Determining what service(s) the incident response team should provide.	✓	✓	✓
9	Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., IT department) and external (e.g., law enforcement agencies)		✓	✓
10	Staffing and training the incident response team. Learn and improve the organisation incident response process		✓	✓
11	Conduct periodic drill testing of cyber security incident response capabilities to test the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies.		✓	✓

12	If a security anomaly can be attributed to a misconfiguration, the remediation might be removing the variance by redeploying the resources with the proper configuration.			✓
13	Track, document and report IT security incidents. Preserve logs, snapshots, and other evidence by copying them to a centralized security cloud account. Use tags, metadata, and mechanisms that enforce retention policies.			✓
14	Review the root cause of incidents to improve the detection and protection processes. The incident management process may need revising.			✓

Table 40: Incident Response Management

Related Tool(s):

8.2.1 Security Incident Response Form

8.2.2 Security Incident Response Records

7.16. Business Continuity Management

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organisation, and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Establishing and maintaining business continuity management processes begins with three steps:

1. Defining business continuity management;
2. Identifying and defining the key components of a viable BCM framework; and
3. Placing BCM in the context of organisational risk management

Business Continuity Planning (BCP) is the process through which organisations establish the capabilities necessary to protect their assets and continue key business processes after a disaster — an unexpected business interruption caused by natural or man-made events occurs.

BCM is a key contributor to effective corporate governance. It is often positioned under Risk Management and allows stakeholders to ask searching questions, such as:

- The company's business and operating model
- Key value creating products and services
- Key dependencies – critical assets and processes
- How the company will respond to a loss of or threat to any of these
- What the main threats are today and on the horizon
- Evidence that the business continuity plans will work in practice

Business Continuity Management		Stakeholder(s): Management		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Identify the NGO's strategy, objectives and culture to develop the BCM policy: <ol style="list-style-type: none"> 1. Interview the Top Management team 2. Perform Business Impact Analysis 3. Review documents produced by the organisation <ul style="list-style-type: none"> • Business plans, Strategic plans • Annual report, Marketing report • Current management information reports outlining process details, volumes, targets and, quantified value of the activity 		✓	✓
2	Perform Business Impact Analysis (BIA) <ul style="list-style-type: none"> • To identify and priorities products and services and determine the NGO's business continuity requirements at a strategic level. • To determine the process or processes required for the delivery of the NGO's prioritized products and services. • To identify and prioritise the activities that deliver the most urgent products and services, and to determine the resources required for the continuity of these activities. 		✓	✓

3	<p>Decisions about Cyber Risk Appetite</p> <p>When making a decision on cyber risk appetite, the following questions can be considered:</p> <ul style="list-style-type: none"> • What are the critical assets and business processes that support achieving our organisational goals? • What are the organisation's risk tolerances, in general and with What losses would be catastrophic? • What can the organisation live without and for how long? • What information absolutely cannot fall into the wrong hands or be made public? • What could cause personal harm to employees, customers, partners, visitors? 		✓	✓
4	<p>Establishing the business continuity plan. The business continuity policy sets the boundaries and requirements for the business continuity programme and states the reasons why it is being implemented. It defines the guiding principles which the organisation follows and measures its performance against.</p>		✓	✓
5	<p>BCM Competencies and Skills:</p> <ul style="list-style-type: none"> • Project management skills and an understanding of the importance of continual improvement. • An understanding of the organisational culture and how to influence it. • Knowledge of the business continuity competencies and skills required and training and awareness raising capabilities. • Analytical skills relating to the BIA, including the ability to analyse information, identify problems, and develop workable solutions. • An understanding of risk assessment and mitigation measures. 		✓	✓
6	<p>Business Continuity Plan (BCP) design and implementation</p> <ul style="list-style-type: none"> • Continuity and recovery strategy and tactics including redundancy, diversification and manual workaround • Threat mitigation for unacceptable risks • Incident Response structure 		✓	✓
7	<p>Reviewing and testing the BCP are important steps.</p> <ul style="list-style-type: none"> • Conducts a high-level check on the plan, ensuring that all objectives are still being met - Yearly. • Review of the risk assessment, BIA and recovery plans – Ever Other Year • Structure walk-through of the plan – Every Other Year • Comprehensive review – Every Other Year • Recovery simulation test – Every two or three Years 		✓	✓

8	After reviewing and testing the BCP, use the results to: <ul style="list-style-type: none"> • Update the business recovery plan • Develop the testing schedule for next year • Present a test report to senior management/board of directors 		✓	✓
---	---	--	---	---

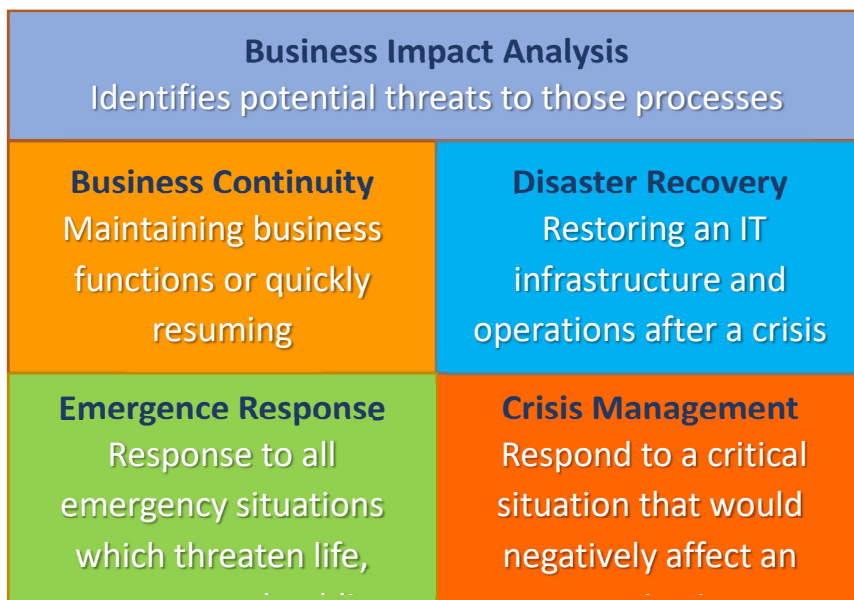


Figure 6: Business Continuity Management Tasks
Table 41: Business Continuity Management

7.17. Log Management and Monitoring

Logging and monitoring are closely related because log data is one of the critical data sources available to the organisation for performing application/access control monitoring. While logs are not the only source of valuable application metrics for the organisation monitoring tools, logs created by applications, servers, network infrastructure and more offer detailed windows into the ways in which an application is performing.

The objective of Log Management and Monitoring is to detect unauthorized information processing activities. Effective log management is essential to both security and compliance.

Without properly managed logs that make data from across an environment available to application monitoring tools, the organisation may lack a critical source of data for monitoring. Without monitoring, the IT admin/security officer will not be able to make sense of log data in order to understand how the organisation's application is performing; nor will the system admin/security officer be able to troubleshoot problems and prevent problems from recurring.

Possibly the Log Management/SIEM (Security Information Event Management) solutions are aplenty. A wide array of open-source solutions is available, but usually require strong technicality and time to set up and operationalize. Another option is to implement the NCSC's⁵¹ Logging Made Easy⁵² (LME) to gain a basic level of centralised security logging for Windows clients and provide functionality to detect attacks.

Log Management and Monitoring		Stakeholder(s): Management, IT Admin		
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Systems should be monitored, and information security events should be recorded.		✓	✓
2	Logs should be collected from these sources: Anti-Malware software, critical applications, user authentication, firewalls, IDS/IPS, NAS, network devices, operating systems, remote access software (e.g.: VPN, RDP), web proxies, and web servers.		✓	✓
3	Operator logs and fault logging should be logged and reviewed regularly to ensure information system problems are identified.		✓	✓
4	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.		✓	✓

⁵¹ National Cyber Security Centre, UK (NCSC)

<https://www.ncsc.gov.uk>

⁵² Logging Made Easy, NCSC, UK

<https://github.com/ukncsc/lme>

5	Log management systems must be configured to parse events and data that matter to the organisation so that reports have business and technical value.		✓	✓
6	Periodically review the alert console, thereby system admin/security officer will not be missing critical security events.		✓	✓
7	Committing to log management technology should also have to review log entries regularly.		✓	✓
8	Server time should be synchronised to align the timestamp of log records. This can be done by configuring time server.		✓	✓
9	Log server disk space capacity should be planned according to number of days of records to retain.		✓	✓
10	Use log data to figure out what is happening or what just happened.			✓
11	Outsource or implement Log Management System/SIEM for security events monitoring.			✓

<p>Action (mostly human)</p> <ul style="list-style-type: none"> - Response, remediation and recovery - Escalation - Investigation - Incident management - Reporting - Change management 	<p><i>Figure 7: Cyber Security Monitoring Key Components</i></p>	<p>Collection (mostly machine)</p> <ul style="list-style-type: none"> - Log identification - Normalisation - Retention - Filtering
<p>Analysis (mostly human)</p> <ul style="list-style-type: none"> - Predetermined rules - Triage - Workflow - Trends/patterns/risk analysis - Threat intelligence 	<p><i>Figure 8: Umbrella View of SIEM</i></p>	<p>Fusion (mostly machine)</p> <ul style="list-style-type: none"> - Automation - SIEM rules - Firewall rules - IDS/IPS signatures - IOC

Table 42: Log Management and Monitoring

Related Tool(s):

9.6 Logging Made Easy

8. Checklists and Templates

8.1. IT Asset Valuation List Template

An IT asset valuation is a list of all computing and networking related devices owned, managed, or otherwise used by an NGO. These devices include computers (desktops, notebooks, servers), network devices (switches, routers, etc), printers, appliances (network attached storage, network capable cameras, etc) and NGO’s data asset.

There are a number of reasons that maintaining an inventory of IT assets is important and useful.

- Provides a record of valuable assets for accounting/tracking purposes
- Helps identify areas of potential risk (notebooks storing private data, servers with expired warranties, etc.)
- Important piece of information for business continuity planning
- Provides information useful during technical support or in the event of loss/theft.

Asset No	Asset Information	Description	Reference	Location	Asset Val	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update Integrity	Resilience (Availability)	Accessed By	Threat Level	Consequence (Livelihood)	Probability (Livelihood)	Security Score	
1	WAS-001	WebApp Internet Facing, Cross NGO	Internet Facing Web Application for Cross NGOs	IBM-0001-xxxx-0001	NGO DC-001	High	Restricted	Over 3 Years	Planned	Backup	Own & Partners	Low	Very High	High	11
2	WAS-002	WebApp Backend system (Confident)	NGO Internal Backend Web Application	IBM-0001-xxxx-0002	NGO DC-002	High	Confidential	Once	Planned	Backup	Own	Medium	Very High	Low	10
3	WAS-003	Website for Public	NGO Public Web Application	Azure Win2019	Public Cloud (Azure)	High	Public	Once	Outdated	Backup	Public	High	Medium	Medium	10
4	SYS-001	WebApp for NGO & Public Users	Self Service System for Public and NGO Users	Azure Win2019	Public Cloud (Azure)	High	Internal	Once	Outdated	Backup	Own & Public	High	High	Very High	13
5	SYS-002	WebApp for Internal Users	NGO Application for internal users	Windows 2018	On-premises	Medium	Internal	Periodically	Outdated	Backup	Own	Low	Medium	Low	7
6	SYS-003	WebApp Internal (Sensitive)	NGO Application for internal users (Sensitive)	Windows 2018	On-premises	Medium	Restricted	Once	Outdated	Backup	Own	High	High	Low	10
7	Mobile-001	Mobile App for Internal	NGO Application for users (Sensitive)	iPhone, Android	handphone	Out Door	Medium	Internal	Once	Outdated	Not Available	Own	High	Medium	10
8	NGO-Data	NGO Proprietary Info.	NGO Proprietary Information (Internal Use Only)	Proprietary	NGO	Medium	Restricted	Once	Outdated	Backup	Own	High	High	Low	10
9	NGOs-Data	NGO Shared Info.	NGOs Shared Information (Cross-NGOs units)	Cross-NGOs Data	G Suite-Google	Medium	Restricted	Once	Planned	Not Available	Own	Medium	High	Medium	10
10	WEB-001	NGO Main Site	The NGO portal website	NGO Server	Cloud	Medium	Restricted	Once	Planned	Not Available	Public	Medium	High	High	11
11	WEB-002	NGO Intranet	The NGO intranet portal	NGO Server	On-premises	Medium	Internal	No Plan	Planned	Backup	Own	High	Medium	Low	9
12	HRS-1002	227.12.27.5	Human Resource Management Application	Annual-HR-12-089-001-6	HRM-Azure-Cloud	Medium	Internal	Over 3 Years	Planned	Backup	Own	Low	Medium	Low	7
13	FIN-1001	226.50.1.10	Finance Application	Annual-FIN-12-539-001-5	FIN-Azure-Cloud	Medium	Restricted	Over 3 Years	Planned	Backup	Own	Low	High	Low	8
14	NGO-APP-001-P	NGO Public Application	NGO Cases Application For Public	MS Windows 2016	HQ-DC-01-P	Medium	Internal	Once	Outdated	Backup	Own & Public	High	Medium	Very High	12
15	IFS-HQ-DC-OA-01	10.10.20.100	Office File Sharing server (HQ)	MS Windows 2016	HQ-DC-01	Medium	Internal	No Plan	Outdated	Not Available	Own	Very High	Medium	Medium	11
16	IFS-HQ-DC-CASE-01	10.10.20.101	NGO Cases File server (HQ)	MS Windows 2016	HQ-DC-01	Medium	Internal	No Plan	Outdated	Not Available	Own	Very High	Medium	Medium	11
17	WEB-HQ-DC-01	10.10.1.10/225.128.1.2	NGO Web Server	Ubuntu 17-04 Zesty Zapus	Cloud AWS	Medium	Internal	Once	Planned	Not Available	Public	Medium	Medium	High	10
18	IDB-HQ-DC-01	10.10.5.5	NGO Cases Database (HQ)	MS Windows 2016/MSSQL 2016	HQ-DC-01	High	Restricted	Over 3 Years	Outdated	Backup	Own	Medium	Very High	Low	10
19	IDB-HQ-DC-02	10.10.5.6	NGO Cases Database (HQ) Shared with NGOs	MS Windows 2016/MSSQL 2016	HQ-DC-01	High	Internal	Once	Outdated	Backup	Own & Partners	High	High	High	12

Figure 9: IT Asset Valuation Template (Templates)



IT_Asset_Valuation_Template (Eng)

8.2. Security Incident Response Form and Records (Template)

8.2.1 Security Incident Response Form

This form provides a template of reporting the from initial to end details of an information security incident within an organisation.

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 Use <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Unplanned Downtime <input type="checkbox"/> Other: ..	
Description of Incident: ..	
Severity Level: ..	
Counter measure was: ..	
Names and Contact Information of Others Involved: ..	
1. XXXXX Operation Department 2. XXXX Operation Department <NGO> Incident Response Team XXXXXX	
INCIDENT NOTIFICATION – OTHERS	
<input type="checkbox"/> IS Leadership <input type="checkbox"/> System or Application Owner <input type="checkbox"/> System or Application Vendor.. <input type="checkbox"/> Security Incident Response Team <input type="checkbox"/> Public Affairs <input type="checkbox"/> Legal Counsel.. <input type="checkbox"/> Administration <input type="checkbox"/> Human Resources .. <input type="checkbox"/> Other: ..	
ACTIONS	
Identification Measures (Incident Verified, Assessed, Options Evaluated): ..	
Containment Measures: ..	
Evidence Collected (Systems Logs, etc.): ..	
Registry changes by malware: ..	

Figure 10: Security Incident Reporting Form (Template)



Incident
Response Report |

8.2.2 Security Incident Response Records

This form provides a template for information security incident reported within an organisation recording.

Information security incident reporting spreadsheet	
Reporting Quarter / Year	Choose
Department	e.g. Department of Social Welfare and Public Works
Business Unit	e.g. NGO Information Office (If applicable)
Agency Contact	
email	
Phone	
Date	
Instructions	<p>The following process should be used when completing this spreadsheet:</p> <ol style="list-style-type: none"> 1. Complete this 'Cover' sheet with the required details 2. Click on the 'Detailed reporting' tab and fill out ALL 'Mandatory' fields 3. Indicators of Compromise (IOC's) is a 'Mandatory' field however, there may be more IOC's than can fit in the cell. In this instance, click the 'IOC' tab, reference the relevant 'Incident number', assign the 'Type' of IOC and finally enter the actual IOC data. 4. Once the 'Cover', 'Detailed reporting' and 'IOC' sheets have been completed, please ensure it is emailed to the NGO Information Security Response Team <p>- Email: ITSec_XXXX@XXXX.org.hk - Subject: <Department Name> - Q<number> - <year> - Quarterly Information Security Incident Report</p>
Further information	Refer to the NGO Information security incident reporting guideline

Figure 11: Security Incident Reporting Records (Template)



8.3. Vendor Risk Assessment Checklist

Engaging third-party vendors for the provision of goods and services is common in NGOs.

Vendor risk management is important because managing vendor risk is foundational to cyber security, ensuring business continuity and maintaining regulatory compliance. A robust vendor risk management (VRM) program can help organisations under their vendor risk profile and mitigate third-party and fourth-party risk rather than relying on incident response.

A vendor risk assessment questionnaire is designed to help your organisation identify potential weaknesses among your third-party vendors and partners that could result in a data breach, data leak or other type of cyberattack.

#	Vendor Code	Vendor Name	Who Manages This Relationship?	Purpose of Vendor	Do They Access Customer Information?	Do They Access Financial Information?	Information?	Criticality Rating
1								
2								
3								
4								
5								
6								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								

Figure 12: Vendor Risk Assessment Management Record (Template)



8.4. Security Audit Checklist Template

In an IT compliance audit, auditors examine the risk management and security policies your organisation put in place to determine the thoroughness and strength of the organisation compliance efforts. Failing a compliance audit indicates security flaws in the organisation system, and the consequences of not taking action can be dire, including the eventual jeopardise of the organisation business.

NGO Name:		Date:		
Security Audit Checklist				
Topic	Question	Status	Client Response	Remark
1 Security Program				
1.1 Roles & Responsibilities	Has your organization formally appointed a central point of contact for security coordination?			
	a) If so, whom, and what is their position within the organization?			
	b) Responsibilities clearly documented? i.e. job descriptions, information security policy			
1.2 External Parties	Do you work with third parties, such as IT service providers, that have access to your information?			
	a) Does your organization have Business Associate agreements in place with these third parties?			
	b) If not, what controls does your organization have in place to monitor and assess third parties? i.e. Logging of VPN connections, etc.			
2 Security Policy				
2.1 Information Security Policy & Procedures	Do you have documented information security policies and procedures?			
	a) Do you have a formal information classification procedure? Please describe it. For example, critical, essential, and normal.			
	b) Have formal acceptable use rules been established for assets? Example assets include data assets, computer equipment, communications equipment, etc.			
	c) Do you have formal processes in place for security policy maintenance and exceptions?			
3 Training & Awareness				
3.1 During Employment – Training, Education & Awareness	a) Have your employees been provided formal information security training?			

Figure 13: NGO IT Audit Checklist (Template)



8.5. Seven Habits of Cyber Security

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) have compiled a “Seven Habits of Cyber Security” which cover seven areas:

- Security Policy and Security Management
- Endpoint Security
- Network Security
- System Security
- Security Monitoring
- Incident Handling
- User Awareness

This Seven habits includes security best practices and a simple checklist for security self-assessment, which aims to help SMEs as well as NGOs with limited resources to cope with the increasingly complex cyber security threats.

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.	<ul style="list-style-type: none"> <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. 	<ul style="list-style-type: none"> <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

Figure 14: Seven Habits of Cyber Security



8.6. Security Risk Assessment Guidelines

Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks. Rather, organisations employ risk assessments on an ongoing basis throughout the system development life cycle and across all of the tiers in the risk management hierarchy—with the frequency of the risk assessments and the resources applied during the assessments, commensurate with the expressly defined purpose and scope of the assessments.

This Security Risk Assessment Guidelines focuses on the risk assessment component of risk management—providing a step-by-step process for organisations on: (i) how to prepare for risk assessments; (ii) how to conduct risk assessments; (iii) how to communicate risk assessment results to key organisational personnel; and (iv) how to maintain the risk assessments over time.

Security Risk Assessment Guideline

1. Security Risk Assessment

1.1. Type of Security Risk Assessment

Depending on the purpose and the scope of the assessment, security risk assessment can be categorised into different types. The exact timing depends on your system requirements and resources.

1.1.1. High-level Assessment

Organisations with many information systems are looking for a high-level risk analysis of their information systems rather than a detailed and technical control review.

1.1.2. Comprehensive Assessment

This assessment is typically conducted periodically for the security assurance of information systems of an organisation. It can be used to evaluate the risks of a particular system in an organisation and to provide recommendations for improvement.

1.1.3. Pre-production Assessment

Similar to the works performed in a "Comprehensive Assessment", this assessment is commonly conducted on a new information system before it is rolled out or after there is a major functional change.

Figure 15: Security Risk Assessment Guidelines



Security_Risk_Assessment_Guidelin

9. Security Risk Assessment Tools

9.1. WinAudit

Windows Asset Audit Tool, Freeware – (Windows)

WinAudit is an inventory utility for Windows computers. It creates a comprehensive report on a machine's configuration, hardware, and software. WinAudit is free, open source and can be used or distributed by anyone.

WinAudit performs PC audits and inventory of software, licenses, security configuration, hardware, network settings and more.

WinAudit Features:

- Easy to use
- No setup
- Export report to csv/html/pdf/xml format, by E-mail
- Database export
- Execute from command line
- Fully documented

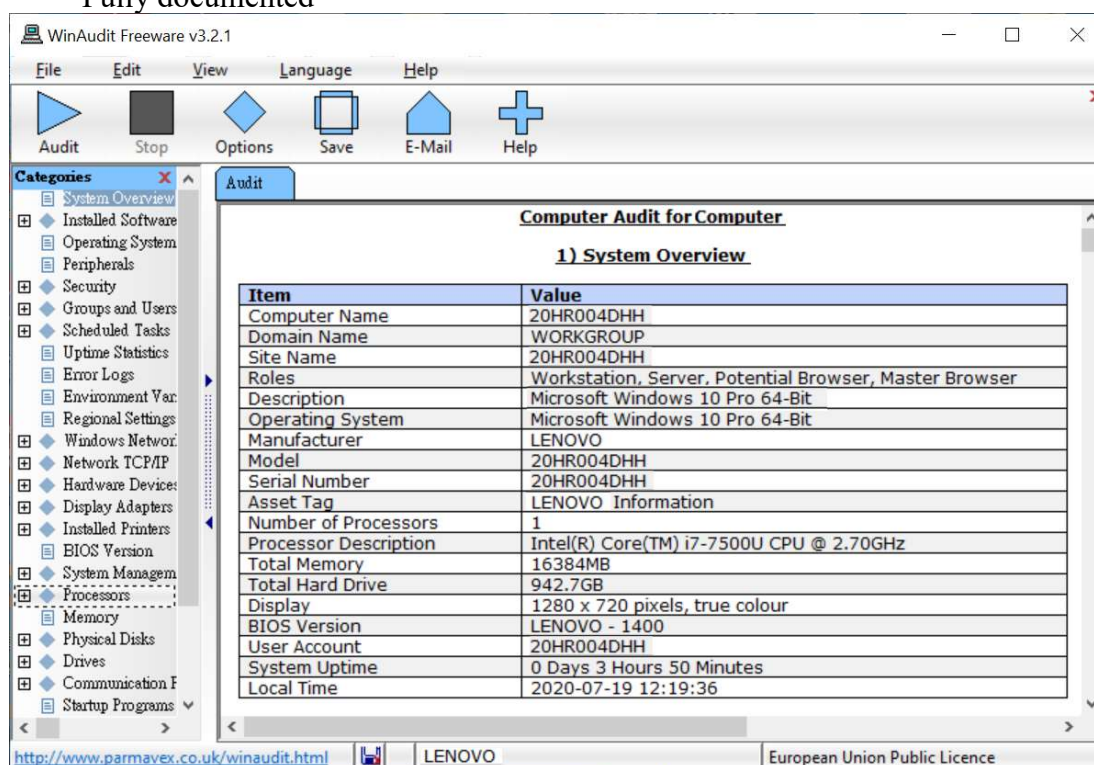


Figure 16: WinAudit Asset Audit Tool

WinAudit Inventory Tool <http://www.parmavex.co.uk/winaudit.html>

WinAudit Demonstration <https://briian.com/7359/>

9.2. NMap/Zenmap Security Scanner

A network mapper and port scanner (Windows, Linux, Mac OS X)

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

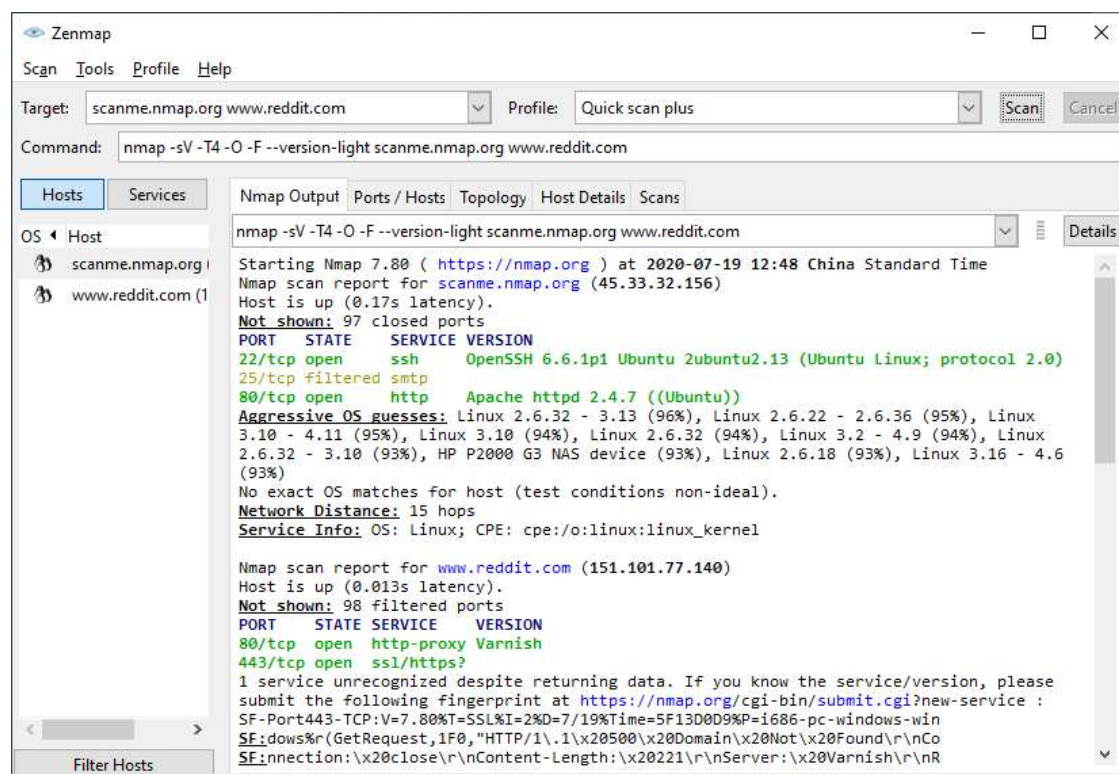


Figure 17: Nmap Network Scanner

Nmap Security Scanner GUI <https://nmap.org/download.html>

How to use Zenmap to Scan a Network https://linuxhint.com/zenmap_scan_network/

9.3. Nessus Essentials

Network and Host Vulnerability Scanner (Windows, Linux, Mac OS X)

Nessus is one of the most popular vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks.

Nessus can be used to perform a variety of tasks, including vulnerability detection, configuration auditing and patch status reporting. After the scanning, detailed report can be generated for further analysis and remediation.

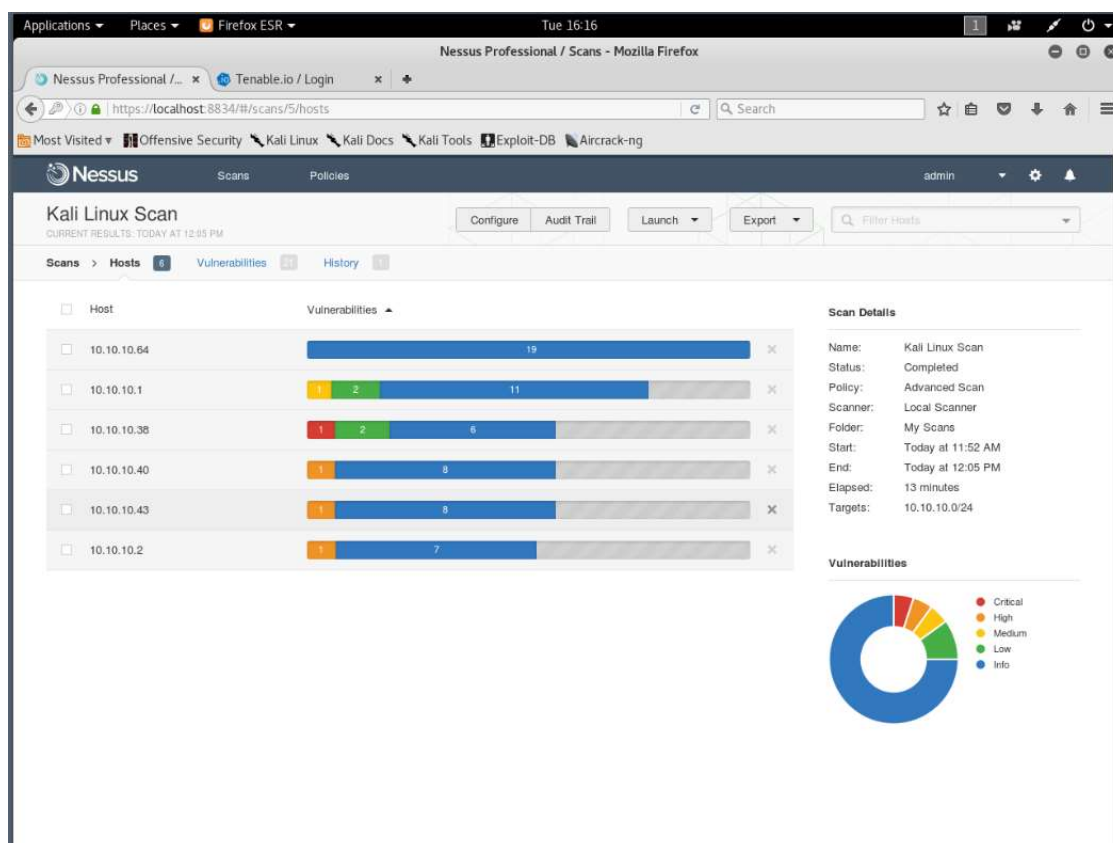


Figure 18: Nessus Vulnerability Scanner

Nessus Vulnerability Scanner <https://www.tenable.com/products/nessus>

Get your Nessus vulnerability assessment tool up and running
<https://zh-tw.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus>

9.4. OWASP Zed Attack Proxy (ZAP)

Web Application Scanner (Windows, Linux, Mac OS X)

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.

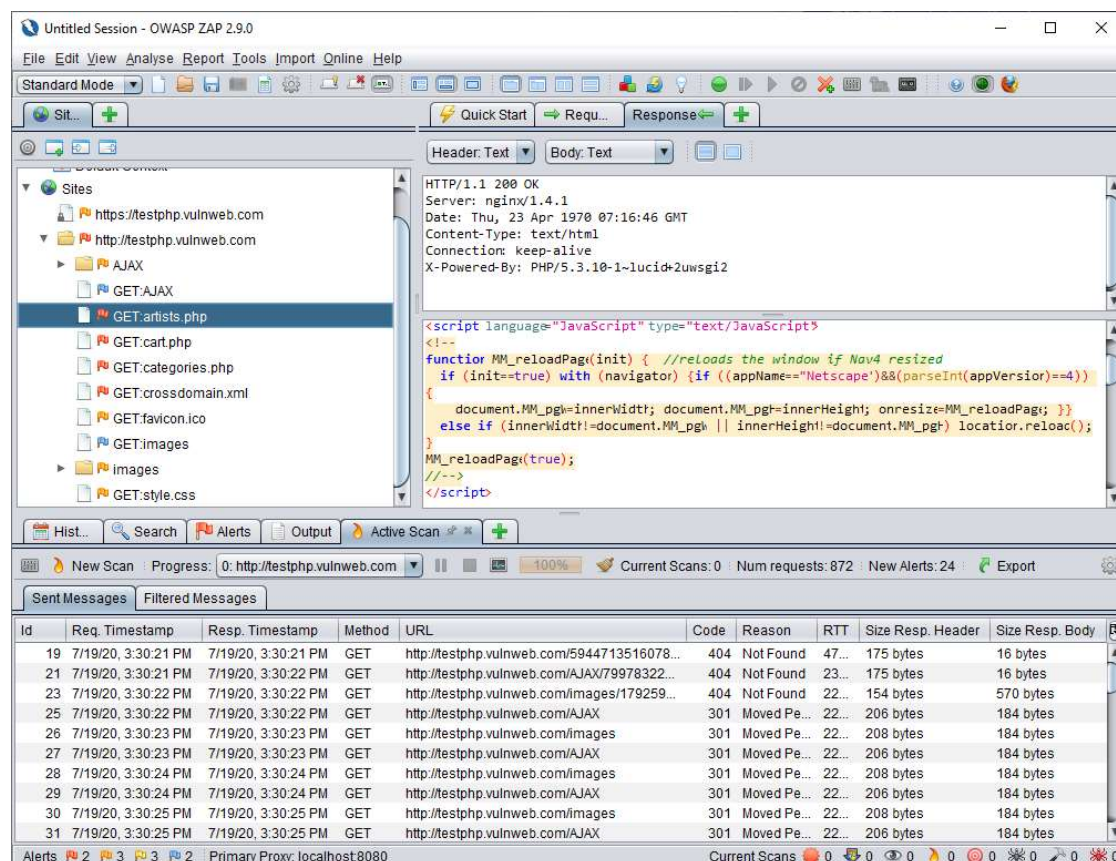


Figure 19: Zed Attack Proxy OWASP

The OWASP Zed Attack Proxy (ZAP) <https://www.zaproxy.org/>

Zaproxy Video Tutorials <https://github.com/zaproxy/zaproxy/wiki/VideoTutorials>

9.5. Kali Linux

Professional Penetration-Testing Distribution (Linux)

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.

It has preinstalled with over 600 penetration-testing programs, including nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper (a password cracker), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP (both web application security scanners).

Kali Linux can run natively when installed on a computer's hard disk, can be booted from a live CD or live USB, or it can run within a virtual machine.

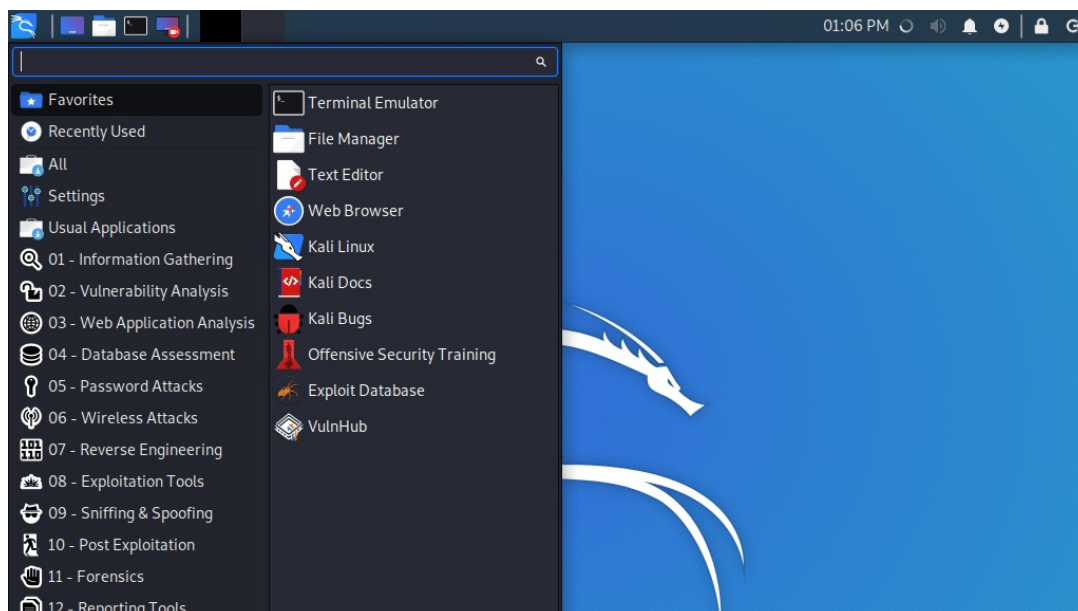


Figure 20: Kali Linux

Kali Linux <https://www.kali.org/>

Penetration Tutorial <https://wizardforcel.gitbooks.io/daxueba-kali-linux-tutorial/content/>

9.6. Logging Made Easy (LME)

Logging Made Easy (LME)

Logging Made Easy is a self-install tutorial for small organisations to gain a basic level of centralised security logging for Windows clients and provide functionality to detect attacks. It's the coming together of multiple free and open-source software (some which is covered under licences other than Apache V2), where LME helps the reader integrate them together to produce an end-to-end logging capability. We also provide some pre-made configuration files and scripts, although there is the option to do it on the system admin/security officer their own.

Logging Made Easy (LME) is for NGO if:

- The NGO don't have a SOC, SIEM or any monitoring in place.
- The NGO lack the budget, time or understanding to set up the organisation own logging system.
- The NGO recognise the need to begin gathering logs and monitoring the organisation IT operation.
- The NGO understand the LME has limitations, and is better than nothing - but no match for a professional tool.
- Small isolated networks where NGO monitoring doesn't reach

Logging Made Easy (LME) can:

- Tell system team about software patch levels on enrolled devices
- Show where administrative commands are being run on enrolled devices
- See who is using which machine
- In conjunction with threat reports, it is possible to query for the presence of an attacker in the form of Tools, Techniques and Procedures (TTPs)

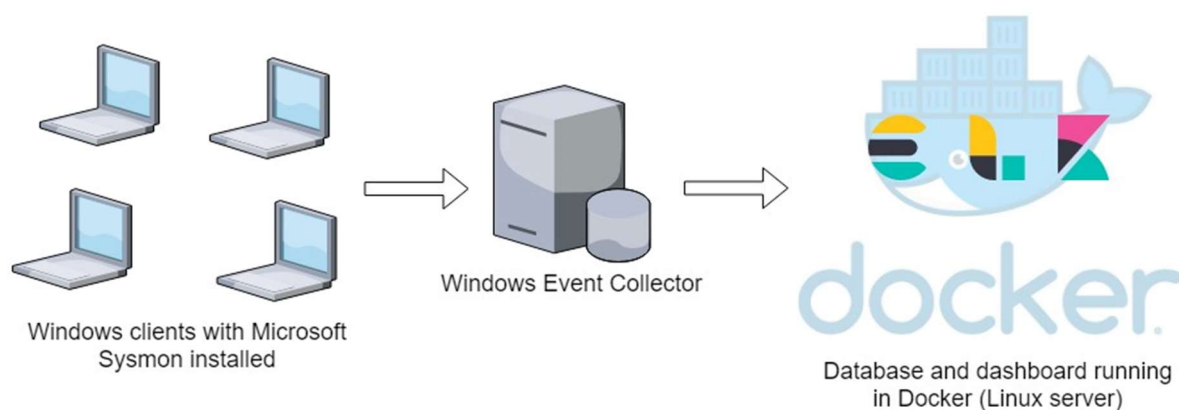


Figure 21: Logging Made Easy

Logging Made Easy, NCSC, UK <https://github.com/ukncsc/lme>

9.7. VeraCrypt

VeraCrypt (Windows, Linux, Mac OS X)

VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux.

VeraCrypt main features:

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed (pre-boot authentication).
- Encryption is automatic, real-time(on-the-fly) and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- Provides plausible deniability, in case an adversary forces you to reveal the password: Hidden volume (steganography) and hidden operating system.

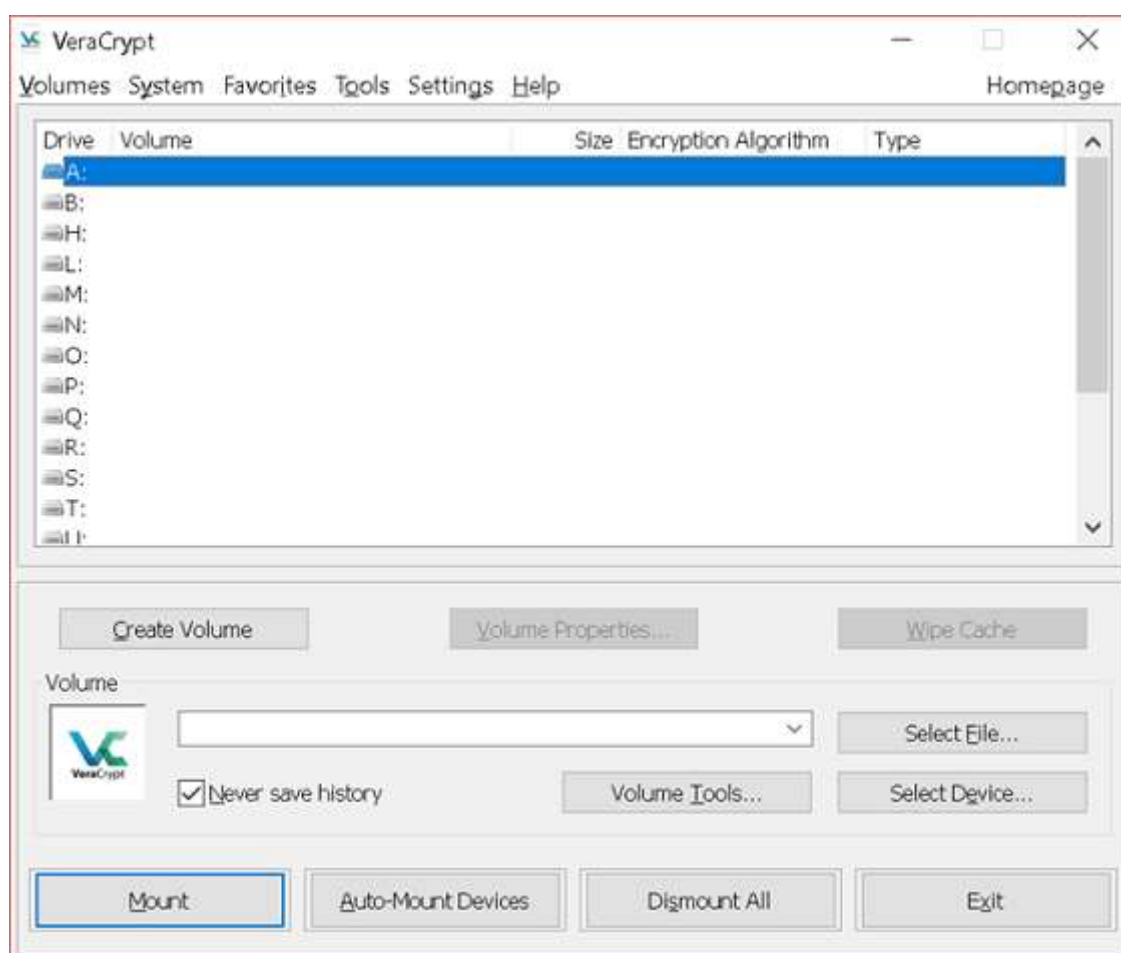


Figure 22: VeraCrypt

VeraCrypt <https://www.veracrypt.fr/code/VeraCrypt/>

VeraCrypt Tutorial <https://izaka.tw/2015-3-8-226/>

Appendix A - References

Law, Regulations, Standards, Policies, and Guidelines

This Guide draws on a variety of sources, including security controls from the defense, audit, financial, industrial/process control, and intelligence communities, as well as controls defined by national and international standards organisations. The guidelines have been developed from a technical perspective to create a sound and broadly applicable set of security controls for computer systems and NGO members.

The following documents, principles, and best practices constitute foundational references:

- A. ISO/IEC 27001:2013 Information Security Management System (ISMS)
 - ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.
 - <https://www.iso.org/standard/54534.html>
- B. ISO/FDIS 9001:2015 Quality Management System (QMS)
 - ISO 9001:2015 applies to any organisation, regardless of size or industry. ISO 9001 is based on the plan-do-check-act (PDCA) methodology and provides a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management in an organisation.
 - <https://www.iso.org/standard/62085.html>
- C. Security and Privacy Controls for Code of Practice
 - The international standard for security controls covering Six Data Protection Principles (DPP 6).
 - https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html
- D. Office of the Government Chief Information Officer (OGCIO) Information and Cyber Security
 - Reference the Government of Hong Kong's IT Security Guidelines (G3) to elaborate on the policy requirements and sets the implementation on the security requirements.
 - https://www.ogcio.gov.hk/en/our_work/information_cyber_security/
- E. Small Business Information Security: The Fundamentals (NISTIR 7621)
 - Outlines the actions that are absolutely necessary for a small business to take to protect its information, systems, and networks.
 - <https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final>
- F. Security and Privacy Controls for Federal Information Systems and Organisations (NIST SP 800-53.r4)
 - The international standard for security controls covering 17 areas, including: access control, incident response, business continuity, and disaster recoverability.
 - <http://dx.doi.org/10.6028/NIST.SP.800-53r4>

Appendix B - Glossary

Common Terms and Definitions

Acronyms	Description
APT	An Advanced Persistent Threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time. APT attacks are initiated to steal data rather than cause damage to the target organisation's network.
Assets	Any items belonging to or held by the business with some value (including information, in all forms and computer systems).
BCM	Business Continuity Management, BCM is part of the overall management system that implements, operates, monitors, reviews, maintains and improves business continuity.
BCP	Business Continuity Plan, a documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical products and services at an acceptable predefined level.
BEC	Business Email Compromise (BEC) is one of the most financially damaging online crimes. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request issue instruction, such as approving payments or releasing client data. The emails often use social engineering to trick the victim into making money transfers to the bank account of the fraudster.
BitLocker	BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
Breach	A security breach is a gap in security that arises through negligence or deliberate attack. It may be counter to policy or the law, and it is often exploited to foster further harmful or criminal action.
CSRF	Cross-Site Request Forgery, CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf.
Cyber	Relating to computers, software, communications systems and services used to access and interact with the Internet.
DKIM	Domain Keys Identified Mail (DKIM) is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain.

DMARC	Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email validation system designed to protect the organisation's email domain from being used for email spoofing, phishing scams and other cybercrimes. DMARC leverages the existing email authentication techniques SPF (Sender Policy Framework) DKIM (Domain Keys Identified Mail).
Encrypting File System	The Encrypting File System (EFS) on Microsoft Windows that provides filesystem-level encryption.
Encryption	Converting information into a code that can only be read by authorized persons who have been provided with the necessary (and usually unique) "key" and special software so that they can reverse the process (e.g., decryption) and use the information.
Firewall	A firewall is a type of security barrier placed between network environments. It may be a dedicated device or a composite of several components and techniques. Only authorized traffic, as defined by the local security policy, is allowed to pass.
GCHQ	Government Communications Headquarters, commonly known as GCHQ, is an intelligence and security organisation responsible for providing signals intelligence (SIGINT) and information assurance to the government and armed forces of the United Kingdom. GCHQ
Identity Theft	Copying another person's personally identifying information (such as their name and Social Insurance Number) and then impersonating that person to perpetrate fraud or other criminal activity.
Indicator of Compromise	Indicators of compromise (IOCs) are artifacts observed on a network or in an operations system where we have a high confidence that said artifact indicates a computer intrusion.
IDS/IPS	Intrusion Detection system (IDS) analyse network traffic for signatures that match known cyberattacks then sends out alerts to alert the operator. Intrusion Prevention Systems (IPS) also analyses packets but can also stop the packet from being delivered based on what kind of attacks it detects, helping stop the attack.
ITSPG	Information Technology Security Practice Guide
Malware	Malicious software created and distributed to cause harm. The most common instance of malware is a "virus."
OAuth2	The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

OpenID	OpenID is a decentralized authentication protocol. It allows users to be authenticated by co-operating sites (known as relying parties, or RP) using a third-party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log into multiple unrelated websites without having to have a separate identity and password for each.[
Patch	An update to or repair for any form of software that is applied without replacing the entire original program. Many patches are provided by software developers to address identified security vulnerabilities.
Penetration Test	Penetration test aims to identify weaknesses in specific system configurations and organisational processes and practices that can be exploited to compromise security.
Phishing	A specific kind of spam targeting one or more specific people while pretending to be a legitimate message, with the intent of defrauding the recipient(s).
Risk	Exposure to a negative outcome if a threat is realized.
Safeguard	A security process, physical mechanism or technical tool intended to counter specific threats. Sometimes also referred to as a control.
SIEM	Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
SOAR	SOAR (Security Orchestration, Automation, and Response) refers to a collection of software solutions and tools that allow organisations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.
SPF	The Sender Policy Framework (SPF) is an email-authentication technique which is used to prevent spammers from sending messages on behalf of the organisation domain. With SPF an organisation can publish authorized mail servers.
SRA	SRA (Security Risk Assessment) refers to quantifies or qualitatively describes the information security risk and enables organisations to prioritise risks according to their seriousness. It determines the value of an information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risks identified, determines the potential consequences and finally prioritises them.
Threat	Any potential event or action (deliberate or accidental) that represents a danger to the security of the business.
Vulnerability Scanning	Vulnerability scanning aims to identify any systems that are subject to known vulnerabilities

Vulnerability	A weakness in software, hardware, physical security or human practices that can be exploited to further a security attack.
WAF	A Web Application Firewall (WAF) monitors and filters traffic to and from the organisation website, blocking bad actors while safe traffic proceeds normally.

Table 43: Glossary

Appendix C - Acronyms

Common Abbreviations

Abbreviation	Description
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
AP	Wireless Access point
APT	Advanced Persistent Threat
Audit	Security Audit
BEC	Business Email Compromise
BIOS	Basic Input Output System
BitLocker	BitLocker Drive Encryption
BYOD	Bring Your Own Device
CASB	Cloud Access Security Brokers
CIO	Chief Information Officer
COPE	Company Owned/Personally Enabled
CSO	Chief Security Officer
CSRF	Cross-Site Request Forgery
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
EFS	Microsoft Encrypting File System
G-Suite	Google Cloud Computing Suite - Gmail, Google Drive and Google Doc etc.
Guide	IT Security Practice Guide
GCHQ	Government Communications Headquarters, UK
HTTP	Hyper Text transfer Protocol
IDS/IPS	Intrusion Detection system / Intrusion Prevention System
IOC	Indicator of Compromise
IP	Internet Address
ISP	Information Security Policies
IPSec	Internet Security Protocol
IT	Information Technology
LAN	Local Area Network
Malware	A Malicious Software - Viruses, Trojans, Spyware, and Ransomware etc.
MDM	Mobile Device Management
NAS	Network Attached Storage
NCSC	National Cyber Security Centre, a UK Government department
NDA	Non-Disclosure Agreement
NGO	Non-Government Organisation
NIST	National Institute of Standards and Technology (USA)
O365	Office 365 Cloud Services – Office mail, Cloud Drive etc.
OAuth2	OAuth 2.0 Framework
OpenID	OpenID Foundation (OIDF)
Pen. Test	Penetration Testing
PKI	Public Key Infrastructure

Port Scan	Scan networking device/system for Open Ports.
RDP	Remote Desktop Protocol
RSA	RSA (Rivest–Shamir–Adleman), an Asymmetric-Key Cryptosystem
PBKDF2	Password-based Key Derivation Function 2
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation and Response
SPF	Email Sender Policy Framework
SRA	Security Risk Assessment
SSL	Secure Sockets Layer
SWD	Social Welfare Department
TLS	Transport Layer Security, a successor of SSL
UAC	User Account Control
USB	Universal Serial Bus
User ID	User Identity
VLAN	Virtual Local Area network
VPN	Virtual Private Network
Vuln. Scan	Vulnerability Scanning
WAF	Web Application Firewall
WAP	Wireless Application Protocol
WIFI	Wireless Fidelity

Table 44: Common Abbreviations

*** * * END OF REPORT * * ***