



# ASEAN Data Management Framework

---

Data governance and protection throughout the  
data lifecycle

## Contents

Background and overview .....	3
The growth of the digital economy .....	3
Data Management Framework as a key for boosting digital economy .....	4
Introduction .....	6
ASEAN Framework on Digital Data Governance: strategic priorities and initiatives .....	6
Gain and retain stakeholder trust while unlocking the potential for innovation.....	7
Scope of application .....	8
Objectives .....	8
6 foundational components of the DMF.....	11
1. Governance and oversight.....	12
2. Policies and procedures.....	15
3. Data inventory.....	16
4. Impact / risk assessment.....	19
5. Controls .....	21
6. Monitoring and continuous improvement.....	25
Conclusion .....	26

## Background and overview

### The growth of the digital economy

Data is the fuel of the new economy, and even more so of the economy to come. The world's most valuable resource is no longer oil, but data<sup>1</sup>. It is estimated that the digital economy today is worth almost \$3 trillion<sup>2</sup>.

The digital economy is the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyper-connectivity which means growing interconnectedness of people, organisations, and machines that results from the internet, mobile technology and the internet of things (IoT)<sup>3</sup>. Such an economy is characterised by advanced manufacturing, robotics and factory automation, new sources of data from mobile and ubiquitous internet connectivity, cloud computing, big data analytics, and artificial intelligence.

The growth of digital economy is taking place at an unprecedented speed and scale. It is predicted that by 2022, 60% of global GDP<sup>4</sup> will be digitised with growth in every industry driven by digitally-enhanced offerings, operations, and relationships. Additionally, the World Economic Forum predicts that some 60-70% of new value will be “based on data-driven digitally enabled networks and platforms”. Half the world's population is online, a third is on a social network. Mobile internet has penetrated 53% of the online population with digital advertising amounting to \$170 billion<sup>5</sup>. If ASEAN has the right data connectivity infrastructure and enablers in place, it has potential to create 35 smart cities by 2025 across 10 countries<sup>6</sup>.

Powered by a large, growing, and incredibly engaged internet user base, it is estimated that the ASEAN<sup>7</sup> internet economy has reached \$72 billion in gross merchandise value (GMV) in 2018 across online travel, e-Commerce, online media, and ride hailing, and is on track to exceed \$240 billion by 2025, \$40 billion higher than previously estimated<sup>8</sup>. Moreover, ASEAN is also expected to see rapid increase in the use of technology. Digital technologies in ASEAN could be worth up to \$625 bn by 2030<sup>9</sup>. This is expected to contribute to the growth of its digital economy by 6.4 times, from \$31 billion in 2015 to \$197 billion by 2025<sup>10</sup>

---

<sup>1</sup> “Which Countries Are Leading the Data Economy?”, Harvard Business Review, 2019

<sup>2</sup> “The Digital Economy In 5 Minutes”, Forbes, 2016

<sup>3</sup> “What is digital economy? Unicorns, transformation and the internet of things”, Deloitte, 2017

<sup>4</sup> “Multiplied Innovation Takes Off, Powered by AI, Distributed Public Cloud, Microservices, Developer Population Explosion, Greater Specialization and Verticalization, and Scaling Trust”, International Data Corporation, 2018

<sup>5</sup> “The Digital Economy In 5 Minutes”, Forbes, 2016

<sup>6</sup> The ASEAN Digital Revolution, A.T. Kearney

<sup>7</sup> ASEAN comprises of ten-member states which are Brunei Darussalam, the Kingdom of Cambodia, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand, and the Socialist Republic of Vietnam.

<sup>8</sup> “e-Conomy SEA 2018: Southeast Asia's internet economy hits an inflection point”, Google-TEMASEK, 2018

<sup>9</sup> “Master Plan on ASEAN connectivity 2025

<sup>10</sup> “Southeast Asia: An Emerging Market with Booming Digital Growth”, Jeff Desjardins, 2018

Small and medium enterprises (SMEs) are the engine of growth in Southeast Asia and they are responsible for up to 99% of all business establishments, over 90% of employment and contribute almost 60% of the gross domestic product (GDP) in many ASEAN countries. To remain competitive, 68% of SMEs are using emerging technologies to improve payment applications and 66% are investing in deeper implementation of big data analytics, artificial intelligence and cognitive computing<sup>11</sup>. The success of these technologies is heavily reliant on data sharing.

### Data Management Framework as a key for boosting digital economy

Due to the growing interactions between data, connected things and people, trust in data has become the pre-condition for fully realising the gains of digital transformation. SMEs are threading a fine line between balancing digital initiatives and concurrently managing data protection and customer privacy safeguards to ensure that these do not impede innovation<sup>12</sup>. Therefore, there is a motivation to focus on digital data governance as it is critical to boost economic integration and technology adoption across all sectors in the ten ASEAN Member States (AMS).

To ensure that their data is appropriately managed and protected, organisations need to know what levels of technical, procedural and physical controls they need to put in place. The categorisation of datasets help organisations manage their data assets and put in place the right level of controls. This is applicable for both data at rest as well as data in transit. The establishment of an ASEAN Data Management Framework will promote sound data governance practices by helping organisations to discover the datasets they have, assign it with the appropriate categories, manage the data, protect it accordingly and all these while continuing to comply with relevant regulations. Improved governance and protection will instil trust in data sharing both between organisations and between countries, which will then promote the growth of trade and the flow of data among AMS and their partners in the digital economy.

---

<sup>11</sup> "Redesigning for the digital economy", EY, 2018

<sup>12</sup> "Redesigning for the digital economy", EY, 2018



# Introduction

## Introduction

### ASEAN Framework on Digital Data Governance: strategic priorities and initiatives

The ASEAN Framework on Digital Data Governance was endorsed at the 18<sup>th</sup> ASEAN TELMIN meeting in December 2018. The ASEAN Framework on Digital Data Governance sets out the strategic priorities, principles and initiatives to guide AMS in their policy and regulatory approaches towards digital data governance in the digital economy.

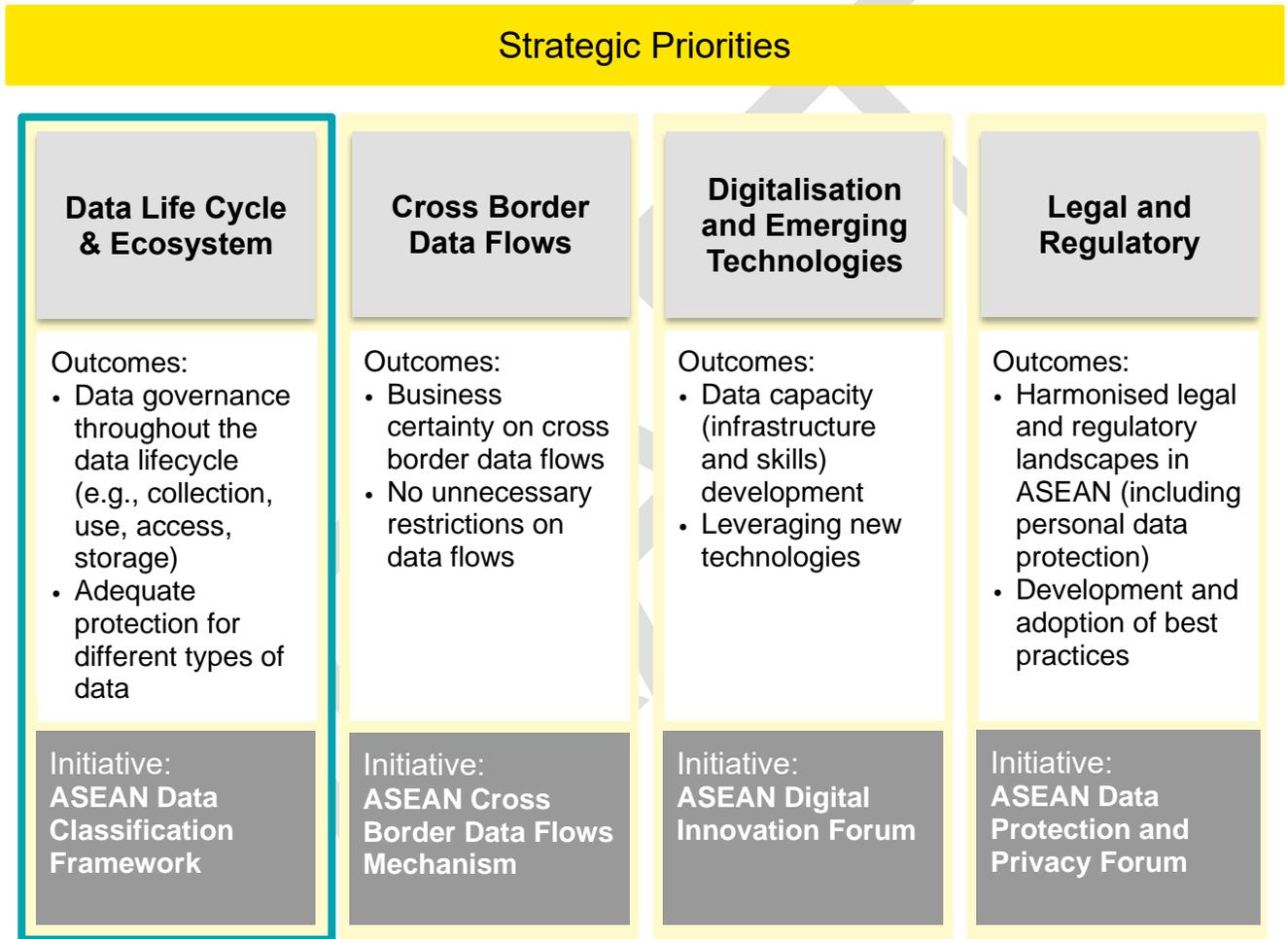


Figure 1: ASEAN Framework on Digital Data Governance

The ASEAN Framework on Digital Data Governance has identified four initiatives that are undertaken in support of the four strategic priorities of digital data governance, which are:

- i. ASEAN Data Classification Framework
- ii. ASEAN Cross Border Data Flows (CBDF) Mechanism
- iii. ASEAN Digital Innovation Forum
- iv. ASEAN Data Protection and Privacy Forum

The ASEAN Data Classification Framework has been renamed as the ASEAN Data Management Framework<sup>13</sup> (hereafter referred to as the “DMF”) to recognise that companies need to develop data governance structure and appropriate data protection safeguards based on the purpose of data use throughout the data lifecycle (e.g. data in transmission, data at rest). Categorisation is a key pre-cursor for three out of six foundational components of the DMF, which will be elaborated in the following sections. Categorisation guides downstream decisions in safeguarding data with the appropriate level of access and protection. It is an approach to identify, assess, manage, and protect data with appropriate protection measures. To achieve this, understanding the value of information and the protection measures designed to protect the confidentiality, integrity and availability of the information are crucial<sup>14</sup>. To support the categorisation process, organisations must also have adequate policies and procedural documents, and established governance and oversight function along with monitoring and continuous improvement of their data management practices.

### Gain and retain stakeholder trust while unlocking the potential for innovation

The DMF has been developed to support the Data Life Cycle & Ecosystem<sup>15</sup> strategic priority. It is aimed at helping all businesses operating in ASEAN participate in the digital economy and practice data governance across all data types within an organisation throughout the data lifecycle and consider adequate protection for different types of data. With a DMF, organisations would be better equipped to protect data and instil trust and confidence in their customers and organisations they interact with, while the data is being leveraged for business innovation purposes.

The process of valuing information is a fundamental starting point for the development of a positive security culture across businesses. Businesses working with data have an obligation to respect the information they create, access and use, and are accountable for safeguarding these information assets.

---

<sup>13</sup> In developing the framework, we learned that the initial name did not fully represent the entire process of enabling organisations in their own data management journey. It would involve more than just classifying data, as organizations would need to discover the data they have; protect it accordingly; monitor the data they hold; and comply with relevant regulations. As such, the revised name “Data Management Framework” is proposed to encapsulate the intended outcome set out in the Digital Data Governance initiative through this framework’s 6 foundational components.

<sup>14</sup> “Data in the Digital Age”, OECD, 2019

<sup>15</sup> One of the four strategic priorities identified in the ASEAN Framework on Digital Data Governance with the objective of data governance throughout the data lifecycle (e.g., collection, use, access, storage) and adequate data protection for different types of data.

Regardless of whether the data is processed or stored in on-premise systems or in the cloud, according the data appropriate protection measures is the starting point for maintaining confidentiality, integrity and availability of the data.

### Scope of application

1. The DMF is designed to provide **voluntary and non-binding guidance** based on best practices in the area of data management for businesses within AMS. The content should not be read as nor constitute as legal advice, nor construed as a tool for compliance to any law and regulations.
2. The DMF is intended to be adapted to varying business needs for **adoption and tailoring by the businesses** to their own systems of managing data.
3. “Data” as used in this DMF refers to all data a business creates, collects, accesses, processes and transfers. This may include personal data<sup>16</sup> and business transactional data.
4. The DMF is **intended for** the use of **all private sector businesses** operating in any ASEAN member state (AMS), including **small and medium enterprises**.

### Objectives

1. Help policy makers in ASEAN **promote a robust digital economy** by:
  - Reducing the likelihood of shocks arising from data leakage and breaches
  - Promoting economic growth and innovation
  - Encouraging intra-company and inter-company data flows within the domestic economy
  - Supporting cross border data flows for companies operating across AMS
2. Help all businesses operating in ASEAN **participate in the digital economy** by:
  - Establishing a common language to support data management
  - Instilling trust, transparency and accountability in data use and management for the businesses to participate as “Trusted Data Partners”, leveraging and sharing data to achieve better business outcomes, as well as to pursue cross border opportunities with the confidence that the data they transfer will be adequately protected.
3. Help all businesses in ASEAN **practise data governance** throughout the data lifecycle by:
  - Providing organisations with **practical guidance** to enable them to build their own policies and procedures using a **risk-based data management methodology**

---

<sup>16</sup> Personal data should be defined as information which could be used to identify a specific natural individual (e.g., the data owner), directly or indirectly. Source: US-ASEAN Business Council

- Supporting businesses to **identify appropriate controls** that they can implement in a **cost-effective manner** for the adequate protection of different types of data in the different stages of the data lifecycle.



# Foundational components of the DMF

## 6 foundational components of the DMF

These 6 foundational components aim to enable the organisation to leverage on a corporate governance structure to define, manage and monitor its data management processes.

1	2	3	4	5	6
<b>Governance and oversight</b>	<b>Policies and procedural documents</b>	<b>Data inventory</b>	<b>Impact / Risk assessment</b>	<b>Controls</b>	<b>Monitoring and continuous improvement</b>
Provide direction for employees across the organisation in implementing and executing the DMF and oversee the function to confirm it is operating as designed.	Develop data management policies and procedures based on the DMF throughout the data lifecycle, to ensure a clear mandate within the organisation.	Identify and gather the data used and collected as well as storage type, so as to enable understanding of data taxonomy and data purpose.	Assess the impact using different impact categories if confidentiality (C), integrity (I) or availability (A) parameters are compromised.	Design and implement protection controls within the systems according to the categories assigned and data lifecycle.	Monitor, measure, analyse and evaluate the DMF components implemented to keep it up-to-date and optimised.

## 1. Governance and oversight

The DMF is relevant to every individual who is employed by the organisation, whether on a permanent or temporary basis. To develop and implement the 6 foundational components of the DMF, an organisation is required to identify and determine different roles and responsibilities in order to ensure adoption, operation and compliance, in accordance with business needs:



Each of the functions has distinct and important responsibilities for meeting operational and compliance obligations.

Some of the activities that the **data management function** performs include the following:

- Owns and designs the organisation's processes to support the 6 foundational components that make up the DMF
- Defines policies and procedures
- Determines roles of the individuals to implement the control measures, including the skills and expertise
- Promotes awareness through the distribution of the 6 foundational components
- Reviews the categories assigned to datasets
- Manages risk by establishing the protection controls
- Manages data protection-related queries and complaints

Some of the activities that the **business process function** performs include the following:

- Identifies the data and complete the data inventory
- Implements protection controls and comply with defined policies and procedures
- Reports any security incident or non-compliance

Some of the activities that the **risk management function** performs include the following:

- Monitors the implementation of effective data risk management practices to keep risk within the organisation's risk appetite
- Evaluates the effectiveness of the controls
- Reports findings to the management and recommend measures to improve effectivity of policies

Depending on the organisation size, structure and culture, the number of individuals holding the roles listed above may vary. In smaller organisations, these roles can be held by 1 or more

individuals, while in larger enterprises, it would typically be held by various individuals across different departments.

The following diagrams are illustrations of how various functions in an organisation work together with respect to data management:

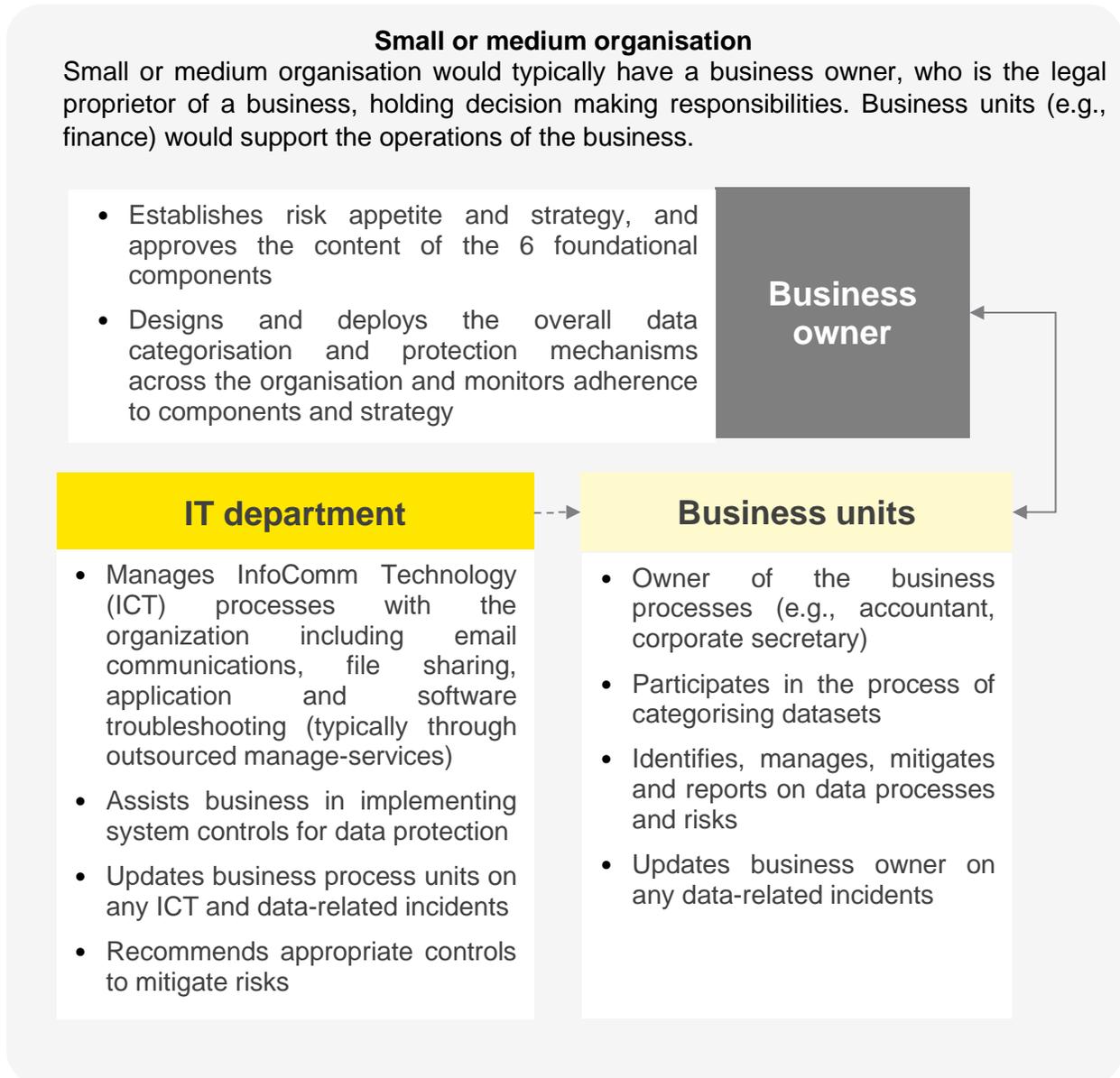


Figure 2: An illustration of operating model for a small-medium sized organisation

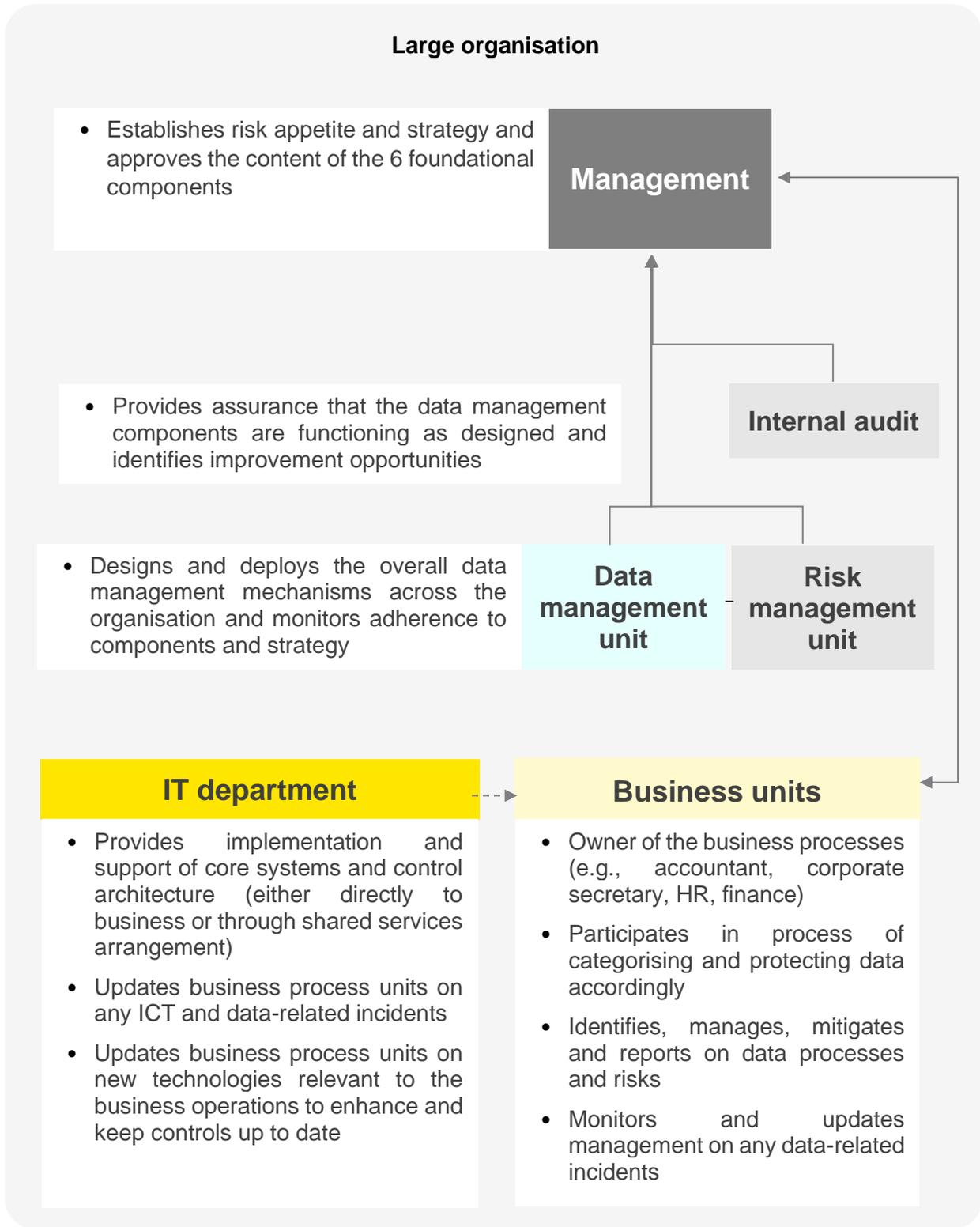


Figure 3: An illustration of operating model for a large sized organisation

## 2. Policies and procedures

The policies and procedures around data management support the development and implementation of a Data Management Framework within an organisation and promote the monitoring and continuous review of the data management practices.

In addition, an organisation should include data management policies as part of its corporate governance to ensure a clear mandate within the organisation. This also demonstrates accountability and provide clarity to both its internal stakeholders (e.g., employees) and external parties (e.g., suppliers) on the ways in which the organisation handles data.

To achieve complete policies and procedures the following sections need to be included:

### What the policies and procedures of a DMF should include

<b>1. Leadership commitment</b> (who)	<b>2. Data management objectives, scope and consideration</b> (what and why)	<b>3. Data management approach</b> (how)
Management should provide their commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of data management initiatives.	The objectives, scope of application and considerations, among others, should be defined, documented and maintained to enable clear understanding of the parameters of the DMF implementation specific to the organisation.	Organisations can follow a data management approach that is effective to define, establish, monitor and maintain its data management, including the definition and formalisation of the activities that form the categorisation and protection of datasets, within the organisation and its continued improvement.

Policies and procedures should recognize the distinct obligations and implications of the 3 areas mentioned above. To this end, different sections and content relating to each of them must be included in the policies and procedures.

Subsequent foundational components should be reflected as content within the policies and procedures.

### 3. Data inventory

#### Understand the data

Today, companies have to manage a wide spectrum of data elements from different business units and processes, including production and consumption of digital products, services and platforms. Varying combinations of these data elements exist in the form of files, system tables, and reports, also known collectively as datasets<sup>17</sup>.

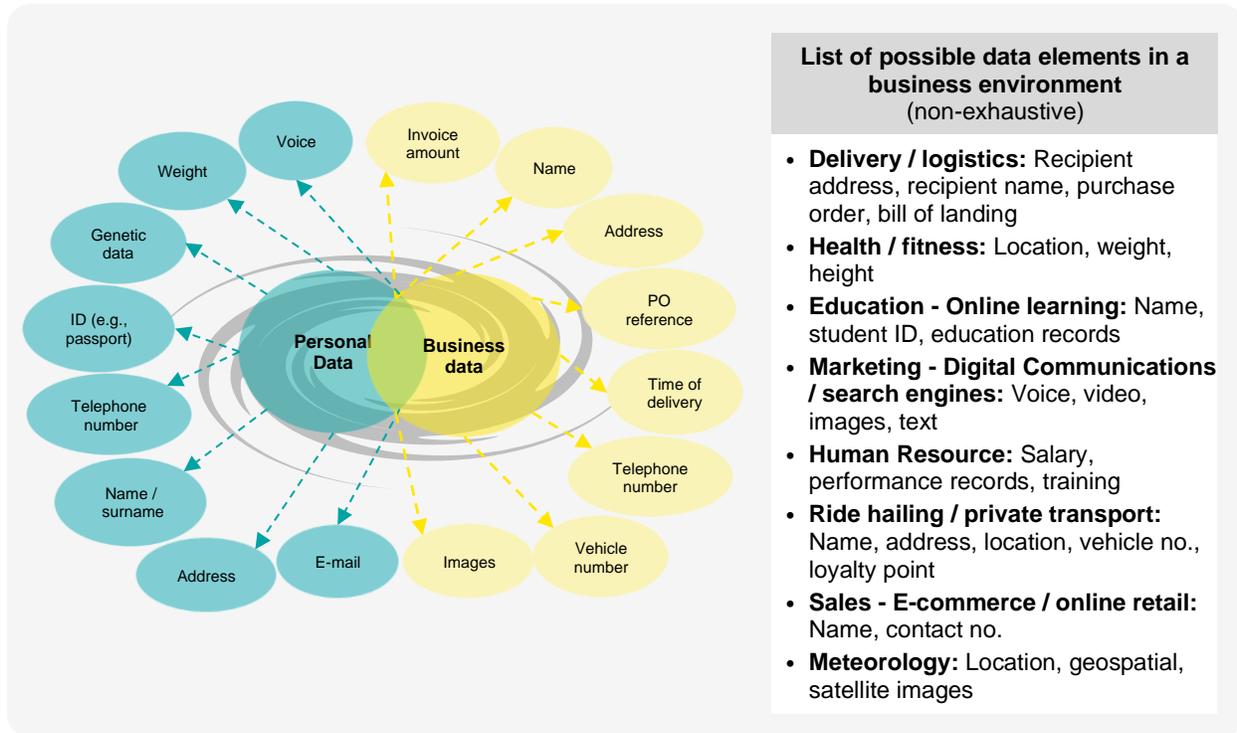
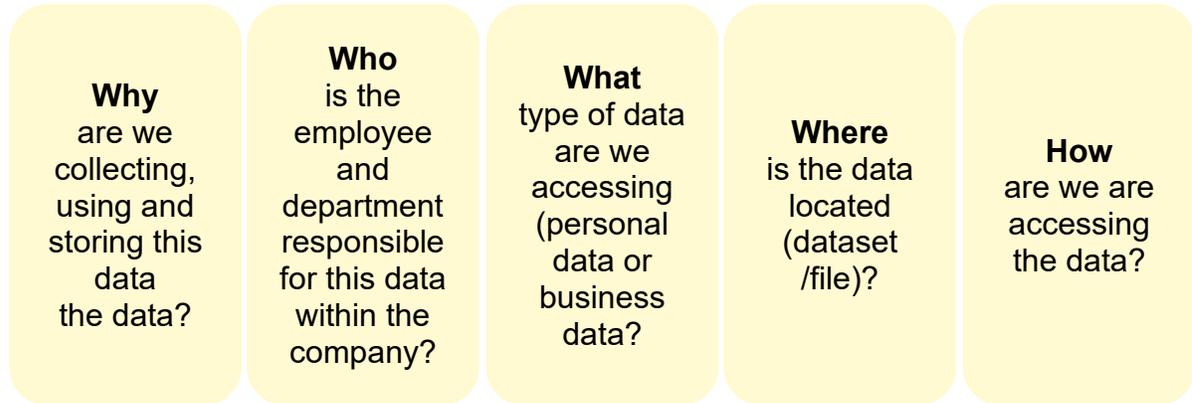


Figure 4: An illustration of data types and data elements

Due to the high volume and the various types of data an organisation manages today, the process begins with the identification of the data that the organisation is in possession of. As the organisation evolves, there may be new types of data that the organisation needs to handle. In such cases, the data inventory needs to be updated as and when these new types of data are collected.

<sup>17</sup> A dataset should be defined as any permanently stored collection of information usually containing either case level data, aggregation of case level data, or statistical manipulations of either the case level or aggregated data. Source: Economic Commission for Europe of the United Nations (UNECE), "Glossary of Terms on Statistical Data Editing"

To populate the information regarding the data in possession, it is important for the business to answer the following questions:



In order to adequately understand the data at hand, the following information about the data can be captured in the data inventory:

Purpose	Data owner	Data type <sup>18</sup>	Data fields <sup>19</sup>	Dataset <sup>20</sup>	Location (System)
Analysis of item costing	Finance	Business data	Item descriptions and cost	Procurement transactions	SharePoint
General health trends awareness program	Programme Management	Business and Personal data	Diseases and pathologies and the number of people who suffer from them	General Health analysis	CRM
HIV testing	I+D department	Personal data	Patient data and the results on whether the HIV test is positive	HIV analysis	HIV database

Figure 5: An illustration of the data inventory key element

<sup>18</sup> Personal data: any information that relates to an identified or identifiable individual. Business data: any information in relation to operating the business.

<sup>19</sup> Data field: it is the smallest component under which data is entered through data capture or data entry. Several data fields make up a data record, several data records make up a dataset.

<sup>20</sup> Dataset: a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. It is the combination of one or more data records, formed up by data fields.

The DMF recognises that the same data fields may appear in multiple datasets, and therefore, it is important that the organisations know the different areas to consider when defining the data management practices, in order to meet the business needs that best suits the organisation.

### Overarching considerations when categorising and protecting data

Companies have the flexibility in categorising their own datasets, appropriate to their respective needs and sectors. The areas for consideration listed here aim to assist businesses in assessing the sensitivity and value of the dataset and in establishing the risk-based controls.

As controls should be applied based on the categorisation of dataset, businesses can keep these considerations in mind when performing the impact and risk assessment so as to assign the appropriate tiers, avoiding over protection of datasets that may hinder use of data for business purposes.

The areas to consider are the following:

- **Nature and type of services provided:** Consider the sector in which the organisation operates in and the service provided, in order to understand and take into account the usage of the information in possession of the organization (e.g., purpose for the information collection, methods of use, target customer).
- **Regulation:** Consider current personal data legislations within AMS (e.g., PDPA, GDPR) and the sector / industry regulations if applicable (e.g., banking regulations and healthcare regulations).
- **Competitive landscape:** The currency of the information (e.g., Patents, R&D)
- **Cost of safeguards vs. risk appetite<sup>21</sup>:** Consider the aggregate amount of risk regarding to data breach, that the organisation is able to accept in pursuit of its strategic goals and objectives. Furthermore, it is needed to consider the following aspects:
  - The aggregation of information in datasets (e.g., combination of data as they reside in files/ system tables and/or reports).
  - The volume of data contained in a particular dataset, in most of the cases the greater the number of data lost / disclosed without authorization the greater the impact or people affected (e.g., 1 day's transaction history vs 1 year's transaction history).
- **Customer expectations:** Consider the data subject (e.g., high profile individuals, minors) and the contractual obligations defined on data protection safeguards to apply.

---

<sup>21</sup> The risk appetite should be defined as the amount and type of risk that an organization is prepared to pursue, retain or take. Source: ISO 31000 "Risk Management"

## 4. Impact / risk assessment

### Assess the categories

After establishing the data inventory, the next step for the organisation is to tailor its own thresholds for categorising data and to determine the assignment of appropriate category to the dataset by assessing the impact to the organisation if the dataset be compromised.

The key element to carry out this impact / risk assessment is the categorisation matrix. The categorisation matrix provides guidelines and thresholds to be able to assess the impact on individuals and on the business environment within an organisation.

Any proposed categorisation matrix should outline appropriate impact categories with broad expectations and provide clear guidance on the tiers to assign the dataset based on its risk impact level for each impact category. Moreover, this categorisation matrix should be defined in a way that allows organizations to easily apply the right categories, marking and handling, and for industries to self-regulate.

Given that this is not a prescriptive guideline, the number of tiers/categories depend on the business consideration and needs. The more the organisations want to granulate the protection measures, the more tiers/categories should be defined.

Consider the impact when the data is compromised in the following three parameters are compromised:

- **Confidentiality (C):** Risk of unauthorised / inappropriate disclosure. For information to be confidential, the access to some information needs to be restricted because it could harm interests of the stakeholders.
- **Integrity (I):** Risk to information quality / corruption. For information to be useful and serve the purpose, it must be accurate and complete.
- **Availability (A):** Risk to information not being available to intended users. For information to be useful and serve the purpose, it must be available when it is needed and, in a form that is able to be consumed by users.

Consider the following four primary impact categories:

- **Financial:** risks affecting the financial processes of the company (e.g., accounting and reporting, tax, etc.)
- **Strategic:** risks affecting achievement of the strategic objectives of the company (e.g., governance, strategic planning, major initiatives, etc.)
- **Operational:** risks affecting the operations of the organization (e.g., sales & marketing, supply chain, etc.)
- **Compliance:** risks affecting the company's compliance with regulatory requirements (e.g., legal, code of conduct, etc.)

In order to adequately understand how an impact level matrix looks like, the following impact level matrix structure is provided:

Impact categories	Financial Impact	Operational Impact	Reputational Impact	Legal / Compliance Impact
Tier 1	Compromise of information to cause <b>significant</b> harm / damage towards operations, organisations and individuals			
Tier 2	Compromise of information to cause <b>moderate</b> harm / damage towards operations, organisations and individuals			
Tier 3	Compromise of information to cause <b>limited</b> harm / damage towards operations, organisations and individuals, or does not cause any harm			

Figure 6: An illustration of a categorisation matrix key element

## 5. Controls

### **Protect the data**

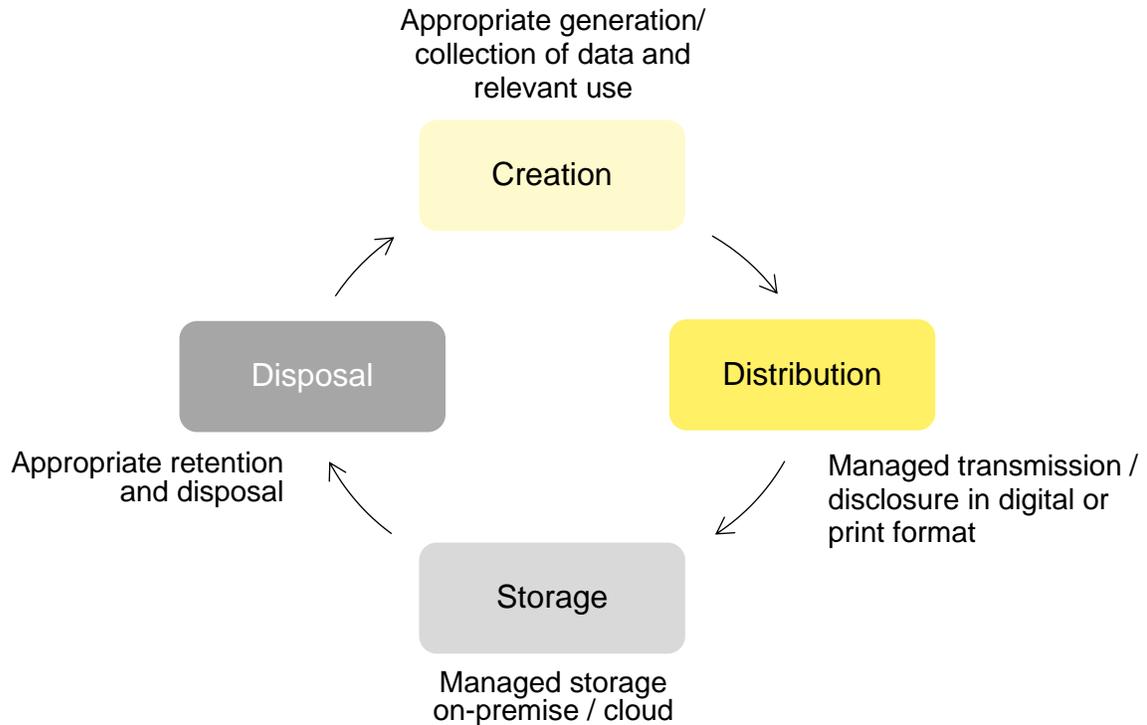
The final step is to implement risk-based controls that are commensurate to the potential impact of the data being compromised. A control includes any procedure that is used and relied upon to prevent errors from occurring during data collection, use and/or disclosure processes (preventive controls) or to detect and correct errors that may have occurred in these processes mentioned above (detective controls).

A control involves taking an action to mitigate or manage the risk that data will be compromised and increase the probability that the organisation will achieve its intended purpose. The organisation needs to establish the risk tolerance, which determines the acceptable level of risk that they are willing to take on. Controls are then identified to sufficiently mitigate the risk and bring it within the risk appetite. Often times, the risk is not completely mitigated. The residual risks that exist after considering controls or other management activities will be assessed and accepted by management in a risk acceptance process.

Employees should be encouraged to comply with appropriate technical, procedural and physical safeguards to ensure the confidentiality, integrity and availability of data at all stages of the data lifecycle. The technical safeguards compile the IT controls established within the IT application programs and environment, to protect the data within the organisations' systems. The procedural safeguards include the baseline, clarity and constraint or gap in design on how to protect the data. The physical safeguards are referred to the protection measures around the hard copy versions including data that confirms the limited access.

The data lifecycle is the sequence of stages that the data goes through from its initial generation or capture to its eventual deletion at the end of its useful life. The protection applied to the data would vary depending on the stage of the data lifecycle (e.g., collection, use, in transmission, at rest, when accessed, storage). Design of these protection measures should also take into consideration the sensitivity of the data based on the nature of business and type of services offered.

The stages of the data life cycle are illustrated below:



Having too many categories and/or over- inclusion of data may lead to the organisation incurring additional costs when implementing controls due to additional resources required for securing, monitoring, measuring, remediating and reporting risks.

Each organization, depending on its size or volume of information handled, may apply varying degrees of protection that it deems necessary. When regulations are not prescriptive, organisations should define their own categories and protection controls matrix to determine the appropriate level of protection tailored to their needs, organization's consideration, strategy and objectives. Stricter information handling requirements are often required for the transmission, storage and disposal of data that may present a significant negative impact on a customer or organisation if confidentiality, integrity and / or availability is compromised.

Existing international standards, such as those developed by the International Standards Organization (ISO), should be used to guide organizations in assessing how their own data should be categorised and organised. The below are some possible standards which can be used as reference:

- Mapping Types of Information and Information Systems: National Institute of Standards and Technology (NIST) 800—60
- Global Quality Standard: International Standards Organization (ISO) 9001:2015
- Information Security Management Systems: ISO 27001
- Information technology – security techniques – code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: ISO 27018
- Privacy Information - Management Systems: ISO 27701
- Standards for Security Categorisation: NIST Federal Information Processing Standard (FIPS) 199
- Cybersecurity: NIST Cybersecurity Framework
- Risk Management: NIST Risk Management Framework

Additional controls may be required to meet regulations in place when applicable (e.g., Sarbanes–Oxley Act).

Data protection matrix for detailed illustration on controls for each category based on the data lifecycle:

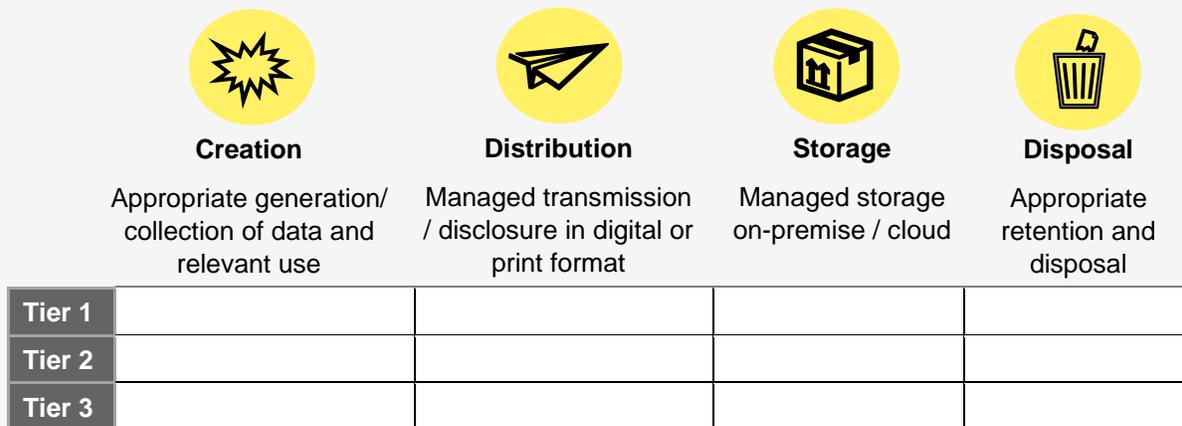


Figure 7: An illustration of a data protection control matrix

The protection applied to the data would vary depending on the stage of the data lifecycle as illustrated below:

	 <b>Creation</b>	 <b>Distribution</b>	 <b>Storage</b>	 <b>Disposal</b>
<b>Tier 1</b>	<ul style="list-style-type: none"> <li>• Multi factor authentication</li> <li>• Encryption (at rest)</li> <li>• Firewalls</li> <li>• Protection markings</li> </ul>	<ul style="list-style-type: none"> <li>• Encryption (in transit)</li> <li>• Non-disclosure agreements and Confidentiality Agreements</li> <li>• Data Loss Prevention (DLP) technologies</li> <li>• Information Labelling (Hardcopy)</li> </ul>	<ul style="list-style-type: none"> <li>• No Data Caching</li> <li>• Hot/ warm disaster recovery site</li> <li>• End-point encryption</li> <li>• Vulnerability Management &amp; Penetration testing</li> </ul>	<ul style="list-style-type: none"> <li>• Media sanitisation prior to disposal</li> </ul>
<b>Tier 2</b>	<ul style="list-style-type: none"> <li>• Acceptable Usage Policy (e.g., mobile Device Management)</li> <li>• Password Protection / authentication</li> </ul>	<ul style="list-style-type: none"> <li>• Session Management</li> <li>• Control printing</li> </ul>	<ul style="list-style-type: none"> <li>• Cache management</li> <li>• Cold Disaster Recovery Site</li> </ul>	<ul style="list-style-type: none"> <li>• Media sanitisation prior to disposal</li> </ul>
<b>Tier 3</b>	<ul style="list-style-type: none"> <li>• Access Control (general and privileged users)</li> </ul>	<ul style="list-style-type: none"> <li>• Printing on a need-to basis</li> </ul>	<ul style="list-style-type: none"> <li>• Data backup</li> </ul>	<ul style="list-style-type: none"> <li>• Retention policy</li> </ul>

Figure 8: An illustration of data protection controls

In addition, many organisations already maintain their own comprehensive data management policies that distinguish between different types of data through a categorisation mechanism and attribute different levels of protection to that information according to its sensitivity.

## 6. Monitoring and continuous improvement

Monitoring, measurement, analysis and evaluation are key activities to keep the foundational components up to date and optimised.

Organisation shall determine:

- What needs to be monitored and measured
- How: method of monitoring, measurement, analysis and evaluation
- When monitoring and measuring to be performed and who will perform
- When results of monitoring to be analysed and evaluated
- Who will perform it

The organisations have to consider the following monitoring and continuous improvement activities:

- **Review controls associated with each category:** periodically review the design of the process for assigning categories to datasets, such as objectives, categories and data protection controls matrix, taking into account results of security audits, incidents, effectiveness measurements, suggestions and feedback from the business.
- **Review categories assigned to datasets:** periodically review the categories assigned to the dataset, as well as the current life cycle for each of them.
- **Data protection controls testing:** test the operating effectiveness of controls. Measure the effectiveness of controls to verify that security requirements have been met.
- **Update policies, procedures and processes:** to incorporate the findings from monitoring and reviewing activities.

The review of design and operating effectiveness of established controls with periodic testing supports the organisation in its continuous improvement of data management, specifically the fifth foundational component '*Controls*'.

## Conclusion

The growth of the digital economy brings many opportunities for innovation across businesses. At the same time, the changing regulatory and threat landscape increases the need for appropriate data protection measures. Lack of clarity on the kind of data and the manner in which data can be shared between businesses may also discourage businesses from leveraging the use of data to drive business growth. Businesses are working to balance between using data to create innovative products and services in the digital world while at the same time, protecting data adequately. On one hand, businesses face increasing pressure to preserve personally identifiable and business critical information and instil trust in data privacy amongst stakeholders. On the other hand, they are pressured to innovate business operations, products and services in order to survive and are rewarded for the use of data as a driver for digital economy. To overcome this, it is essential for ASEAN to establish common frameworks to support the sharing of best practices and equipping SMEs with the capabilities to unlock the value of data<sup>22</sup>.

---

<sup>22</sup> *“Master Plan on ASEAN connectivity 2025”*, The ASEAN Secretariat, 2016



Copyright 2021 — Association of Southeast Asian Nations (ASEAN)

The contents of this publication are protected by copyright, trademark or other forms of proprietary rights and may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.

This publication gives a general introduction to contractual terms and conditions and templates that can help identify key issues when transferring personal data across borders.