KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

Privacy and Data Protection

Cybersecurity Bootcamp 2024

Disclaimer

This learning material is addressed and used only for Cybersecurity Bootcamp 2024 and should not be used or relied upon for any other purposes. Our learning material is not to be disseminated to or used by any third party in whole or in part without prior consent and permission from Kasikorn Technology Group Secretariat Company Limited (KBTGSec). Accordingly, we will not accept or take any responsibility or liability for any party or any person, whether or not such material is shown, disseminated, obtained, or possessed to such party or person since such material is only for educational purposes. We reserve all of our rights, including but not limited to intellectual property rights in our learning material, such as presentations, spreadsheets, system techniques, ideas, concepts, information, forms, electronic tools, forming parts of the materials, etc. © 2024 KASIKORN Business-Technology Group (KBTG) All rights reserved."

Let’s know more about…

01

What’s DATA?

02

Data classification and data handling

03

Threats to Data protection

04

Data security techniques available

05

Data privacy laws (GDPR, PDPA Thailand)

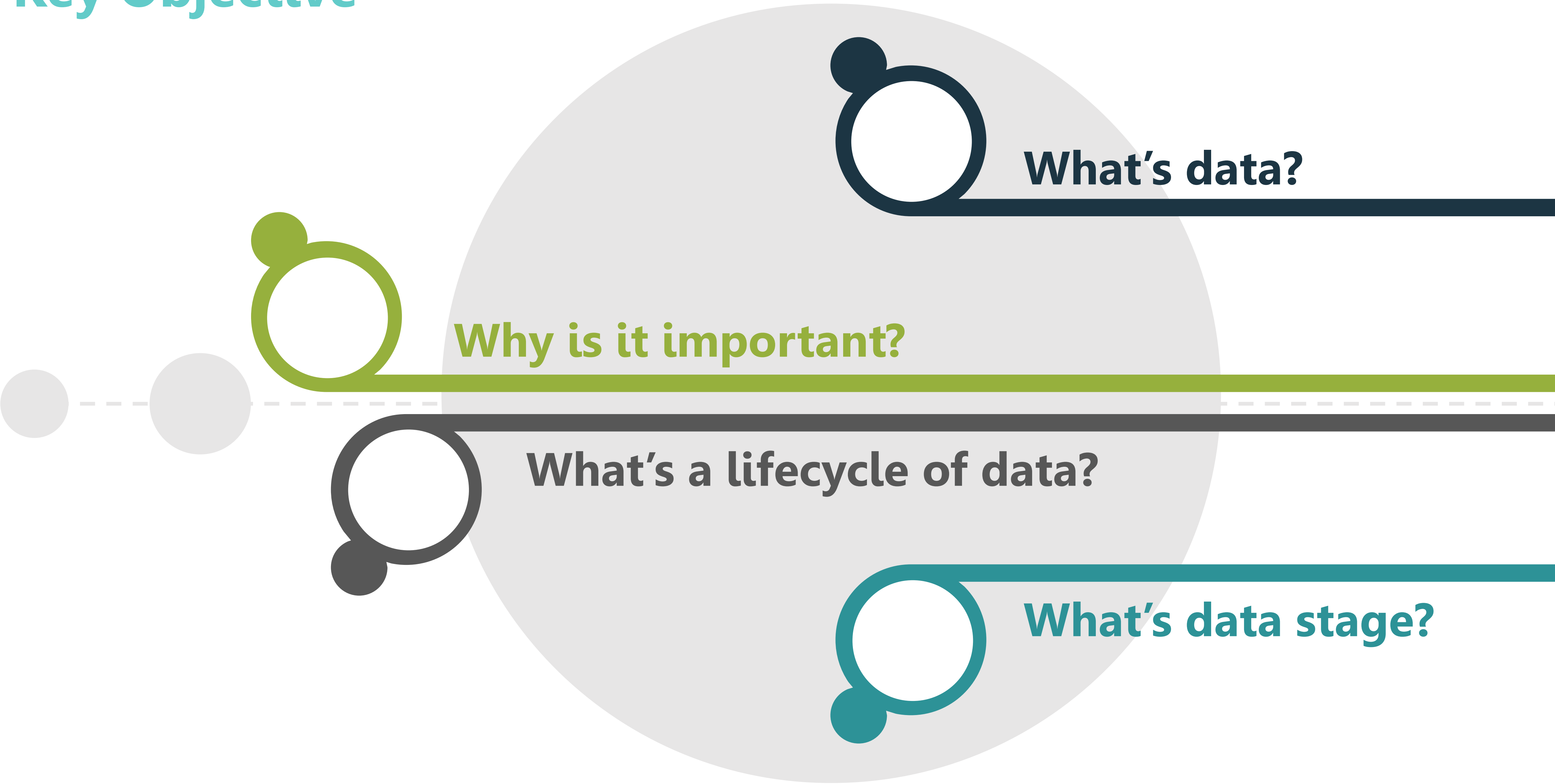
06

International Security and Privacy control framework (NIST 800-53,NIST Privacy Framework, ISO 27701)

01

Let’s know more about DATA

Key Objective



What's data?

Why is it important?

What's a lifecycle of data?

What's data stage?

What is Data?

Data is a unit or group of facts that has not yet been organized or interpreted.

Data can be...

- Field noted
- Videos
- Audio recordings
- Photographs
- Documents
- Transcripts

Why data is important?

#1 For Informed Decision-Making

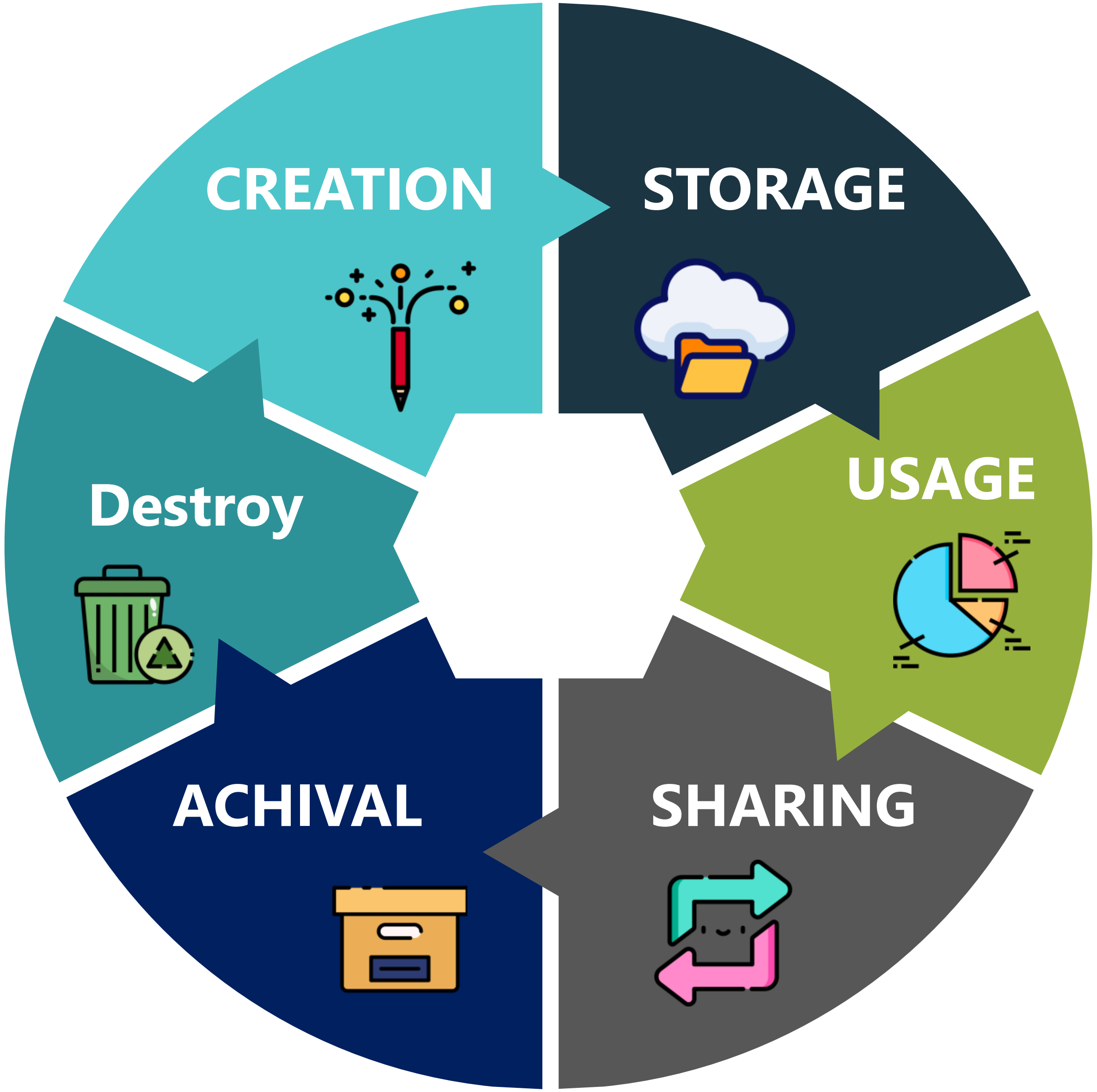
#2 For Problem-Solving

#3 For Greater Understanding

#4 For Improving Processes

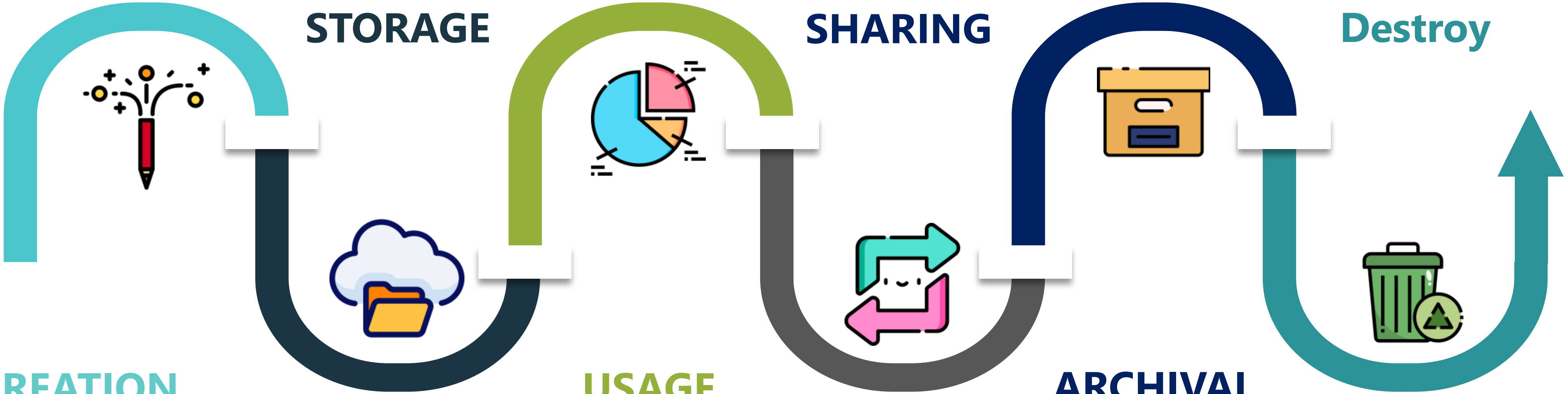
#5 For Understanding Behavior

Data Life cycle



Reference: ISC2

Data Life cycle



CREATION

Creating the knowledge from data, which is usually tacit knowledge at this point.

STORAGE

Storing or recording it in some fashion (which makes it explicit).

USAGE

Using the knowledge, which may cause the information to be modified, supplemented or partially deleted.

SHARING

Sharing the data with other users, whether as a copy or by moving the data from one location to another.

ARCHIVAL

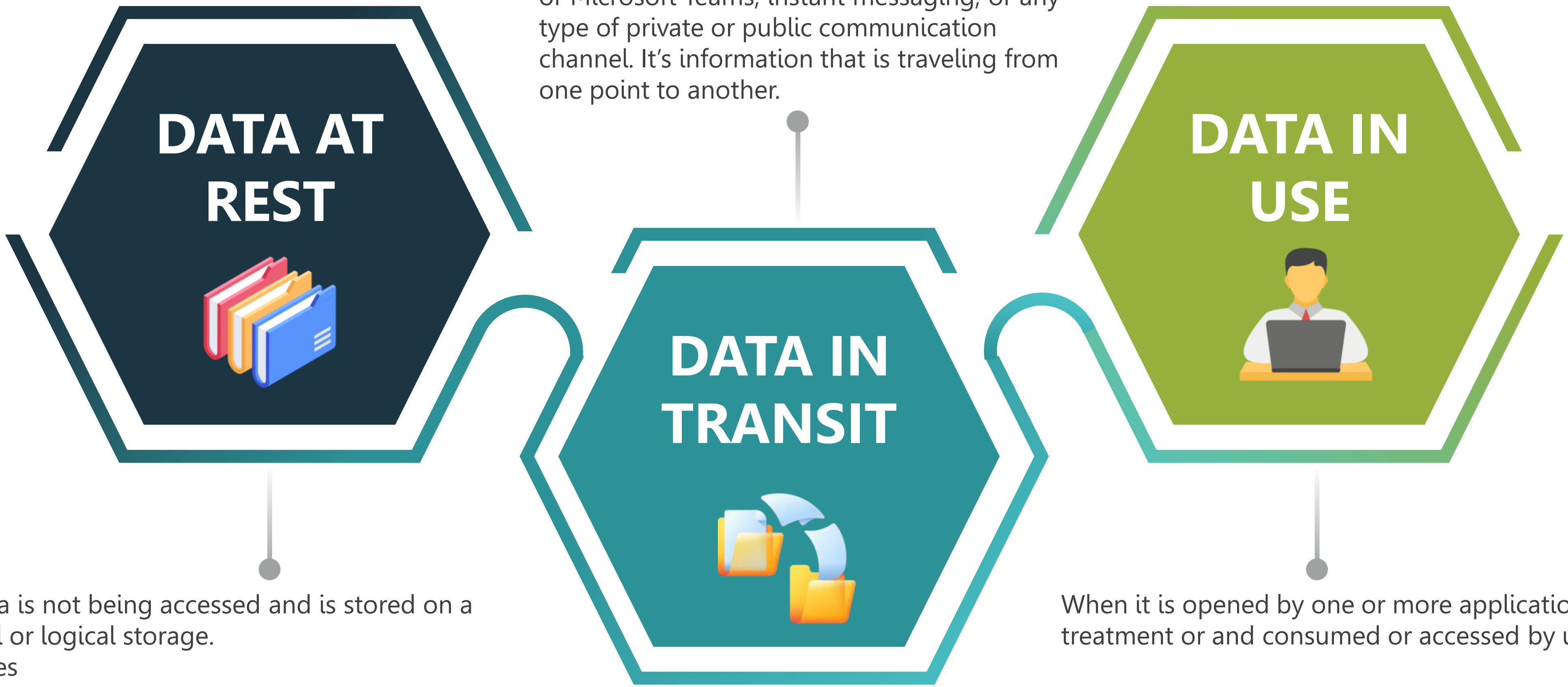
Archiving the data when it is temporarily not needed.

Destroy

Destroying the data when it is no longer needed.

Reference: ISC2

The three states of data



DATA AT REST

DATA IN TRANSIT

DATA IN USE

Data that travels through an email, web, collaborative work applications such as Slack or Microsoft Teams, instant messaging, or any type of private or public communication channel. It's information that is traveling from one point to another.

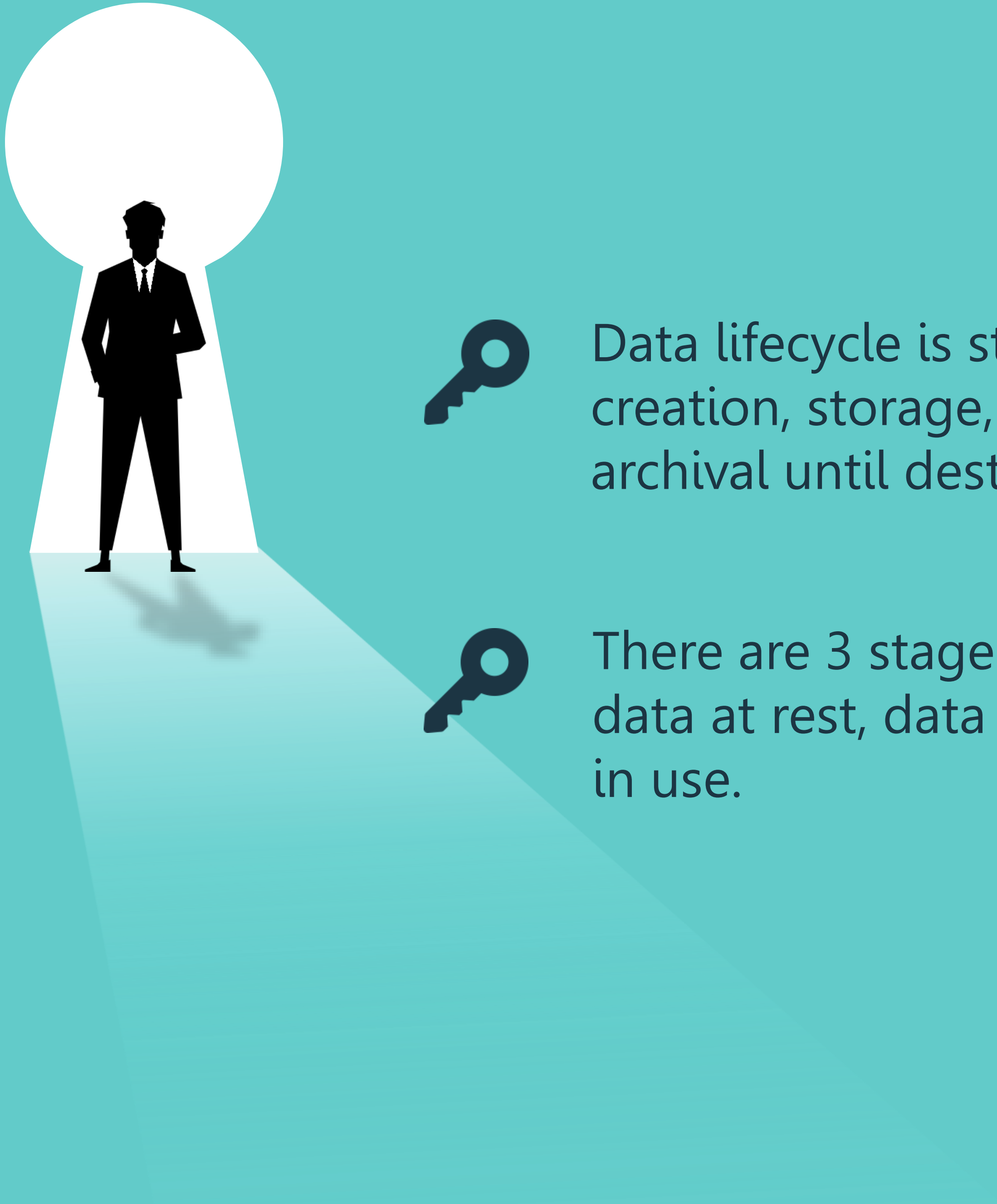
The data is not being accessed and is stored on a physical or logical storage.
Examples

- Files that stored on file servers
- Records in databases
- Documents on flash drives
- Hard disks etc.

When it is opened by one or more applications for its treatment or and consumed or accessed by users.

Reference: Sealpath

KEY TAKEAWAYS



- Data lifecycle is started from data creation, storage, usage, sharing, archival until destroy.
- There are 3 stages of data which are data at rest, data in transit and data in use.

02

Data classification and handling based on its classification

Key Objective

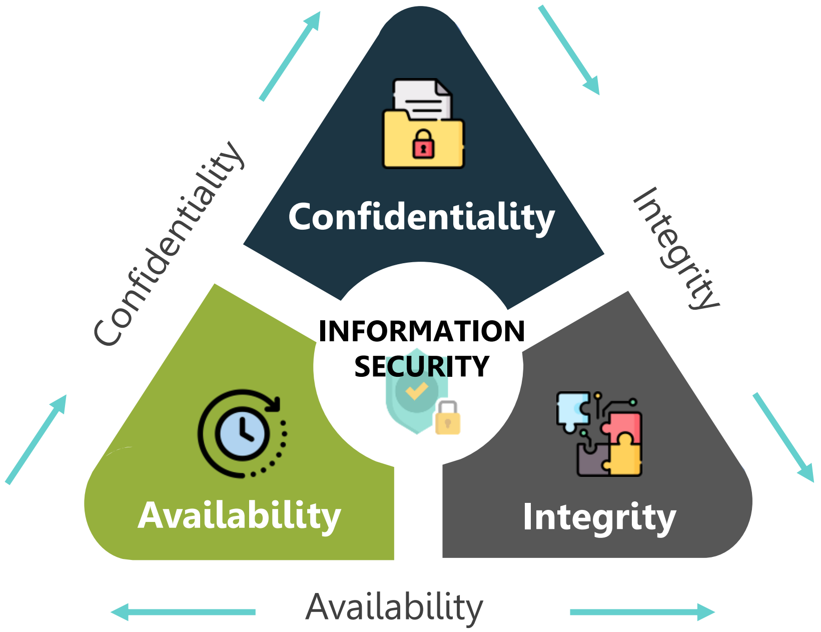
The importance of data privacy and protection in information security

How do we protect data by classification and handling process?

Why is data protection and Privacy so important in Information security

Data protection and privacy are critical components of information security because they help to safeguard sensitive and confidential information from unauthorized access, use, disclosure, modification, or destruction.

Data protection is important to provide:



Businesses recognize that information has value and others might steal their advantage if the information is not kept confidential, so they classify it.

Data Classification steps

01 Enter your assets into an inventory

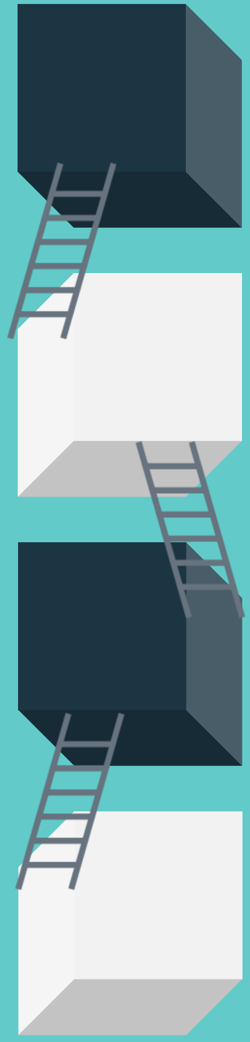
02 Classification

03 Labelling

04 Handling

Reference: Luke Irwin

Data Classification steps



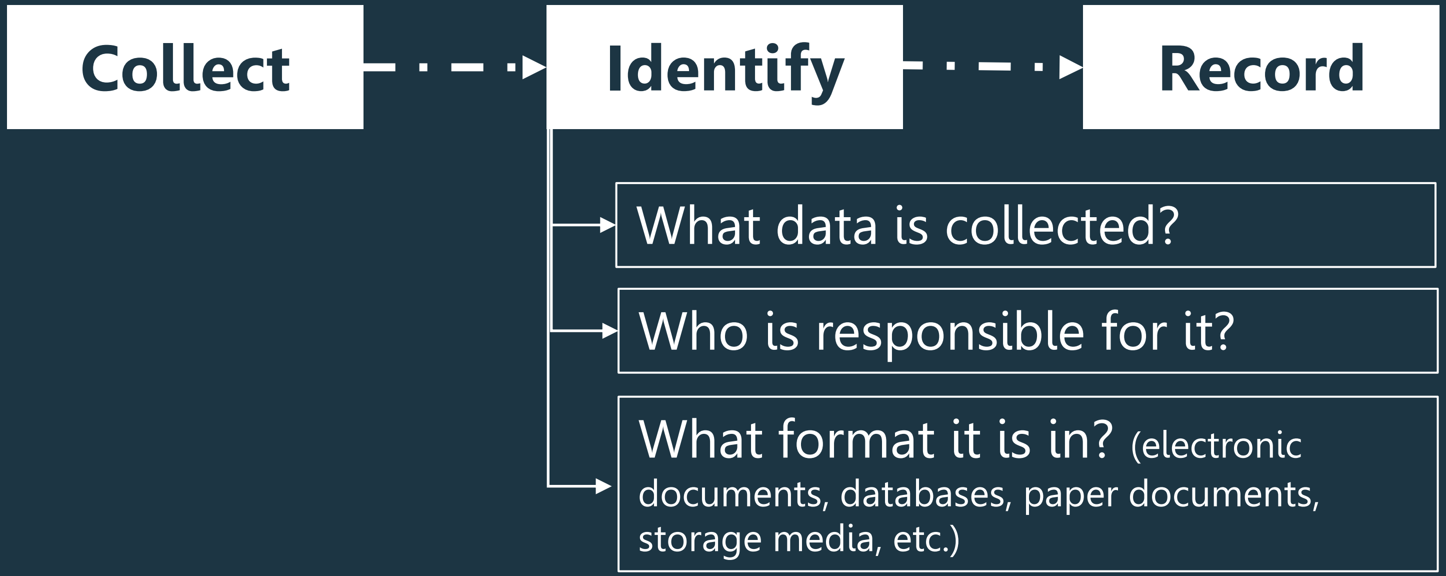
01 Enter your assets into an inventory

02 Classification

03 Labelling

04 Handling

01 Enter your assets into an inventory



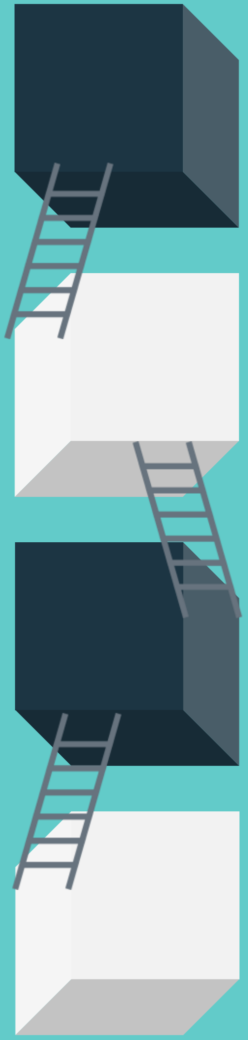
Collect → Identify → Record

- What data is collected?
- Who is responsible for it?
- What format it is in? (electronic documents, databases, paper documents, storage media, etc.)

Example of data inventory

# of data	Name of data/file	Description	Classification	Data owner	Location
ABC-Sec-001	Customer information	Customer name, and contact information	Internal	CRM Dept.	SharePoint

Data Classification steps



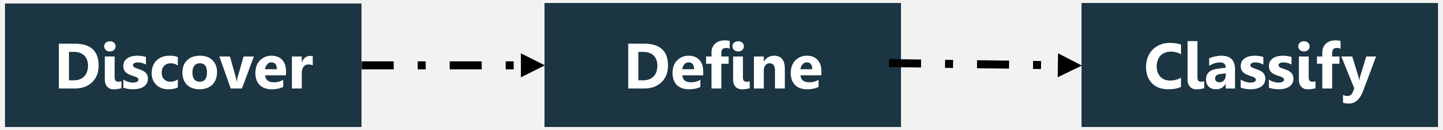
01 Enter your assets into an inventory

02 Classification

03 Labelling

04 Handling

02 Classification



Discover → Define → Classify

A sample of data classification definition

Secret:

Compromise of data with this sensitivity label could possibly put the organization’s future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.

Confidential:

Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.

Internal use:

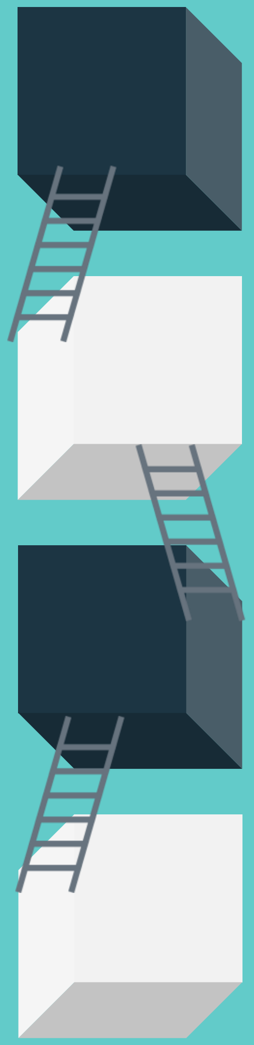
Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.

Public:

As this data is already published, no harm can come from further dissemination or disclosure.

Reference: ISC2

Data Classification steps



01 Enter your assets into an inventory

02 Classification

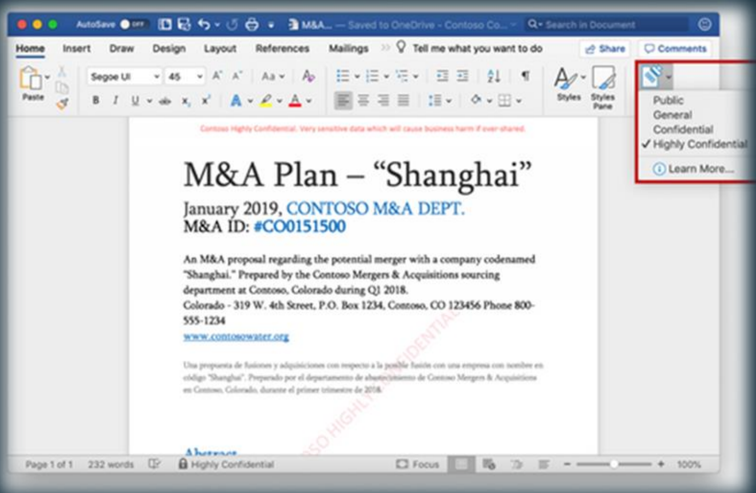
03 Labelling

04 Handling

03 Labelling

Labelling could be both at the data inventory and data itself, but it should be consistent and clear.

For example...



Contoso Highly Confidential. Very sensitive data which will cause business harm if over-shared.

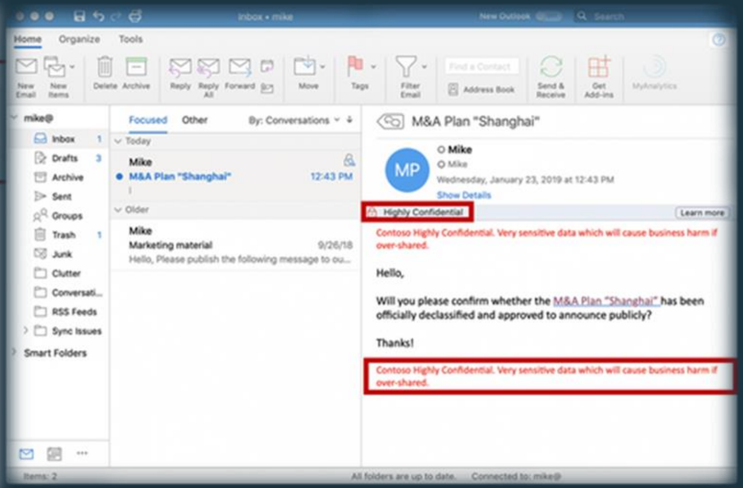
M&A Plan – "Shanghai"

January 2019, CONTOSO M&A DEPT.
M&A ID: #CO0151500

An M&A proposal regarding the potential merger with a company codenamed "Shanghai." Prepared by the Contoso Mergers & Acquisitions sourcing department at Contoso, Colorado during Q1 2018.
Colorado - 319 W. 4th Street, P.O. Box 1234, Contoso, CO 123456 Phone 800-555-1234
www.contosowater.org

Una propuesta de fusiones y adquisiciones con respecto a la posible fusión con una empresa con nombre en código "Shanghai". Preparado por el departamento de abastecimiento de Contoso Mergers & Acquisitions en Contoso, Colorado, durante el primer trimestre de 2018.

Abstract



Mike
M&A Plan "Shanghai" 12:43 PM

Mike
Marketing material 9/26/18
Hello, Please publish the following message to ou...

M&A Plan "Shanghai"

Mike
Mike
Wednesday, January 23, 2019 at 12:43 PM
Show Details

Highly Confidential   Learn more

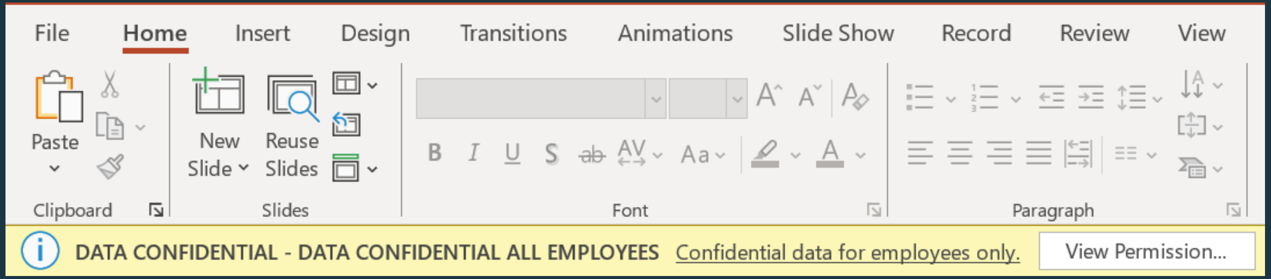
Contoso Highly Confidential. Very sensitive data which will cause business harm if over-shared.

Hello,

Will you please confirm whether the M&A Plan "Shanghai" has been officially declassified and approved to announce publicly?

Thanks!

Contoso Highly Confidential. Very sensitive data which will cause business harm if over-shared.



DATA CONFIDENTIAL - DATA CONFIDENTIAL ALL EMPLOYEES Confidential data for employees only.

Reference: Adam Jung

Data Classification steps

01 Enter your assets into an inventory

02 Classification

03 Labelling

04 Handling

04 Handling

Finally, the rules must be established for how to protect each information asset based on its classification and format.

For example...

Level/Activities	Secret	Confidential	Internal use	Public
Accessing	1. Authroized persons must be set and reviewed every significant change by owner. 2. Must be approved by owner before accessing.	1. Authroized persons must be set and reviewed every significant change by owner. 2. Must be approved by owner before accessing.	Only employees within organization can access.	No limited.
Storage	Data must be encrypted.	Data should be encrypted.	Data should be encrypted.	No limited.
Internal transfering	Data must be encrypted.	Data should be encrypted.	Data should be encrypted.	No limited.
External transfering	Data must be encrypted.	Data must be encrypted.	Data should be encrypted.	No limited.
Destruction	1. Data must be destroyed when it is not necessity use. 2. Permanently deletion or reduce risks by controlling rights of accessing.	1. Data must be destroyed when it is not necessity use. 2. Permanently deletion or reduce risks by controlling rights of accessing.	Use the data deletion normal method.	No limited.

KEY TAKEAWAYS

- Data inventory is starting point to classify your data.
- Data classification can be customized to fit the business context.
- Data handling can be designed based on its classification incorporating with data stage.
- All employees shall adhere to Data classification and handling standard or process – not only Security team.

03

Threat to Data protection

Key Objective

Common threats to data protection

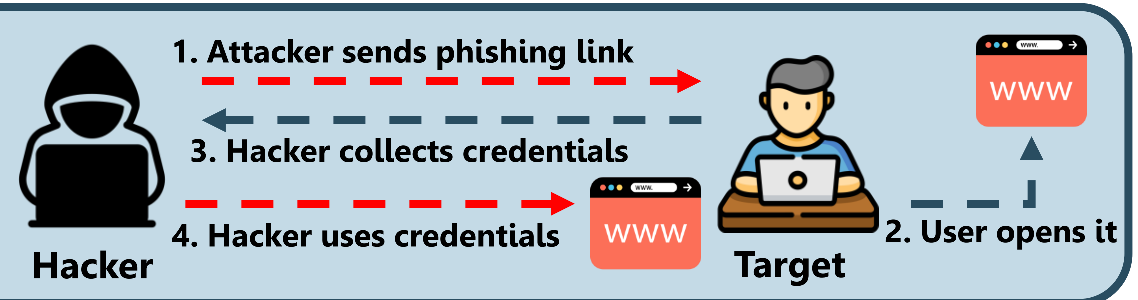
How data protection is being attacked

Threats to Data protection

1

Phishing Attack

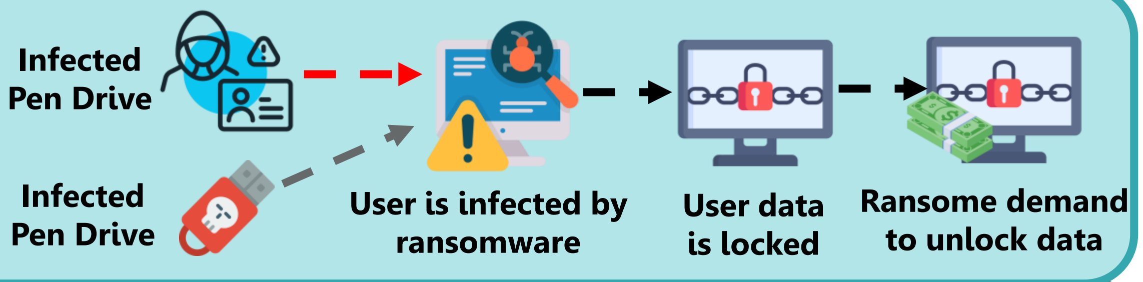
Deceptive emails, messages, or websites to obtain sensitive information.


Hacker
1. Attacker sends phishing link
3. Hacker collects credentials
4. Hacker uses credentials
www
Target
www
2. User opens it

2

Ransomware

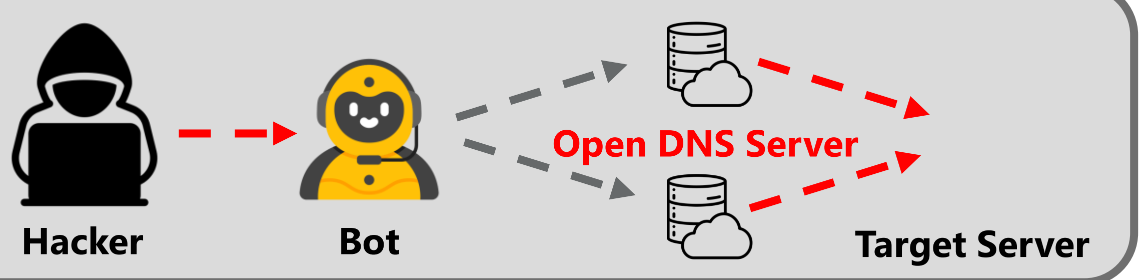
Software designed to encrypt files and demand payment for their release.



3

Denial-of-Service (DoS)

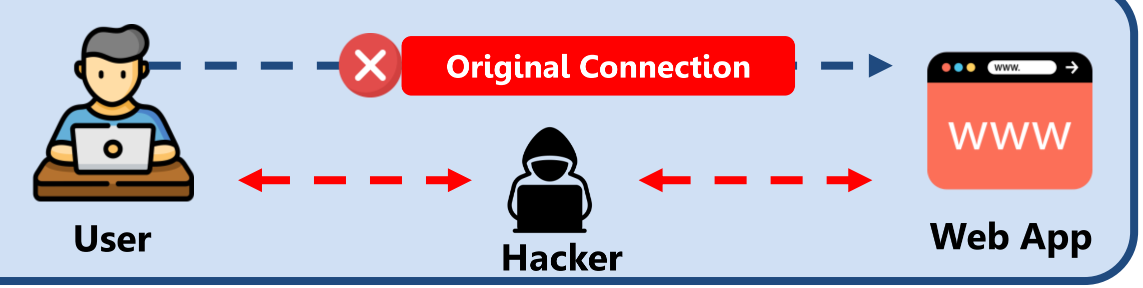
Overloading a system or network to disrupt normal functioning.



4

Man-in-the-Middle (MitM)

Intercepting and manipulating communication between two parties without their knowledge.



5

SQL Injection

Exploiting vulnerabilities in database queries to gain unauthorized access.

6

Cross-Site Scripting (XSS)

Injecting malicious scripts into websites viewed by other users.

7

Zero-Day Exploits

Attacks exploiting unknown vulnerabilities before developers can address them.

8

DNS Spoofing

Redirecting DNS queries to malicious sites for unauthorized access.

Reference: Brij Kishore Pandey

Threats to Data protection

KBTG
KASIKORN BUSINESS-TECHNOLOGY GROUP

1 Phishing Attack

Deceptive emails, messages, or websites to obtain sensitive information.

2 Ransomware

Software designed to encrypt files and demand payment for their release.

3 Denial-of-Service (DoS)

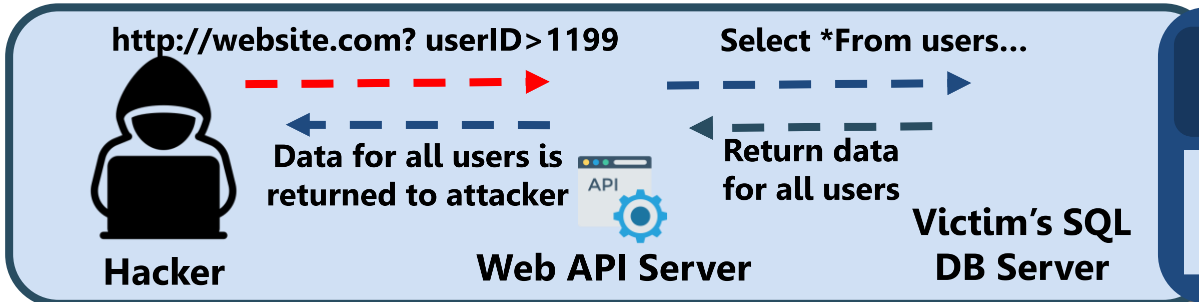
Overloading a system or network to disrupt normal functioning.

4 Man-in-the-Middle (MitM)

Intercepting and manipulating communication between two parties without their knowledge.

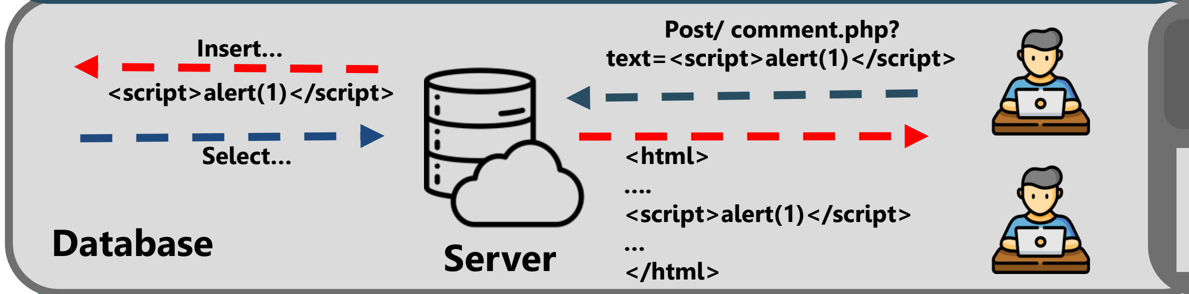
5 SQL Injection

Exploiting vulnerabilities in database queries to gain unauthorized access.


http://website.com? userID>1199
Select *From users...
Data for all users is returned to attacker
Return data for all users
API
Hacker
Web API Server
Victim's SQL DB Server

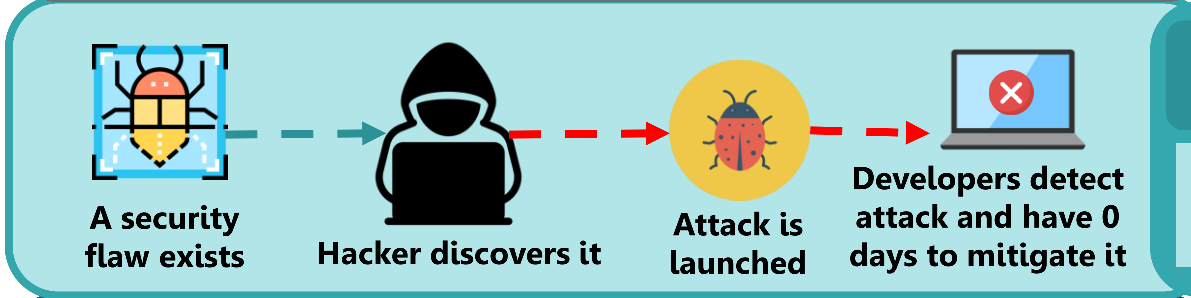
6 Cross-Site Scripting (XSS)

Injecting malicious scripts into websites viewed by other users.


Insert...
<script>alert(1)</script>
Select...
Database
Server
Post/ comment.php? text=<script>alert(1)</script>
<html>
....
<script>alert(1)</script>
...
</html>

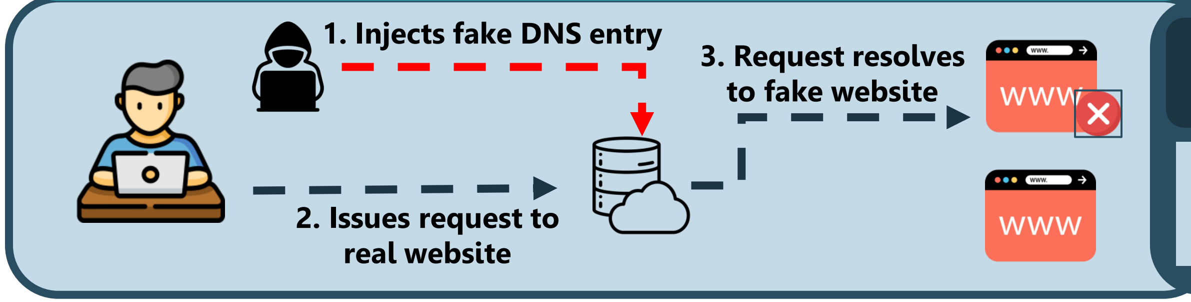
7 Zero-Day Exploits

Attacks exploiting unknown vulnerabilities before developers can address them.



8 DNS Spoofing

Redirecting DNS queries to malicious sites for unauthorized access.


1. Injects fake DNS entry
2. Issues request to real website
3. Request resolves to fake website
www
www

Reference: Brij Kishore Pandey

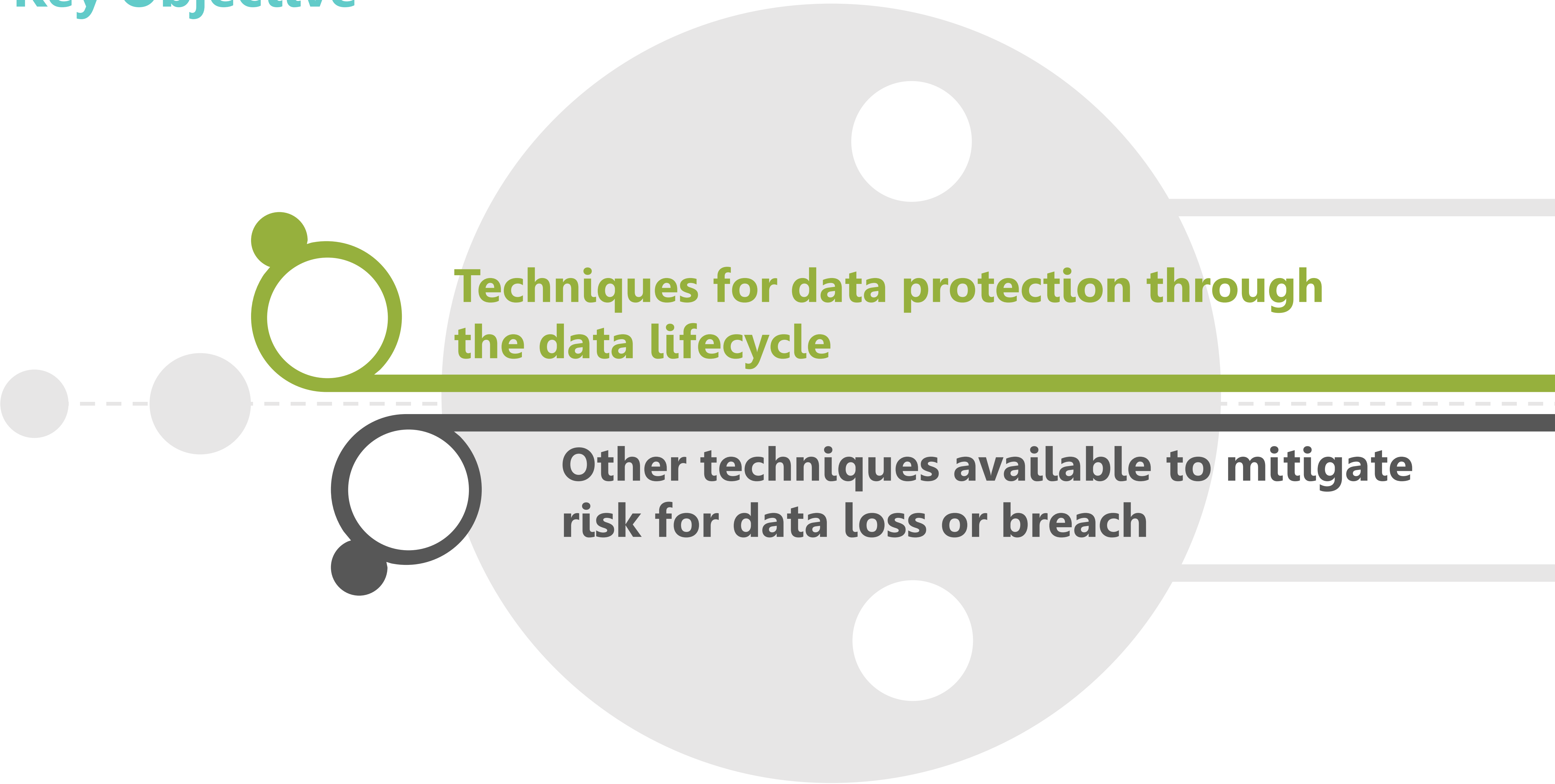
KEY TAKEAWAYS

- Data protection control is not 100% guaranteed that data is all safe.
- Threats to data protection are also involved with human – awareness is one of foundation that organization can reduce risk to threats.
- Detection controls are complimentary controls to data protection controls.

04

Data security techniques available

Key Objective

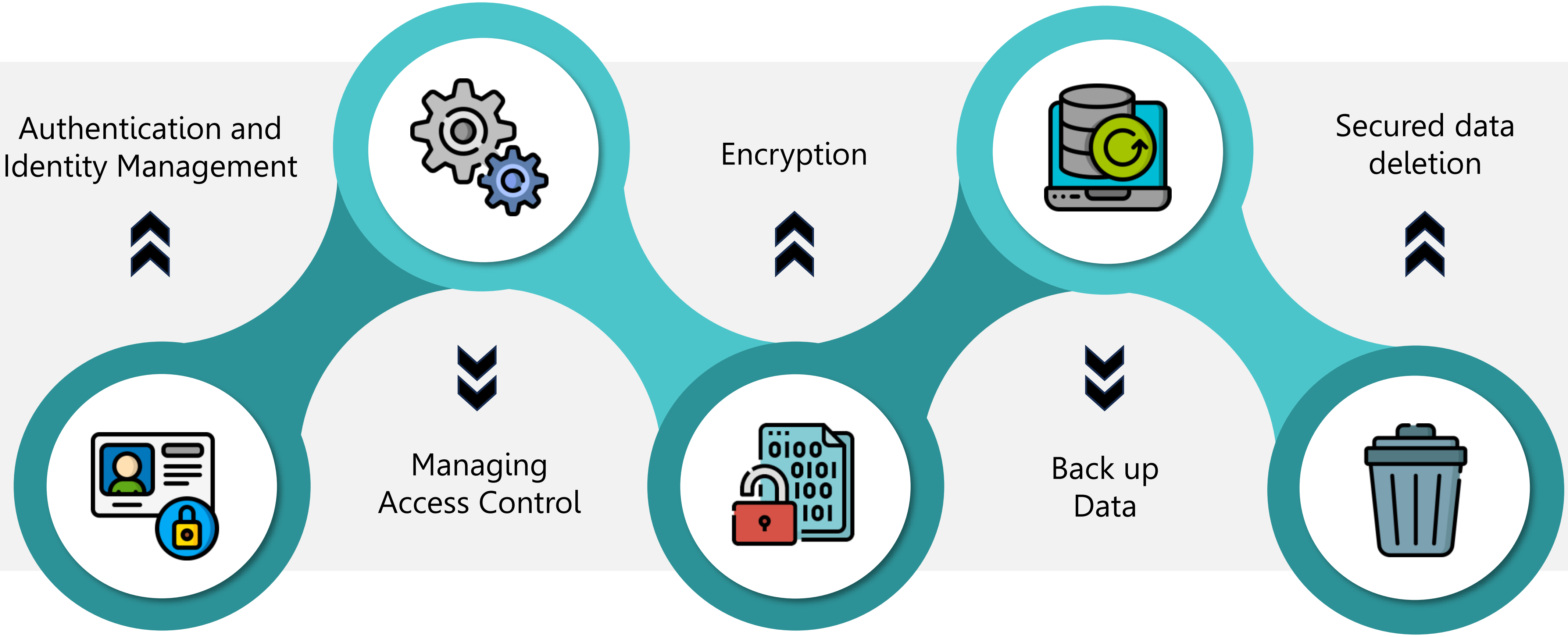


Techniques for data protection through the data lifecycle

Other techniques available to mitigate risk for data loss or breach

KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

5 Security common techniques for Data Protection



Authentication and Identity Management

Managing Access Control

Encryption

Back up Data

Secured data deletion

Reference: Fortinet

Other Data Protection Techniques

Data Masking

Substitutes sensitive data with altered or fictional values

Data Anonymization

Removes or modifies identifiable information from data

Data Tokenization

Replaces sensitive data with unique tokens or references

Hashing

Converts data into a fixed-size alphanumeric string (hash value)

Data Redaction

Selectively removes or obscures sensitive information

Data Scrambling

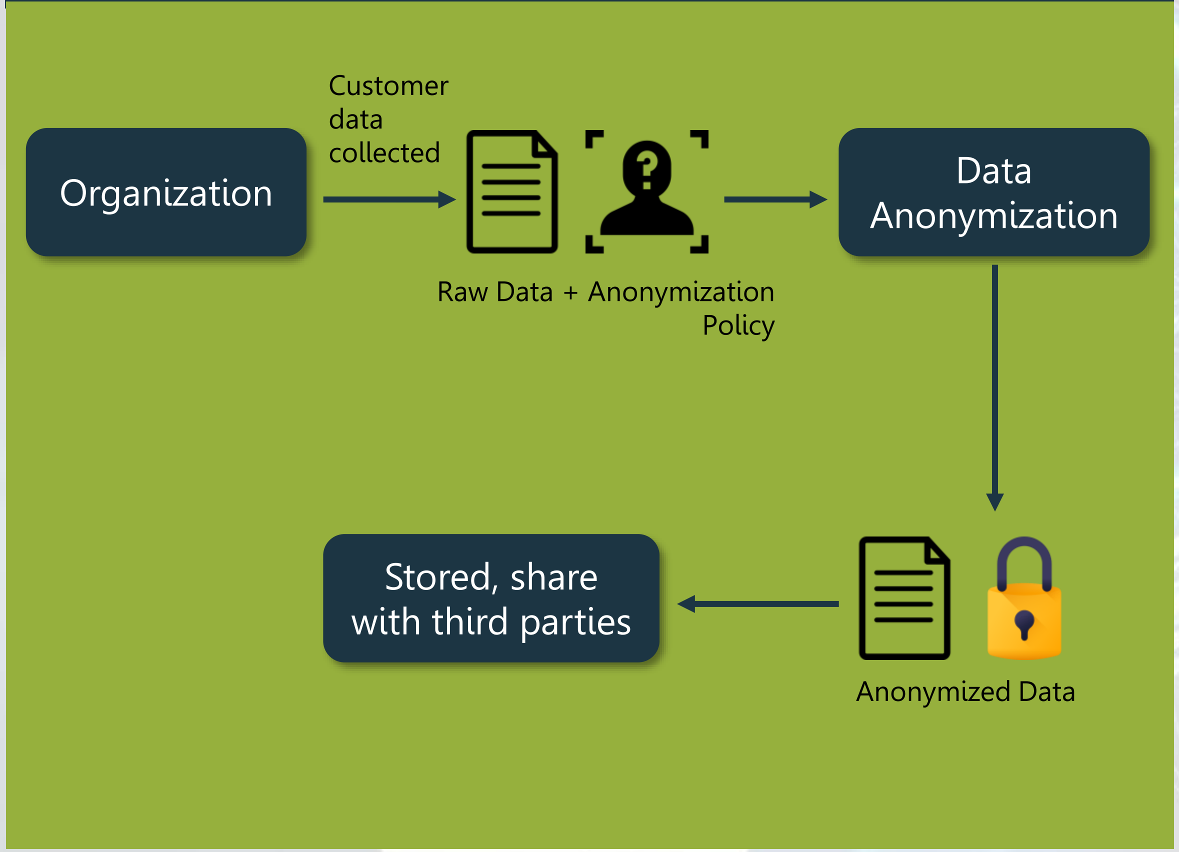
Rearranges or reorganizes data to make it unreadable

Reference: Qulix, imperva

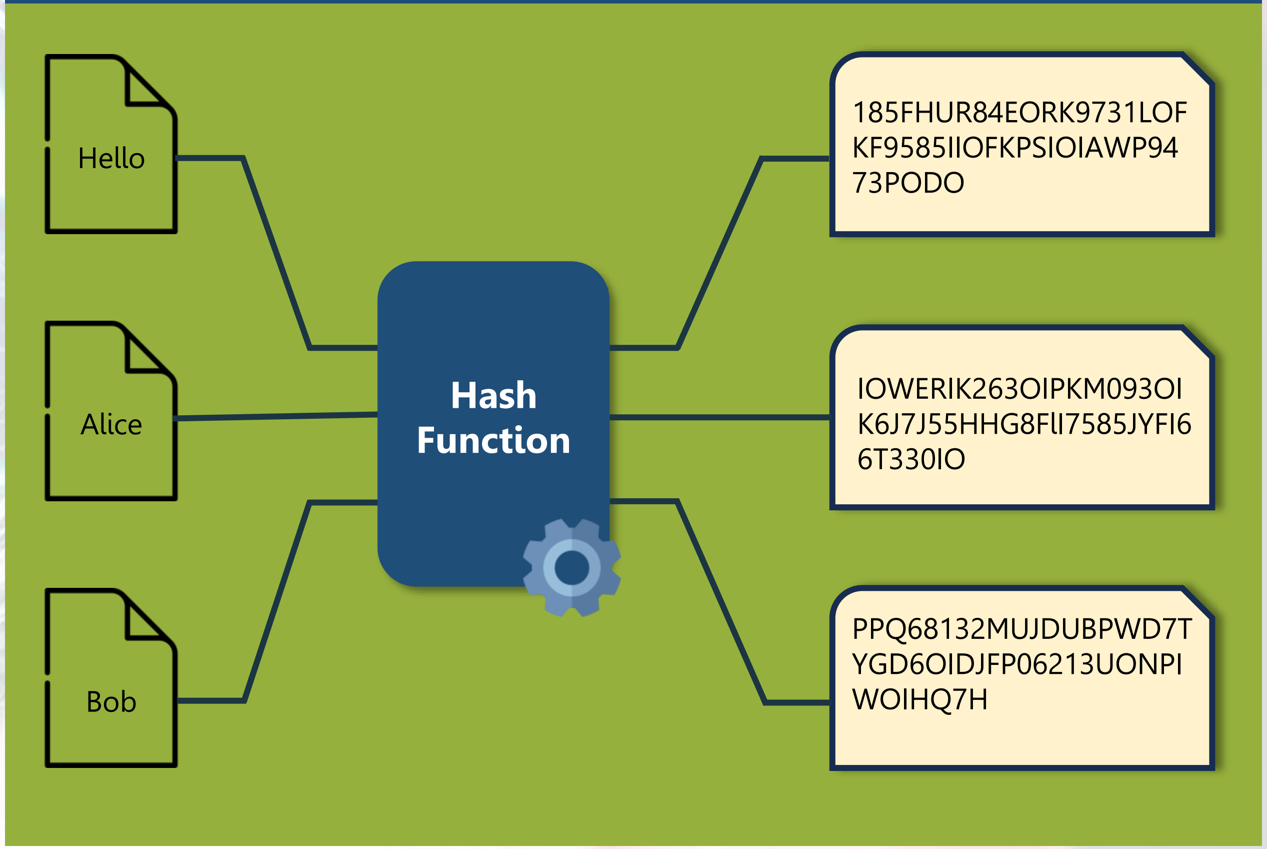
Other Data Protection Techniques

Use case :

Data Anonymization



Hashing



185FHUR84EORK9731LOF
KF9585IIOFKPSIOIAWP94
73PODO

IOWERIK263OIPKM093OI
K6J7J55HHG8FlI7585JYFI6
6T330IO

PPQ68132MUJDUBPWD7T
YGD6OIDJFP06213UONPI
WOIHQ7H

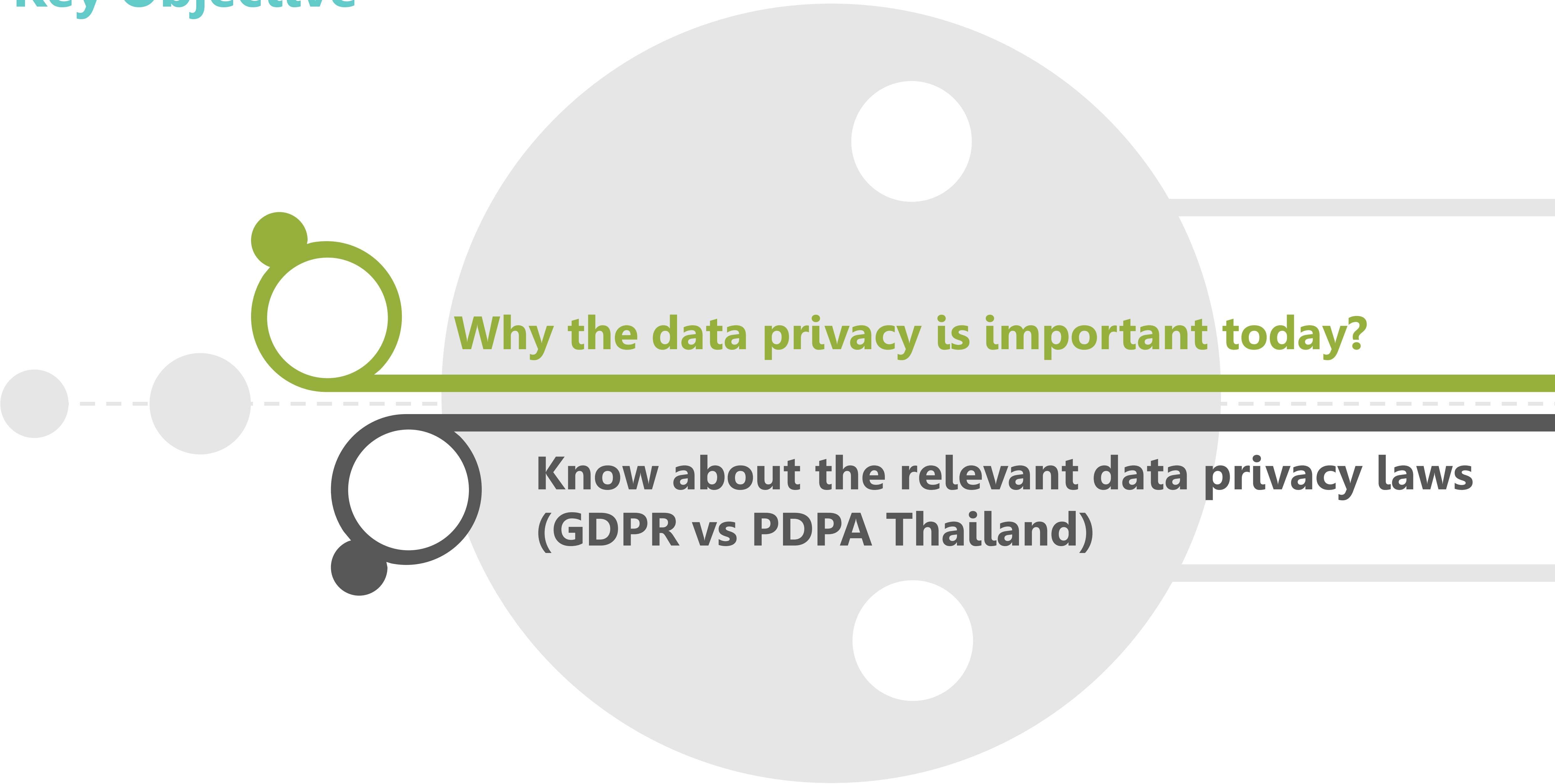
KEY
TAKEAWAYS

- There is not only one data protection control that protects all threats.
- There is no one solution for all organization’s IT environment and context.
- Organization can consider to implement controls that fit with organization risk appetite.

05

Data privacy laws (GDPR, PDPA Thailand)

Key Objective



Why the data privacy is important today?

Know about the relevant data privacy laws (GDPR vs PDPA Thailand)

Importance of Data Privacy

Data privacy, or information privacy, means handling all **data related to a person's identity** with respect for confidentiality and anonymity.

Personally Identifiable Information (PII)

Protection of Personal Information

Data privacy safeguards individuals' personal information from unauthorized access.

Trust and Confidence

To build a reputation for reliability and integrity. Leading to stronger relationships and long-term loyalty of customer.

Legal and Regulatory Compliance

Compliance with data privacy regulations helps businesses avoid legal repercussions, hefty fines, and damage to their reputation.

Ethical Data Practices

Respecting data privacy is an ethical responsibility to show their commitment to respecting individuals' rights and promoting transparency in organization's operations.

Data-driven Innovation

can be used to derive valuable insights, drive personalized experiences, and advance research and development across various industries.

Preserving Individual Autonomy

Data privacy empowers individuals to maintain control over their personal information.

Reference: Donal Tobin

The relevant data privacy laws

GDPR

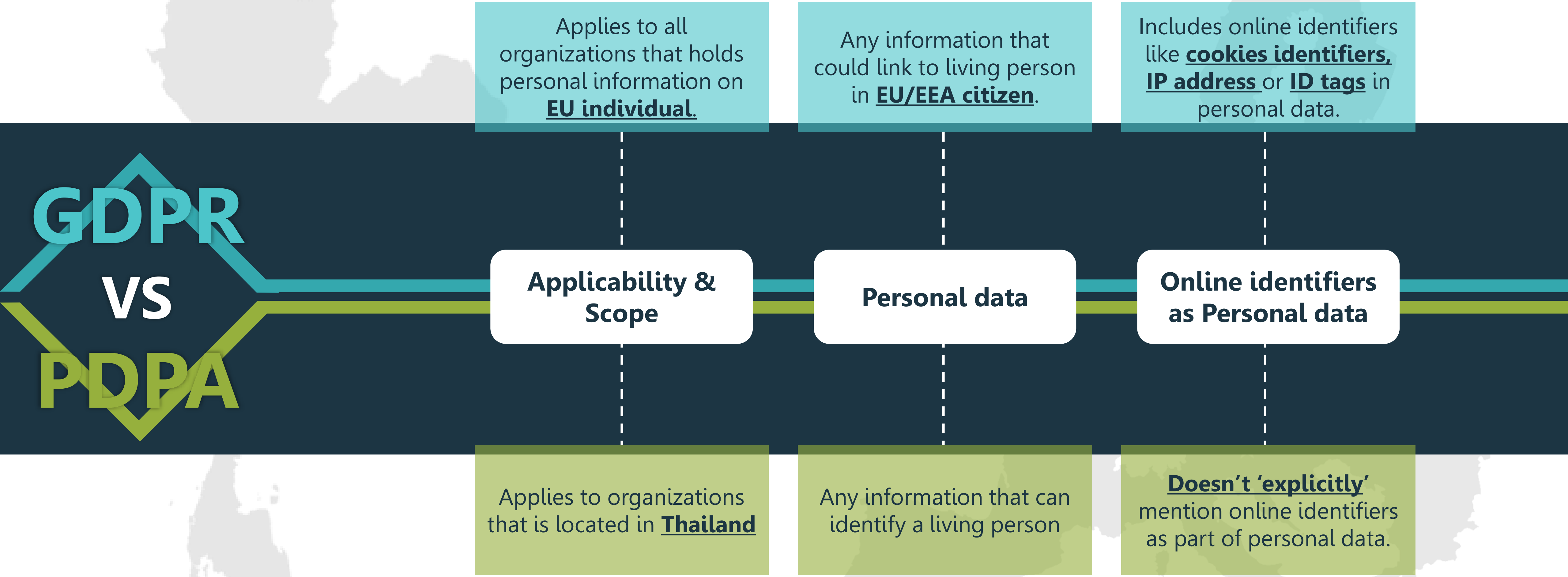
VS

PDPA

The General Data Protection Regulation is a European Union privacy law that was effective on May 25, 2018.

Thailand's Personal Data Protection Act BE 2562 (PDPA) is a Thai privacy law that was effective on June 01, 2021.

The relevant data privacy laws



GDPR VS PDPA

	Applicability & Scope	Personal data	Online identifiers as Personal data
GDPR	Applies to all organizations that holds personal information on **EU individual**.	Any information that could link to living person in **EU/EEA citizen**.	Includes online identifiers like **cookies identifiers, IP address** or **ID tags** in personal data.
PDPA	Applies to organizations that is located in **Thailand**	Any information that can identify a living person	**Doesn't 'explicitly'** mention online identifiers as part of personal data.

Reference: http://cookiesyes.com/thailand

The relevant data privacy laws

✓	**Opt-in & opt-out for data collection**	✓
16 years	**Age of consent**	**20** years
8 data subject rights	**User rights**	**8** data subject rights
Authority to be notified within **72 hours.**	**Data breach notification**	Authority to be notified within **72 hours.**
Up to 20 million (USD 22 million) or 4% of annual global turnover, whichever is greater.	**Penalty**	Punitive damages up to 1 year in prison, or fines that could go up to 5 million Baht.

The relevant data privacy laws

KBTG
KASIKORN BUSINESS-TECHNOLOGY GROUP

✓

16 years

8 data subject rights

Authority to be notified within **72 hours.**

Up to 20 million (USD 22 million) or 4% of annual global turnover, whichever is greater.

Opt-in & opt-out for data colle

ghts

Data breach

✓

es
n, or
go
ht.

GDPR

- Right to access
- Right to be informed
- Right to delete
- Right to correct
- Right to restrict processing
- Right to object/opt out of processing
- Right to portability
- Right to object user profiling or automated decision-making

PDPA

- Right to access and copy
- Right to file a complaint
- Right to delete
- Right to correct
- Right to restrict processing
- Right to object/opt out of processing
- Right to portability
- Right to consent withdrawal

Personal Data Protection Act

PDPA Summary

By KBTG DPO

1 What is the PDPA?

The PDPA standard for **The Personal Data Protection Act, B.E.2562** (Effective from 1 June 2022), is designed <u>to protect a data subject from unauthorized or unlawful collection, use, or disclosure and processing of their personal data by a Data Controller or a Data Processor</u> that is in Thailand, regardless of whether those actions takes place in Thailand or not.

<u>Personally Identifiable Information (PII)/Personal data</u>: Any information relating to a living person, which <u>directly or indirectly</u> enables them to be identified.		**<u>Sensitive personal data:</u>** Special category of personal data that is at risk of being used for discriminatory purposes.
<u>EX : Directly personal data</u> Name - Surname Identification number Employee ID / CIS ID Personal/working Email Photo of applicant in resume.	<u>EX : Indirectly personal data</u> Nickname Position Address Height Weight IP Address	<u>EX : Sensitive Personal data</u> Racial, Ethnic origin / Political opinions / Cult, Religious or Philosophical beliefs / Sexual behavior / Trade union information / Genetic data, Biometric data / Health data, Disability / Criminal Records

2 Key players

<u>Data Subject (DS)</u> > Any living individual whose personal data is collected, held or processed by a organization or third party.

<u>Data controller (DC)</u> > Person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the personal data.

<u>Data processor (DP)</u> > Person or a juristic person that is responsible for processing personal data on behalf of the controller.

3 PDPA requirements

1 No Surprise : we **must** inform data subject how organization collect, process or disclose their personal data (Privacy Notice).

2 Legal Basis : any personal data processing **shall** be relied on a legal basis as below

- ➢ Contract
- ➢ Legal obligations
- ➢ Legitimate interest
- ➢ Consent
- ➢ Public Interest
- ➢ Scientific or Archives
- ➢ Vital interests

3 Record of processing activity (ROPA) :

- ➢ To support PDPA B.E. 2562 compliance in section 39 and 40 that 'Data controller (DC) and Data processor (DP) shall prepare Record of Processing Activities (ROPA)'.

4 Eight rights of data subjects : As required by PDPA, shall respond to the data subject rights when is requested by data subject.

- Right of access and copy
- Right to data portability
- Right to object
- Right to restrict processing
- Right of rectification
- Right to erasure / Right to be forgotten
- Right to withdraw consent
- Right to file a complaint

5 Personal data breach management : Address without undue delay and, where feasible, not later than 72 hours after becoming aware of the incident.

6 Penalties for PDPA non-compliance :

- ➢ Administrative not exceeding Baht 5 million
- ➢ Civil punitive damages in addition to actual compensation at the courts' discretion but not exceed twice that actual compensation
- ➢ Criminal imprisonment of up to 1 year and/or fine of up to Baht 1 million

7 Data Protection Officer (DPO): is responsible for

- ➢ Providing PDPA related consultation
- ➢ Oversighting and assuring the company's PDPA compliance
- ➢ Collaboratively working with PDPC and/or external parties for PDPA related works.

KEY TAKEAWAYS

Data privacy law is designed to protect a data subject from unauthorized or unlawful collection, use, or disclosure and processing of their personal data by a Data Controller or a Data Processor.

Personal data processing in Thailand is not limited to only PDPA compliance – but it may be applicable to privacy law around the world that organization shall consider.

06

International Security and Privacy control framework (NIST 800-53, NIST Privacy Framework, ISO 27701)

Key Objective

International standards available for information security, data protection and data privacy

NIST Special Publication 800-53

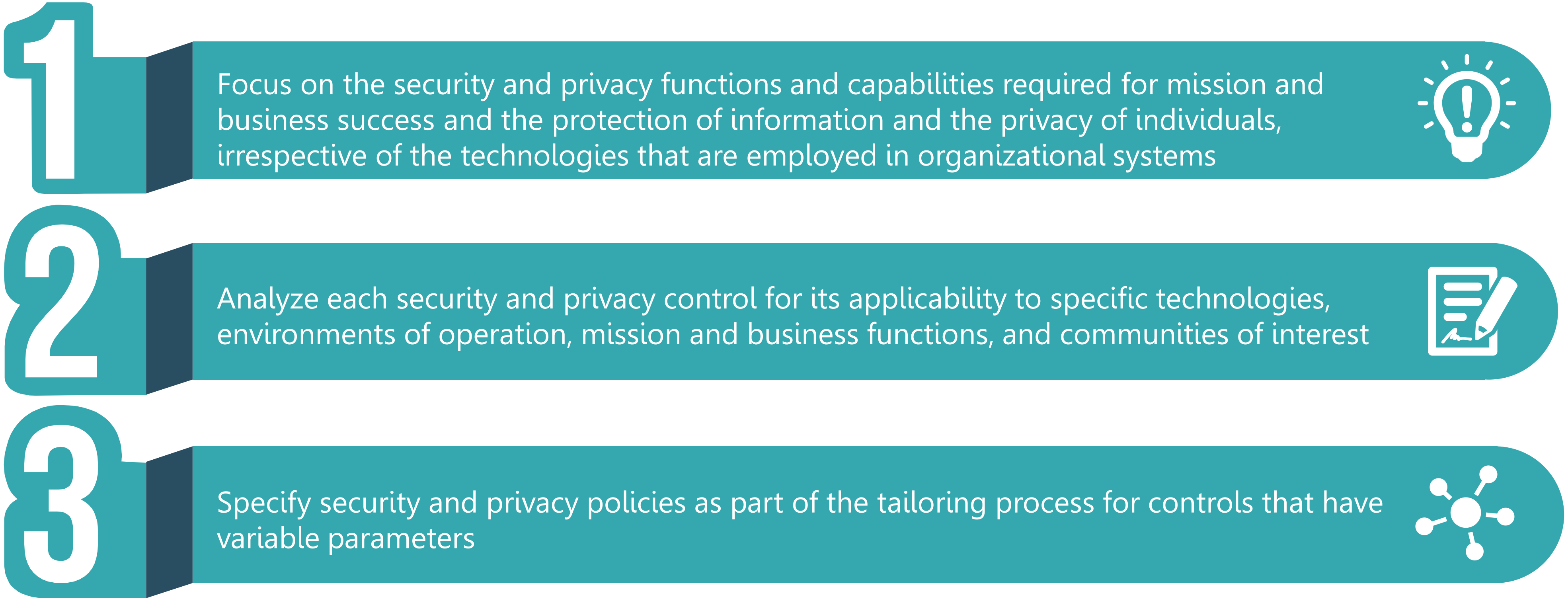
THE CONTROLS :

SECURITY AND PRIVACY CONTROLS AND CONTROL ENHANCEMENTS

This catalog of security and privacy controls provides protective measures for systems, organizations, and individuals.

The controls are designed to facilitate risk management and compliance with applicable federal laws, executive orders, directives, regulations, policies, and standards. With few exceptions, the security and privacy controls in the catalog are policy, technology, and sector-neutral, meaning that the controls focus on the fundamental measures necessary to protect information and the privacy of individuals across the information life cycle.

It encourages organizations to:



1. Focus on the security and privacy functions and capabilities required for mission and business success and the protection of information and the privacy of individuals, irrespective of the technologies that are employed in organizational systems

2. Analyze each security and privacy control for its applicability to specific technologies, environments of operation, mission and business functions, and communities of interest

3. Specify security and privacy policies as part of the tailoring process for controls that have variable parameters

Reference: Reference: https://www.nist.gov/

NIST Special Publication 800-53

THE CONTROLS :

01 ACCESS CONTROL

02 AWARENESS AND TRAINING

03 AUDIT AND ACCOUNTABILITY

04 ASSESSMENT, AUTHORIZATION, AND MONITORING

05 CONFIGURATION MANAGEMENT

06 CONTINGENCY PLANNING

07 IDENTIFICATION AND AUTHENTICATION

08 INCIDENT RESPONSE

09 MAINTENANCE

10 MEDIA PROTECTION

11 PHYSICAL AND ENVIRONMENTAL PROTECTION

12 PLANNING

13 PROGRAM MANAGEMENT

14 PERSONNEL SECURITY

15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

16 RISK ASSESSMENT

17 SYSTEM AND SERVICES ACQUISITION

18 SYSTEM AND COMMUNICATIONS PROTECTION

19 SYSTEM AND INFORMATION INTEGRITY

20 SUPPLY CHAIN RISK MANAGEMENT

NIST Special Publication 800-53

For example,

01 ACCESS CONTROL

- Account Management
- Access Enforcement
- Information Flow Enforcement
- Separation of Duties
- Least Privilege
- Unsuccessful Logon Attempts
- Device Lock/Session Termination
- Remote/Wireless Access
- Mobile Devices

07 IDENTIFICATION AND AUTHENTICATION

- Organizational Users
- Single Sign-on/Multi-factor Authentication
- Authenticator Management
- Password/Publish Key-based Authentication
- Re-authentication
- Identity Proofing

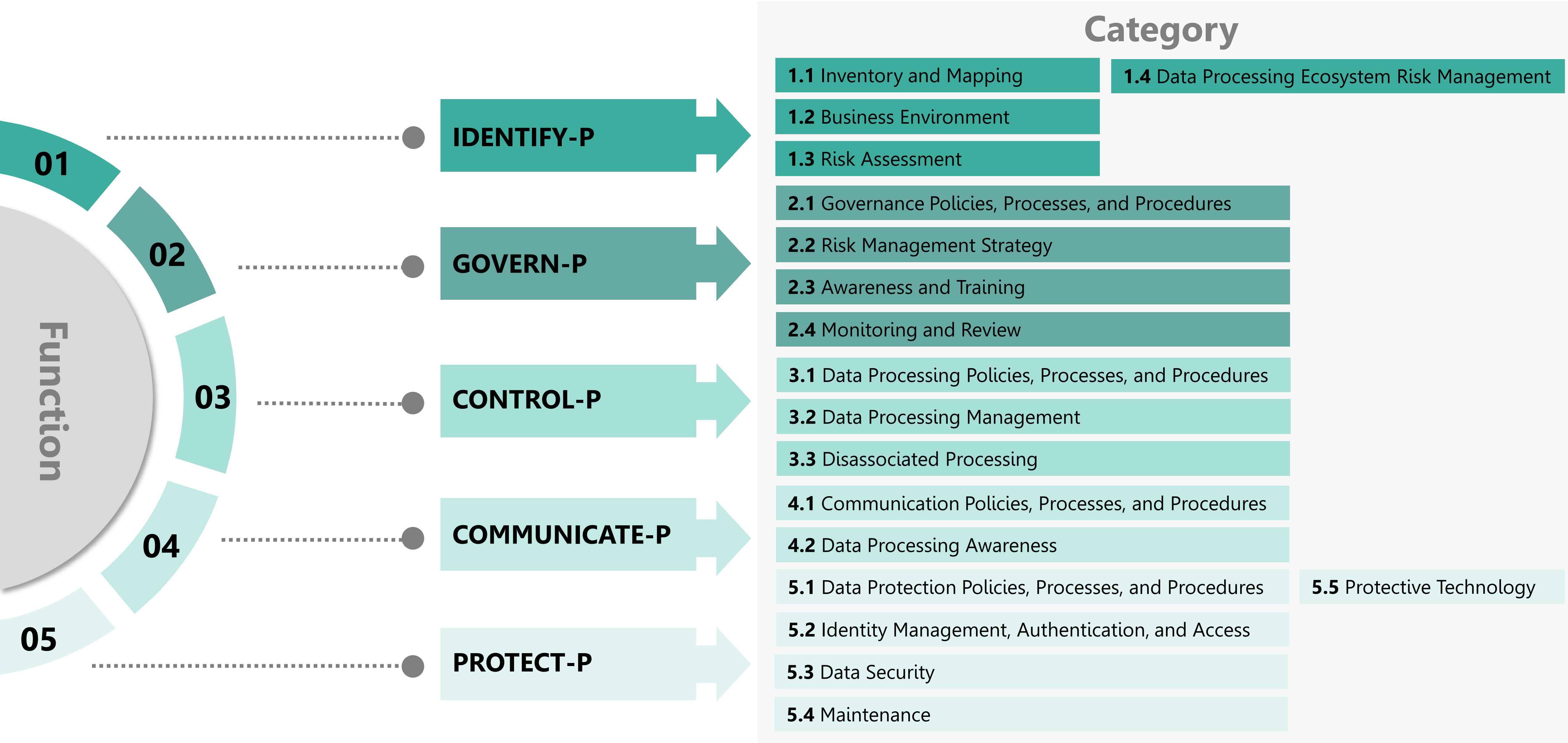
18 SYSTEM AND COMMUNICATIONS PROTECTION

- Denial-of-Service Protection
- Transmission Confidentiality and Integrity
- Protection of Information at Rest
- System Time Synchronization
- System Monitoring
- Software, Firmware and Information Integrity
- Spam Protection
- Information Input Validation
- Information Management and Retention

KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core



Function

Category

01 IDENTIFY-P
- **1.1** Inventory and Mapping
- **1.2** Business Environment
- **1.3** Risk Assessment
- **1.4** Data Processing Ecosystem Risk Management

02 GOVERN-P
- **2.1** Governance Policies, Processes, and Procedures
- **2.2** Risk Management Strategy
- **2.3** Awareness and Training
- **2.4** Monitoring and Review

03 CONTROL-P
- **3.1** Data Processing Policies, Processes, and Procedures
- **3.2** Data Processing Management
- **3.3** Disassociated Processing

04 COMMUNICATE-P
- **4.1** Communication Policies, Processes, and Procedures
- **4.2** Data Processing Awareness

05 PROTECT-P
- **5.1** Data Protection Policies, Processes, and Procedures
- **5.2** Identity Management, Authentication, and Access
- **5.3** Data Security
- **5.4** Maintenance
- **5.5** Protective Technology

A comparison between NIST Privacy Framework and NIST CSF

KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

Privacy Framework | Category	Cybersecurity Framework | Category
IDENTIFY	
Inventory and Mapping (ID.IM-P) (ID.BE-P)	Inventory and Asset Management (ID.AM)
Business Environment (ID.BE-P)	Business Environment (ID.BE)
Governance (ID.GV-P)	Governance (ID.GV)
Risk Assessment (ID.RA-P)	Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM-P)*	Risk Management Strategy (ID.RM)*
Supply Chain Risk Management (ID.SC-P)	Supply Chain Risk Management (ID.SC)
PROTECT	
Identity Management, Authentication, and Access Control (PR.AC-P)	Identity Management, Authentication, and Access Control (PR.AC)
Awareness and Training (PR.AT-P)	Awareness and Training (PR.AT)
Data Security (PR.DS-P)	Data Security (PR.DS)
Data Protection Processes and Procedures (PR.DP-P)	Information Protection Processes and Procedures (PR.IP)
Maintenance (PR.MA-P)	Maintenance (PR.MA-P)
Protective Technology (PR.PT-P)	Protective Technology (PR.PT)
Protected Processing (PR.PP-P)	

Reference: https://www.nist.gov/

* indicates that the Privacy Framework Subcategory and the CSF Subcategory are identical

A comparison between NIST Privacy Framework and NIST CSF

Privacy Framework | Category	Cybersecurity Framework | Category
CONTROL	None
Data Management Processes and Procedures (CT.PO-P)	
Data Management (CT.DM-P)	
INFORM	None
Transparency Processes and Procedures (IN.TP-P)	
Data Processing Awareness (IN.AW-P)	
None	**DETECT**
	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM)
	Detection Processes (DE.DP)
RESPOND	
Response Planning (RS.RP-P)	Response Planning (RS.RP)
Communications (RS.CO-P)*	Communications (RS.CO)*
Analysis (RS.AN-P)	Analysis (RS.AN)
Mitigation (RS.MI-P)	Mitigation (RS.MI)
Improvements (RS.IM-P)	Improvements (RS.IM)
Redress (RS.RE-P)	None

Reference: https://www.nist.gov/

* indicates that the Privacy Framework Subcategory and the CSF Subcategory are identical

A comparison between NIST Privacy Framework and NIST CSF

Privacy Framework | Category	Cybersecurity Framework | Category
None	**RECOVER**
	Recovery Planning (RC.RP) Improvements (RC.IM)
	Communications (RC.CO)

Reference: https://www.nist.gov/

* indicates that the Privacy Framework Subcategory and the CSF Subcategory are identical

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: IDENTIFY-P

1.1 Inventory and Mapping	ID.IM-P1: Systems/products/services that process data are inventoried
	ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried
	ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried
	ID.IM-P4: Data actions of the systems/products/services are inventoried
	ID.IM-P5: The purposes for the data actions are inventoried
	ID.IM-P6: Data elements within the data actions are inventoried
	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties)
	ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services
1.2 Business Environment	ID.BE-P1: The organization's role(s) in the data processing ecosystem are identified and communicated
	ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated
	ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: IDENTIFY-P

1.3 Risk Assessment	ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties)
	ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias
	ID.RA-P3: Potential problematic data actions and associated problems are identified
	ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk
	ID.RA-P5: Risk responses are identified, prioritized, and implemented
1.4 Data Processing Ecosystem Risk Management	ID.DE-P1: Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders
	ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process
	ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks
	ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations

NIST Privacy Framework

KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: GOVERN-P

2.1 Governance Policies, Processes, and Procedures	GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated
	GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place
	GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy
	GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners)
	GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed
	GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks
2.2 Risk Management Strategy	GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders
	GV.RM-P2: Organizational risk tolerance is determined and clearly expressed
	GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem
2.3 Awareness and Training	GV.AT-P1: The workforce is informed and trained on its roles and responsibilities
	GV.AT-P2: Senior executives understand their roles and responsibilities
	GV.AT-P3: Privacy personnel understand their roles and responsibilities
	GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: GOVERN-P

2.4 Monitoring and Review	GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change
	GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated
	GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place
	GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place
	GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events)
	GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions
	GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place

NIST Privacy Framework

KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: CONTROL-P

3.1 Data Processing Policies, Processes, and Procedures	CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place
	CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention)
	CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
	CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems
3.2 Data Processing Management	CT.DM-P1: Data elements can be accessed for review
	CT.DM-P2: Data elements can be accessed for transmission or disclosure
	CT.DM-P3: Data elements can be accessed for alteration
	CT.DM-P4: Data elements can be accessed for deletion
	CT.DM-P5: Data are destroyed according to policy
	CT.DM-P6: Data are transmitted using standardized formats
	CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place
	CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization
	CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed
	CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: CONTROL-P

3.3 Disassociated Processing	CT.DP-P1: Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography)
	CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization)
	CT.DP-P3: Data are processed to limit the formulation of inferences about individuals’ behavior or activities (e.g., data processing is decentralized, distributed architectures)
	CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements
	CT.DP-P5: Attribute references are substituted for attribute values

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: COMMUNICATE-P

4.1 Communication Policies, Processes, and Procedures	CM.PO-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place
	CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established
4.2 Data Processing Awareness	CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place
	CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place
	CM.AW-P3: System/product/service design enables data processing visibility
	CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure
	CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem
	CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure
	CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event
	CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: PROTECT-P

5.1 Data Protection Policies, Processes, and Procedures	PR.PO-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality)
	PR.PO-P2: Configuration change control processes are established and in place
	PR.PO-P3: Backups of information are conducted, maintained, and tested
	PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met
	PR.PO-P5: Protection processes are improved
	PR.PO-P6: Effectiveness of protection technologies is shared
	PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed
	PR.PO-P8: Response and recovery plans are tested
	PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening)
	PR.PO-P10: A vulnerability management plan is developed and implemented
5.2 Identity Management, Authentication, and Access	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices
	PR.AC-P2: Physical access to data and devices is managed
	PR.AC-P3: Remote access is managed
	PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
	PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation)
	PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

NIST Privacy Framework

A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 Core

Function: PROTECT-P

5.3 Data Security	PR.DS-P1: Data-at-rest are protected
	PR.DS-P2: Data-in-transit are protected
	PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
	PR.DS-P4: Adequate capacity to ensure availability is maintained
	PR.DS-P5: Protections against data leaks are implemented
	PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
	PR.DS-P7: The development and testing environment(s) are separate from the production environment
	PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity
5.4 Maintenance	PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
	PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
5.5 Protective Technology	PR.PT-P1: Removable media is protected and its use restricted according to policy
	PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
	PR.PT-P3: Communications and control networks are protected
	PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

ISO 27701:2019

ISO 27701 as a privacy add-on for ISO 27001

Category (Ref Annex **A**)) | For organization that is a data controller

Conditions for Collecting and Processing 01

- Identify and document purpose
- Identify lawful basis
- Determine when and how consent is to be obtained
- Obtain and record consent
- Privacy Impact Assessment
- Contracts with PII processors
- Joint PII Controller
- Records related to processing PIIs

Obligations to PII principals 02

- Determining and fulfilling obligations to PII principals
- Determining information to PII principals
- Providing information to PII principals
- Providing mechanism to modify or withdraw consent
- Providing mechanism to object to PII processing
- Access, correction and/ or erasure
- PII Controllers' obligation to inform third parties
- Providing copy of PII processed
- Handling requests
- Automated Decision Making

Privacy by Design and Privacy by Default 03

- Limit collection
- Limit processing
- Accuracy and quality
- PII minimisation objectives
- Temporary files
- PII de-identification and deletion at the end of processing
- Retention
- Disposal
- PII transmission controls

PII sharing, transfer and disclosure 04

- Identify basis for PII transfer between jurisdictions
- Countries and international organisations to which PII can be transferred
- Records of transfer of PII
- Records of PII disclosure to third parties

ISO 27701:2019

ISO 27701 as a privacy add-on for ISO 27001

Category (Ref Annex **B**) | For organization that is a data processor

Conditions for Collecting and Processing 05

- Customer agreement
- Organisation's purpose
- Marketing and advertising use
- Infringement instructions
- Customer obligations
- Records related to processing PIIs

Obligations to PII principals 06

- Obligations of PII principals

Privacy by Design and Privacy by Default 07

- Temporary files
- Return, transfer or disposal of PII
- PII transmission controls

Conditions for Collecting and Processing 08

- Basis of PII transfer between jurisdictions
- Countries and international organisations to which PII can be transferred
- Records of PII disclosure to third parties
- Notification PII disclosure request
- Legally binding PII disclosure
- Disclosure of sub- contractors used to process PII
- Engagement of a subcontractor to process PII
- Change of subcontractor to process PII

KEY

TAKEAWAYS

- NIST800-53 is a guideline that organization can tailor it to fit with business context and risk appetite
- NIST Cybersecurity Framework and NIST Privacy framework have common objectives and controls
- ISO27701 is not standard alone certification but complementary to ISO27001

Thank You

Address

KBTG Building
46/6 Popular Rd, Ban Mai, Pak Kret District,
Nonthaburi 11120

Social channel

FB : KBTG
IN : KASIKORN Business-Technology Group [KBTG]
Website : https://www.kbtg.tech/
YouTube : KBTG_official