



Mahidol University
Faculty of Medicine
Siriraj Hospital



Mahidol University
IT Management

ธรรมาภิบาลข้อมูลและพรบ.คุ้มครองข้อมูลส่วนบุคคล สำหรับงานทางเทคโนโลยีสารสนเทศและข้อมูลในโรงพยาบาล

ผศ.ดร.โชทศรัตน์ ธรรมบุษดี

IT Management Division

Faculty of Engineering – Mahidol University



Outline

- Module 1: Data Governance
- Module 2: Introduction to PDPA
- Module 3: Personal Data Identification
- Module 4: PDPA Lawful Basis
- Module 5: Data Protection Impact Assessment
- Module 6: Related Technical Issues for PDPA
- Module 7: ISO/IEC 27701

ผศ.ดร.โชทศรัตน์ ธรรมบุษดี

- อาจารย์ประจำหลักสูตร IT Management คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล
- หัวหน้าโครงการฝึกอบรม Datalent Team
- วิทยาการและที่ปรึกษาด้าน Data Governance ทั้งหน่วยงานภาครัฐและเอกชน
- วิทยาการและที่ปรึกษาด้าน Data Science and Data Analytics
- พ.ศ. 2563 – ปัจจุบัน ที่ปรึกษาระบบบริหารข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล
คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล
- พ.ศ. 2562 – ปัจจุบัน คณะกรรมการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล
มหาวิทยาลัยมหิดล
- พ.ศ. 2562 – ปัจจุบัน คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้
พรบ.ดิจิทัล
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
- พ.ศ. 2561 คณะกรรมการศึกษากระบวนการระบบบริหารข้อมูลและการเปิดเผยข้อมูลดิจิทัล
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



<https://cv.zotararat.com>

Module 1

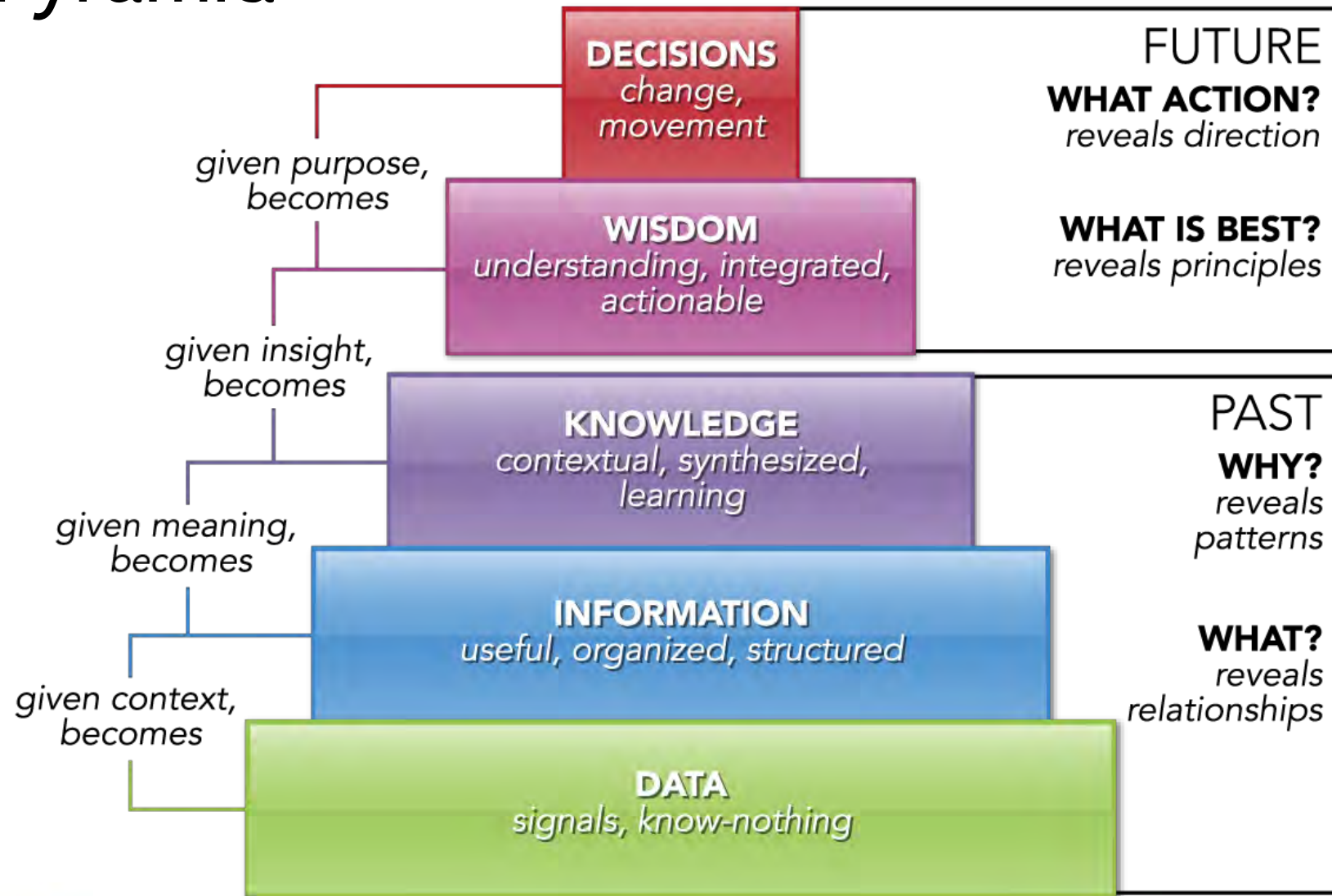
Data Governance

ข้อมูล (Data)

- Data is an ASSET:
 - **ข้อมูล** ถูกจัดอยู่ในประเภทของทรัพย์สินที่มีค่ามากขององค์กร เนื่องจากข้อมูลที่อยู่ในองค์กรนั้น ๆ สามารถบ่งชี้ จุดเด่น จุดด้อย ความชำนาญ และความสามารถในการแข่งขัน นอกเหนือจากทรัพยากรทางการเงิน และทรัพยากรมนุษย์ ที่ถูกจัดเป็นทรัพย์สินภายในองค์กร ตั้งแต่ในอดีต จนถึงปัจจุบัน



DIKW Pyramid



Cost

- ต้นทุนในการจัดหาและจัดเก็บข้อมูล
- ต้นทุนในการหาข้อมูลมาแทนที่ข้อมูลที่สูญหายไป
- ผลกระทบต่อดังกรเมื่อข้อมูลสูญหาย
- ต้นทุนในการลดความเสี่ยงที่เกี่ยวข้องกับข้อมูล
- ต้นทุนในการปรับปรุงข้อมูลให้มีคุณภาพ

Benefit

- ประโยชน์จากข้อมูลที่มีคุณภาพ
- รายได้จากการขายข้อมูล
- รายได้จากการสร้างนวัตกรรมจากข้อมูล
- การเพิ่มประสิทธิภาพการทำงานในองค์กร
- การเพิ่มขีดความสามารถในการแข่งขัน

วงจรชีวิตของข้อมูล และองค์ประกอบการบริหารจัดการข้อมูล



หลักการบริหารจัดการข้อมูล

ข้อมูลมี
คุณค่า

มีการ
สนับสนุน
จาก
ผู้บริหาร

เป็นความ
ต้องการ
ด้านธุรกิจ

มีการ
วางแผน
เพื่อให้
ข้อมูลดีขึ้น

เป็นการ
จัดการ
คุณภาพ
ข้อมูล

ต้องมีเม
ทาดาตาใน
การ
จัดการ
ข้อมูล

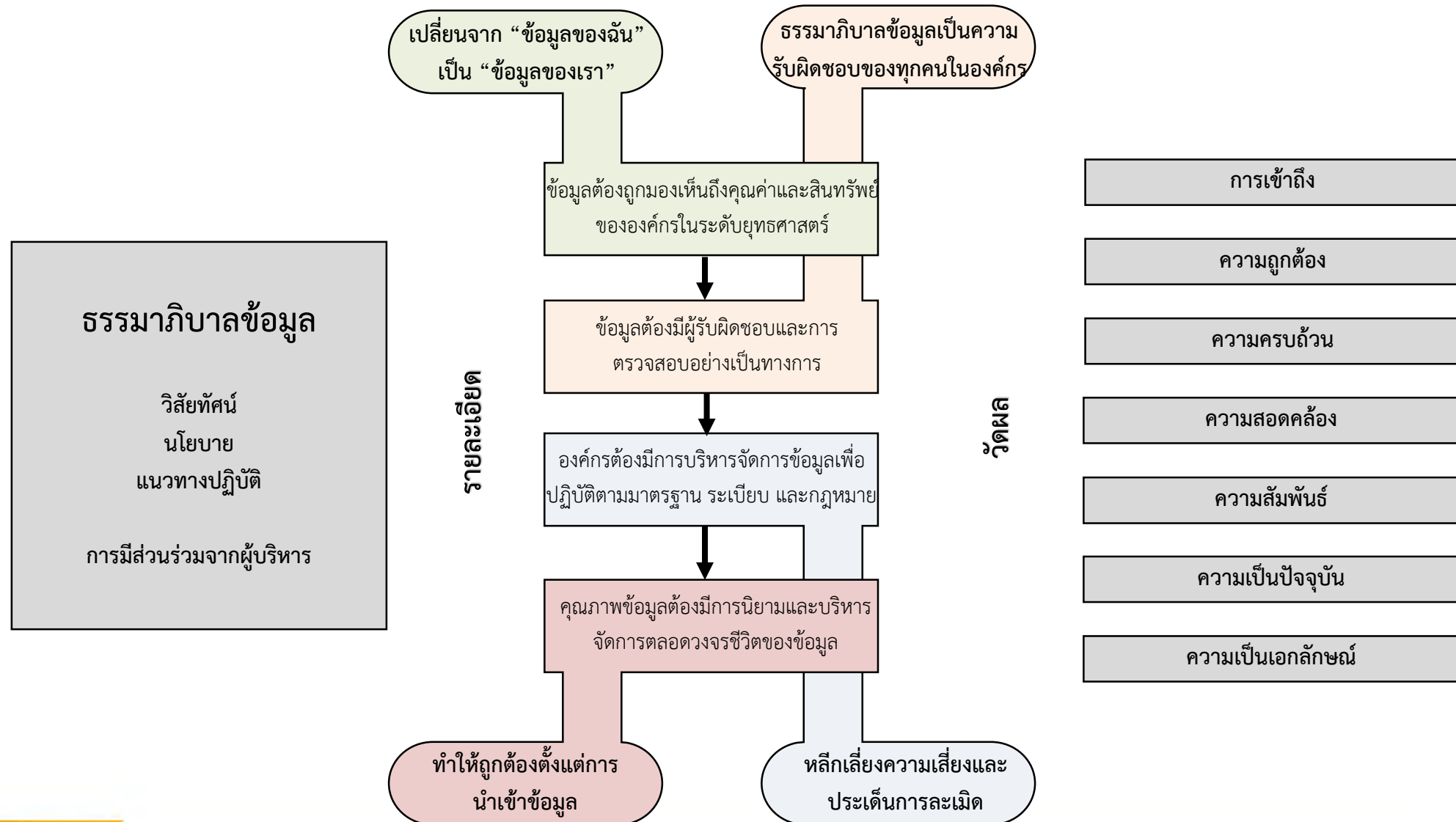
ต้องเป็น
จุดเริ่มต้น
ของการ
ตัดสินใจ
ลงทุนด้าน
เทคโนโลยี

เป็นการ
จัดการ
วงจรชีวิต
ข้อมูล

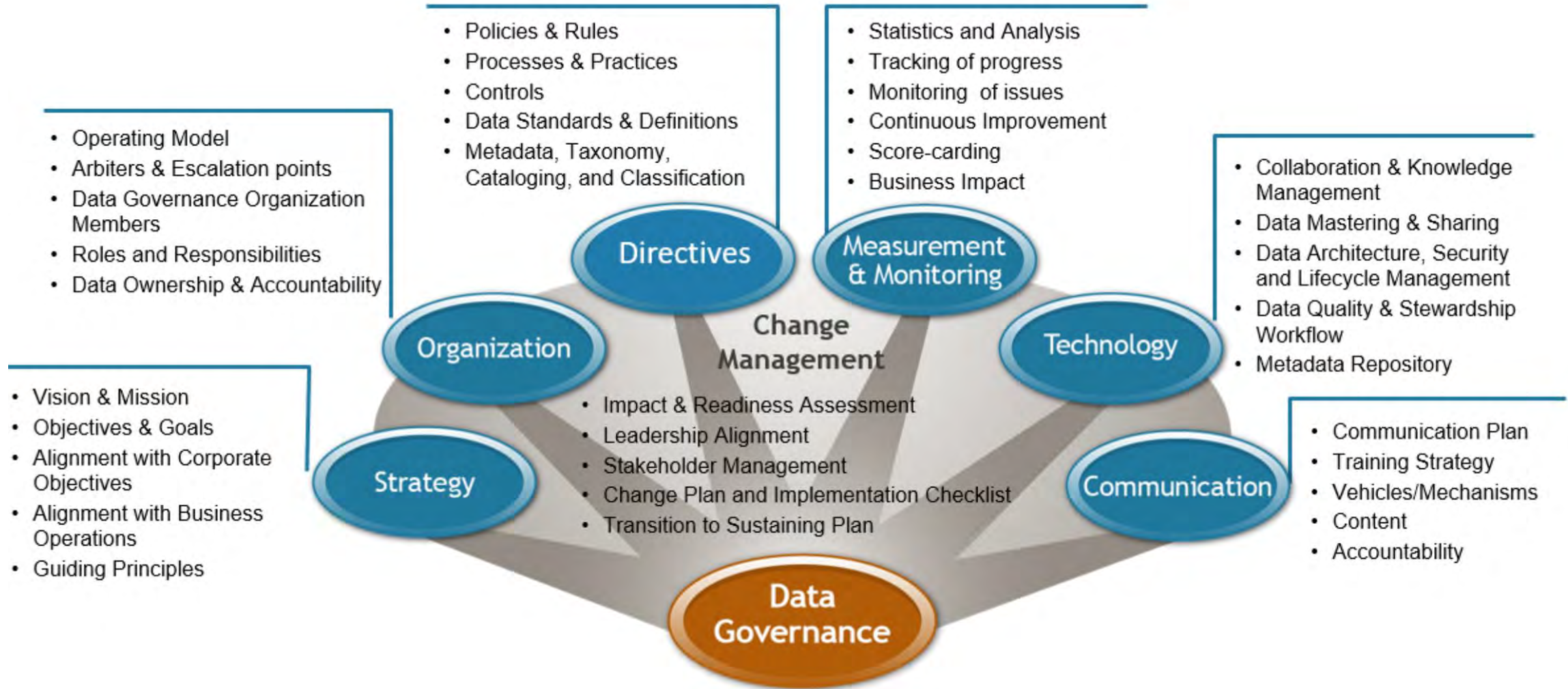
ต้อง
ร่วมมือกัน
หลายฝ่าย

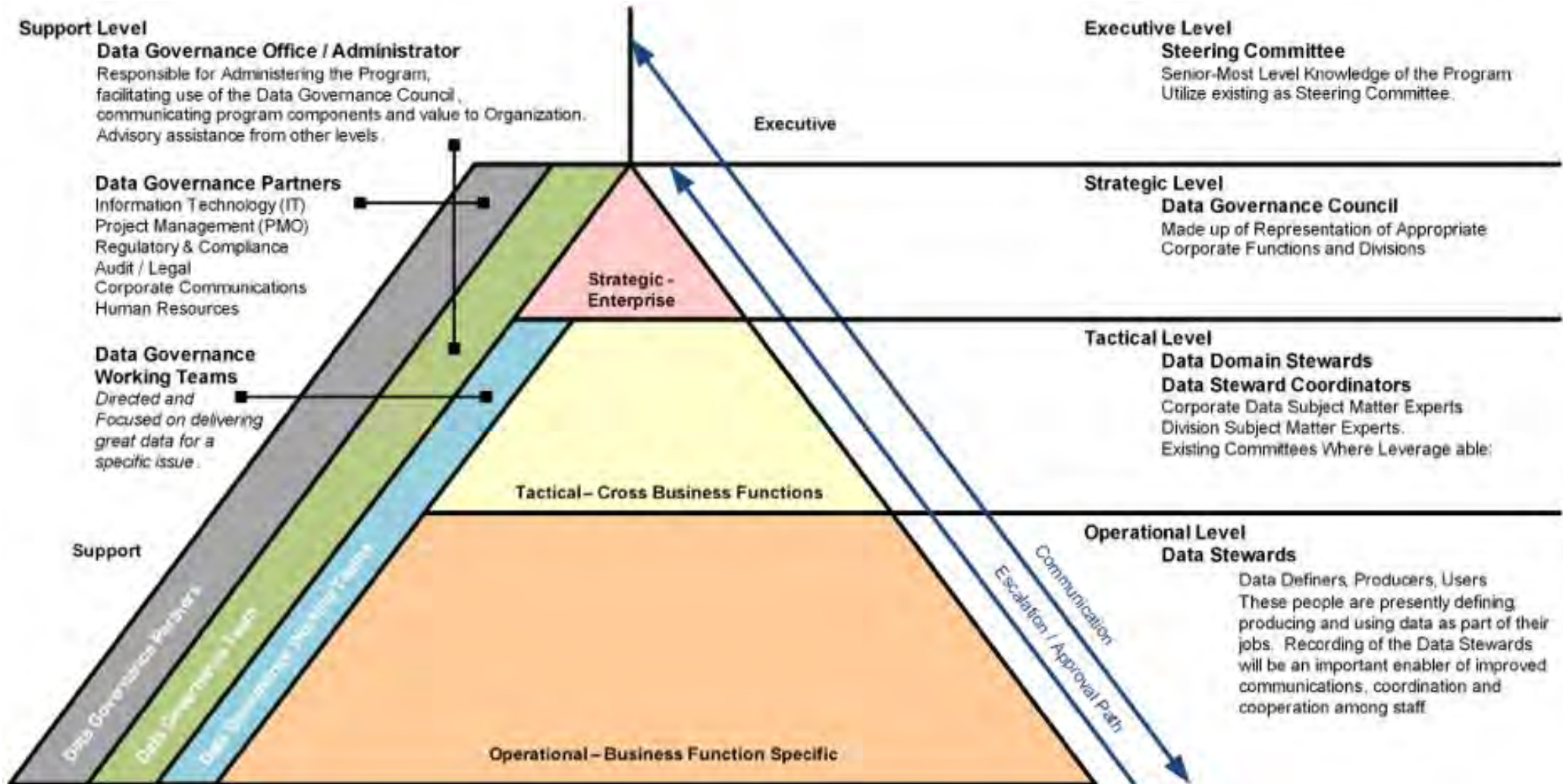
มองเป็น
ระดับ
องค์กร

ข้อมูลคือสินทรัพย์ขององค์กร



Components of Data Governance Framework





<https://tdan.com/data-governance-roles-and-responsibilities/24774>

DETAILED R&R'S FOR THE DATA STEWARD



Identify, Prioritize, Research & Recommend

- Provides context on how the data is managed as part of the business process
- Performs research and presents information on business usage of data (data SME for particular area / data set)
- Assists with determining priority and impact assessments for identified issues
- Makes / reviews recommendations for issue resolution
- Analyzes and makes recommendations on requested exceptions to established standards
- Helps identify data governance-related issues in workstream or within business areas



Define Data and Data Requirements

- Develops and maintains business definitions and transformations / calculations for in-scope data
- Coordinates with other Data Stewards to develop consistent definitions
- Assists in development and maintenance of business requirements / classifications of data (e.g., BoR, retention, security classification, etc.)
- Assists with developing Local Data Governance standards and processes
- Confirms application workstream and B/L alignment with approved standards
- Assist in verifying appropriate usage and distribution of in-scope data



Data Governance Knowledge & Awareness

- Serves as "champion" of Data Governance principles / topics within application workstream & business area
- Assists with development and delivery of Data Governance communications
- Initial point of contact on questions for B/L / application workstream
- Assists in identification of documentation and or process updates needed to respond to standards changes

Potential Future Activities



Data Quality Analysis

- Defines and assists with implementing specific data quality requirements
- Assists with analyzing and investigating data that does not align with requirements
- Capture and maintenance of specific meta data elements
- Assess adherence to other elements of established data standards
- Assists with periodic reporting on quality metrics
- Accountable for aspects of data quality

DG: Principles → Policy → Standards → Processes

Principles

- A statement that articulates Shared Organizational values, underlies strategic vision and mission, and serves as a basis for Integrated decision making

Policies

- Guidelines to manage the data lifecycle, access, integrity and administration that codify the governance standards and principles

Standards

- Standards consist of specific low level Mandatory controls that help enforce and support the data governance policy(s).

Processes

- Step by step activities to Implement policies and standards, Including requirements and monitoring

Creating policies

DGWG Lists
the req'd
Policies

Prioritize
based on
value or req't

Identify sub-
teams and
Assign

Reference the
Guiding
Principles

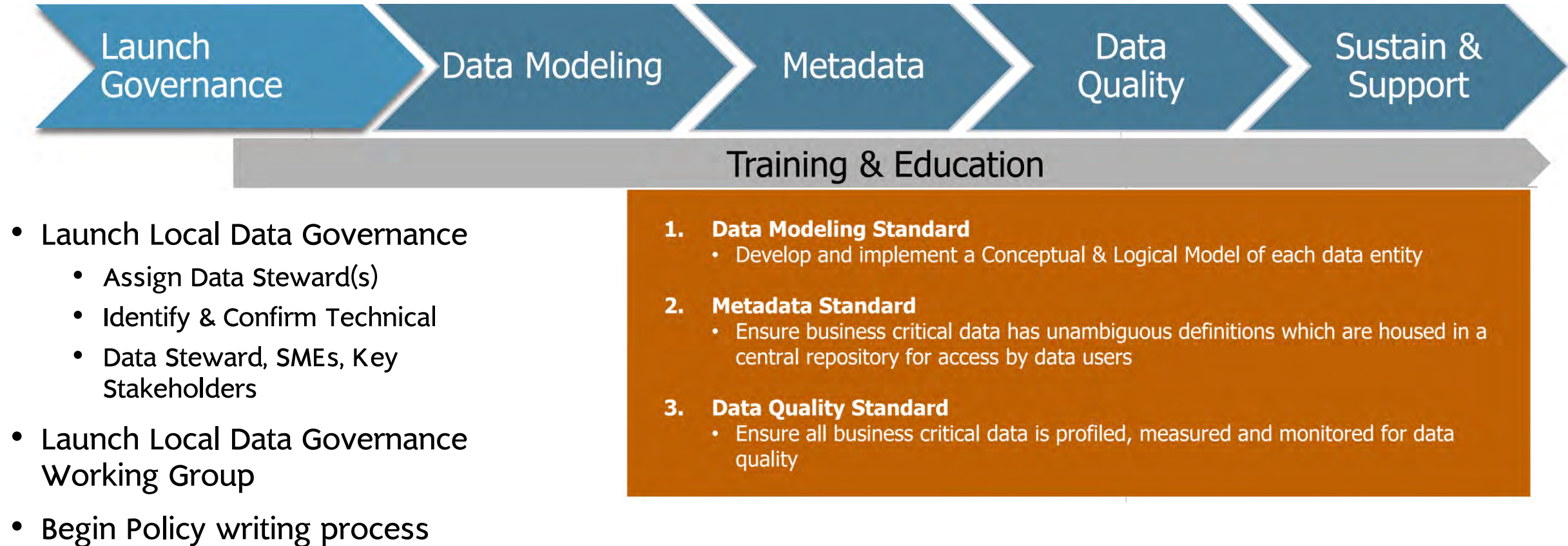
Ensure it's
measurable

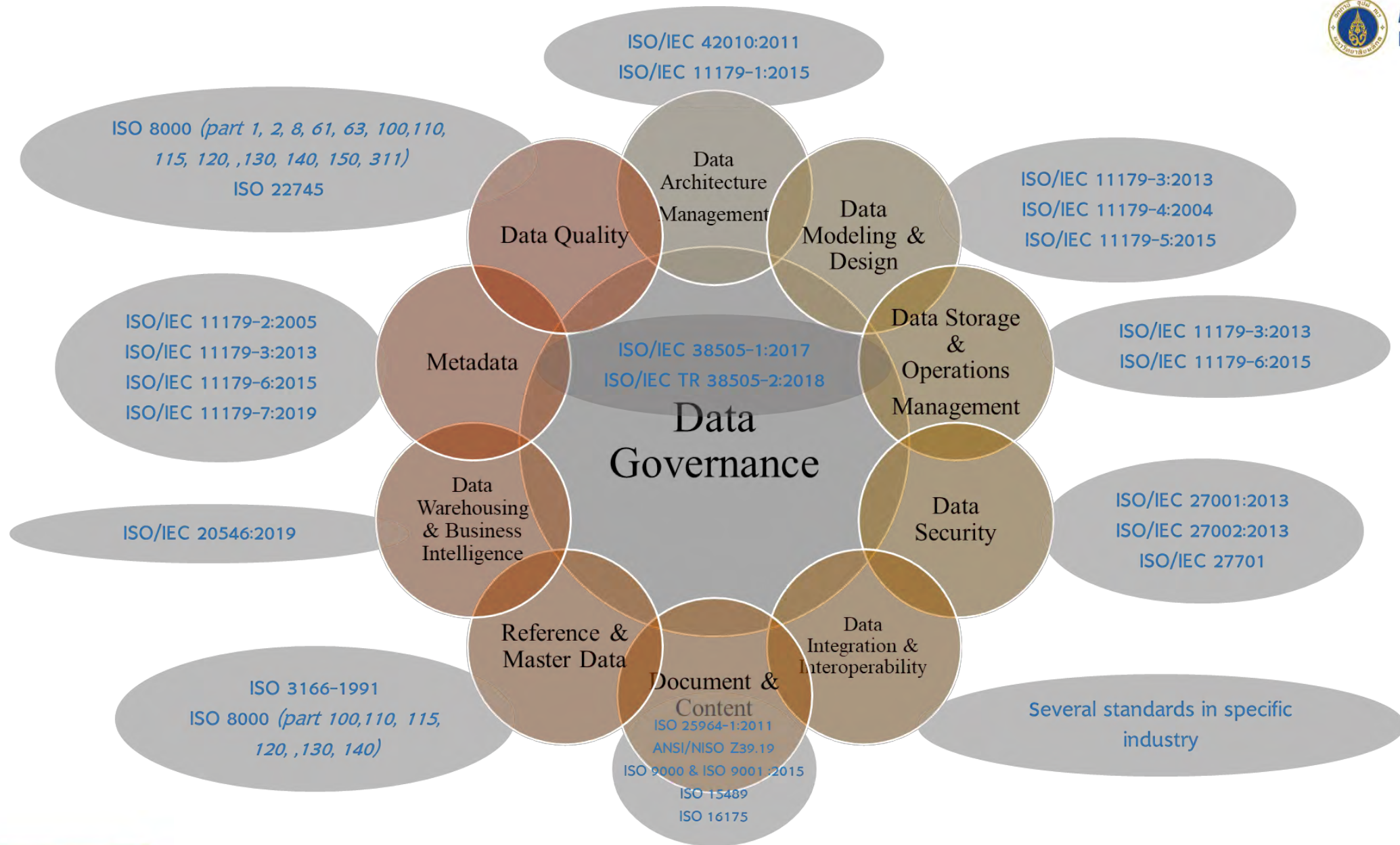
Write per the
Policy
Standard

- Components of policies

- Policy Statement
- Background/ policy rationale
- Policy Scope
- Roles & Responsibilities (RACI)
- Monitoring
- Escalation
- Governance/ Oversight
- Supporting Documents (Definition of Terms, Processes, Standards)

Link policies to the implementation plan





Is there a good cost / benefit case for the data? Is it being optimally used? Does it endanger people's safety or privacy, or the legal responsibilities of the enterprise? Does it support or contradict the corporate image or the corporate message?

Are Data Governance, Data Protection, and Data Security processes in place? What is the reputation of the data, and is it verified or verifiable?

Is the data comparable and compatible With other data? Does it have useful groupings and classifications? Can it be repurposed? Is it easy to manipulate?

Is it stable yet responsive to legitimate change requests?

Is the data understandable, simple, relevant, accessible, maintainable and at the right level of precision?



Common Causes of Data Quality Issues

Lack of Leadership

Data Entry Processes

Data Processing Functions

Issues Caused by System
Design

Issues Caused by Fixing
Issues

Data entry interface
issues

List entry placement

Field overloading

Training issues

Changes to business
processes

Inconsistent business
process execution

Incorrect assumptions
about data sources

Stale business rules

Changed data
structures

Failure to enforce referential
integrity

Failure to enforce uniqueness
constraints

Coding inaccuracies and gaps

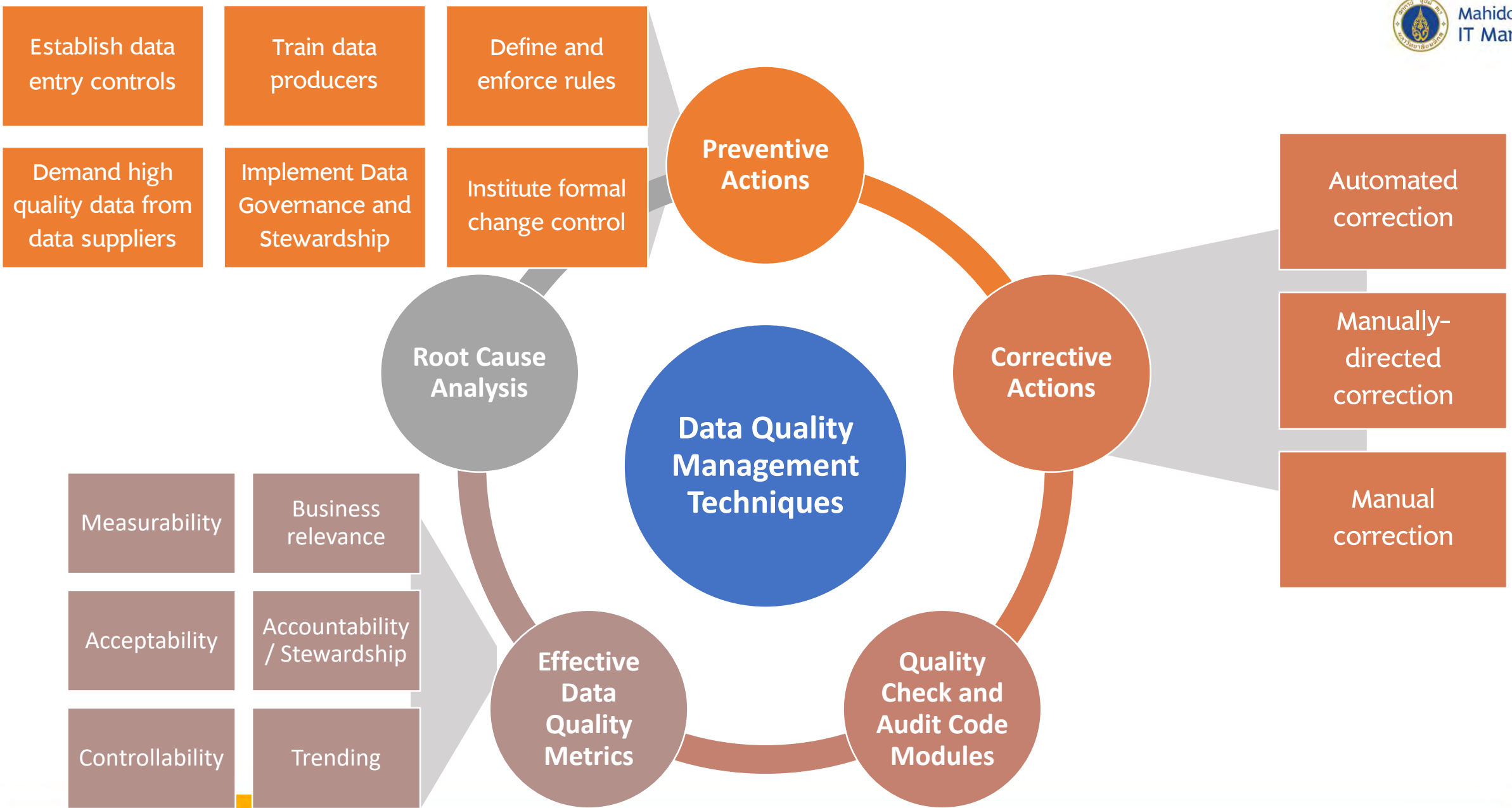
Data model inaccuracies

Field overloading

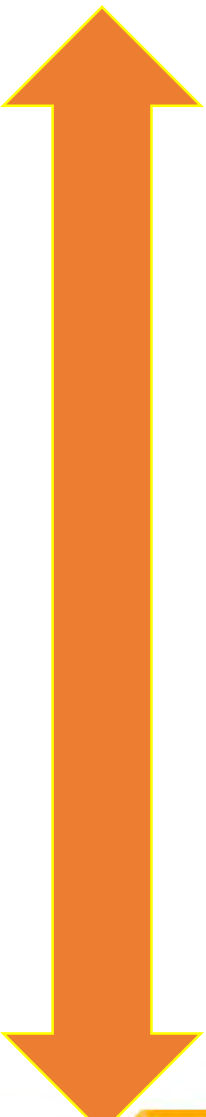
Temporal data mismatches

Weak Master Data
Management

Data duplication (Single vs
Multi- sources)



Master Data Management Lifecycle



Establishing the context of Master Data entities, including definitions of associated attributes and the conditions of their use. This process requires governance.

Identifying multiple instances of the same entity represented within and across data sources; building and maintaining identifiers and cross-references to enable information integration.

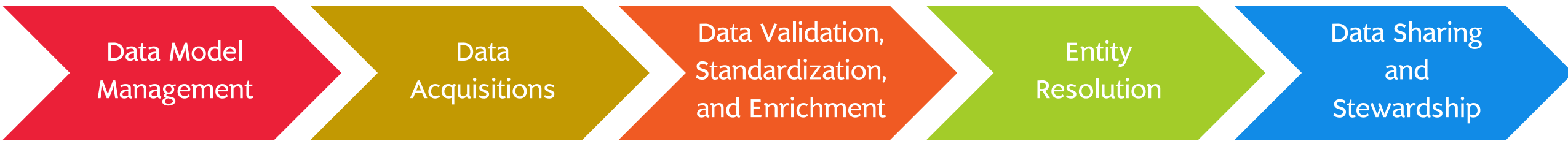
Reconciling and consolidating data across sources to provide a master record or the best version of the truth. Consolidated records provide a merged view of information across systems and seek to address attribute naming and data value inconsistencies.

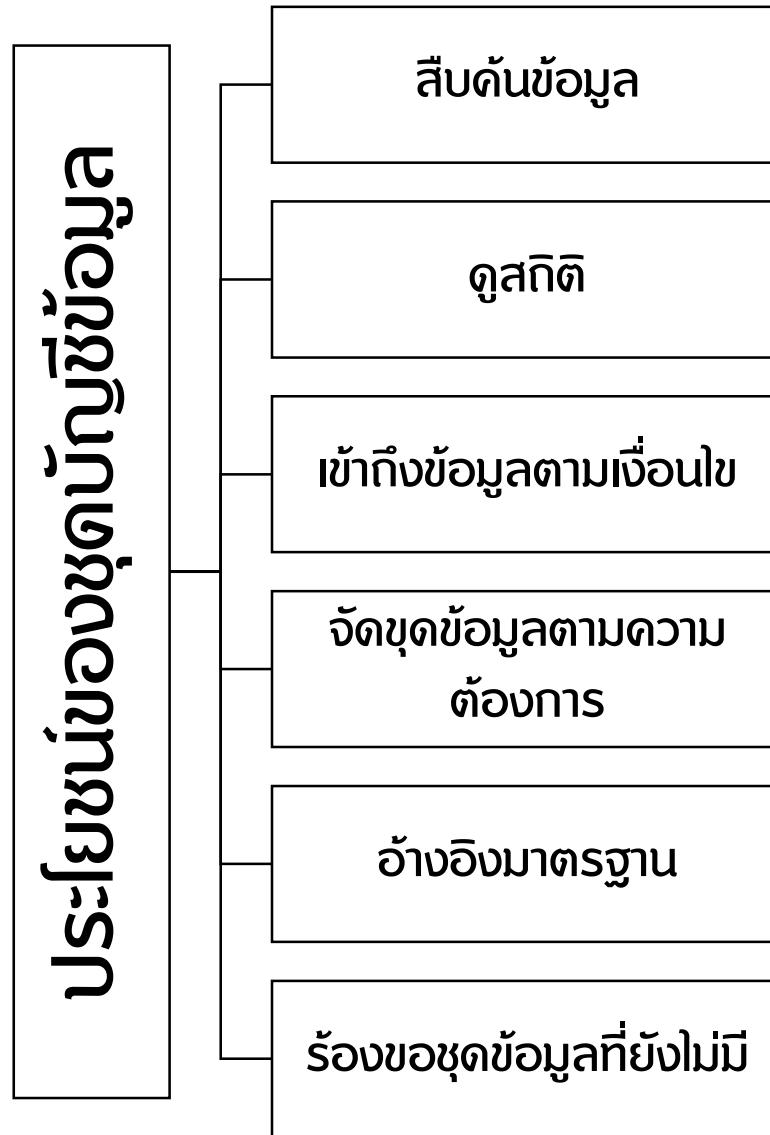
Identifying improperly matched or merged instances and ensuring they are resolved and correctly associated with identifiers.

Provisioning of access to trusted data across applications, either through direct reads, data services, or by replication feeds to transactional, warehousing or analytical data stores.

Enforcing the use of Master Data values within the organization. This process also requires governance and change management to assure a shared enterprise perspective.

Key Processing Steps for MDM





เมทาดาตาเชิงธุรกิจ (Mandatory) (1)

ตารางที่ ๑

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
					ข้อมูลทั่วไป	ข้อมูลสถิติ
๑	ประเภทข้อมูล	data_type	ชุดข้อมูลนี้เป็นข้อมูลประเภทใด	Code (Character ๑ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”	๒ = ข้อมูลระดับย่อย (Microdata)	๔ = ข้อมูลสถิติทางการ
๒	ชื่อชุดข้อมูล	Title	ชื่อของชุดข้อมูลที่กำหนดโดย องค์กรที่รับผิดชอบข้อมูล	Text (๑๕๐ Characters)	รายได้จากการท่องเที่ยว	จำนวนกำลังแรงงานรวม
๓	องค์กร	data_owner	ชื่อองค์กรที่รับผิดชอบข้อมูล	Text (๑๕๐ Characters)	สำนักงานปลัดกระทรวงการ ท่องเที่ยวและกีฬา	สำนักงานสถิติแห่งชาติ
๔	ชื่อผู้ติดต่อ	contact_person	ชื่อกอง สำนัก ฝ่าย หรือบุคคลที่ ได้รับการมอบหมายให้รับผิดชอบ ข้อมูล	Text (๑๕๐ Characters)	กลุ่มสารสนเทศด้าน เศรษฐกิจ	กองสถิติสังคม
๕	อีเมลผู้ติดต่อ	contact_email	อีเมลกอง สำนัก ฝ่าย หรือบุคคล ที่ได้รับการมอบหมายให้ รับผิดชอบข้อมูล	Text (๕๐ Characters)	bets@mots.go.th	slaborfs@nso.go.th
๖	คำสำคัญ	tag_string	หัวข้อ คำ วลี หรือแท็ก (tag) ที่ ใช้ระบุคำสำคัญในชุดข้อมูล	Text แยกแต่ละ keywords ด้วย “,” (comma) (๒๐๐ Characters)	รายได้, ท่องเที่ยว, จังหวัด	แรงงาน, กำลังแรงงาน

เมทาดาตาเชิงธุรกิจ (Mandatory) (2)

ตารางที่ ๑

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
					ข้อมูลทั่วไป	ข้อมูลสถิติ
๗	รายละเอียด	Notes	คำอธิบายรายละเอียดที่สำคัญของชุดข้อมูลอย่างสั้น เช่น คำนิยาม ชุดข้อมูลเกี่ยวกับอะไร มีวิธีการจัดเก็บแบบใด กลุ่มเป้าหมายผู้ใช้งานข้อมูลเป็นใคร	Text (๑,๐๐๐ Characters)	รายได้จากการท่องเที่ยว จําแนกรายจังหวัด	กำลังแรงงานรวม หมายถึงบุคคลทุกคนที่มี อายุ ๑๕ ปีขึ้นไป ในสัปดาห์แห่งการสำรวจเป็นผู้อยู่ในกำลังแรงงานปัจจุบัน และเป็นผู้ถูกจัดจําแนกอยู่ในประเภทกำลังแรงงานที่รอฤดูกาล
๘	วัตถุประสงค์	objective	อธิบายที่มาและวัตถุประสงค์ของการจัดทำชุดข้อมูล เช่น กฎหมายภารกิจ โครงการตามแผนยุทธศาสตร์ และเพื่อใช้ในการวิเคราะห์หรือตอบเจตยในประเด็นยุทธศาสตร์ในเรื่องใดที่ผู้ต้องการ	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”	๐๔ = แผนพัฒนาการ ท่องเที่ยวแห่งชาติ ฉบับที่ ๒ (พ.ศ. ๒๕๖๐-๒๕๖๔) ๑๑ = พันธกิจของ สป.กก. - เพื่อรายงานสถานการณ์ ด้านการท่องเที่ยว	๑๐ = กฎกระทรวง ๑๑ = พันธกิจของสำนักงาน สถิติแห่งชาติ - เพื่อประมาณจำนวนและ ลักษณะของกำลังแรงงาน ภายในประเทศ
๙.๑	หน่วยความถี่ของการปรับปรุงข้อมูล	update_frequency _unit	สำหรับข้อมูลทะเบียน ข้อมูลระดับย่อย และข้อมูลภูมิสารสนเทศเชิงพื้นที่ : ความถี่ที่ข้อมูลในระบบคลังข้อมูลถูกปรับปรุง/เพิ่ม หรือเปลี่ยนแปลง สำหรับข้อมูลสถิติทั่วไปและสถิติทางการ : ความถี่ในการเผยแพร่ต่อผู้ใช้ข้อมูล	Code (Character ๑ digits (A-Z)) ดูรายละเอียด “ภาคผนวก ข.”	A	M

เมทาดาตาเชิงธุรกิจ (Mandatory) (3)

ตารางที่ ๑

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
					ข้อมูลทั่วไป	ข้อมูลสถิติ
๙.๒	ค่าความถี่ของการปรับปรุงข้อมูล	update_frequency_interval	ใช้คุณสมบัตินี้ประกอบกับหน่วยความถี่ในการปรับปรุงข้อมูล ตัวอย่างเช่น ถ้าชุดข้อมูลมีการปรับปรุงทุก ๆ ๒ ปี ท่านสามารถใส่ “๒” สำหรับค่าความถี่ และ “รายปี” สำหรับหน่วยความถี่	Number หรือ เว้นว่างไว้	๒	๑
๑๐	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	geo_coverage	สำหรับข้อมูลทะเบียน ข้อมูลระดับย่อย และข้อมูลภูมิสารสนเทศเชิงพื้นที่: มิติการจัดจำแนกข้อมูลพื้นที่ในระดับย่อยสุดที่ในการจัดเก็บข้อมูล สำหรับข้อมูลสถิติทั่วไปและสถิติทางการ: มิติการจัดจำแนกข้อมูลพื้นที่ในระดับย่อยสุดที่ในการนำเสนอข้อมูล	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”	๐๖ = จังหวัด	๐๖ = จังหวัด
๑๑	แหล่งที่มา	data_source	แหล่งที่มาของข้อมูลที่น่ามาจัดทำชุดข้อมูล พร้อมหน่วยงานที่จัดทำ เช่น สํารวจภาวะการทำงานของประชากร (สำนักงานสถิติแห่งชาติ) ฐานข้อมูลทะเบียนราษฎร (กรมการปกครอง)	Text (๒๐๐ Characters)	รายงานสถานการณ์ด้านการท่องเที่ยว	สำรวจภาวะการทำงานของประชากร (สำนักงานสถิติแห่งชาติ)

เมทาดาตาเชิงธุรกิจ (Mandatory) (4)

ตารางที่ ๑

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
					ข้อมูลทั่วไป	ข้อมูลสถิติ
๑๒	รูปแบบการเก็บข้อมูล	data_format	รูปแบบของการจัดเก็บข้อมูล	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”	๐๒ = csv ๐๗ = text	๐๑ = Database ๑๐ = XLS ๐๗ = text ๙๙ = อื่นๆ ระบุ SPSS
๑๓	หมวดหมู่ข้อมูลตามธรรมชาติ ตามธรรมชาติ ภาคีข้อมูล ภาคีข้อมูล	data_category	หมวดหมู่ข้อมูลตามธรรมชาติ ข้อมูลภาคี	Code (Character ๑ digits (๑-๙)) ดูรายละเอียด “ภาคผนวก ข.”	๑ = ข้อมูลสาธารณะ	๑ = ข้อมูลสาธารณะ
๑๔	สัญญาอนุญาตให้ใช้ข้อมูล	right_of_usage	สัญญาอนุญาตให้ใช้ข้อมูล ต้องสอดคล้องกับหมวดหมู่ข้อมูลตามธรรมชาติข้อมูลภาคี	Code (Character ๑ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”	๑ = DGA Open Government License	๗ = License not specified

เมทาดาตาเชิงธุรกิจ (Optional – ประเภทข้อมูลระดับย่อย)

ตารางที่ ๒

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
๑๕	เงื่อนไขในการเข้าถึงข้อมูล	accessible_condition	เงื่อนไขเพื่อให้สามารถเข้าถึงหรือใช้ข้อมูลได้ ในกรณีที่เลือกหมวดหมู่ข้อมูลตามธรรมชาติข้อมูลภาครัฐในรายการที่ ๑๓ เป็นข้อมูลความมั่นคง ข้อมูลความลับทางราชการ ข้อมูลส่วนบุคคล	ในกรณีรายการที่ ๑๓ เป็นข้อมูลสาธารณะ กำหนดเป็นค่า “ไม่มี” ในกรณีที่รายการที่ ๑๓ ไม่ใช่ข้อมูลสาธารณะ กำหนดเป็นค่า “มี” พร้อมระบุเงื่อนไขในการเข้าถึงข้อมูล
๑๖	วันที่เริ่มต้นสร้าง	created_date	วัน เดือน ปี ที่เริ่มต้นสร้างหรือจัดทำข้อมูล โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.
๑๗	วันที่ทำการปรับปรุงข้อมูลล่าสุด	last_updated_date	วัน เดือน ปี ที่มีการปรับปรุงหรือเผยแพร่ข้อมูลล่าสุด โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.
๑๘	URL	url	URL ที่สามารถเข้าถึงชุดข้อมูลได้	Text (๑๐๐ Characters)
๑๙	ผู้สนับสนุนหรือผู้ร่วมดำเนินการ	data_support	องค์กรสนับสนุนหรือร่วมดำเนินการ นอกเหนือจากองค์กรที่รับผิดชอบข้อมูล	Code (Character ๑ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”
๒๐	หน่วยที่ย่อยที่สุดของการจัดเก็บข้อมูล	data_collect	หน่วยที่ย่อยที่สุดของการจัดเก็บข้อมูล เช่น บุคคล สถานประกอบการ ประเทศ	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”
๒๑	ภาษาที่ใช้	data_language	ภาษาที่ใช้ในชุดข้อมูล เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”
๒๒	ชุดข้อมูลที่มีคุณค่าสูง	high_value_dataset	ชุดข้อมูลที่มีคุณค่าสูง โดยหน่วยงานที่นำเข้าข้อมูลไม่ต้องการ	BOOLEAN (เป็น และ ไม่เป็น)
๒๓	ข้อมูลอ้างอิง	reference_data	ข้อมูลอ้างอิง โดยหน่วยงานที่นำเข้าข้อมูลไม่ต้องการ	BOOLEAN (เป็น และ ไม่เป็น)

เมทาดาตาเชิงธุรกิจ (Optional – ประเภทข้อมูลสถิติ) (1)

ตารางที่ ๓

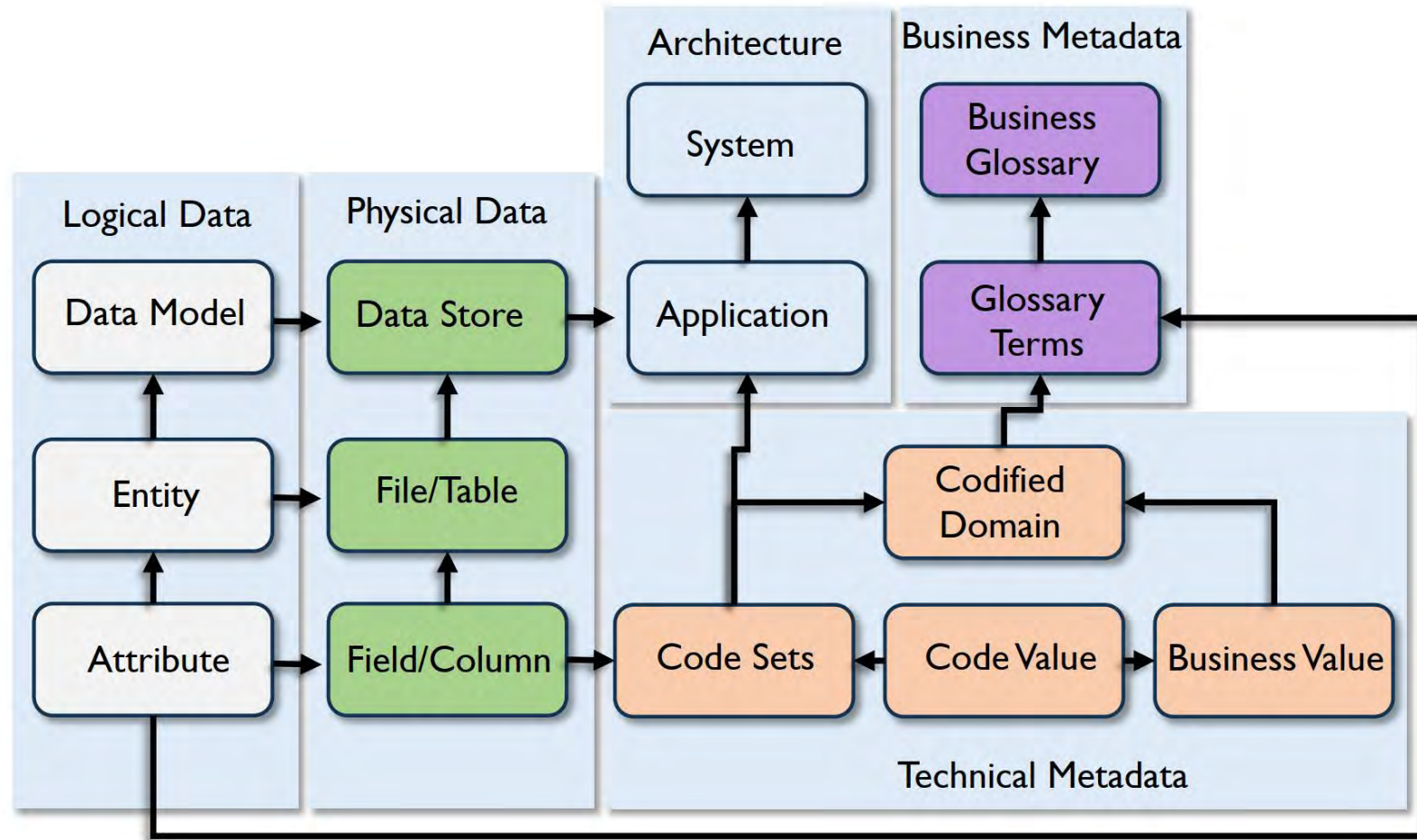
No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
๑๕	เงื่อนไขในการเข้าถึงข้อมูล	accessible_condition	เงื่อนไขเพื่อให้สามารถเข้าถึงหรือใช้ข้อมูลได้ ในกรณีที่เลือกหมวดหมู่ข้อมูลตามธรรมชาติตามข้อมูลภาครัฐในรายการที่ ๑๓ เป็นข้อมูลความมั่นคง ข้อมูลความลับทางราชการ ข้อมูลส่วนบุคคล	ในกรณีรายการที่ ๑๓ เป็นข้อมูลสาธารณะ กำหนดเป็นค่า “ไม่มี” ในกรณีที่รายการที่ ๑๓ ไม่ใช่ข้อมูลสาธารณะ กำหนดเป็นค่า “มี” พร้อมระบุเงื่อนไขในการเข้าถึงข้อมูล
๑๖	ปีข้อมูลที่เริ่มต้นจัดทำ	first_year_of_data	ปีข้อมูลที่เริ่มต้นจัดทำ ในกรณีความถี่ในการจัดทำมากกว่าปีละครั้ง ให้ระบุ วันที่หรือเดือนหรือไตรมาสที่เริ่มต้นจัดทำ เช่น มี.ค./๒๕๔๐	DATE: YYYY-MM-DD โดยในกรณีที่ไม่สามารถระบุวัน หรือเดือน ให้แสดงเฉพาะปี (ในรูปแบบปี พ.ศ.) หรือเดือนที่เลือก
๑๗	ปีข้อมูลล่าสุดที่เผยแพร่	last_year_of_data	ปีข้อมูลล่าสุดที่เผยแพร่ ในกรณีที่ความถี่ในการเผยแพร่มากกว่าปีละครั้ง ให้ระบุ วันที่หรือเดือนหรือไตรมาสล่าสุดที่เผยแพร่ เช่น มี.ค./๒๕๖๒	DATE: YYYY-MM-DD โดยในกรณีที่ไม่สามารถระบุวัน หรือเดือน ให้แสดงเฉพาะปี (ในรูปแบบปี พ.ศ.) หรือเดือนที่เลือก
๑๘	วันที่กำหนดเผยแพร่ข้อมูล	data_release_calendar	แสดงกำหนดการเผยแพร่วัน เดือน ปี หรือในกรณีที่ สามารถระบุเป็นชั่วโมงหรือนาทีได้ให้ระบุ ทั้งนี้ขึ้นกับลักษณะของสถิติทางการ	DATETIME: YYYY-MM-DD-hh-mm ในกรณีกำหนดการเผยแพร่เป็น ปี-เดือน-วัน-ชั่วโมง-นาที หากสามารถระบุได้ชัดเจน หรือ ระบุ..... ในกรณีที่ไม่สามารถกำหนดเป็นวันเวลาที่ชัดเจน เช่น ทุกวันที่ ๓ ของเดือน หรือ เวลา ๙.๐๐ น. ของวันที่ ๑ ของทุกเดือน เป็นต้น
๑๙	วันที่ทำการปรับปรุงข้อมูลล่าสุด	last_updated_date	วัน เดือน ปี ที่มีการปรับปรุงหรือเผยแพร่ข้อมูลล่าสุด โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.

เมทาดาทาเชิงธุรกิจ (Optional – ประเภทข้อมูลสถิติ) (2)

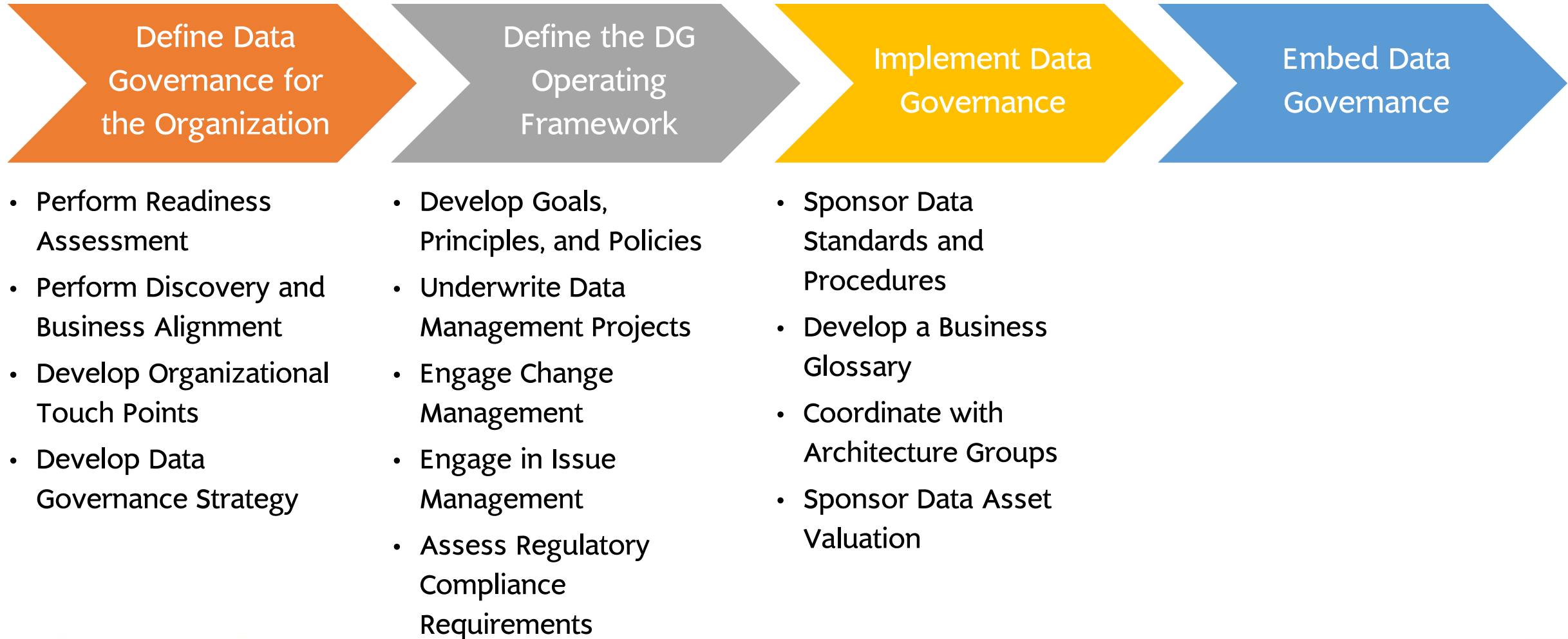
ตารางที่ ๓

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
๒๐	การจัดจำแนก	disaggregation	การจัดจำแนกที่ใช้ในการจัดทำสถิติทางการ เช่น เพศ อายุ ศาสนา ระดับการศึกษา อาชีพ ประเทศ	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”
๒๑	หน่วยวัด	unit_of_measure	หน่วยนับจำนวน เช่น บาท ไร่ ครัวเรือน คน คดี ขึ้น อัน เครื่อง งาน กิโลกรัม กิโลเมตร ต่อประชากร ๑,๐๐๐ คน หรือไม่มีหน่วยในกรณีที่เป็นดัชนี	Text (๑๐๐ Characters)
๒๒	หน่วยตัวคูณ	unit_of_multiplier	ตัวคูณของหน่วยวัด เช่น ข้อมูลมูลค่าการลงทุน หน่วย: ล้านบาท หน่วยวัดคือ บาท หน่วยตัวคูณคือ ๑ ล้าน	Code (Character ๒ digits (๐-๙)) ดูรายละเอียด “ภาคผนวก ข.”
๒๓	วิธีการคำนวณ	calculation_method	วิธีการคำนวณหรือสูตรในการคำนวณที่ใช้ในการจัดทำสถิติหรือตัวชี้วัด	Text (๕๐๐ Characters)
๒๔	มาตรฐานการจัดทำข้อมูล	standard	มาตรฐานต่างๆ ทั้งที่เป็นมาตรฐานสากลและมาตรฐานในประเทศที่นำมาใช้อ้างอิงในการจัดทำสถิติทางการทั้งวิธีการจัดทำ รหัส การเผยแพร่ เช่น มาตรฐานการจัดทำตามSNA, มาตรฐาน ISO, มาตรฐานรหัสTSIC, มาตรฐานรหัสHS มาตรฐานการเผยแพร่ SDDS	Text (๒๐๐ Characters)
๒๕	URL	url	URL ที่สามารถเข้าถึงชุดข้อมูลได้	ใช้คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: <u>ประเภทข้อมูลทะเบียนและข้อมูลระดับย่อย</u> ในรายการที่ ๑๘ URL
๒๖	ภาษาที่ใช้	data_language	ภาษาที่ใช้ในชุดข้อมูล เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	ใช้คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: <u>ประเภทข้อมูลทะเบียนและข้อมูลระดับย่อย</u> ในรายการที่ ๒๑ ภาษาที่ใช้

Example Metadata Repository Metamodel



Data Governance Activities





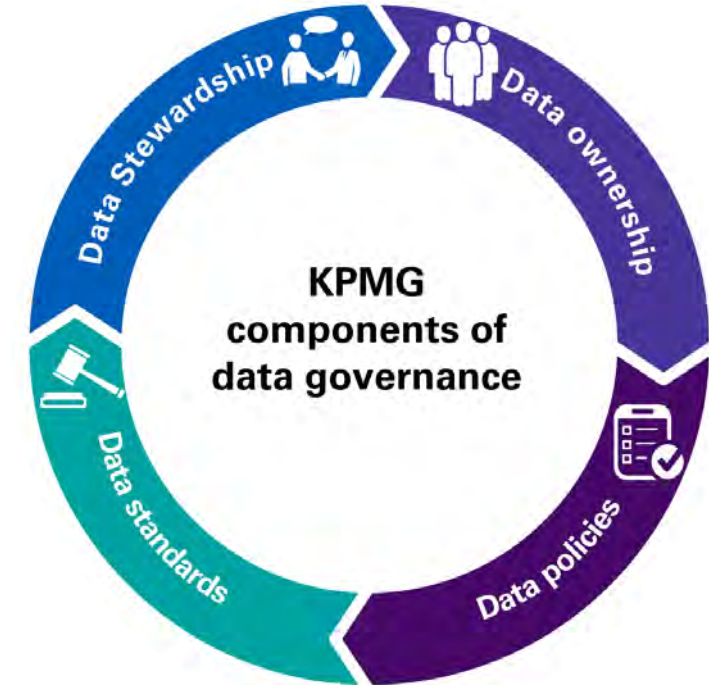
Data governance: Driving value in healthcare

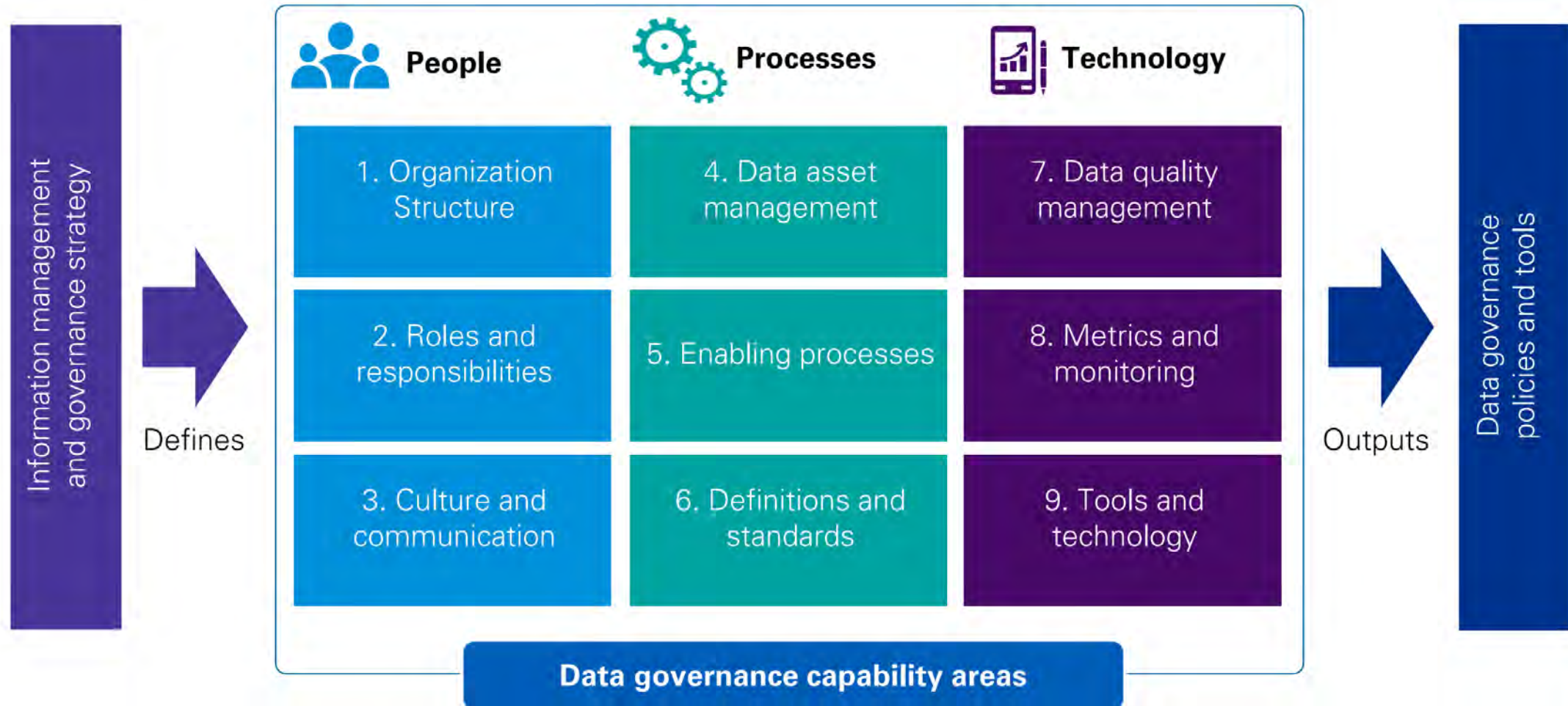
KPMG International

kpmg.com/healthcare



1	Data Stewardship is the accountability for the management of data assets. Data Stewards do not own the data, but instead are the caretakers of the enterprise data assets, ensuring the quality, accuracy and security of the data.
2	Data ownership is the responsibility for the creation of the data and the enforcement of enterprise business rules. It constrains or defines data use in the organization.
3	Data policies are the rules that an enterprise utilizes to manage its data assets, including enforcing authentication and access rights to data and compliance with laws and regulations.
4	Data standards are the precise criteria, specifications and rules for the definition, creation, storage and usage of data within an organization.



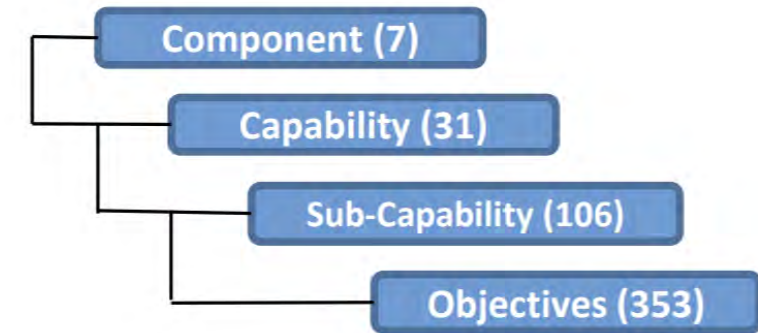
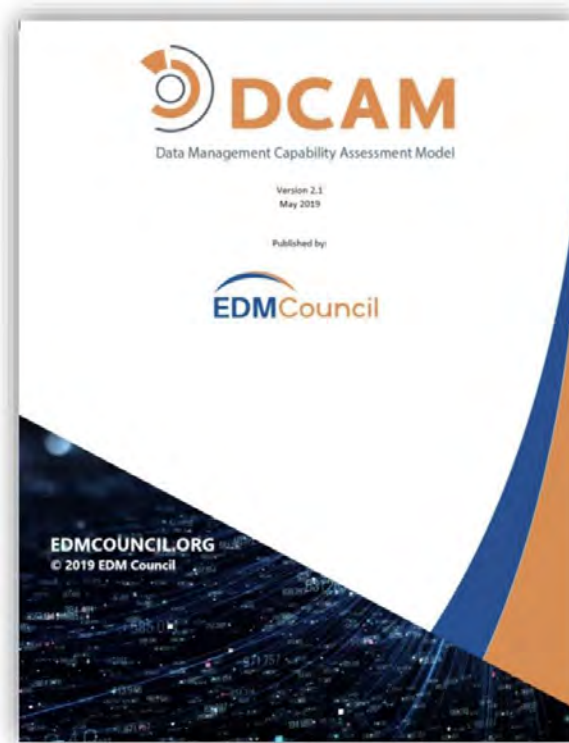


Capability areas		Aware DG vision, investment, and commitment yet to be identified	Tactical Some siloed DG initiatives; no true sponsor	Focused Stronger focus and commitment to DG, driving specific initiatives	Strategic Clearly defined DG strategy with executive sponsorship	Pervasive Pervasive DG and data oriented culture	Capability levels
		Level1	Level 2	Level 3	Level 4	Level 5	
Organization structure	Informal	Awareness of the purpose and importance of data governance	Limited to separate, internal business units	Formalized data governance team structure and model	C-level presence and support	Chief Data Officer function or equivalent	Formalized and integrated
Roles and responsibilities	Uncoordinated/independent	DG resources not clearly defined at the organizational level	Siloed of data governance responsibilities	Pool of subject matter experts supports organizational initiatives and needs	Defined data stewards, data owners, and data consumers	Accountability and connectivity of roles, vertically and horizontally	Formalized enterprise level accountability
Culture & communication	Closed/opaque	Individual responsibility to maintain commitment to DG vision	Disconnected communities of practice across business units	Established internal customer service function	Open, accessible, and transparent processes, stewards, and resources	Cultural shift towards continuous improvement of data governance	Open/transparent
Data asset management	Uncatalogued/disorganized	Poor understanding of data assets and their ownership	Individual businesses maintain disjointed catalogs of their own data assets	Standardized management of data assets across business units	Standardized management of enterprise-level data catalog	Maintenance plan in place that can handle growth in volume and complexity of data	Enterprise-wide cataloguing
Enabling processes	External integrity/ non standardized	Unclear/poorly-managed informal processes	Defined response times to data requests	Pathways for new data assets, with clear processes and approvals	Enable multi-level access definition to data under management	Data Governance 'as-a-Service' model within the organization	External & internal integrity/standardized
Definitions & standards	Variable/poorly understood	Inconsistent adherence to industry standards	Incentivized adoption of industry standards where possible	Appropriate usage guidelines for data sources aligned to standards	Openly accessible metadata resources, data standards, and policies	Collaborative process in place to manage data assets and common taxonomies	Well defined/accessible
Data quality management	Unreliable/imprecise	No rigorous or reliable processes in place for maintaining data quality	Business units assume individual responsibility for data quality	Documented measures of data quality and scope of application	Ability to affect changes in source system to maintain data quality	DG representation in organization's Change Advisory Boards	Reliable/trustworthy
Metrics & monitoring	Impromptu/ as needed	Inconsistent identification of quality metrics within or across business units	Monitoring of key metrics at the business unit level	Support growth of real-time systems, especially clinical decision support	Standard reporting and real-time dashboard of data quality measures	Automated data quality monitoring and detection capability	Planned/disciplined
Tools & technology	Siloed/ disparate tools	Disparate tools used across units, with no consideration for DG implications	Individual units assess new toolsets in context of benefit to DG improvement	Solution architecture incorporates data quality and access controls	Easily-accessible system to record breaches and suggestions for improvements	Framework and policies address cloud-based or managed services	Integrated solution

Data Management Maturity Assessment (DCAM)

<https://edmcouncil.org/>

- Integration of key data management disciplines
 - Data Management Strategy
 - Program Design
 - Organizational Change
 - Dedicated Funding
 - Data Engineering
 - Technology Architecture
 - Governance
 - Collaboration



Model is made up of 7 components.

- Each components is made up of a series of capabilities
- Each capability is made up of a series of sub-capabilities
- Each sub-capability is defined by a series of objectives
- All supported by artifacts of evidence

7 Components of the Data Management Capability

Assessment Model

Component 1.0

Defines the vision and the purpose of the data management program – why is data management important

Component 2

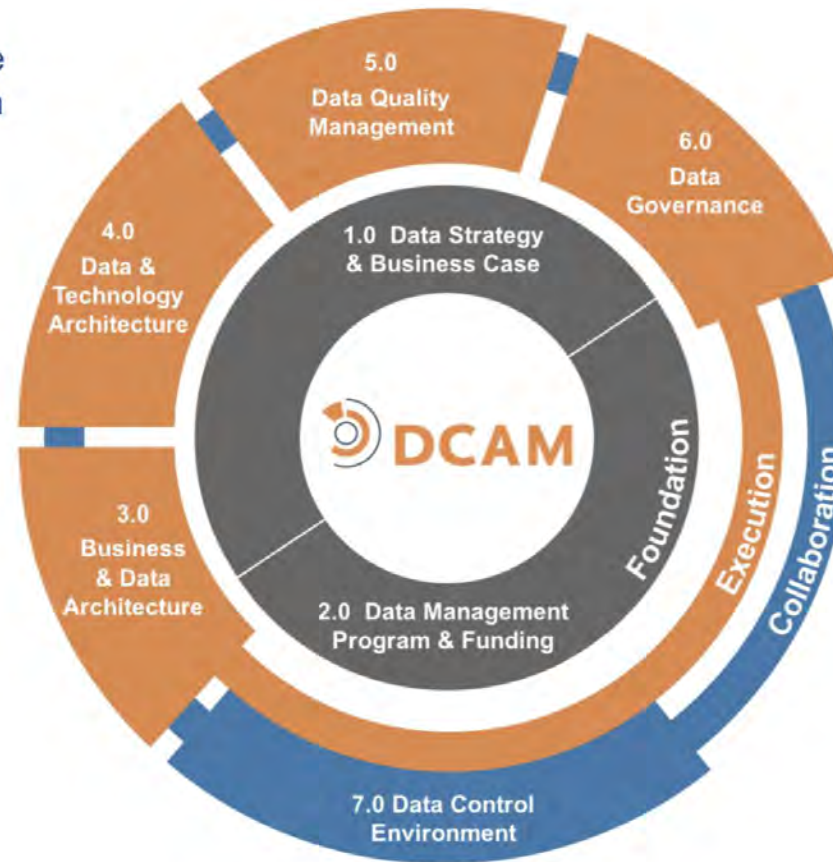
Describes the organizational structure and funding model of the data management program

Component 3.0

Data architecture is the design of information content, driven by business architecture (requirements), aligned to real-world objects and entities

Component 4.0

Technology architecture addresses the physical implementation of data management (platforms, DBs, tool), in collaboration with the business and the data management office



Component 5.0

Deliver data that is trusted and fit-for-purpose, where users have confidence that the data is what they need, without reconciliation

Component 6.0

The rules of engagement for data management, focused on the implementation of policies, standards and operational procedures necessary to ensure that stakeholders *behave*

Component 7.0

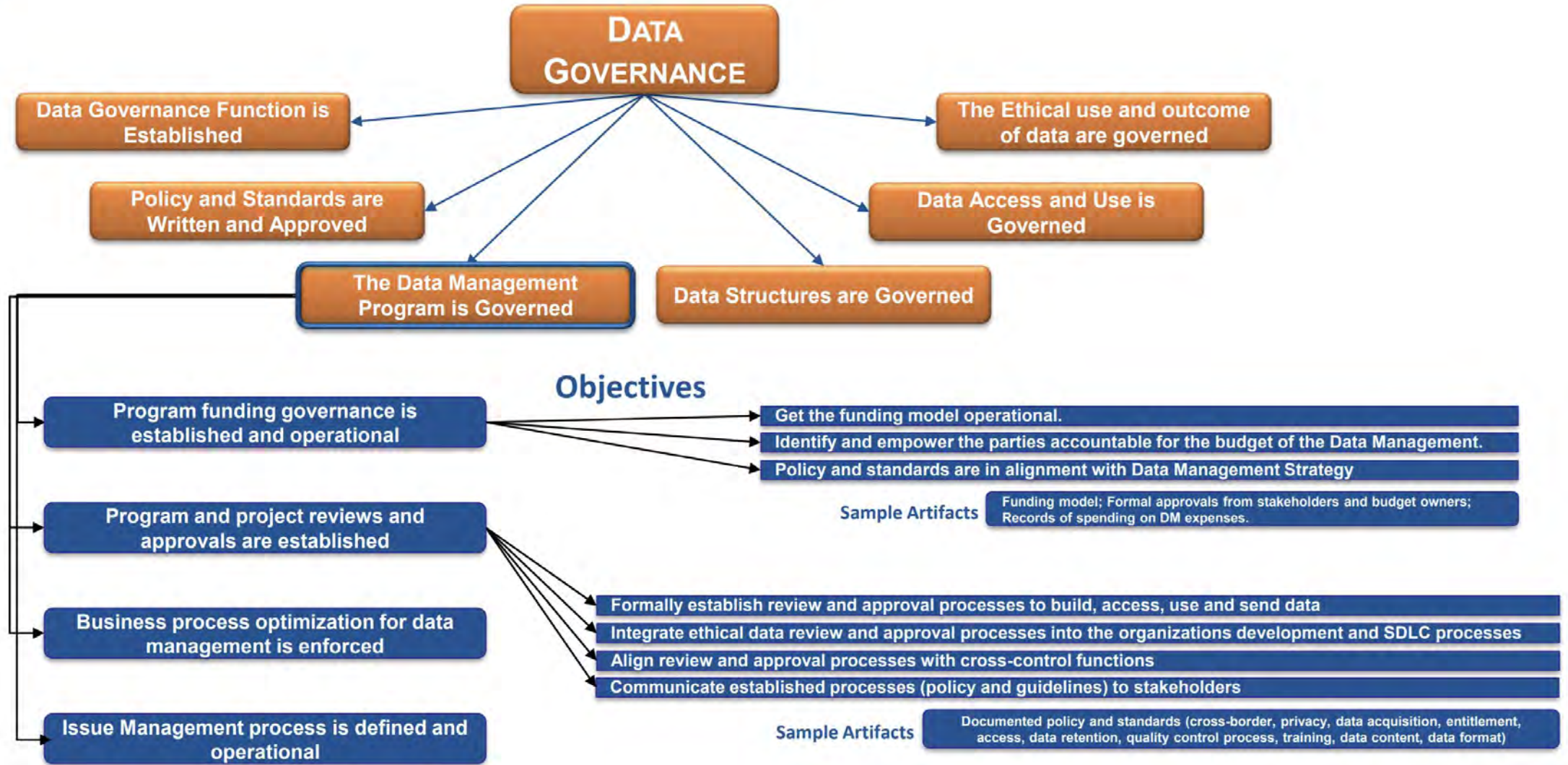
A true *control environment* cannot be achieved until all the data management capabilities are operating collaboratively and in unison across the enterprise

DCAM COMPONENT STRUCTURE

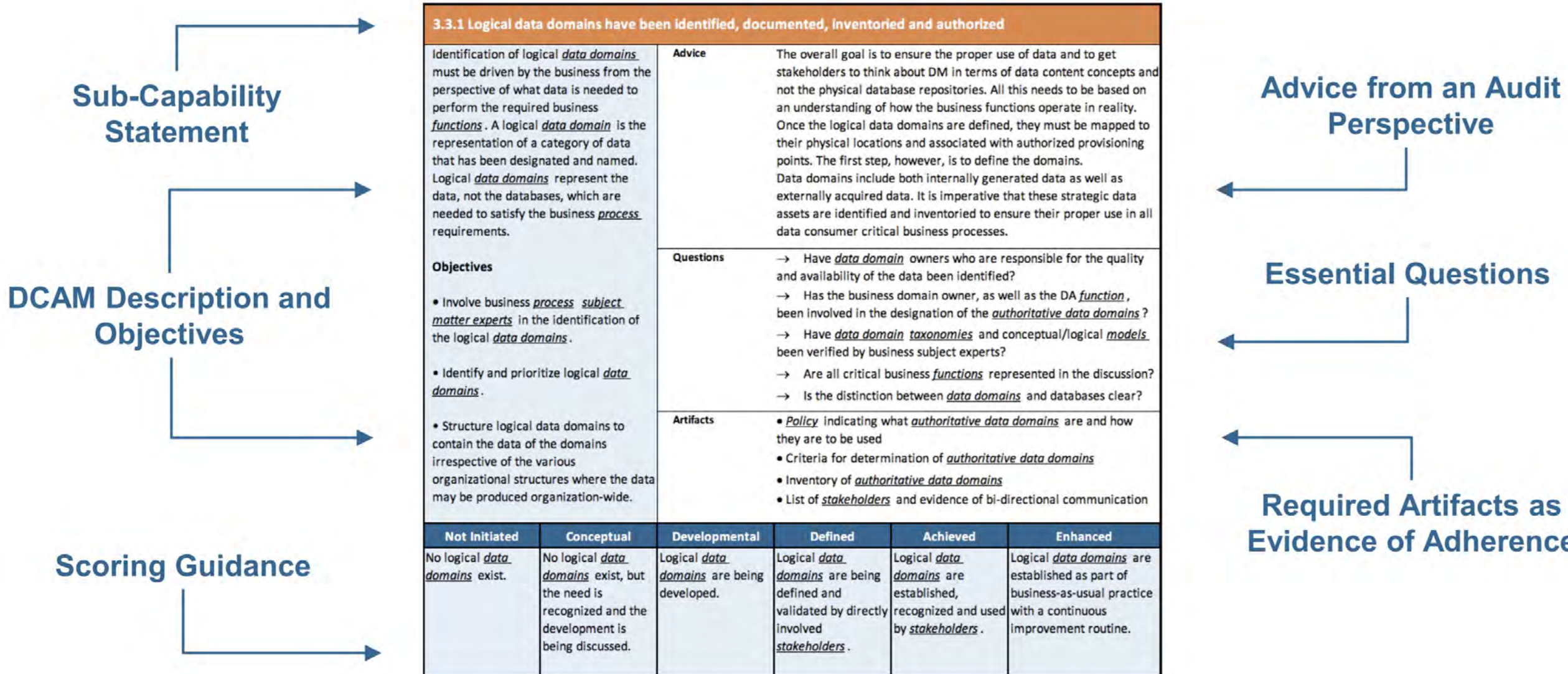
Component

Capability

Sub-Capability



DCAM – DATA CAPABILITY ASSESSMENT MODEL

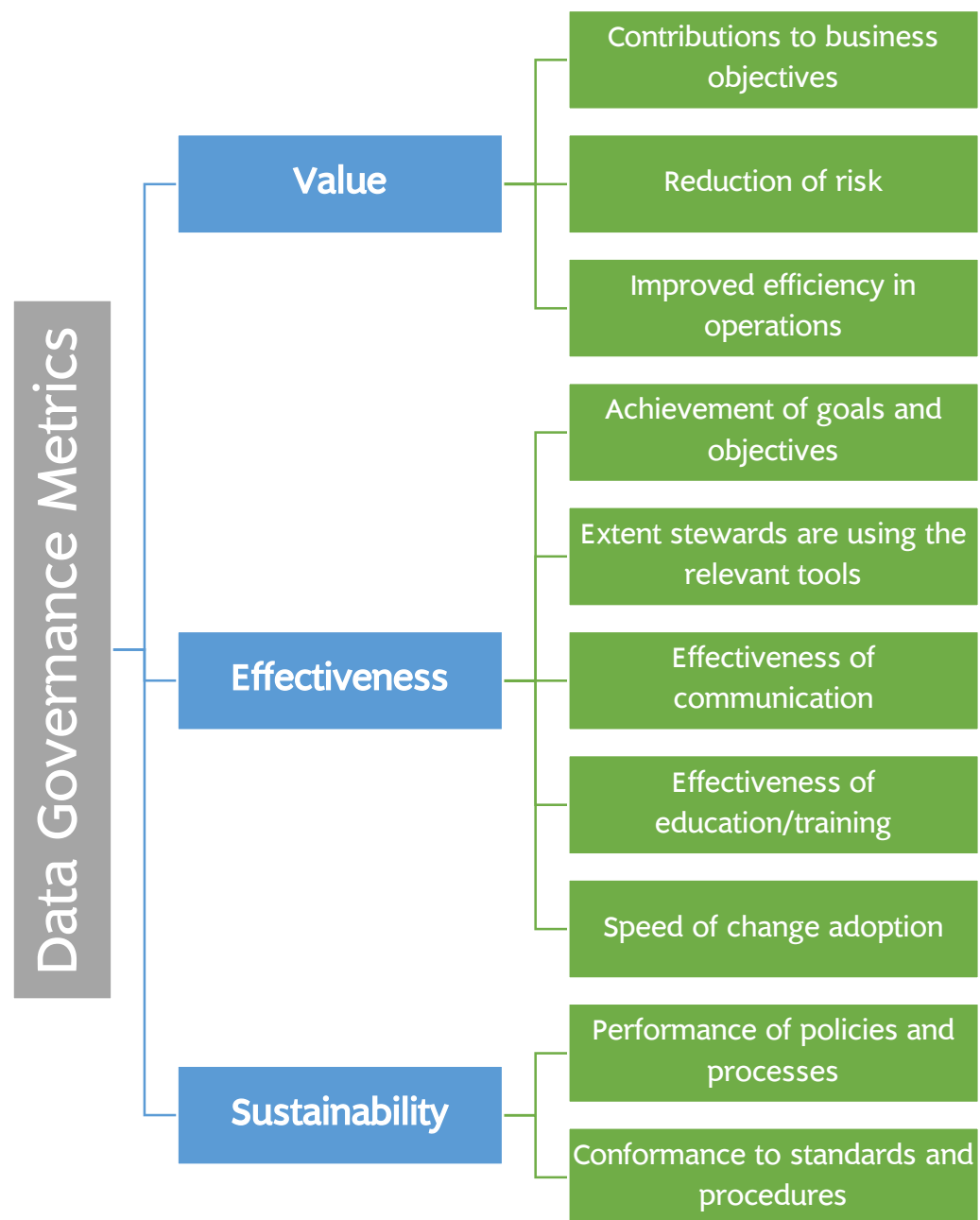


DCAM Scoring Guide

SCORE	CATEGORY	DESCRIPTION	CHARACTERISTICS
1	Not initiated	Not Performed	Ad hoc activities performed by heroes
2	Conceptual	Initial Planning Stages	Issues being debated; whiteboard sessions
3	Developmental	Engagement Underway	Key functional <u>stakeholders</u> identified; workstreams defined; meetings underway; participation growing; <u>policies</u> , roles, and operating <u>procedures</u> being established; project/annual funding
4	Defined	Defined and Verified	Business users active; LOB management with P&L responsibility engaged; requirements verified; responsibilities defined and assigned; <u>policy</u> and <u>standards</u> exist; routines in place; lineage underway; <u>critical data elements</u> (CDEs) identified; adherence tracked; multi-year/sustainable funding
5	Achieved	Adopted and Enforced	Executive management sanctioned; proactive business engagement; responsibilities coordinated; <u>policy</u> and <u>standards</u> implemented; lineage verified; <u>data harmonized</u> across repositories; adherence audited; strategic/investment funding
6	Enhanced	Integrated	Fully embedded in the operational culture of the organization with the goal of continuous improvement

Questions Framed in Requirements to Achieve Capability (“5”)

	Process	Formality	Engagement
Not Initiated	Capabilities are not Being Performed		
	Tactical	Ad Hoc	Heroes
In Process (Conceptual)	Capabilities are in their Initial Planning Stages		
	Issues are under debate	White board planning	Data practitioners
In Process (Developmental)	Capabilities are Being Developed		
	Policies, procedures, standards, roles and accountabilities are being established	Meetings are underway (notes and planning documents)	Stakeholders are identified (negotiated resources/annual budgets)
In Process (Defined)	Capabilities are Defined and Formalized		
	Policies and standards exist (roles, responsibilities and accountabilities are being coordinated)	Routines exist (structured documentation)	Verified by stakeholders (business and functional responsibility/sustainable funding)
Achieved	Capabilities are Achieved and Implemented		
	Policies and standards are implemented (proactive issue management)	Capabilities are embedded into operations (standardized methodologies)	Executive management authority (strategic investment funding)
Enhanced	Capabilities are fully integrated into the operating culture of the organization		



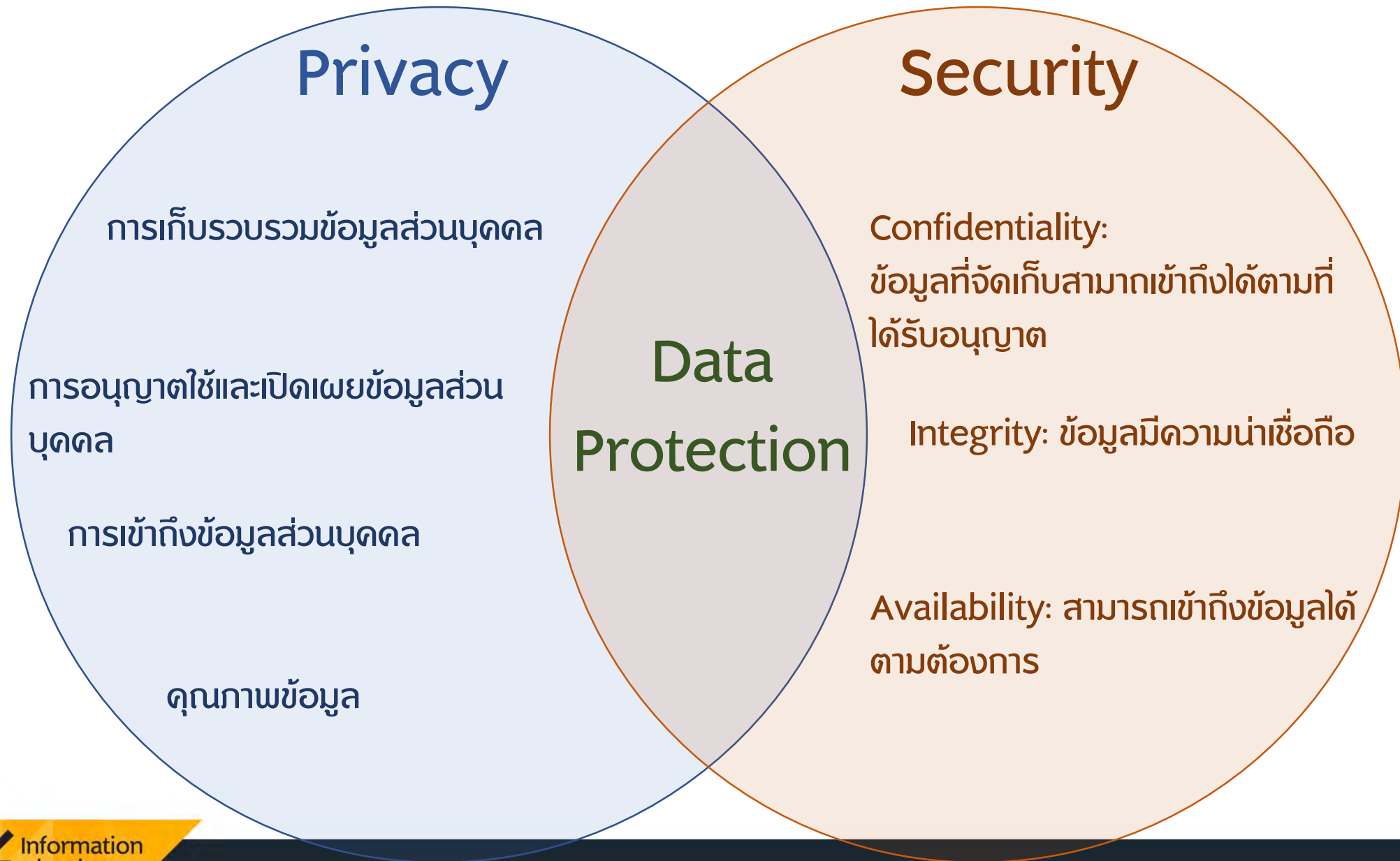


สิ่งที่ควรหลีกเลี่ยง	สิ่งที่ควรปฏิบัติ
กำกับดูแลจากภายในฝ่าย IT	มอบหมายคนที่สามารถจูงใจคนระดับองค์กรจากฝั่งธุรกิจหรือฝ่ายงานหลักขององค์กร
กำกับดูแลข้อมูลที่เป็น Silo	“Think Globally and Act Locally”
เข้าใจว่าทุกคนเห็นความสำคัญของข้อมูล	สื่อสารถึงผลกระทบของการที่ข้อมูลขาดคุณภาพและผลประโยชน์ขององค์กรที่จะได้จากการกำกับดูแลข้อมูล
ใช้ตัวชี้วัดที่ไม่มีความหมาย	ตัวชี้วัดที่กระทบต่อองค์กร
มอง Data Governance เป็นโครงการ	ฝังแนวคิด Data Governance ในการดำเนินงานปกติ
สยบวัฒนธรรมมององค์กร	จัดการการเปลี่ยนแปลงและแรงต่อต้าน
มุ่งเป้าที่ตัวบุคคล	วางบทบาทกับตำแหน่งงาน

Module 2

Introduction to PDPA





พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด ๒ การคุ้มครองข้อมูลส่วนบุคคล

หมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล

หมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด ๕ การร้องเรียน

หมวด ๖ ความรับผิดทางแพ่ง

หมวด ๗ บทกำหนดโทษ

ส่วนที่ ๑ บททั่วไป

ส่วนที่ ๒ การเก็บรวบรวมข้อมูลส่วนบุคคล

ส่วนที่ ๓ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ส่วนที่ ๑ โทษอาญา

ส่วนที่ ๒ โทษทางปกครอง

ขอบเขตการใช้บังคับ

มาตรา
๕



ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลโดยผู้ควบคุมข้อมูล ส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า การเก็บ รวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม



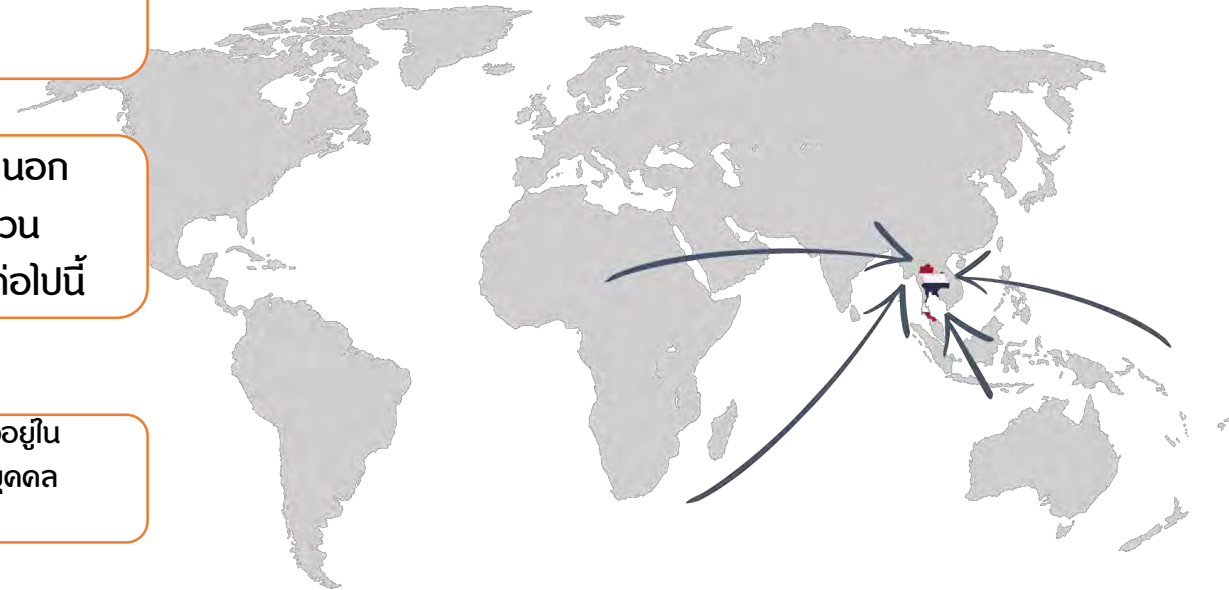
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอก ราชอาณาจักรพรบ.นี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน บุคคลของเจ้าของข้อมูล ส่วนบุคคลซึ่งอยู่ในราชอาณาจักร เมื่อมีกิจกรรมต่อไปนี้



การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ใน ราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคล หรือไม่ก็ตาม



การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นใน ราชอาณาจักร





เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น



การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ



เพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น



การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎรวุฒิสภา รัฐสภา หรือคณะกรรมการการ



การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา



การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ข้อมูลส่วนบุคคล (Personal data)

ข้อมูลส่วนบุคคลที่ทำให้ระบุตัวบุคคลได้ ไม่ว่าจะทางตรงหรือทางอ้อม เช่น

เลขประจำตัวประชาชน

ชื่อ-นามสกุล



เชื้อชาติ



ศาสนา



พฤติกรรมทางเพศ



ประวัติอาชญากรรม



ข้อมูลสุขภาพ



ที่อยู่



เบอร์โทรศัพท์



อีเมล



ข้อมูลทางการเงิน



แต่ไม่รวมถึงข้อมูลของผู้ที่เกี่ยวข้องเฉพาะ

บุคคลที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคล



- เจ้าของข้อมูลส่วนบุคคล (Data Subject)



- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
 - บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
 - บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
 - ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

Lawful Basis in PDPA



Consent ได้รับความยินยอม



Scientific or Historical Research เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ



Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล



Contract เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา



Public task เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐ



Legitimate Interest เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล



Legal Obligation เป็นการปฏิบัติตามกฎหมาย

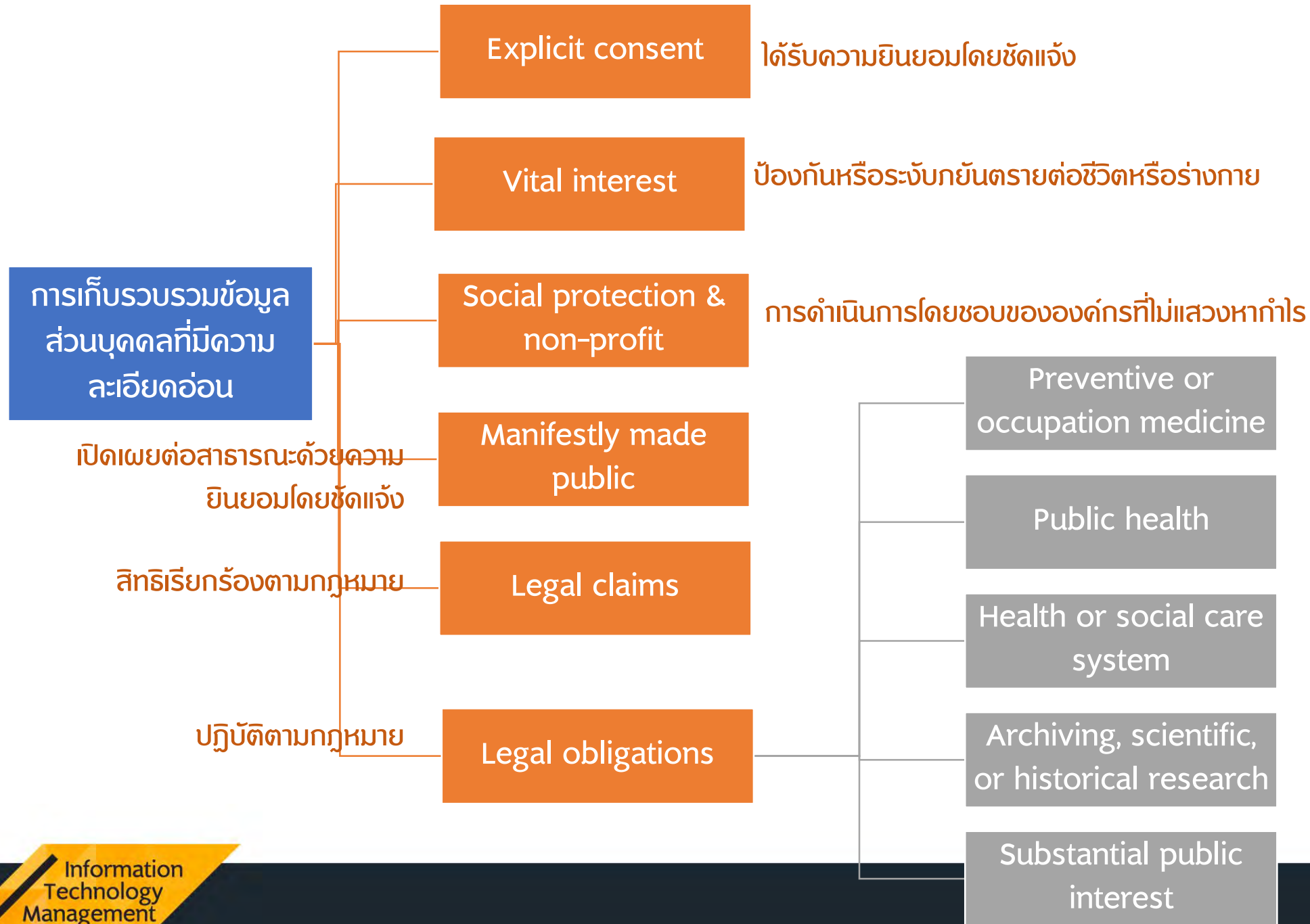
ความยินยอม (Consent)

- ต้องได้รับความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
- ต้องทำโดยชัดแจ้ง (หนังสือ หรือ ระบบอิเล็กทรอนิกส์)
- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย
- ต้องแยกส่วน เข้าใจง่าย ไม่หลอกลวง
- มีอิสระในการให้ความยินยอม
- ก่อนความยินยอมได้เว้นแต่มีข้อจำกัดด้านสิทธิ



ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน

- เชื้อชาติ
 - เผ่าพันธุ์
 - ความคิดเห็นทางการเมือง
 - ความเชื่อในลัทธิ
 - ศาสนาหรือปรัชญา
 - พฤติกรรมทางเพศ
 - ประวัติอาชญากรรม
 - ข้อมูลสุขภาพ ความพิการ
 - ข้อมูลสหภาพแรงงาน
 - ข้อมูลพันธุกรรม
 - ข้อมูลชีวภาพ
- หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูล
ส่วนบุคคลในทำนองเดียวกันตามที่
คณะกรรมการประกาศกำหนด



Legal obligations

Preventive or
occupation medicine

เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์

การประเมินความสามารถของลูกจ้าง

การวินิจฉัยโรคทางการแพทย์

การให้บริการด้านสุขภาพหรือสังคม

การรักษาทางการแพทย์

การให้บริการด้านสังคมสงเคราะห์

Public health

ประโยชน์สาธารณะด้านสาธารณสุข

Health or social care
system

การคุ้มครองแรงงาน

การประกันสังคม

สวัสดิการรักษายาบาล

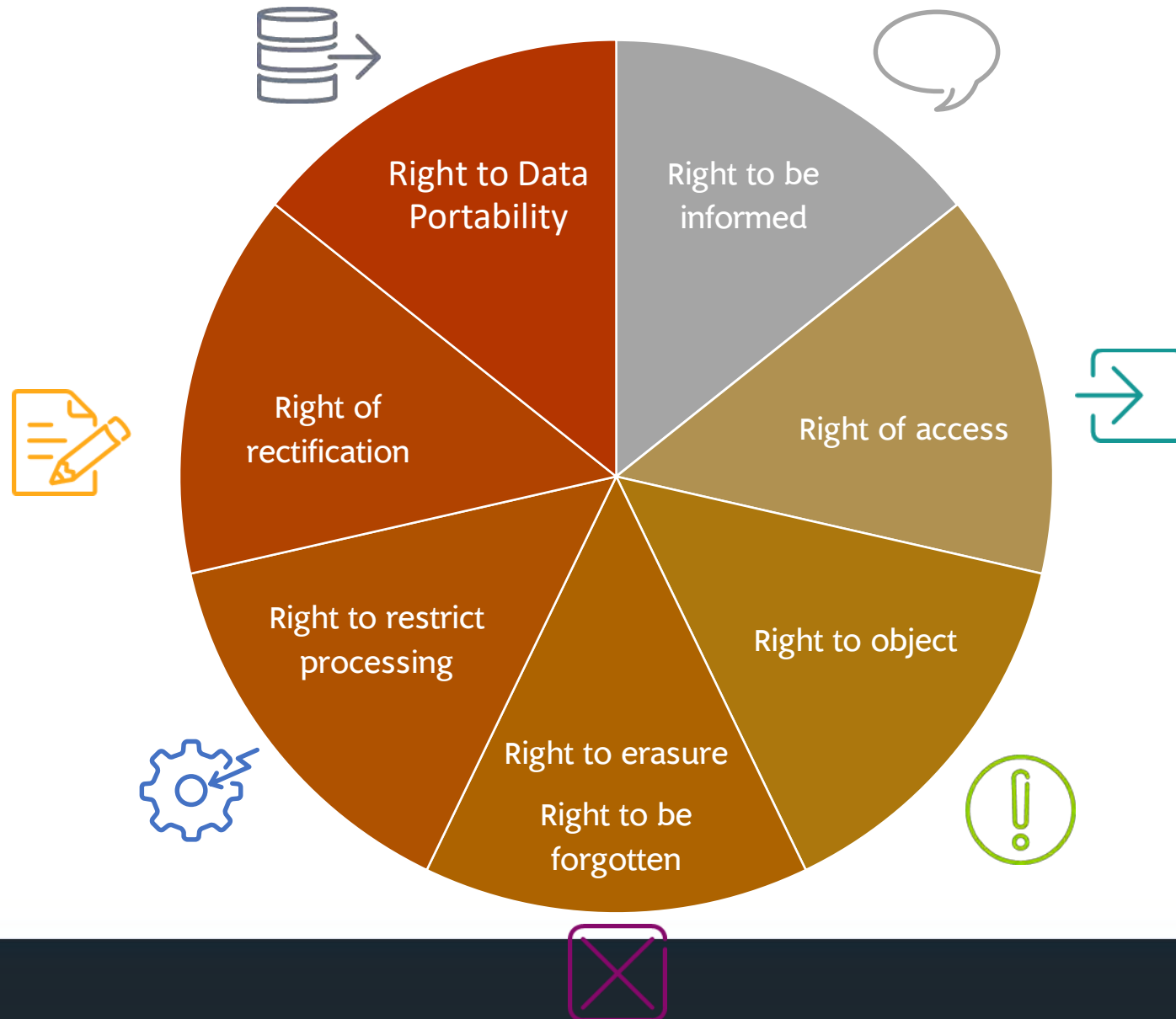
Archiving, scientific, or
historical research

การศึกษาวิจัยทางวิทยาศาสตร์ สติติ หรือ ประวัติศาสตร์ หรือประโยชน์สาธารณะอื่น

Substantial public
interest

ประโยชน์สาธารณะที่สำคัญ

สิทธิของเจ้าของข้อมูลส่วนบุคคล



การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง



เว้นแต่...



ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วัน นับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล



เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

- ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอม
- บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์อื่น
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ได้รับยกเว้นไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้

การส่งหรือโอนข้อมูลไปยังต่างประเทศ

ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
เว้นแต่...



การปฏิบัติตามกฎหมาย



ได้รับความยินยอม



จำเป็นเพื่อการปฏิบัติตามสัญญา



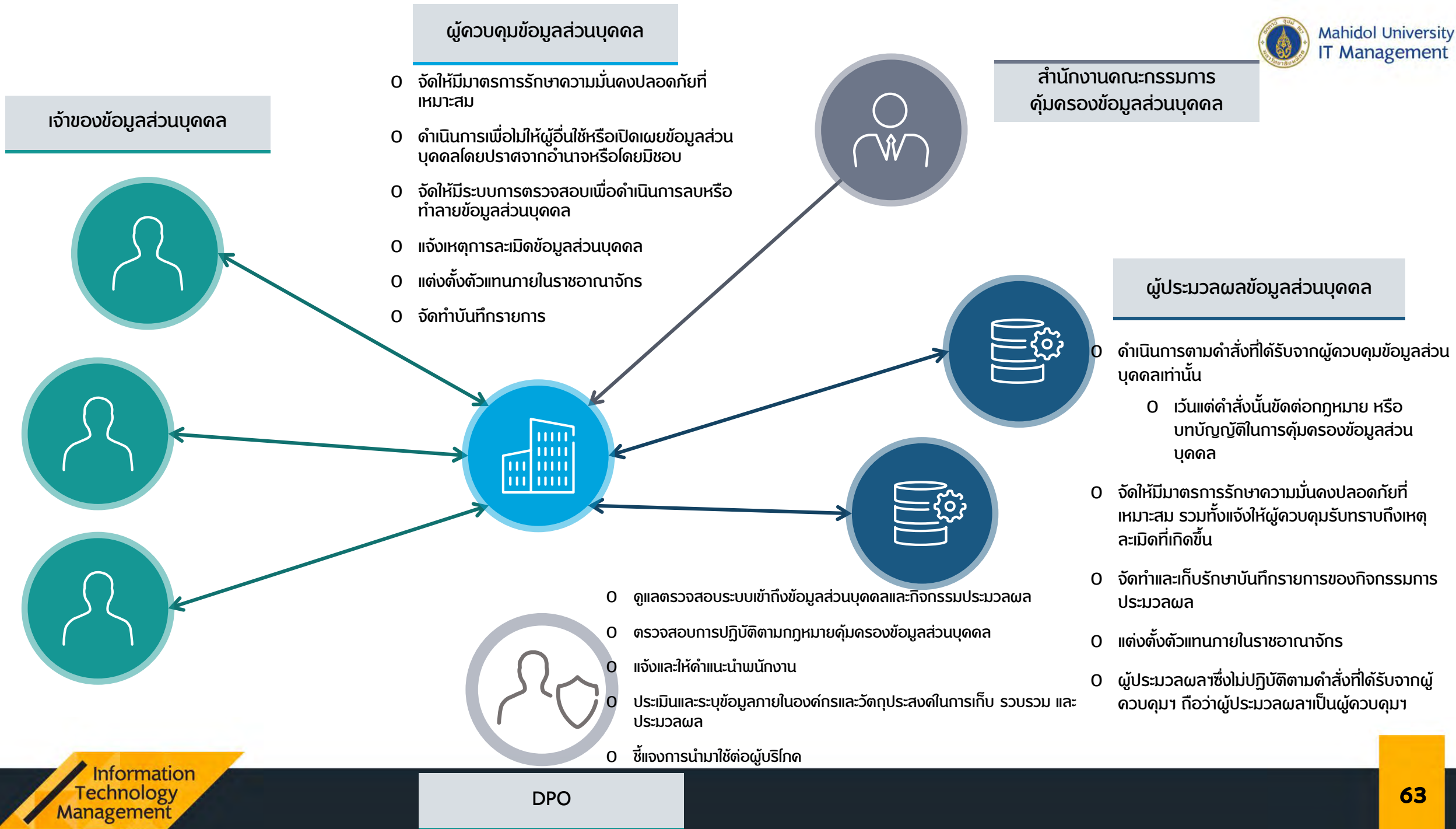
การทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น



ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ



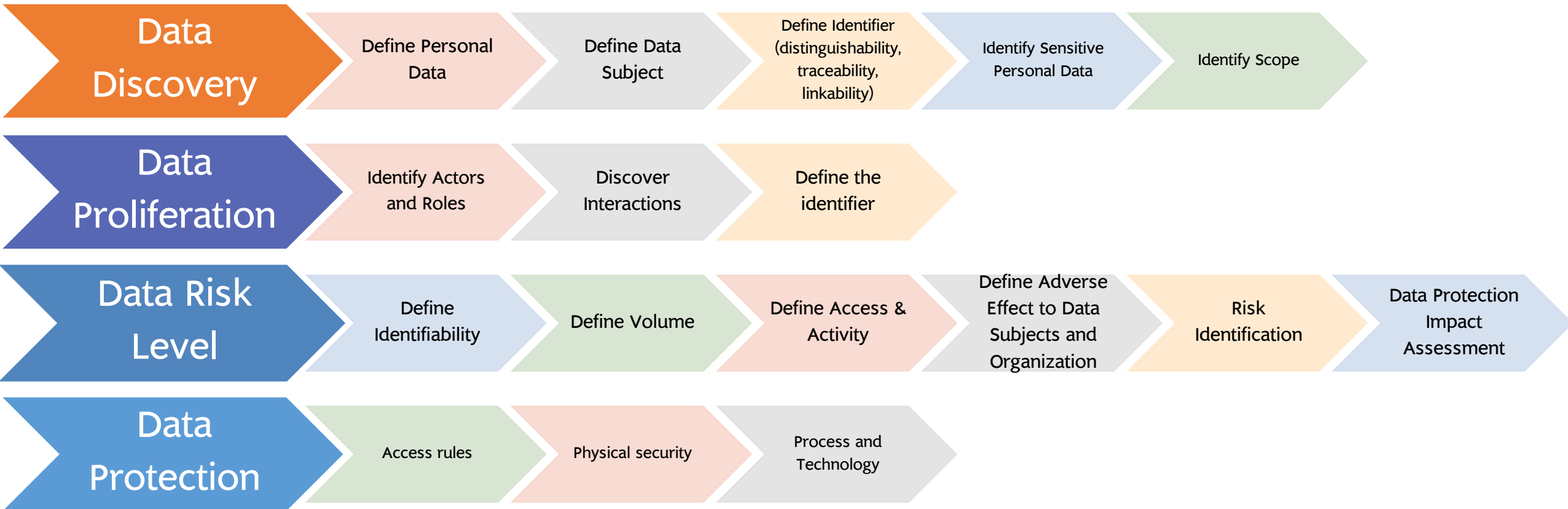
จำเป็นเพื่อประโยชน์สาธารณะที่สำคัญ



Module 3

Personal Data Identification

Personal Data Identification



Module 4

PDPA Lawful Basis

Lawful Basis in PDPA



Consent ได้รับความยินยอม



Scientific or Historical Research เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ



Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล



Contract เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา



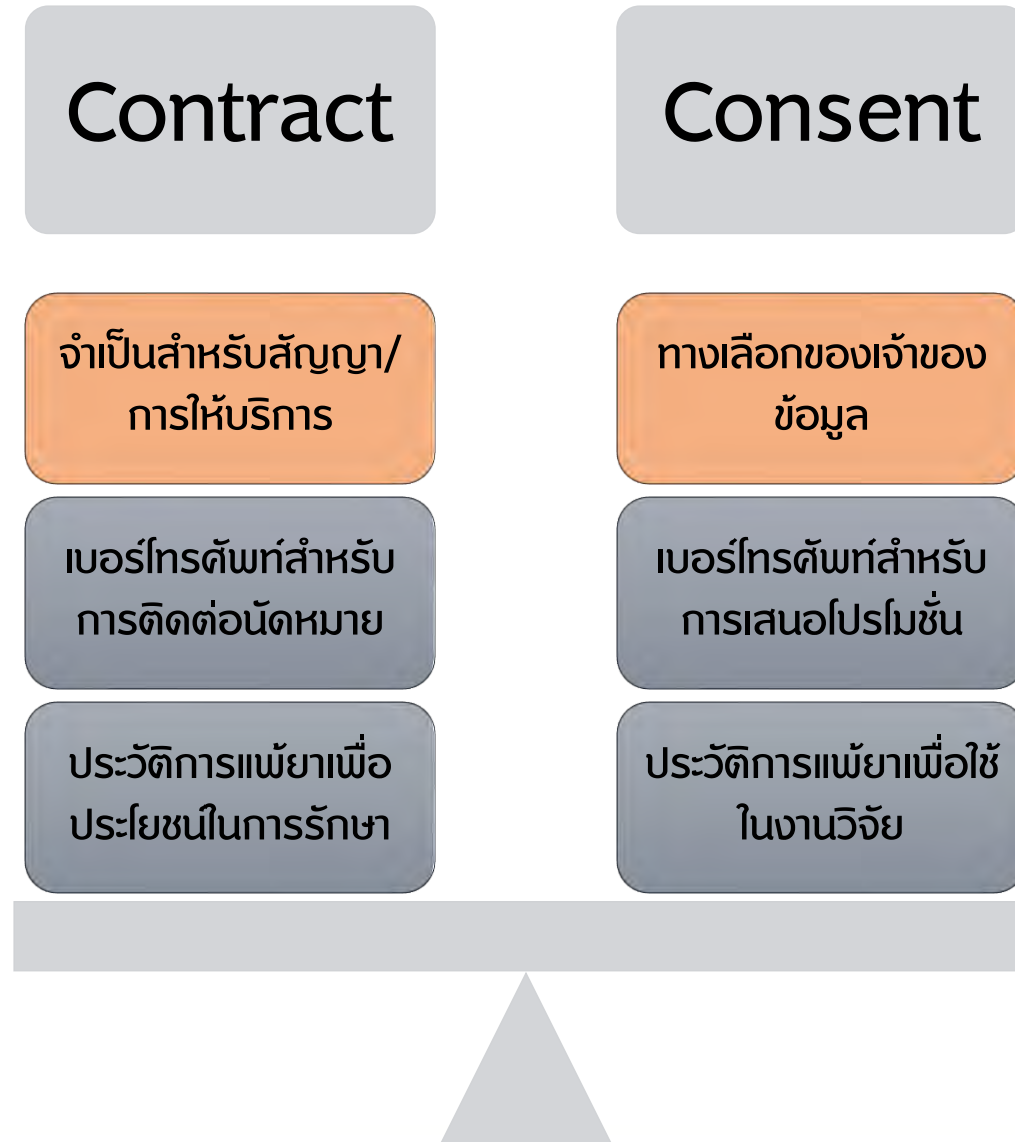
Public task เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐ



Legitimate Interest เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล



Legal Obligation เป็นการปฏิบัติตามกฎหมาย



ฐานสัญญา vs ฐานความยินยอม

- ในกรณีที่ผู้ประมวลผลข้อมูลทำงานให้กับผู้ควบคุมข้อมูลโดยประมวลผลข้อมูลที่จำเป็นต่อการปฏิบัติตามสัญญานั้น ๆ ถือเป็นการประมวลผลตามฐานสัญญา
- ผู้ควบคุมข้อมูลไม่ควรขอความยินยอมพร่ำเพรื่อเพราะจะทำให้ผู้ใช้บริการเข้าใจผิดว่าสามารถถอนความยินยอมได้
- การประมวลผลข้อมูลนั้นอาจเกิดขึ้นโดยใช้ฐานสัญญาที่มีมากกว่าหนึ่งฉบับ
 - เช่น เมื่อเจ้าของเข้ารับบริการที่โรงพยาบาลแล้วทางโรงพยาบาลส่งข้อมูลยอดค่าใช้จ่ายไปให้บริษัทประกันเพื่อให้เบิกจ่ายค่ารักษาพยาบาลที่เกิดขึ้น
 - ในกรณีเช่นนี้มีสัญญาสองฉบับคือ สัญญาบริการระหว่างผู้ป่วยกับโรงพยาบาล และสัญญาประกันสุขภาพระหว่างผู้ป่วยกับบริษัทประกัน
- ภายใต้ฐานสัญญา ผู้ควบคุมต้องพิจารณาความ “จำเป็น” ในการประมวลผลโดยใช้ข้อมูลส่วนบุคคล

ความยินยอม (Consent)

- ต้องได้รับความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
- ต้องทำโดยชัดแจ้ง (หนังสือ หรือ ระบบอิเล็กทรอนิกส์)
- ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย
- ต้องแยกส่วน เข้าใจง่าย ไม่หลอกลวง (Layout / UI)
- มีอิสระในการให้ความยินยอม
- ก่อนความยินยอมได้เว้นแต่มีข้อจำกัดด้านสิทธิ



เนื้อหาของ การขอความยินยอม

ใคร?	อะไร?	อย่างไร?	เมื่อไร?	หากมีปัญหา
☐ ข้อมูลเกี่ยวกับ Data Controller ☐ ข้อมูลเกี่ยวกับ DPO	☐ วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจง ☐ ข้อมูลที่จะถูกเก็บรวบรวมและใช้	☐ วิธีการประมวลผล ☐ การใช้ระบบอัตโนมัติ ☐ การโอนข้อมูลไปต่างประเทศ ☐ การเปิดเผยต่อบุคคลอื่น	☐ ระยะเวลาในการจัดเก็บข้อมูล	☐ วิธีถอนความยินยอม ☐ สิทธิต่างๆของเจ้าของข้อมูล

ข้อควรระวังในการจัดการความยินยอม

ขอความยินยอมเมื่อ
จำเป็นต้องประมวลผลข้อมูล
นั้นเท่านั้น

บันทึกเนื้อหาข้อมูลที่แจ้งตอน
ขอความยินยอม และวิธีการให้
ความยินยอม

แยกประเภทและขอบเขตของ
ความยินยอมรายบุคคลเอาไว้

กำหนดการตรวจสอบความ
เหมาะสมและขอบเขตของความ
ยินยอมเมื่อผ่านไประยะหนึ่ง

กระบวนการก่อนความยินยอม
ต้องชัดเจน ไม่ยุ่งยากกว่าตอน
ที่ให้ความยินยอม

เตรียมพร้อมเพื่อตอบสนอง
ต่อคำขอการใช้สิทธิของเข้า
ของข้อมูล โดยเฉพาะการถอน
ความยินยอมได้อย่างรวดเร็ว

ต้องไม่ลงโทษหรือทำให้เจ้าของ
ข้อมูลเสียประโยชน์เมื่อก่อน
ความยินยอม

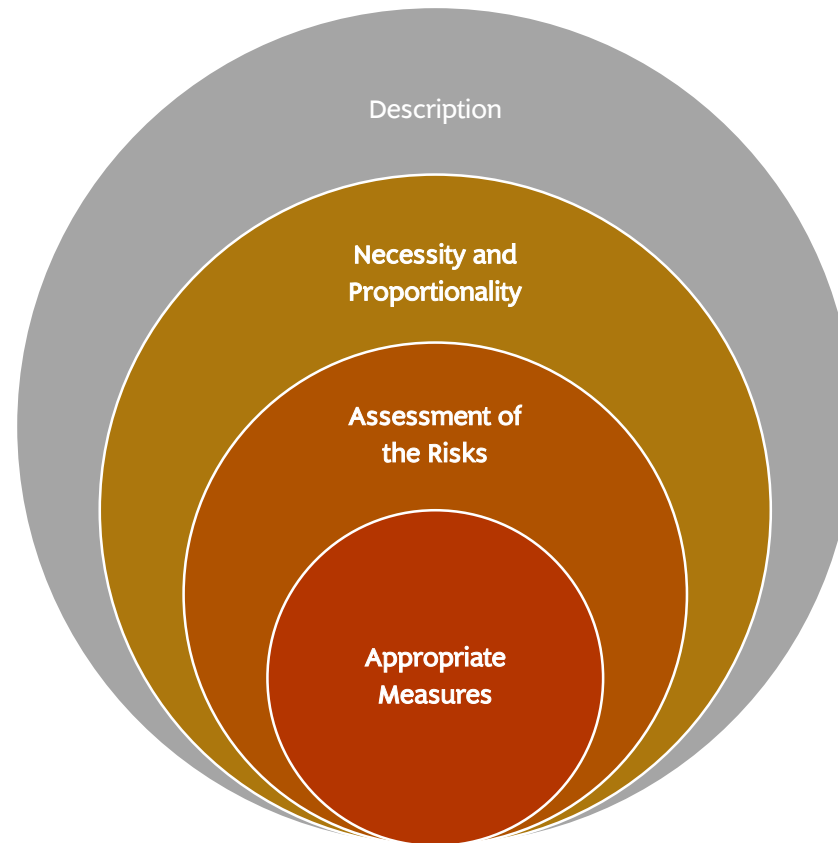


Module 5

Data Protection Impact Assessment

ขอบเขตของ DPIA

- เป็นวิธีการที่จะทำให้สามารถประเมิน**ความเสี่ยง**และแสดงให้เห็นว่าได้มีการปฏิบัติหลักเกณฑ์ต่าง ๆ ตามกฎหมาย



DPIA – Motivation in PDPA

มาตรา 30 กำหนดให้ผู้ควบคุมข้อมูลต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลให้เจ้าของข้อมูลทราบถึงผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

มาตรา 37(4) กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

มาตรา 39 วรรคสาม และมาตรา 40 วรรคสี่ กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องบันทึกการโดยคำนึงถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

มาตรา 37(1) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

มาตรา 39(8) และมาตรา 40(2) กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องบันทึกการโดยคำอธิบายและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

มาตรา 4 วรรคสาม กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นการดำเนินการตามวรรคก่อน ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

การประมวลผลข้อมูลที่มีความเสี่ยงสูง

- กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ รวมถึงการทำโปรไฟล์ ซึ่งการประมวลผลดังกล่าวส่งผลเป็นการตัดสินใจที่ส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
- กรณีที่มีการประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลที่อ่อนไหวหรือข้อมูลประวัติอาชญากรรม
- กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ





1. DPIA Identification

- ผู้ควบคุมข้อมูลควรขอความเห็นจาก DPO ในการประเมินว่าจะต้องจัดทำ DPIA หรือไม่
- บันทึกเหตุผลและการตัดสินใจดังกล่าวเอาไว้

2. Description

Nature		Scope	สภาพและลักษณะของข้อมูลส่วนบุคคล	Context	แหล่งข้อมูลส่วนบุคคล	Purpose
การจัดเก็บข้อมูล	การใช้ข้อมูล	ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล	ความอ่อนไหวของข้อมูลส่วนบุคคล	ลักษณะของความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล	ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล	
ผู้ที่สามารถเข้าถึงข้อมูล	ผู้ที่ได้รับข้อมูล	ระดับและความถี่ของการประมวลผลข้อมูล	ระยะเวลาของการประมวลผลข้อมูล	ระดับความคาดหวังของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูล	มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่	
ผู้ประมวลผลข้อมูล	ระยะเวลาจัดเก็บข้อมูล	จำนวนของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง	พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง	ประสบการณ์ที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน	ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง	
มาตรการความปลอดภัย	เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล			ประเด็นที่เป็นข้อวิตกกังวลของสาธารณะ	มีการปฏิบัติตามมาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องหรือไม่	
กระบวนการแบบใหม่ที่ใช้ในการประมวลผลข้อมูล	ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล					

3. Consultation

- Data subject
- Data processor
- Internal stakeholders
- Independent experts
- Data Protection Agency

4. Necessity and proportionality

- การประมวลผลข้อมูลส่วนบุคคลดังกล่าวช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร
- มีช่องทางอื่นหรือไม่ที่สามารถดำเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์ที่ประสงค์เดียวกัน
- ฐานในการประมวลผลข้อมูลตามกฎหมาย
- แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม
- แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล
- แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็น (data minimization)
- แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล
- แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล
- มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล
- มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ

5. Risk assessment

ร้ายแรงมาก	ระดับต่ำ	ระดับสูง	ระดับสูง
ร้ายแรงพอสมควร	ระดับต่ำ	ระดับกลาง	ระดับสูง
ร้ายแรงน้อย	ระดับต่ำ	ระดับต่ำ	ระดับต่ำ
	โอกาสต่ำ	โอกาสพอสมควร	โอกาสสูง

ผลกระทบต่อ เจ้าของข้อมูล

ทำให้ไม่สามารถใช้สิทธิได้ตามสมควร ทั้งที่เป็นสิทธิความเป็นส่วนตัว และสิทธิอื่นๆ

ทำให้ไม่สามารถเข้าถึงบริการหรือเสียโอกาสบางอย่าง

ทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้

ทำให้ถูกเลือกปฏิบัติ

ทำให้ถูกสวมรอยบุคคล (identity theft) หรือหลอกลวงได้

ทำให้เกิดความเสียหายทางการเงิน

ทำให้เกิดความเสียหายแก่ชื่อเสียง

ทำให้เกิดความเสียหายแก่ร่างกาย

ทำให้สูญเสียความลับ

ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝงข้อมูล (pseudonymization) สามารถระบุตัวบุคคลได้

ผลกระทบอื่นๆทางเศรษฐกิจและสังคมที่มีนัยสำคัญ

6. Mitigating measures

- การไม่จัดเก็บข้อมูลบางประเภท
- การลดขอบเขตของการประมวลผลข้อมูล
- การลดระยะเวลาการจัดเก็บข้อมูล
- การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย
- การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้
- การเฝ้าระวังข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้
- การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง
- การเพิ่มขั้นตอนที่ดำเนินการโดยมนุษย์เพื่อทบทวนการประมวลผลด้วยระบบอัตโนมัติ
- การใช้เทคโนโลยีที่แตกต่างกัน
- การจัดให้มีข้อตกลงการใช้ข้อมูลร่วมกัน (data sharing) ที่ชัดเจน
- การปรับปรุงข้อมูลแจ้งเตือนเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล
- การจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะไม่ให้ความยินยอม
- การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของเขา

7. Documentation and planning

- แผนที่จะดำเนินการมาตรการเพิ่มเติม
- ความเสี่ยงต่างๆได้รับการจัดการให้ลดลงหรือกำจัดให้หมดไปหรืออยู่ในระดับยอมรับได้
- ภาพรวมของความเสี่ยงที่เหลืออยู่ (residual risk) ภายหลังจากที่มีการเพิ่มมาตรการต่างๆ
- เหตุผลที่ไม่ดำเนินการตามความเห็นของ DPO หรือเจ้าของข้อมูลส่วนบุคคล หรือที่ปรึกษาอื่นๆ
- กรณีที่มีความเสี่ยงสูงเหลืออยู่ มีความจำเป็นที่จะต้องปรึกษารื้อกับสำนักงาน
- ดัชนีร่องข้อมูลส่วนบุคคลก่อนที่จะสามารถดำเนินการต่อไปได้

8. Monitoring and review

- ติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการที่ได้จากการทำ DPIA

Module 6

Related Technical Issues for PDPA

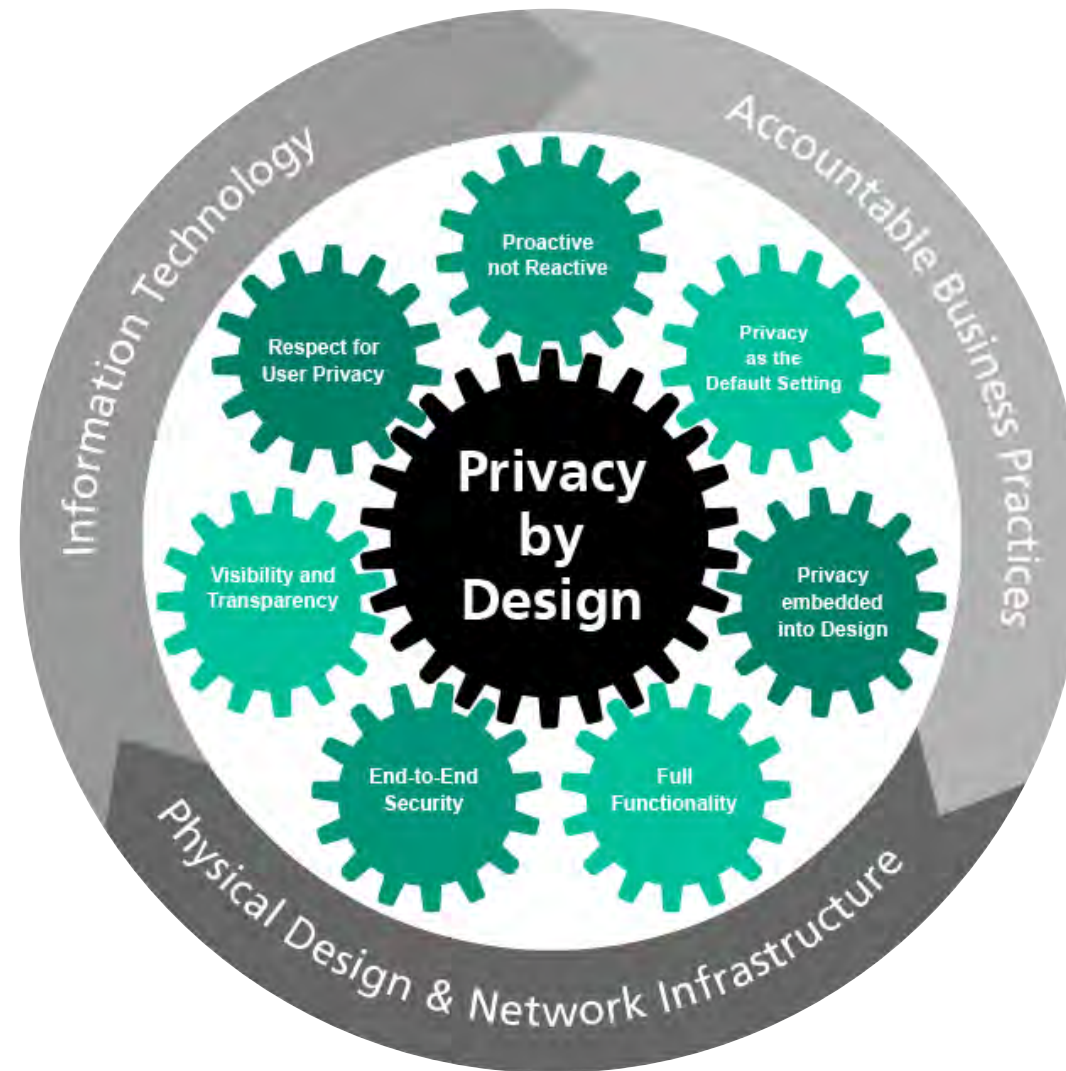
Data Mapping

GDPR Data Map

Designed by: **Anthony Budd** Designed for: **Ideea** Date: **22/1/17** Version: **1.2**

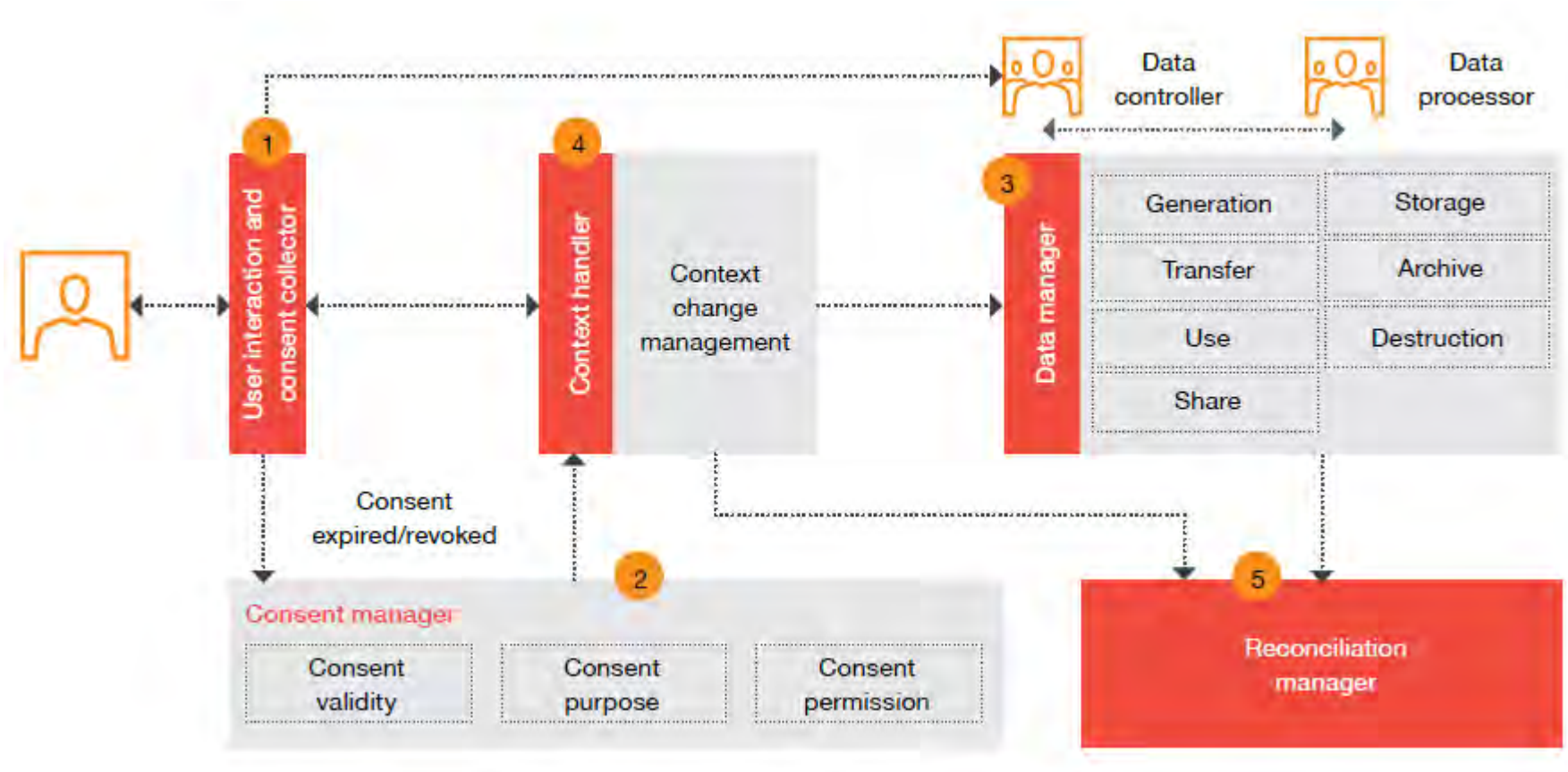
Source How was this data collected? - Contact Form - External Organisation	Personal Data What data are you collecting? - Email Address - IP Address - Ethnic Origin - Phone Number	Reason Why are you collecting this data? - Marketing - CRM - Processing/ Analytics	Handling Explain how you will store the data, how it will be processed and who has access to it.	Disposal When is this data disposed? - Upon Request - After 6 Months	Consent Obtained	Subject is a over 13	Mission critical data	Sensitive personal data
Contact Form	Full Name Email Address IP Address Phone Number	We need this data because this is how we take new business enquiries	WordPress Database Site Admins	Cron - removed after 30days	✓	✓	✓	✗

<https://medium.com/@Ideea/gdpr-data-map-template-31da34ca39d0>



<https://digital-health.blog/2019/07/19/privacy-by-design-theoretical-principle-or-development-methodology/>

Consent Management



<https://www.pwc.in/consulting/technology/data-and-analytics/govern-your-data/insights/a-blueprint-for-robust-consent-management.html>

Cookie



[What is CCPA?](#)

[What is GDPR?](#)

[Pricing](#)

[Help](#)

[Functions](#)

[Resellers](#)

[Log in](#)

[Try for free →](#)



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services

Use necessary cookies only

Allow selection

Allow all cookies

☒ Necessary ☐ Preferences ☐ Statistics ☐ Marketing

Hide details ^

Cookie declaration

About cookies

Necessary (28)

Preferences (8)

Statistics (18)

Marketing (18)

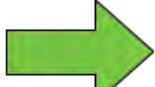
Unclassified (0)

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Name	Provider	Purpose	Expiry	Type
__RequestVerificationT	Cookiebot	Helps prevent Cross-Site Request Forgery (CSRF) attacks.	Session	HTTP
_abck	Cookiebot	Used to detect and	1 year	HTTP

Cookie declaration last updated on 8/12/63 by [Cookiebot](#)

Pseudonymization

John Doe	john.doe@example.com	555-123-456		ECYFRPA	F2EYVE@example.com	555-ND77QQ
Jane Roe	jane.roe@example.com	555-789-456		BQ6ZQSZ	OOTKCL@example.com	555-HW62UK
John Doe	john.doe@example.com	555-123-456		ECYFRPA	F2EYVE@example.com	555-ND77QQ



Anonymization

John Doe	john.doe@example.com	555-123-456		BOC4UM3	VWVN5Y2@example.com	555-YP755KXI
Jane Roe	jane.roe@example.com	555-789-456		W36CC7O	FJ6ZBOC@example.com	555-Y2ZTON7
John Doe	john.doe@example.com	555-123-456		5IZVLPDX	3PAWFXH@example.com	555-OYNUKG

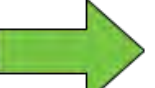


Suppression

John Doe	john.doe@example.com	555-123-456		XXX	XXX@example.com	555-XXXXXX
Jane Roe	jane.roe@example.com	555-789-456		XXX	XXX@example.com	555-XXXXXX
John Doe	john.doe@example.com	555-123-456		XXX	XXX@example.com	555-XXXXXX



Generalization

John Doe	45 years old	555-123-456		Male	40 < Age < 50	New York
Jane Roe	22 years old	555-789-456		Female	20 < Age < 30	Los Angeles
John Doe	45 year old	555-123-456		Male	40 < Age < 50	New York

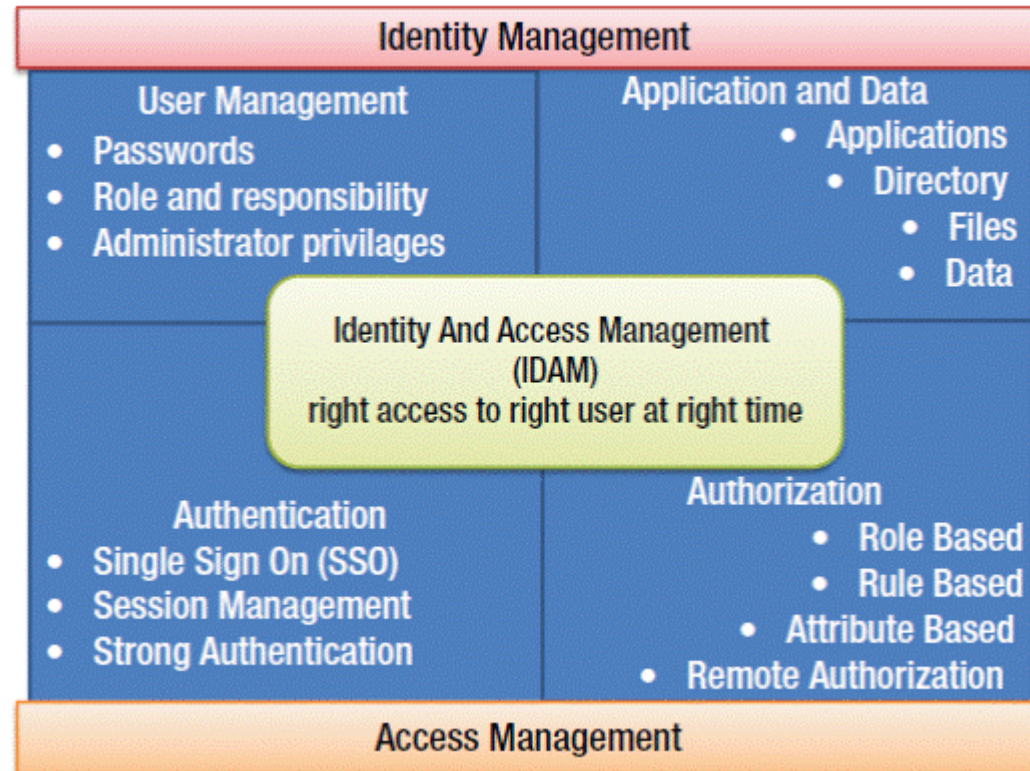


Encryption

John Doe	john.doe@example.com	555-123-456		BOC4UM3	VWVN5Y2@example.com	555-YP755KXI
Jane Roe	jane.roe@example.com	555-789-456		W36CC7O	FJ6ZBOC@example.com	555-Y2ZTON7
John Doe	john.doe@example.com	555-123-456		5IZVLPDX	3PAWFXH@example.com	555-OYNUKG



Identity and Access Management (IDAM)



https://ebrary.net/26660/computer_science/ldap_active_directory

Module 7

ISO/IEC 27701

ISO/IEC 27701 Structure

- A. Reference control objectives for controllers
- B. Reference control objectives for processors
- C. Mapping to ISO29100
- D. Mapping to GDPR
- E. Mapping to ISO27018 and ISO29151
- F. How to apply ISO27701 to ISO27001/2

ISO/IEC 27701 – Important Extension

- Context
 - Applicable legislation
 - Needs and expectations of interested parties
 - Management system scope (InfoSec + PII)
- Risk assessment
 - Risk assessment aka PIA
 - Risk treatment
- PIMS
 - Policies (now including PII)
 - ISMS Roles (ref. CISO + now DPO)
 - Training and awareness (everyone involved in PII treatment)
 - Data breaches (GDPR)
 - Encryption, secure disposal
 - Identity Management (part of access control)

ISO/IEC 27701 – Important Extension

- PIMS
 - Information Backup
 - Event logging
 - Log protection
 - System development & acquisition (see module 7 & 8)
 - Test data
 - [DO NOT USE PII for test data (use dummy or synthetic)]
 - INCIDENT MANAGEMENT (ref. GDPR data breaches)

ISO/IEC 27701 – Important Extension

- 7. Guidance for controllers
 - Purpose definition
 - Lawful basis
 - Consent management
 - PIA
 - PII Process contracting
 - Subject rights ("PII principal")
 - Information
 - Object to processing
 - Copy of PH data
 - Request handling
 - Privacy by design (GDPR = "data protection by design")
 - Privacy by default (GDPR = "data protection by default")
 - Data minimization principles
 - Accuracy & quality
 - De-identification & disposal
 - PII sharing, transfer & disclosure

ISO/IEC 27701 – Important Extension

- 8. Guidance for processors
 - Agreement (to delegate obligations)
 - Marketing & advertisement
 - Conflict of interest (or legal conflicts)
 - Temporary files
 - PII transfer & disposal
 - transfer between jurisdictions
 - Disclosure requests



Mahidol University
Wisdom of the Land