DGA304

การวิเคราะห์ข้อมูลและการใช้ประโยชน์เพื่อการตัดสินใจสำหรับผู้บริหาร

LC5 กฎหมายและแนวทางป้องกันความเสี่ยงจากการใช้ข้อมูลในยุคดิจิทัล

รุ่นที่ 1 วันที่ 6 พฤศจิกายน 2568

ดร.อรรถศิษฐ์ พัฒนะศิริ

หัวหน้าศูนย์นวัตกรรมและวิทยบริการ และ
อาจารย์ประจำ วิทยาลัยนวัตกรรมสื่อสารสังคม
มหาวิทยาลัยศรีนครินทรวิโรฒ

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

วิทยากร

ดร.อรรถศิษฐ์ พัฒนะศิริ

Dr.Attasit Patanasiri

วิทยาลัยนวัตกรรมสื่อสารสังคม
มหาวิทยาลัยศรีนครินทรวิโรฒ

Education

PhD Management of Technology,
Asian Institute Of Technology, TH
MSc Computer Science,
Chulalongkorn University, TH
BSc Computer Science,
Thammasat University, TH

Certification

Certified Data Protection Officer (DPO) by OCEG
Generative AI for Educators by Google

ความเชี่ยวชาญ

- **Business Management**
- **Digital Marketing**
- **Digital Innovation**
- **Data & Security**
- **Enterprise Architecture**
- **Generative AI**
- **PDPA**

ประสบการณ์

ผู้เชี่ยวชาญ ด้านการขับเคลื่อนเปลี่ยนแปลงทางดิจิทัล และการประยุกต์ใช้เทคโนโลยีในองค์กร

ผู้เชี่ยวชาญเฉพาะเรื่อง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ให้กับบริษัทที่ปรึกษาชั้นนำ [Personal Data Protection Act (PDPA) Subject Matter Expert]

รองผู้อำนวยการ สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

หัวหน้าศูนย์นวัตกรรมและวิทยบริการ และ อาจารย์ประจำ วิทยาลัยนวัตกรรมสื่อสารสังคม มหาวิทยาลัยศรีนครินทรวิโรฒ (มศว)

อาจารย์พิเศษ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยหอการค้าไทย

วิทยากร สมาคมผู้ใช้ดิจิทัลไทย (DUGA) และ สถาบันไอเอ็มซี (IMC)

ที่ปรึกษา โครงการภาครัฐของกระทรวงต่าง ๆ เช่น กระทรวงอุตสาหกรรร กระทรวงมหาดไทย
กระทรวงศึกษาธิการ และ สวทช. เป็นต้น

ที่ปรึกษา โครงการเตรียมความพร้อมปฏิบัติตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หน่วยงานภาครัฐและเอกชนชั้นนำ

Contents

1

กลยุทธ์ข้อมูล
และ
ความเสี่ยงในยุค AI

2

Governance
&
Ethics

3

Information Security
vs
Data Privacy

4

Risk
Management

01

กลยุทธ์ข้อมูลและความเสี่ยงในยุค AI

- **Data Strategy**
- ความเสี่ยงที่เกิดขึ้นกับการใช้ข้อมูลในยุค **AI**

กลยุทธ์ข้อมูลและความเสี่ยงในยุค AI

- Data Strategy
- ความเสี่ยงที่เกิดขึ้นกับการใช้ข้อมูลในยุค AI
  - Disinformation
  - Data Leakage
  - Deepfake
  - AI Bias

เหตุใดข้อมูลจึงจัดเป็นทรัพย์สินทางธุรกิจ?

เหตุใดข้อมูลจึงจัดเป็นทรัพย์สิน

ด้านการตัดสินใจและการวางกลยุทธ์

ข้อมูลช่วยในการตัดสินใจและวางกลยุทธ์องค์กร ทำให้องค์การสามารถใช้ข้อมูลเพื่อวิเคราะห์ทิศทางที่ดีที่สุดสำหรับธุรกิจ

ด้านการบริหารความเสี่ยง

การรวบรวมและวิเคราะห์ข้อมูลช่วยให้องค์กรสามารถระบุและจัดการกับความเสี่ยงในธุรกิจได้อย่างมีประสิทธิภาพ

ด้านการปรับตัวและการพัฒนา

ข้อมูลช่วยในกระบวนการปรับตัวและพัฒนาของธุรกิจ
เพื่อปรับตัวกับการเปลี่ยนแปลงในตลาดและสภาวะทางธุรกิจ

ด้านการสร้างมูลค่าเพิ่ม

การใช้ข้อมูลเพื่อสร้างผลิตภัณฑ์หรือบริการใหม่ หรือเพิ่มมูลค่าให้แก่ลูกค้า

Data Strategy
กลยุทธ์ด้านข้อมูล

Data Strategy

รวบรวมประเภทข้อมูลที่หลากหลาย

Business Process Data ห่วงโซ่อุปทาน, การเรียกเก็บเงินภายใน, การจัดการทรัพยากรมนุษย์

Product or Service Data ค่านิยมหลักของธุรกิจ

Customer Data ข้อมูลธุรกรรมการสำรวจลูกค้าบทวิจารณ์และความคิดเห็น พฤติกรรมการค้นหาและรูปแบบ Pattern

ใช้ข้อมูลเพื่อการตัดสินใจ

มีข้อมูลหัแต่ไม่ได้ใช้

Operations สำหรับการเพิ่มประสิทธิภาพทรัพยากร

Customer คาดการณ์การเปลี่ยนแปลงที่ให้ผลลัพธ์ที่ดีขึ้น

นำข้อมูลไปประยุกต์ใช้กับการสร้างสรรค์ผลิตภัณฑ์ใหม่

แปลงข้อมูลที่มีอยู่ให้เป็นผลิตภัณฑ์ใหม่

รวมข้อมูลข้ามไซโล

หาโอกาสจากข้อมูลที่ผสานกันระหว่างหน่วยงาน

ดูสิ่งที่ลูกค้าทำ ไม่ใช่สิ่งเขาพูด

พฤติกรรมการสืบค้นออนไลน์

Clickstream (สิ่งที่ลูกค้าคลิกหรือสิ่งในตะกร้าของลูกค้า)

Engagement data (ข่าวหรือบทความใดที่ลูกค้าสนใจเป็นพิเศษ)

มีคุณค่ามากกว่า Marketing Research หรือสิ่งที่เขาเล่า

ความเสี่ยงที่เกิดขึ้นกับการใช้ข้อมูลในยุค AI

การใช้ AI ในการสร้างข่าวปลอม

กรณีศึกษาข้อมูลเท็จ 2024

การเมือง: AI สร้างเสียงปลอมของผู้นำการเมือง

ข่าวปลอม: ภาพ Deepfake ของดาราและนักการเมือง

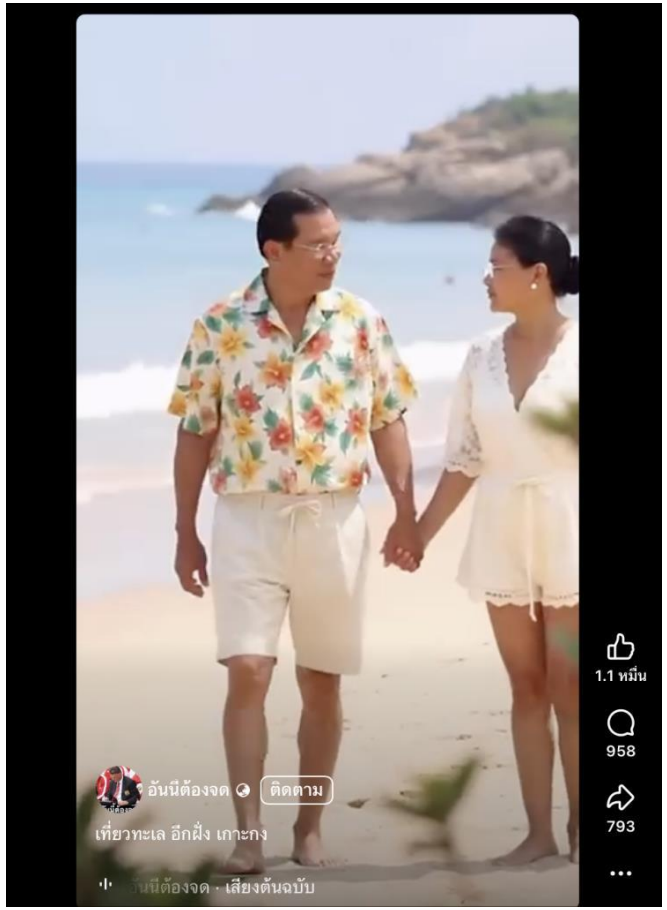
ข้อมูลสุขภาพ: คำแนะนำการรักษาที่ไม่ถูกต้องหรืออันตราย

ข้อมูลทางการเงิน: ราคาหุ้นและคำแนะนำการลงทุนผิด

ข้อมูลวิทยาศาสตร์: การตีความงานวิจัยผิด ๆ

การใช้ AI ปั่นข่าวปลอม

ตัวอย่างภาพปลอม AI ของสมเด็จฮุนเซน ผู้นำกัมพูชา



ที่มา: https://mgronline.com/cyberbiz/detail/9680000073642

Disinformation

การสร้างเนื้อหาปลอม

เช่น บทความ รูปภาพ วิดีโอ เสียง ที่มีความเหมือนจริง

×

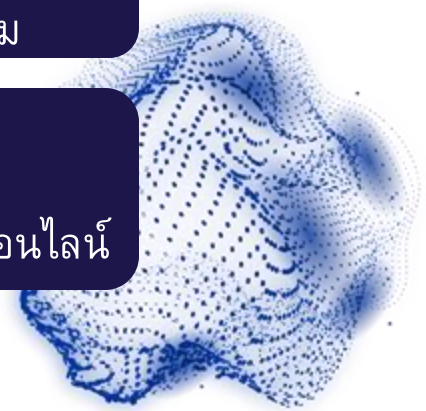
ผลลัพธ์ที่มีความ Bias

การโจมตีทางไซเบอร์

โจมตีระบบขโมยข้อมูล ปลอมแปลงข้อมูล สร้างความเสียหายต่อองค์กร

การขยายวง Disinformation

กระจายข่าวปลอมผ่านโซเชียลมิเดีย แพลตฟอร์มออนไลน์



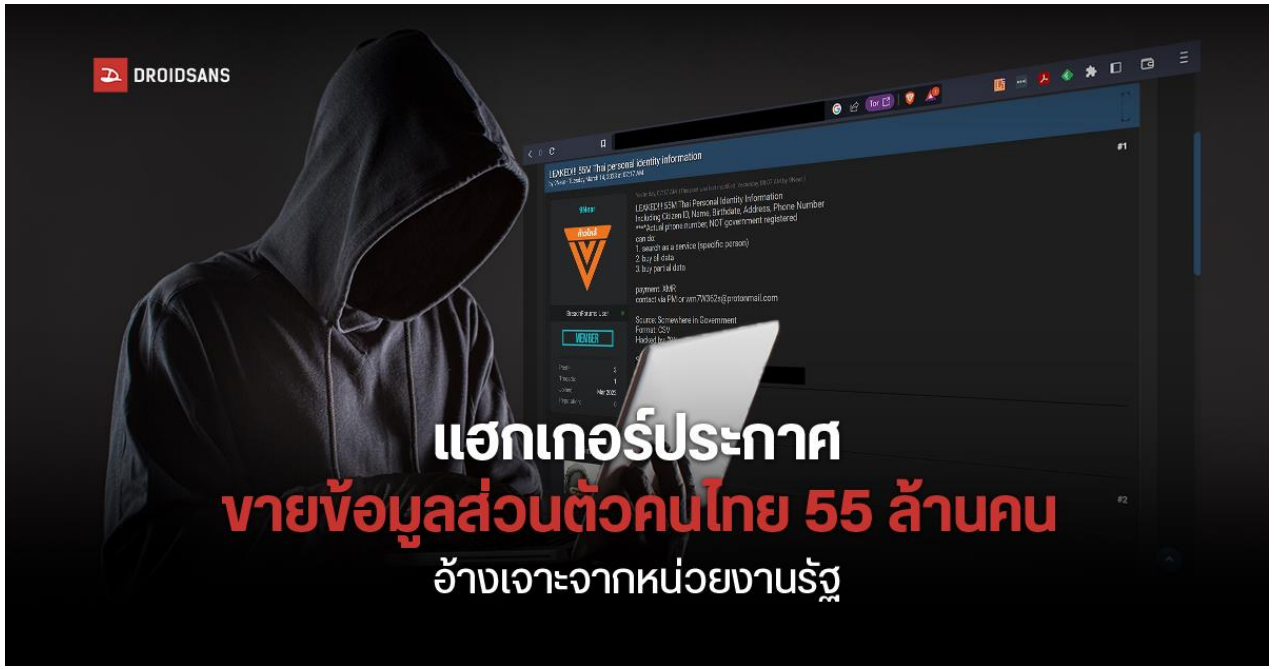
★☆☆

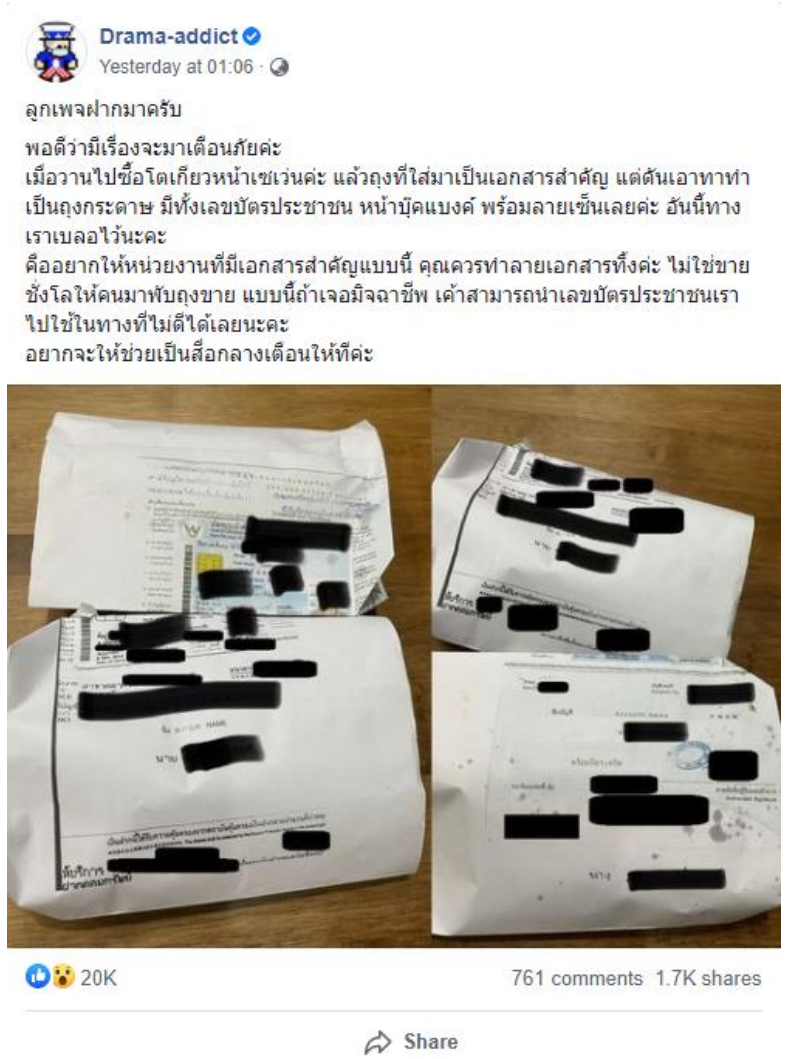
เสียชื่อเสียง

สูญเสียลูกค้า

เสียหายทางการเงิน

ข้อมูลรั่วไหล Data Leakage





ที่มา:
Droidsans
Drama-addict facebook page.

Deepfake

กาลามสูตร & Fake News

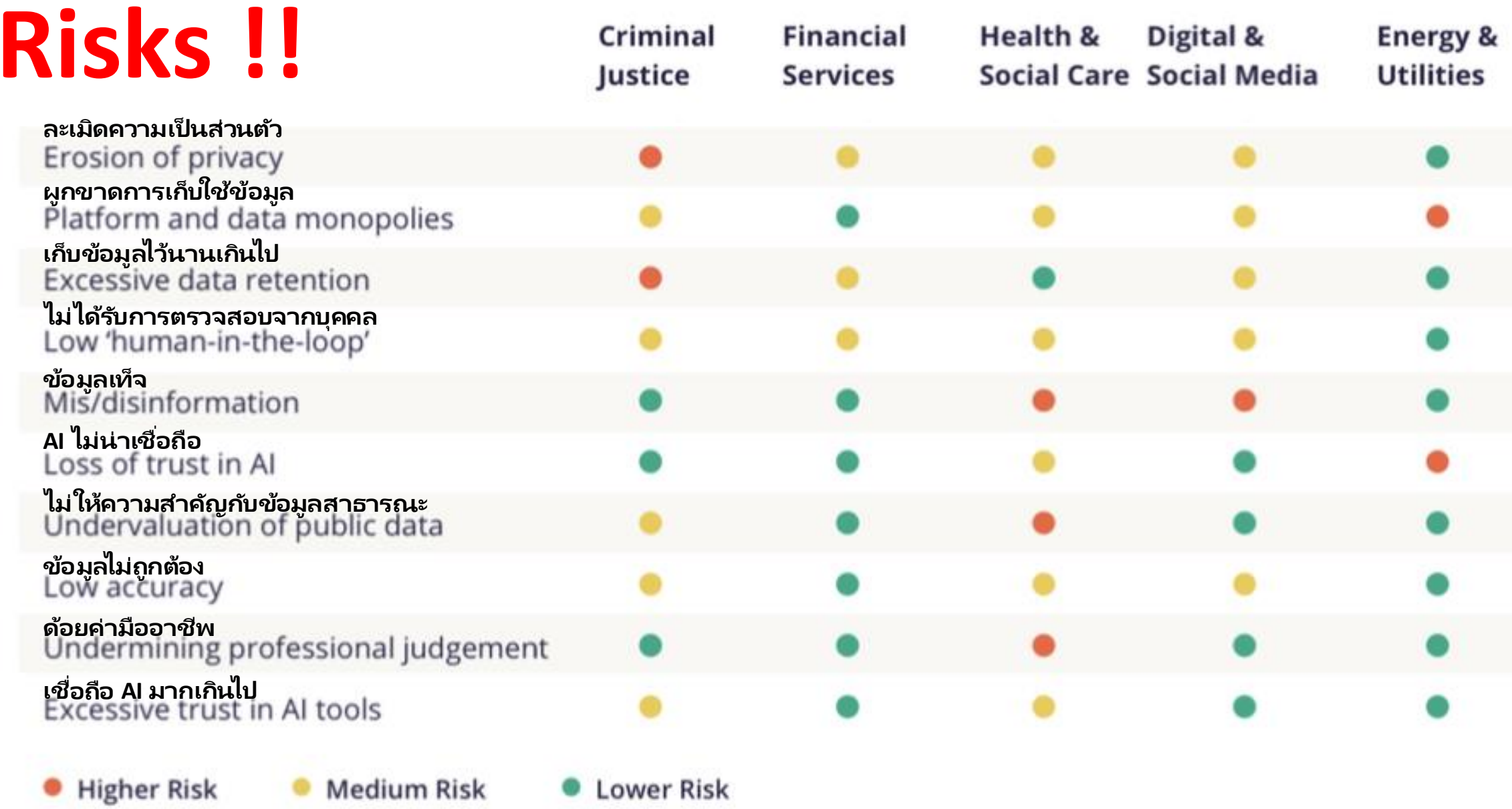
https://www.youtube.com/watch?v=CVcIT-bPzs4

Risks !! Bias ความลำเอียง

Common Risk	Criminal Justice	Financial Services	Health & Social Care	Digital & Social Media	Energy & Utilities
มีความลำเอียง Bias leading to discrimination	🔴	🔴	🔴	🔴	🟡
ไม่มีคำอธิบาย Lack of explainability	🔴	🔴	🟡	🔴	🔴
ไม่ทราบแหล่งข้อมูลอ้างอิง Regulator resourcing	🟡	🟡	🔴	🔴	🔴
เสี่ยงต่อการถูกโจมตี Higher-impact cyberattacks	🟡	🔴	🔴	🟡	🔴
ละเมิดลิขสิทธ์ผลงาน Failure of consent mechanisms	🔴	🟡	🔴	🔴	🟡
ขาดความน่าเชื่อถือ Loss of trust in institutions	🟡	🟡	🔴	🟡	🔴
ขาดความโปร่งใส Lack of transparency	🔴	🟡	🟡	🟡	🟡
ไม่สามารถเข้าถึงเครื่องมือหรือข้อมูลได้อย่างเท่าเทียม Unequal access to services	🟢	🔴	🔴	🟡	🟡
ข้อมูลไม่สมบูรณ์ Effects of low digital/data maturity	🟡	🟡	🔴	🟢	🔴

🔴 Higher Risk 🟡 Medium Risk 🟢 Lower Risk

Risks !!



blishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/894170/CDEI_AI_

02

Governance & Ethics

- Data & AI Governance
- Data & AI Ethics

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

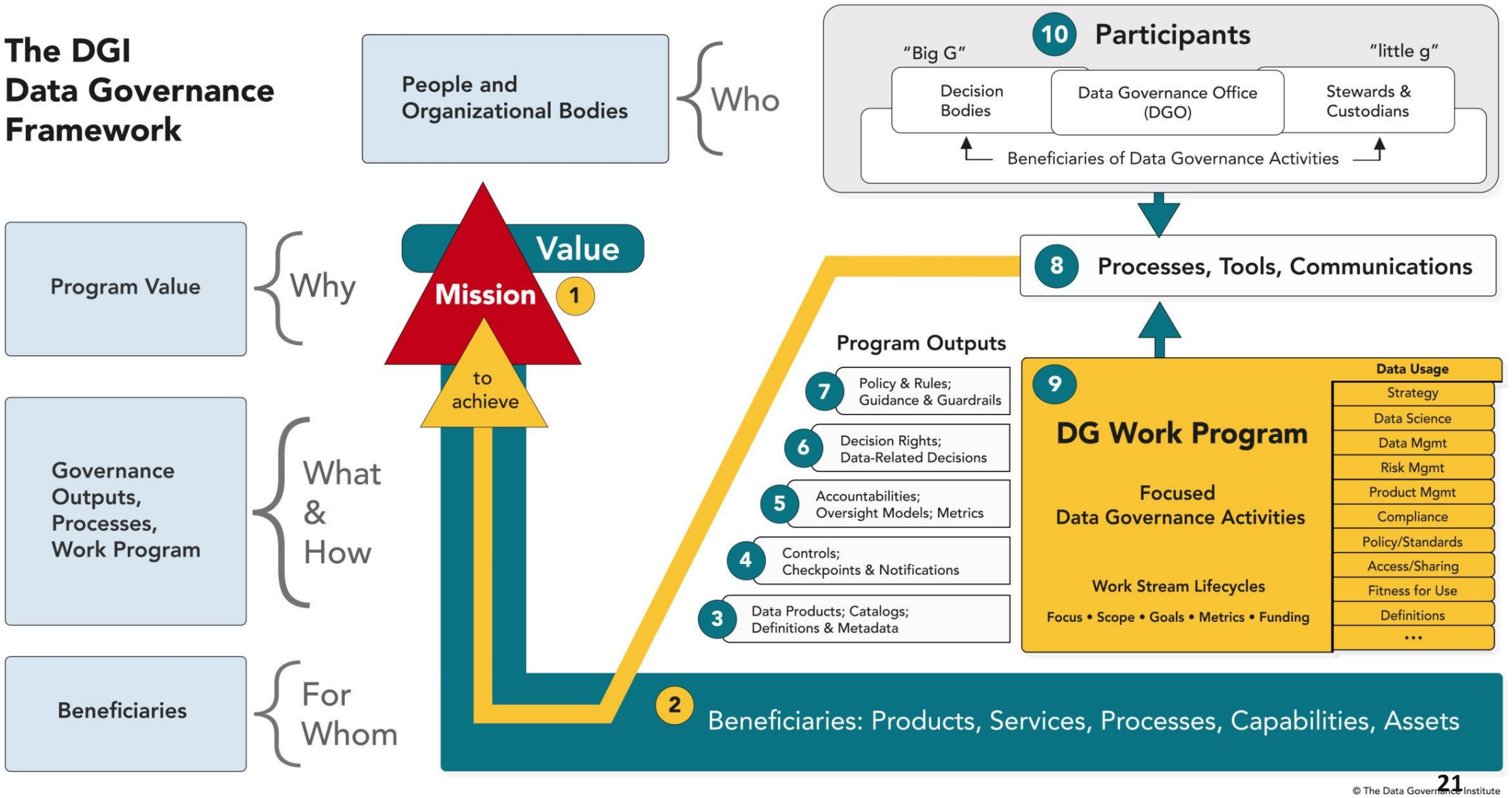
Data Governance

ธรรมาภิบาลข้อมูล

การธรรมาภิบาลข้อมูล คือการบริหารและจัดการอย่างถูกต้องเหมาะสมและสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน โดยเฉพาะอย่างยิ่งข้อมูลที่มีความอ่อนไหว ประกอบด้วยการกำหนด

- **นโยบาย** (Policies)
- **กระบวนการ**(Processes)
- **ความรับผิดชอบ** (Accountabilities)
- **โครงสร้างการตัดสินใจ**ที่เป็นทางการ และ
- **กฎข้อบังคับการใช้ข้อมูล**อย่างชัดเจนเหมาะสม

The DGI Data Governance Framework



กรอบธรรมาภิบาลข้อมูลภาครัฐ

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ในราชกิจจานุเบกษา **เมื่อวันที่ 31 มีนาคม พ.ศ. 2563** เพื่อให้หน่วยงานภาครัฐมีหลักการและแนวทางในการดำเนินการจัดทำธรรมาภิบาลข้อมูลภาครัฐ และสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government)

กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน

คณะกรรมการธรรมาภิบาลข้อมูล
(Data Governance Council)

ทีมบริกรข้อมูล
(Data Steward Team)

ผู้มีส่วนได้เสียกับข้อมูล
(Data Stakeholders)

โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)

ถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนบุคคล เชื่อมโยง เป็นประโยชน์

การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ
(Data Governance Metrics/Success Measures)

สภาพแวดล้อมของธรรมาภิบาลข้อมูล
(Data Governance Environment)

นิยามข้อมูล
(Data Definition)

กฎเกณฑ์ของข้อมูล/นโยบายข้อมูล
(Data Rules/ Data Policies)

นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules)

การวางแผน
(Plan)

การปฏิบัติ
(Do)

ตรวจสอบ วัดผล และรายงาน
(Check, Measure and Report)

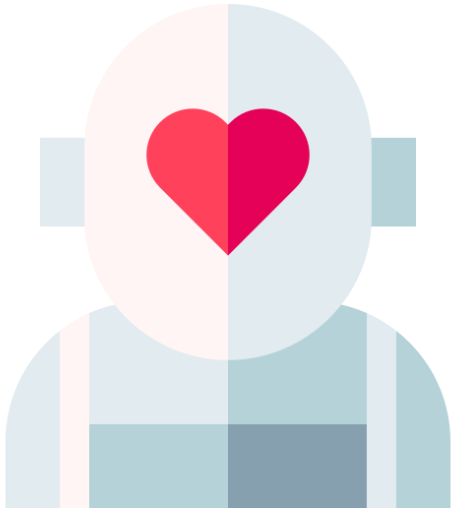
การปรับปรุงธรรมาภิบาลข้อมูล
(Continual Improvement)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐ
(Data Governance Processes)

ผลลัพธ์

- **คุณภาพข้อมูล**
- **ทะเบียนบัญชีรายชื่อข้อมูลภาครัฐ**
  นำไปสู่การเชื่อมโยงและแลกเปลี่ยนข้อมูล
- **การรักษาความปลอดภัยและคุ้มครองข้อมูลส่วนบุคคล**
- **การเปิดเผยข้อมูลเปิดภาครัฐ**
  นำไปสู่การใช้ประโยชน์ข้อมูลในมิติต่าง ๆ
- **มาตรฐานการแลกเปลี่ยนข้อมูล คู่มือแนวปฏิบัติ**
- **นโยบายในการขอใช้ข้อมูล**

AI Governance



AI Governance Framework

3-Key Components

1

AI GOVERNANCE STRUCTURE

Establishing an organization's structure for governing the use of AI

1.1 AI Governance Council
1.2 Roles & Responsibilities
1.3 Competency Building

2

AI STRATEGY

Defining AI strategy as well as managing AI-related risks

2.1 Responsible AI Strategy
2.2 AI Risk Management

3

AI OPERATION

Governing operations and providing AI-related services

3.1 AI Lifecycle
3.2 AI Service and Feedback

AI Governance Guideline for Executives

1. AI Governance Structure
"Preparing Organization"

1.1 AI Governance Council
(Establishment of a governing body)

Members:
- Senior Management, Relevant teams (e.g., Technical, Business, Compliance), External Parties (e.g., Regulators, Domain Expert)

Roles:
- Defining direction, monitoring performance & compliance, and evaluation

1.2 Defining Roles and Responsibilities

Strategic Level
- Overseeing and ensure that the use of AI aligns with objectives, laws, and regulations.
- Overseeing risk management.

Implementation Level
- Operating in accordance with strategy, laws, and regulations.
- Design, develop, and deploy AI models.
- Risk control.

1.3 Competency Building
1) Business knowledge
2) Technology knowledge
3) Regulatory knowledge

2. AI Strategy
"Setting Strategies and AI-related Risk Management"

2.1 Setting Responsible AI Strategy

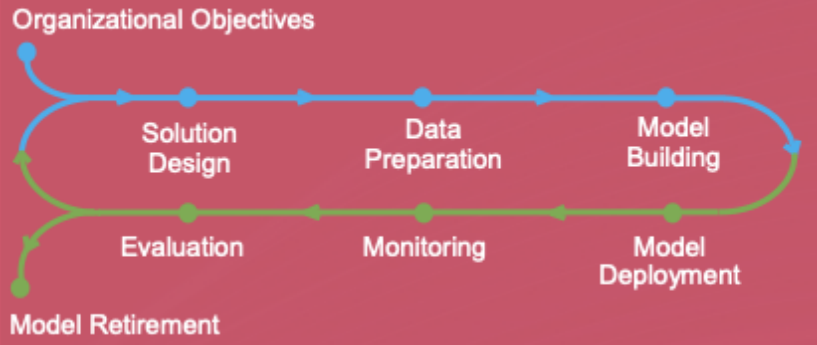
2.2 AI Risk Management
(Managing risks associated with the use of AI)

Organization/ Business Value
- **Defining objectives & areas where AI can add values, considering:** Benefits to the organization, alignment with goals of organization or business, limitations and challenges, etc.
- **Developing AI Roadmap:** Prioritizing tasks, creating a roadmap, and developing a prototype.

AI-Related Risk
- **Example of risks:** Cyber Attack, Trust & Reputation, Privacy, Data Quality, Non-Compliance, Fairness & Non-Discrimination.
- **Relevant standard:** NIST & ISO Standard
- **Human involvement:**
  1) Human-in-the-loop
  2) Human-over-the-loop
  3) Human-out-of-the-loop

3. AI Operation
"Governing Operations and Providing AI-related Services"

3.1 AI Lifecycle



3.2 AI Services

1) Announce policies and provide information about the use of AI to users, such as AI usage policy, relevant AI ethics principles, how to use AI, how to disable AI, AI capabilities and limitations.

2) Providing feedback channels
Getting user feedback, problems, and errors found in use.

Toolkits supporting AI Governance 1) AI Readiness Assessment 2) AI Use Case Canvas 3) Risk Assessment

Ethics

จริยธรรม AI คืออะไร ?

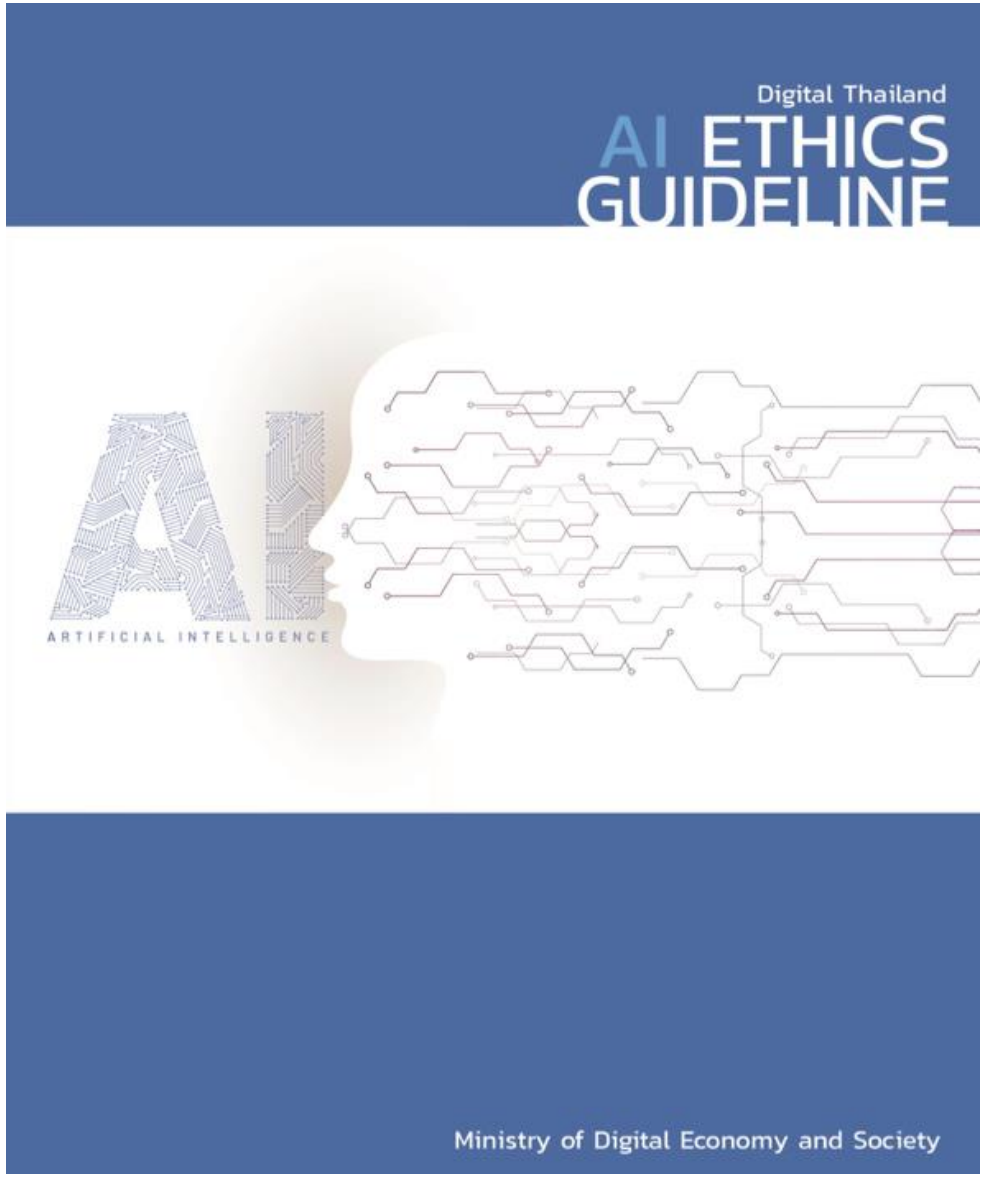
“จริยธรรม AI คือชุดของค่านิยม หลักการ และเทคนิค ที่ใช้มาตรฐานที่ได้รับการยอมรับอย่างกว้างขวางเกี่ยวกับสิ่งที่ถูกและผิด เพื่อเป็นแนวทางในการปฏิบัติทางศีลธรรมในการพัฒนาและการใช้เทคโนโลยี AI”

ที่มา: Dr. David Leslie
https://www.turing.ac.uk/sites/default/flies/2019-06/understanding_artificial_intelligence_ethic_and_safety.pdf

ทำไม จริยธรรม AI จึงสำคัญ ?

- **ปกป้องสิทธิและความเป็นส่วนตัว** AI มักใช้ข้อมูลส่วนบุคคล หากไม่มีหลักจริยธรรมอาจละเมิดสิทธิและกฎหมาย เช่น PDPA
- ลดอคติและความไม่เป็นธรรม AI อาจสร้างผลลัพธ์ที่เลือกปฏิบัติจากข้อมูลฝึกที่มี bias
- เพิ่มความโปร่งใสและความน่าเชื่อถือ ผู้ใช้ต้องเข้าใจว่า AI ตัดสินใจอย่างไร
- ป้องกันผลกระทบทางสังคม ลดความเสี่ยงเรื่องการตกงาน, การแพร่ข่าวปลอม, Deepfake
- ใช้เทคโนโลยีอย่างรับผิดชอบ ให้ AI เป็นประโยชน์ต่อสังคม ไม่ถูกนำไปใช้ในทางที่ผิด

Ethics Guideline by ETDA



1 ความสามารถในการแข่งขันและการพัฒนาอย่างยั่งยืน (Competitiveness and Sustainability Development)

2 ความสอดคล้องกับกฎหมายจริยธรรมและมาตรฐานสากล (Laws Ethics and International Standards)

3 ความโปร่งใสและภาระความรับผิดชอบ (Transparency and Accountability)

4 ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy)

5 ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness)

6 ความน่าเชื่อถือ (Reliability)

WORKSHOP

การประเมินการกำกับดูแลข้อมูลขององค์กร

Data Governance Assessment

ระดับความพร้อมของการกำกับดูแลข้อมูล

ดับ	โครงสร้างการกำกับดูแล	กระบวนการกำกับดูแล	นโยบายข้อมูลและการตรวจสอบ	การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	การวัดความ การปรับป ต่อเนื่
	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมี ทางก
	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมี ทางก
ed	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐานส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมี ทางก
rdized	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมี ทางก
ced	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	ไม่มีหรือมี ทางก
zed	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	มีการวัดความ ปรับปรุงกระ อย่างต่อ

03

Security vs Privacy

- Cyber Security and PDPA
- ISO/IEC 27001 & 27701

Security vs Privacy

- Information Security vs Data Privacy
- Cyber Security & ISO/IEC 27001
- PDPA Law & ISO/IEC 27701
- แนวทางปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) สำหรับผู้บริหาร
- วิเคราะห์กรณีละเมิด PDPA

Information Security *vs* Data Privacy

Information Security vs. Data Privacy

ทำความเข้าใจความแตกต่างที่สำคัญ

1. ความปลอดภัยของข้อมูล (Information Security)

เป็นการปฏิบัติและเทคนิคที่มุ่งเน้นการ **ปกป้องข้อมูล** และระบบสารสนเทศจากการเข้าถึง, ใช้งาน, เปิดเผย, ดัดแปลง, หรือทำลายโดยไม่ได้รับอนุญาต

🎯 เป้าหมายหลัก: CIA Triad

เพื่อให้มั่นใจว่าข้อมูลบรรลุหลักการ 3 ประการ: การรักษาความลับ (Confidentiality), ความสมบูรณ์ (Integrity), และความพร้อมใช้งาน (Availability)

2. ความเป็นส่วนตัวของข้อมูล (Data Privacy)

เป็น **สิทธิของบุคคล** ในการควบคุมว่าข้อมูลส่วนบุคคลของตนจะถูกเก็บรวบรวม, จัดเก็บ, ใช้, และแบ่งปันอย่างไร และด้วยวัตถุประสงค์ใด

🎯 เป้าหมายหลัก: การปฏิบัติตามข้อกำหนด

เพื่อให้มั่นใจว่าองค์กรปฏิบัติต่อข้อมูลส่วนบุคคลอย่างยุติธรรม, ชอบธรรม, และโปร่งใส สอดคล้องกับข้อกฎหมาย (เช่น PDPA)

Information Security vs Data Privacy

ตารางสรุปความแตกต่าง

การเปรียบเทียบแบบเจาะจงใน 4 คุณสมบัติหลัก

คุณสมบัติ	ความปลอดภัยของข้อมูล (Security)	ความเป็นส่วนตัวของข้อมูล (Privacy)
จุดเน้น	ปกป้อง **ข้อมูล** (ทั้งหมด) จากภัยคุกคาม	ปกป้อง **สิทธิ** ของบุคคลใน **ข้อมูลส่วนบุคคล**
คำถามหลัก	เราจะป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตได้อย่างไร?	เราได้รับอนุญาตให้ใช้ข้อมูลนี้หรือไม่ และใช้อย่างไร?
ขอบเขต	**เทคนิคและเครื่องมือ** (Firewall, Encryption)	**กฎหมายและนโยบาย** (PDPA, GDPR)
สิ่งที่ปกป้อง	ข้อมูลและระบบทั้งหมดขององค์กร	ข้อมูลที่ระบุตัวบุคคลได้ (PII)

Information Security vs Data Privacy

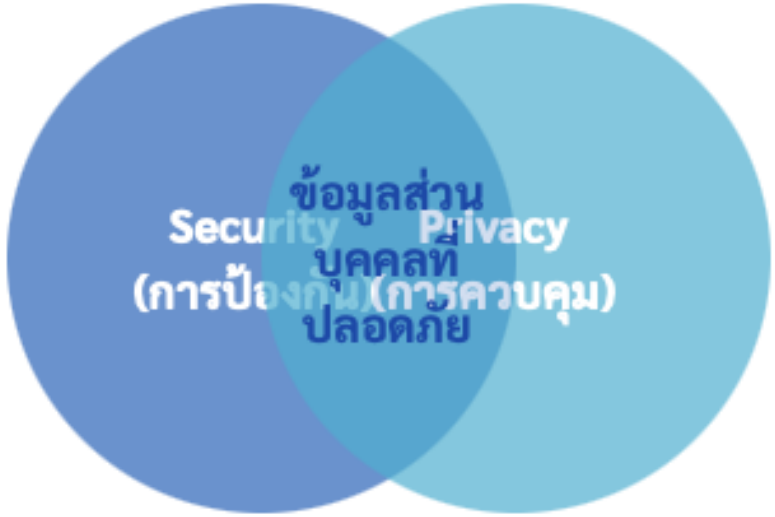
Security คือเครื่องมือ, Privacy คือเป้าหมาย

คุณไม่สามารถมีความเป็นส่วนตัวของข้อมูล (Privacy) ได้ หากไม่มีความปลอดภัยของข้อมูล (Security) ที่ดีพอ

➡️ **ตัวอย่าง:** หากข้อมูลส่วนบุคคลถูกแฮ็ก (Security ล้มเหลว), ความเป็นส่วนตัว (Privacy) ก็ถูกละเมิดทันที

แต่การมี Security ที่ดี **ไม่ได้** แปลว่ามี Privacy เสมอไป

➡️ **ตัวอย่าง:** บริษัทอาจเก็บข้อมูลคุณอย่างปลอดภัยสูงสุด (Security ดีเยี่ยม) แต่กลับนำข้อมูลนั้นไปขายโดยที่คุณไม่ยินยอม (ละเมิด Privacy)



Information Security, Cyber Security Law and ISO/IEC 27001

Infosec, กฎหมายไซเบอร์ไทย, และ ISO 27001

ทำความเข้าใจ 3 เสาหลักแห่งความมั่นคงปลอดภัยไซเบอร์

1. Information Security (Infosec)

บทบาท: การปฏิบัติ (Practice)

คือหลักการพื้นฐาน, มาตรการ และเครื่องมือทางเทคนิค (เช่น Firewall, การเข้ารหัส) ที่ใช้เพื่อปกป้องข้อมูลให้ปลอดภัย

2. พ.ร.บ. ไซเบอร์ฯ (Cyber Law)

บทบาท: ข้อบังคับ (Mandate)

คือกฎหมายที่ "บังคับ" ให้องค์กร (โดยเฉพาะ CII) ต้องนำมาตรการ Infosec มาใช้ เพื่อรักษาความมั่นคงของชาติ

3. ISO/IEC 27001

บทบาท: ระบบบริหารจัดการ (System)

คือกรอบการทำงาน (Framework) สากล ที่กำหนด "วิธีการ" สร้างระบบ (ISMS) เพื่อบริหารจัดการ Infosec อย่างเป็นระบบ

InfoSec, CyberSec & ISO 27001

ตารางสรุปบทบาท

องค์ประกอบ	บทบาทหลัก	ขอบเขตการทำงาน
Infosec	การปฏิบัติ (Practice)	การกระทำและเครื่องมือที่ใช้ปกป้องข้อมูล (CIA Triad)
กฎหมายไซเบอร์	ข้อบังคับ (Mandate)	กำหนดขีดจำกัดความปลอดภัยขั้นต่ำที่ "ต้อง" มีตามกฎหมาย
ISO 27001	ระบบบริหารจัดการ (System)	กำหนด "วิธีการ" สร้างระบบเพื่อจัดการความเสี่ยงด้าน Infosec

Data Privacy, PDPA Law and ISO/IEC 27701

Data Privacy, PDPA, และ ISO 27701

ความสัมพันธ์ของ 3 เสาหลักแห่งการคุ้มครองข้อมูลส่วนบุคคล

1. Data Privacy

บทบาท: หลักการ (Concept)

คือ "แนวคิดและสิทธิพื้นฐาน" ของบุคคลในการควบคุมข้อมูลส่วนตัวของตนเอง เป็นรากฐานและเป้าหมายสูงสุด

2. PDPA Law (พ.ร.บ.)

บทบาท: ข้อบังคับ (Mandate)

คือ "กฎหมาย" ที่นำหลักการ Privacy มาบังคับใช้, กำหนดหน้าที่, ความรับผิดชอบ และบทลงโทษที่รุนแรง

3. ISO/IEC 27701

บทบาท: ระบบบริหารจัดการ (PIMS)

คือ "วิธีการ" หรือกรอบการทำงานสากล ที่ช่วยองค์กรสร้างระบบ (PIMS) เพื่อจัดการ Privacy และปฏิบัติตาม PDPA

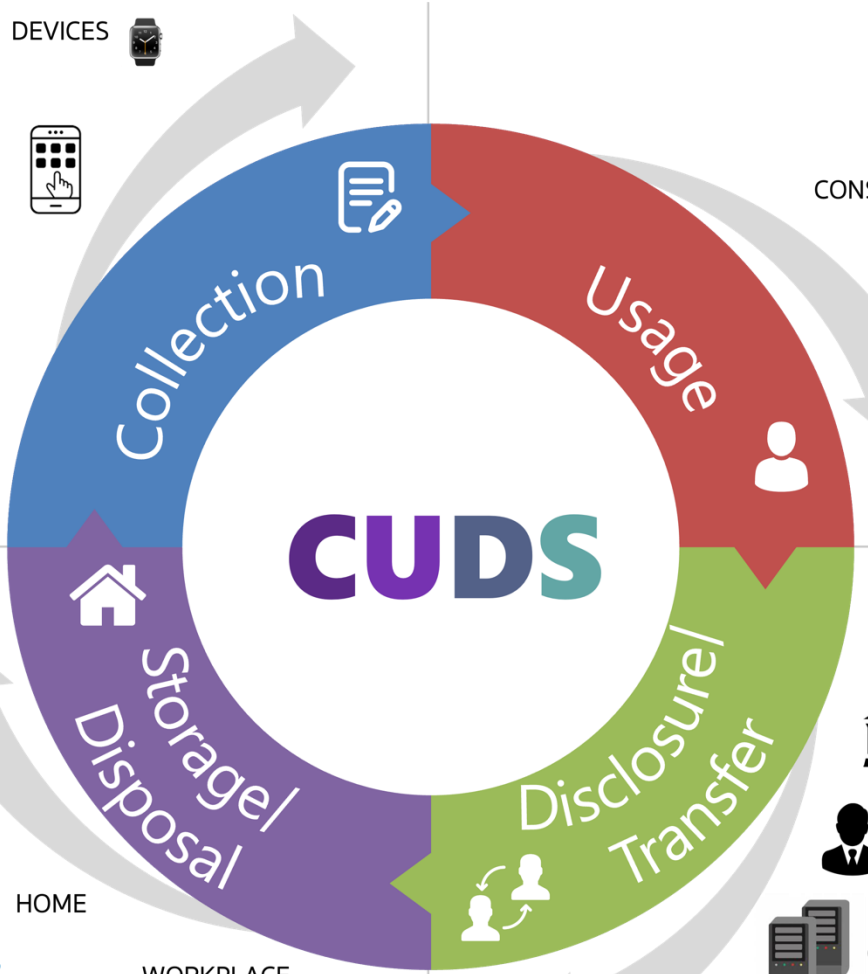
Data Privacy, PDPA & ISO 27701

ตารางสรุปบทบาท

องค์ประกอบ	บทบาทหลัก	ขอบเขตการทำงาน
Data Privacy	หลักการ (Concept)	สิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคล
PDPA Law	ข้อบังคับ (Mandate)	กฎหมายที่ "บังคับ" ให้องค์กรต้องคุ้มครองข้อมูลและมีบทลงโทษ
ISO 27701	ระบบบริหารจัดการ (PIMS)	กำหนด "วิธีการ" สร้างระบบเพื่อจัดการข้อมูลส่วนบุคคลและบรรลุ Compliance

การบริหาร Privacy Management ตามวงจรข้อมูล

การบริหาร Privacy Management ตามวงจรข้อมูล



จุดที่เก็บรวบรวมข้อมูล (Collection point)

ความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล (Exposure and risk)

DEVICES

MOBILE APP

CCTV

CALL CENTRE

ONLINE FORMS

การใช้ข้อมูลหลังจากที่เก็บรวบรวมข้อมูล

CONSENT

ความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล (Exposure and risk)

เก็บข้อมูลไว้ตามระยะเวลาที่กำหนด (retention period)

สถานที่จัดเก็บข้อมูลมีความปลอดภัยเพียงใด

COMPUTER/ DEVICES

CLOUD STORAGE

FILES

HOME

WORKPLACE

ความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล (Exposure and risk)

เปิดเผยข้อมูลไปนอกองค์กร

OUTSOURCED SERVICES

AUTHORITIES

PARTNERS

OUTSIDE SERVER

PRINTING PLACE

เปิดเผยข้อมูลไปนอกประเทศไทย

ความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล (Exposure and risk)

ข้อแนะนำเมื่อต้องเก็บต้องเก็บข้อมูลส่วนบุคคล

แจ้ง เจ้าของข้อมูลว่า เก็บเพื่ออะไร นานแค่ไหน

ขอ ความยินยอมจากเจ้าของข้อมูล (เมื่อจำเป็นเท่านั้น)

จัดการ คำขอใช้สิทธิเจ้าของข้อมูล

รักษา ข้อมูลอย่าให้รั่วไหล

ทำลาย ข้อมูลเมื่อครบกำหนด

Template เอกสาร PDPA จากหน่วยงาน DGA

สามารถนำไปปรับใช้ตามความเหมาะสม

https://www.dga.or.th/document-sharing/article/59030/

คลิปอบรม PDPA เบื้องต้น

จัดทำโดย มหาวิทยาลัยหอการค้าไทย ให้กับกระทรวง DES

EP1 https://www.youtube.com/watch?v=MBeK0KrHd5w

EP2 https://www.youtube.com/watch?v=7h72snD29Ls

Discussion #1

Youtuber ชื่อ Eddy ถ่ายทำรายการ “กินแหลก” มาหลาย Episode แล้ว Youtuber Eddy ต้องเข้าข่ายปฏิบัติตาม PDPA หรือไม่?

- **YouTuber Eddy** ถือเป็น **Data Controller** ที่จะต้องพิจารณาถึงความเป็นส่วนตัวในข้อมูลส่วนบุคคลของคนอื่น ๆ ที่ติดมาจากการถ่ายทำที่มาทานอาหารใน Clip เพราะเห็นหน้าและอิริยาบถของคนเหล่านั้นชัดเจน

Photo source: thaismescenter.com

Discussion #2

บริษัทใช้กล้อง CCTV ตรวจสอบความเรียบร้อยของสถานที่เพื่อใช้เป็นหลักฐานป้องกันเหตุอันตราย บริษัทมี Lawful Basis ในการใช้ข้อมูลส่วนบุคคลหรือไม่?

เฉลย

บริษัทใช้กล้อง CCTV ตรวจสอบความเรียบร้อยของสถานที่เพื่อใช้เป็นหลักฐานป้องกันเหตุอันตราย บริษัทมี Lawful Basis ในการใช้ข้อมูลส่วนบุคคลหรือไม่?

ตอบ: ฐานผลประโยชน์อันชอบธรรม (Legitimate Interest)

ซึ่งการใช้ข้อมูลส่วนบุคคลในกิจกรรมนี้ต้องไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject

04

Risk Management

- แนวทางการจัดการความเสี่ยง

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

แนวปฏิบัติในการป้องกันความเสี่ยง และบรรเทา

5 Pillars to managing risk and ethical compliance

Data Security

ความปลอดภัยของข้อมูล

The practice of protecting data from unauthorized access, corruption, or theft throughout its entire life cycle.

Data Privacy

ความเป็นส่วนตัวของข้อมูล

Determines whether, or how, data is used internally, shared with third parties, how data is legally collected or stored, and the regulatory restrictions in which the business operates.

Data Ethics

จริยธรรมข้อมูล

The responsible use of data, doing the right thing for people and society even when no one is looking or checking.

Data Compliance

การปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับการใช้ข้อมูล

Ensuring that data is organized and managed so that organizations meet enterprise business rules and legal and governmental regulations.

Data Fraud Prevention

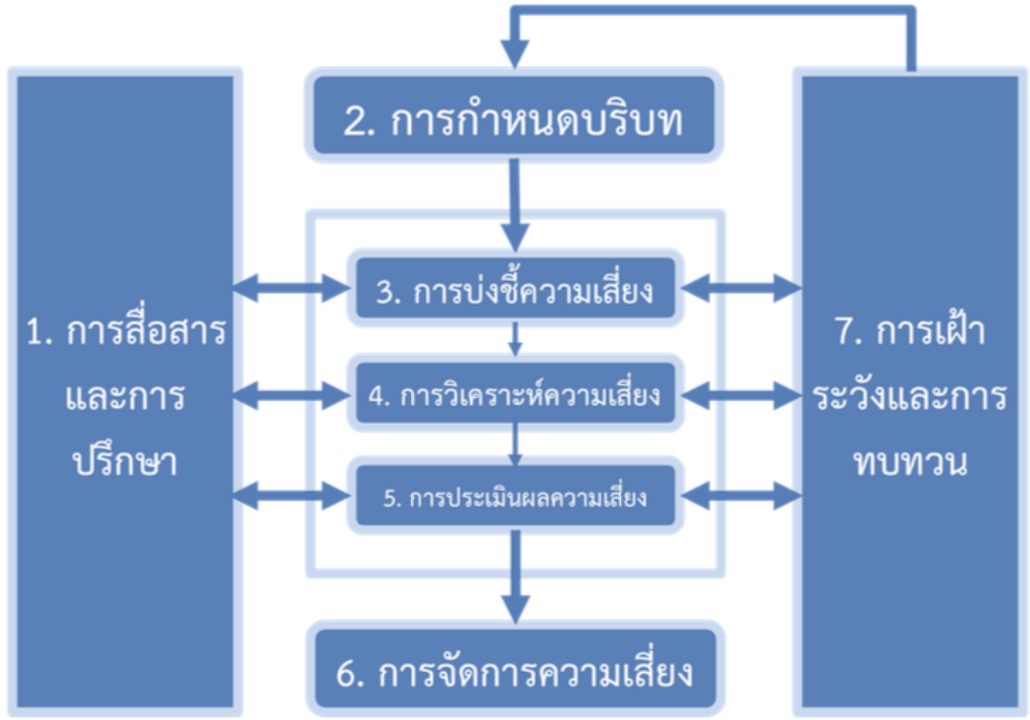
การป้องกันการปลอมแปลงข้อมูล

The deliberate fabrication or falsification of data for financial gain.

หลักการและขั้นตอน

ISO 31000 คือ มาตรฐานที่เป็นหลักการและแนวทางในการบริหารความเสี่ยงขององค์กร ซึ่งสามารถนำไปประยุกต์ใช้ได้กับองค์กรทั้งภาครัฐและเอกชน ได้ทุกขนาดและทุกชนิดของธุรกิจ

กระบวนการบริหารความเสี่ยง



ประเภทของความเสี่ยง

- ความเสี่ยงด้านกลยุทธ์
- ความเสี่ยงด้านการปฏิบัติงาน
- ความเสี่ยงด้านการปฏิบัติตาม กฎ ระเบียบ ข้อบังคับ กฎหมาย
- ความเสี่ยงด้านการเงิน
- ความเสี่ยงด้านข้อมูล

ประเภทของความเสี่ยง

- ความเสี่ยงด้านกลยุทธ์
- ความเสี่ยงด้านการปฏิบัติงาน
- ความเสี่ยงด้านการปฏิบัติตาม กฎ ระเบียบ ข้อบังคับ กฎหมาย
- ความเสี่ยงด้านการเงิน
- ความเสี่ยงด้านข้อมูล

โดยระบุ เหตุการณ์หรือกิจกรรม และ ความเสี่ยงที่อาจจะเกิดขึ้น

ตัวอย่างเงื่อนไข การวิเคราะห์ความเสี่ยง

- โอกาสจะเกิดความเสี่ยง ความถี่ และ คะแนน
- ผลกระทบ มูลค่าความเสี่ยหาย และ คะแนน

โอกาสจะเกิดความเสี่ยง	ความถี่	ระดับคะแนน
สูงมาก	มีโอกาสเกิดเกือบทุกครั้ง	5
สูง	มีโอกาสเกิดค่อนข้างสูงหรือบ่อย ๆ	4
ปานกลาง	มีโอกาสเกิดบางครั้ง	3
น้อย	อาจมีโอกาสเกิดแต่นาน ๆ ครั้ง	2
น้อยมาก	มีโอกาสเกิดในกรณียกเว้น	1

ผลกระทบ	มูลค่าความเสียหาย	ระดับคะแนน
รุนแรงที่สุด	มีการสูญเสียทรัพย์สินอย่างมหันต์ บาดเจ็บถึงชีวิต	5
ค่อนข้างรุนแรง	สูญเสียทรัพย์สินมาก บาดเจ็บสาหัสถึงขั้นพักงาน	4
ปานกลาง	สูญเสียทรัพย์สินมาก บาดเจ็บสาหัสถึงขั้นหยุดงาน	3
น้อย	สูญเสียทรัพย์สินพอสมควร บาดเจ็บรุนแรง	2
น้อยมาก	สูญเสียทรัพย์สินเล็กน้อย ไม่มีการบาดเจ็บรุนแรง	1

ที่มา: Danairat T.

ตัวอย่างเงื่อนไข การวิเคราะห์ความเสี่ยง

- โอกาสจะเกิดความเสี่ยง ความถี่ และ คะแนน
- ผลกระทบ มูลค่าความเสี่ยหาย และ คะแนน

โอกาสจะเกิดความเสี่ยง	ความถี่	ระดับคะแนน
สูงมาก	1 เดือนต่อครั้งหรือมากกว่า	5
สูง	1-6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้ง	4
ปานกลาง	1ปีต่อครั้ง	3
น้อย	มากกว่า 1 ปี แต่ไม่เกิน 3 ปีต่อครั้ง	2
น้อยมาก	มากกว่า 3 ปีต่อครั้ง	1

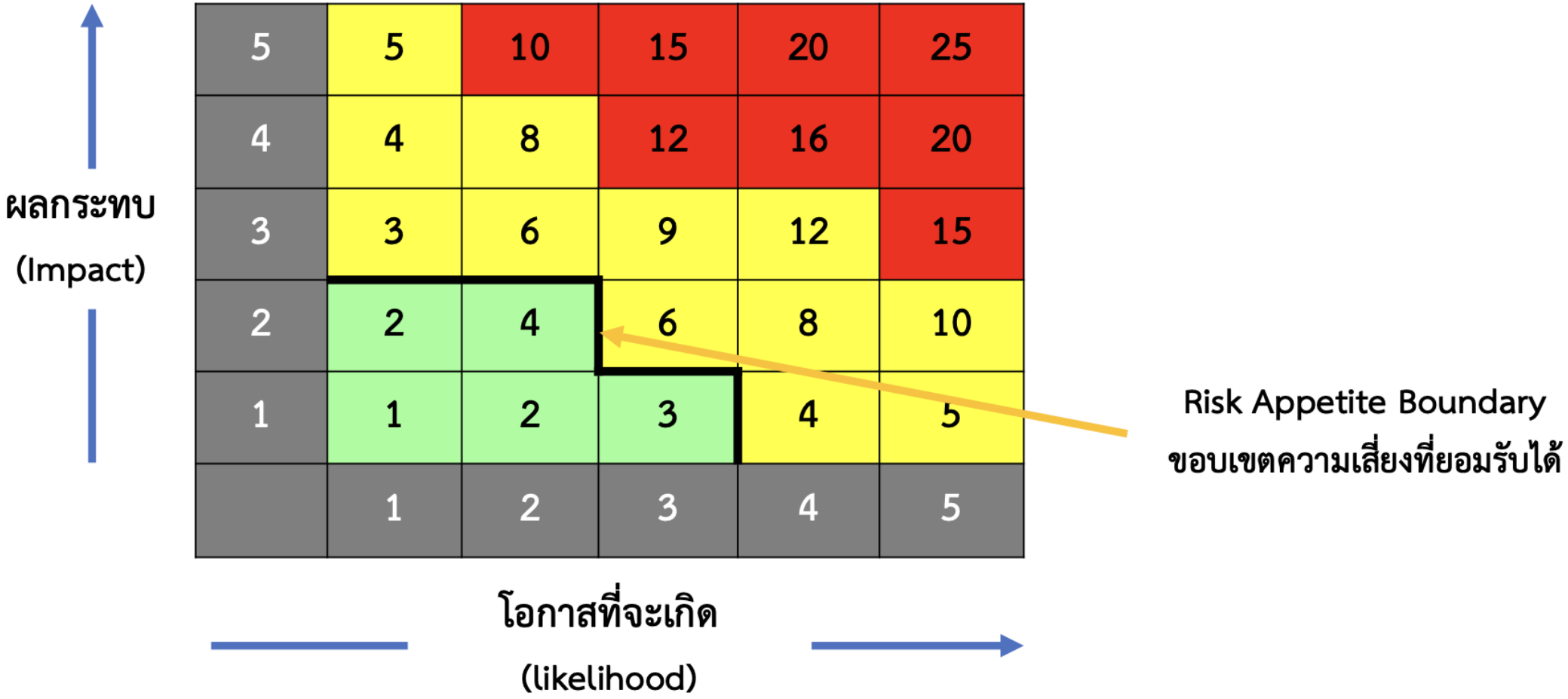
ผลกระทบ	มูลค่าความเสียหาย	ระดับคะแนน
สูงมาก	> 10,000,000 บาท	5
สูง	> 250,000 – 10,000,000 บาท	4
ปานกลาง	> 50,000 – 250,000 บาท	3
น้อย	> 10,000 - 50,000 บาท	2
น้อยมาก	ไม่เกิน10,000 บาท	1

ที่มา: Danairat T.

การประเมินความเสี่ยง

ที่มา: Danairat T.

การประเมินความเสี่ยง



ที่มา: Danairat T.

WORKSHOP

การวางแนวปฏิบัติในการป้องกันและบรรเทาความเสี่ยงในการใช้ Data และ AI เพื่อ Analytics

DGA305 Data/AI Risk Expert

https://tinyurl.com/yc8dwm8j

Acknowledgements

Content Contribution

Mayuree Srikulwong
FB Page: AjT Mayuree

Attasit Pattanasiri

Chatchai Wangwiwattana
Youtube: หมากมัคิจิทัล Mark Digital

Slide Preparation

Akkharawit Somwong

Nannapat Kongphaet

Theerapat Yaso

Generative AI

Time for Reflection