

เสวนา IA Clinic ครั้งที่ 8/2569



PDPA, Data Governance และบทบาทของ Internal Audit ในการคุ้มครองข้อมูลขององค์กร



เสวนา On-site
60 ที่นั่ง

หรือ



Online ผ่าน
Microsoft teams



เสวนาวันที่
19 กันยายน 2569



เวลา
09.00–12.00 น.



ณ ห้องเสรี จินตนา เสรี ชั้น 7
ตลาดหลักทรัพย์แห่งประเทศไทย



คุณรุจคุณ โตนำชัย

CISA, CRISC, CDPSE, AAIA
Managing Partner – ICONIC ADVISORY
กรรมการ – ISACA Bangkok Chapter



คุณจักรกฤษณ์ บุรี

CPIAT, GCIO, ISO/IEC 27001
Lead Auditor
CAE ธนาคารอิสลามแห่งประเทศไทย



ติดต่อ IIA Thailand



member@theiiat.or.th



www.theiiat.or.th



02-7129124 ต่อ 101-108

IA CLINIC ครั้งที่ 8/2569 PDPA, DATA GOVERNANCE และ บทบาทของ INTERNAL AUDIT ในการคุ้มครองข้อมูลขององค์กร

รศคุณ โทวนำชัย CISA, CRISC, CDPSE, AAIA
จักรกฤษณ์ บุรี CPIAT, GCIO, ISO/IEC 27001 Lead Auditor



Institute of
Internal Auditors
Thailand



Today Agenda



1. PDPA



2. DATA GOV



3. AI - PDPA - DATA GOV



Institute of
Internal Auditors
Thailand



1. PDPA



iCONIC
ADVISORY



Institute of
Internal Auditors
Thailand



DPO ควรเป็นใคร

PDPA AUDIT



Institute of
Internal Auditors
Thailand



การกำกับดูแล	เอกสารต่างๆ	การปฏิบัติ (Operation)
 DPO และโครงสร้างการกำกับ  นโยบายและกรอบการดำเนินงาน  การอบรมและสร้างความตระหนัก  การกำกับผู้ประมวลผลและคู่ค้า	 RoPA — บันทึกกิจกรรมการประมวลผล  DPIA — การประเมินผลกระทบ  Privacy Notice และบันทึกความยินยอม  DPA — สัญญากับผู้ประมวลผล	 DSR — การรองรับสิทธิเจ้าของข้อมูล  Retention และการทำลายข้อมูล  Breach Response และการแจ้งเหตุ  การส่งต่อและการโอนข้ามพรมแดน



Institute of
Internal Auditors
Thailand



AI มาช่วย PDPA Audit จุดไหนได้บ้าง?

| IT PDPA AUDIT



Institute of
Internal Auditors
Thailand



Consent Mgmt



DSR Mgmt



Retention



Masking



Anonymisation



DLP



Log / SIEM



IAM

| แล้ว “ผู้ตรวจสอบเอง” ล่ะ?



Institute of
Internal Auditors
Thailand



หลักฐานการตรวจ

Payroll, Timesheet,
สำเนาบัตรประชาชน



ฐานกฎหมายของ IA

Legitimate Interest
+ Audit Charter



ผู้รับตรวจปฏิเสธ โดยอ้าง PDPA

ประเด็นที่เจอบ่อยที่สุด
ในทางปฏิบัติ



การเปิดเผยในรายงาน

ระบุชื่อได้แค่ไหน
และเก็บ/ทำลายอย่างไร



Institute of
Internal Auditors
Thailand



2. Data Governance





Institute of
Internal Auditors
Thailand



DATA เรามีค่าเท่าไร?

| AUDIT ต้องรู้อะไร? สำหรับ DATA GOV



Institute of
Internal Auditors
Thailand



- Critical Data Element - CDE
- Data Steward (R&R)
- Meta Data
- Data Lineage
- Data Risk Management
- Data Lifecycle
- Data Quality Management

| AUDIT ต้องรู้อะไร? สำหรับ DATA GOV



Institute of
Internal Auditors
Thailand



Data Gov Structure & Role
Committee, DPO, Steward

Data policy
Rules and standards

CDE & Ownership

Data Lifecycle
Create to destroy

Metadata & Lineage
meaning & path

Data Risk
risk management, RTP

Data Quality
fit for purpose

Data Security
Protection

Data Privacy
PDPA

คุณลักษณะของ Critical Data Elements



Business Impact

- ข้อมูลที่ใช้ประกอบการตัดสินใจ หรือมีผลต่อรายงานทางการเงินและการดำเนินงาน



Risk of Inaccuracy

- ความเสี่ยงจากข้อผิดพลาด หากข้อมูลไม่ถูกต้อง อาจส่งผลกระทบต่อความเสี่ยงทางกฎหมายหรือภาพลักษณ์องค์กร



High Usage

- ข้อมูลที่มีหลายแผนกใช้งาน และใช้ร่วมกันหลายระบบ



Regulatory Requirements

- ความจำเป็นในการปฏิบัติตามกฎระเบียบ เช่น ข้อมูลลูกค้าที่ต้องรายงานตามกฎหมาย PDPA, GDPR, หรือตามข้อกำหนดของคปภ.

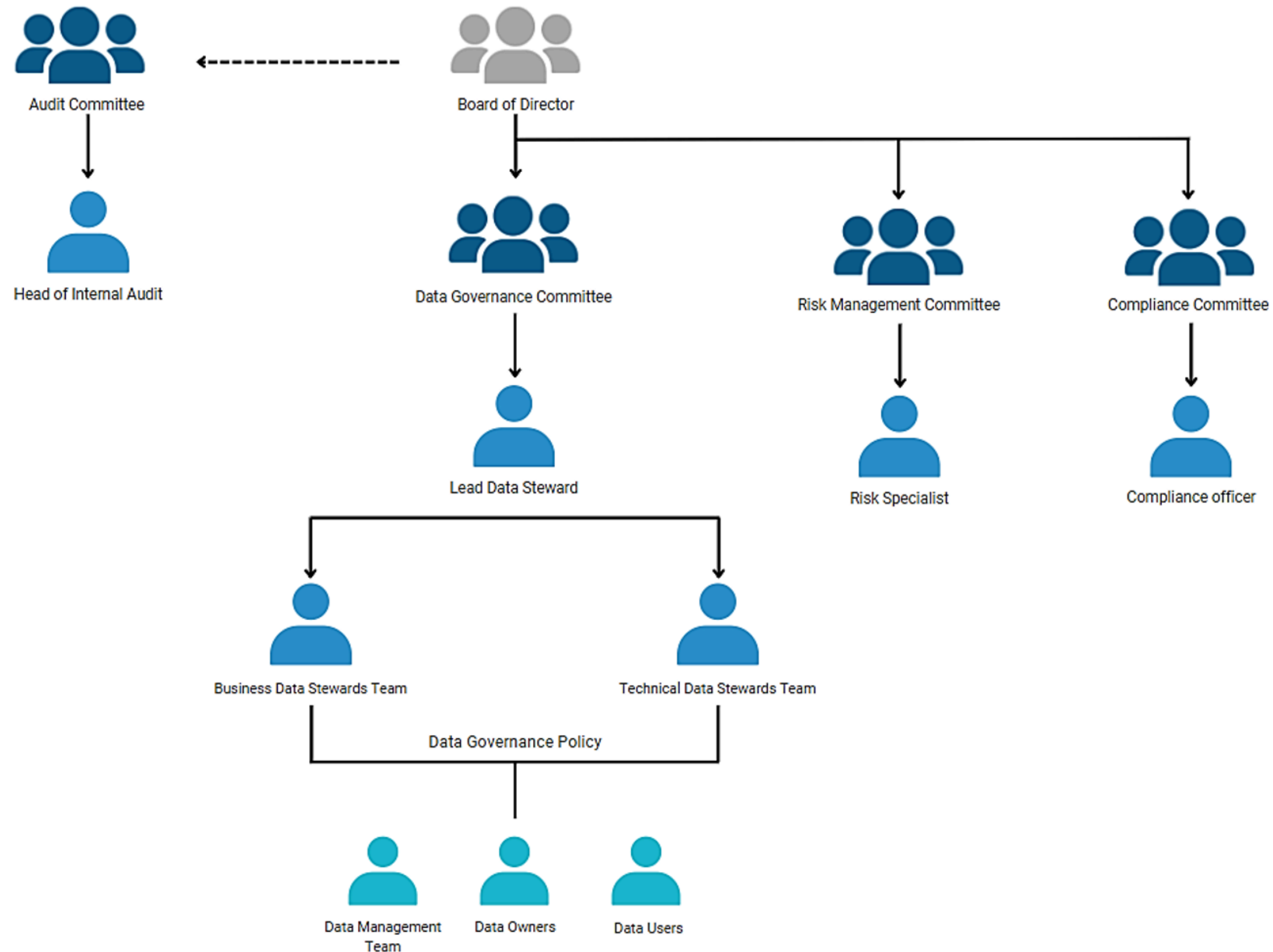
EXAMPLE CDE

ลำดับ	CDE	คำอธิบาย
1	Full Name	ชื่อ-นามสกุล
2	National ID / Passport No.	เลขประจำตัวประชาชน หรือหนังสือเดินทาง (สำหรับชาวต่างชาติ)
3	Date of Birth	วันเดือนปีเกิด
4	Gender	เพศ
5	Address	ที่อยู่ตามทะเบียนบ้าน/ที่ติดต่อ
6	Phone Number	หมายเลขโทรศัพท์
7	Email	อีเมลติดต่อ
8	Occupation	อาชีพ
9	Customer Type	ประเภทลูกค้า เช่น บุคคลธรรมดา/นิติบุคคล
10	Bank Account Number	บัญชีธนาคารของลูกค้า สำหรับการรับเงินคืนหรือเบี่ยงประกัน

DATA GOVERNANCE ORG CHART



Institute of
Internal Auditors
Thailand



DATA GOVERNANCE ORG CHART



Institute of
Internal Auditors
Thailand



Role	Assigned to	Responsibilitites
Data Governance Committee	CIO, CISO, CDO, CRO	- Approve policies, standards, and governance frameworks - Resolve cross-departmental issues - Align governance with strategic and regulatory goals
Lead Data Steward	<i>A senior data professional with cross-domain business knowledge, capable of managing multi-stakeholder interactions and ensuring alignment between business needs and technical execution.</i>	- Oversee all steward activities - Coordinate business and technical stewards
Business Data Steward	Senior Analysts or Champion from departments	- Define and maintain business terms and data definitions - Monitor data quality in business processes
Technical Data Steward	Data engineers, database administrators	- Map business metadata to technical metadata - Manage data lineage and transformation logic - Ensure technical data quality and system compliance
Data Management Team	Data architects (DBA Team)	- Develop and maintain data models, metadata, and dictionaries - Implement data quality tools and governance platforms - Support stewardship and governance tasks
Data Owner	Department heads	- Accountable for data accuracy, access, and usage - Approve definitions and access rights



BUSINESS DATA STEWARD



Create Maintain **Business Metadata**



Define Data **Quality Rules** and Monitor
Data Quality



Data **SME** - Support, Advise, Collaborate

TECHNICAL DATA STEWARD



Create Maintain **Technical Meta Data** and
Data Lineage



Implement **Data Quality Rules**
Develop/Manage Scripts to extract data
for Quality monitoring
Support by: Data Management Team



Technical Data **SME** - Support, Advise, Collaborate

EXAMPLE OF BUSINESS META DATA



Institute of
Internal Auditors
Thailand



#	เลขบัตรประชาชน (พนักงาน)	เบอร์มือถือ (ลูกค้า)
ชื่อทางธุรกิจ	เลขประจำตัวประชาชนพนักงาน	หมายเลขโทรศัพท์มือถือลูกค้า
นิยาม	เลข 13 หลักที่ออกโดยกรมการปกครอง ใช้ระบุตัวพนักงานตามกฎหมาย	หมายเลขมือถือที่ลูกค้าให้ไว้เพื่อติดต่อและยืนยันตัวตน
วัตถุประสงค์การใช้	จ่ายเงินเดือน · ยืนยันภาษี · ประกันสังคม	ยืนยันตัวตน (OTP) · แจ้งเตือนบริการ · การตลาด
Data Business Rules	- ต้องยืนยันตัวตนโดย อ่านซีปจากเครื่องอ่านบัตร เท่านั้น — ไม่รับสำเนาถ่ายเอกสารเป็นหลักฐานหลัก 13 หลัก ต้องผ่านการตรวจ check digit 1 พนักงาน = 1 เลขบัตร ห้ามซ้ำ - ห้ามจัดเก็บภาพบัตรที่ยังไม่ปิดบังช่องศาสนา	- จัดเก็บรูปแบบ E.164 เท่านั้น: +66824590459 - ห้ามเก็บ 082-459-0459 / 0824590459 / เว้นวรรค - ต้องเป็นเบอร์ที่รับ SMS ได้ — พิสูจน์ด้วย OTP ครั้งแรก 1 เบอร์ผูกได้ไม่เกิน 3 บัญชี
เจ้าของข้อมูล	ผอ.ฝ่ายทรัพยากรบุคคล	ผอ.ฝ่ายลูกค้าสัมพันธ์
Data Steward	หัวหน้าส่วนทะเบียนประวัติ	หัวหน้าส่วนข้อมูลลูกค้า
CDE (Y/N)	Yes	Yes

EXAMPLE OF TECHINICAL META DATA



Institute of
Internal Auditors
Thailand

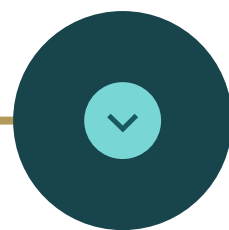


#	เลขบัตรประชาชน (พนักงาน)	เบอร์มือถือ (ลูกค้า)
ชื่อฟิลด์จริง	HRIS.EMP_MST.NATIONAL_ID	หมายเลขโทรศัพท์มือถือลูกค้า
ชนิดข้อมูล / ความยาว	CHAR(13)	VARCHAR(15)
System of Record	HRIS	CRM
จุดรับข้อมูลเข้า	เครื่องอ่านบัตร (chip) → API ไม่เปิดให้คีย์มือ	เว็บ/แอป/สาขา — normalize เป็น E.164 ที่ขึ้น API
การเข้ารหัส	AES-256 at rest · TLS 1.3 in transit	TLS 1.3 in transit
สิทธิ์เข้าถึงข้อมูลเต็ม	Role HR_PAYROLL_RW (7 users)	Role CRM_SUPPORT_RW (42 users)

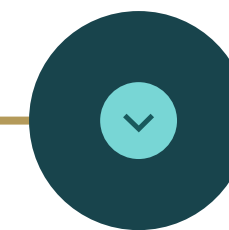
กระบวนการติดตามและแสดงเส้นทางของข้อมูลตั้งแต่ต้นทาง (source) ไปจนถึงปลายทาง (destination) โดยแสดงให้เห็นว่า



ข้อมูลมาจากไหน (แหล่งข้อมูล)



ผ่านการเปลี่ยนแปลงอะไรบ้าง (เช่น การรวม, การกรอง, การคำนวณ)



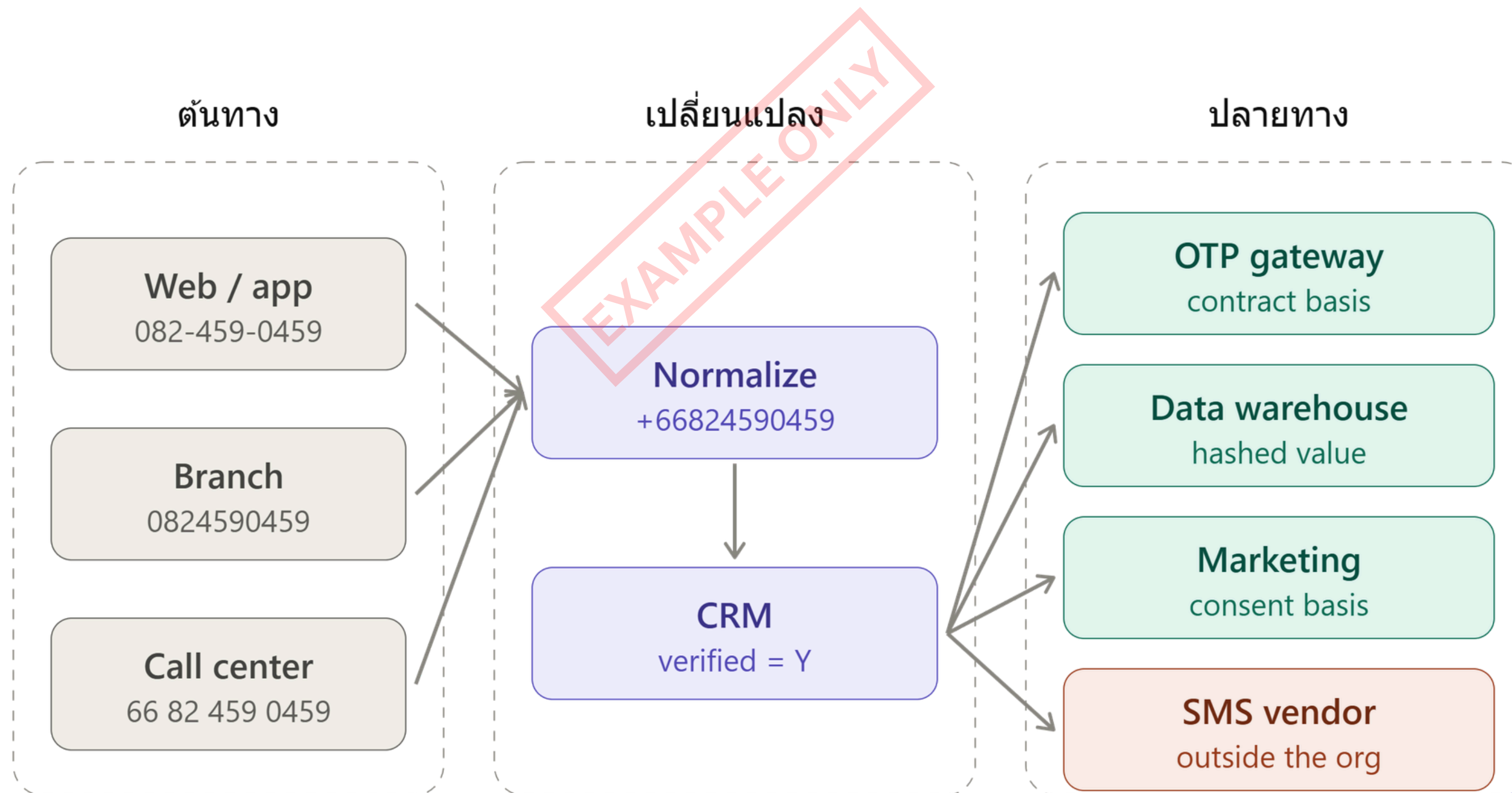
ถูกส่งไปใช้ที่ไหน (รายงาน, dashboard, machine learning model ฯลฯ)



EXAMPLE OF DATA LINEAGE



Institute of
Internal Auditors
Thailand



| DATA QAULITY RISK MANAGEMENT



Institute of
Internal Auditors
Thailand



Scope & Context

CDE, Data Owner

Risk Identification

Risk register, Risk to CDE

Risk Analysis and Evaluation

Impact x Likelihood -Acceptable/Unacceptable

Risk Response/Risk Treatment

prevent, detect, correct, minimize, accept

Monitoring & review

KRI, Threshold, Report

| DATA QUALITY DIMENSION



Institute of
Internal Auditors
Thailand



- **ความถูกต้อง (Accuracy)**
 - เบอร์โทรถูกต้อง
- **ครบถ้วน (Completeness)**
 - ที่อยู่ครบถ้วน
- **สอดคล้องกัน (Consistency)**
 - ข้อมูลระบบ CRM ไม่ตรงกับ Corebank
- **เป็นปัจจุบัน (Timeliness)**
 - Timeliness = Data is up-to-date + available at the right time.
- **ตรงกับความต้องการของผู้ใช้ (Relevancy)**
 - Data Set นี้ช่วยผู้บริหารตัดสินใจได้ง่ายหรือไม่
- **พร้อมใช้งาน (Availability)**
 - Data พร้อมใช้งานตลอดหรือไม่

Uniqueness? e.g. Order Number

Validity? - Data type format etc.

EXAMPLE OF DATA QUALITY RISK



Institute of
Internal Auditors
Thailand



CDE — เบอร์มือถือลูกค้า

Dimension	ความเสี่ยงถ้าล้มเหลว	Rating	Decision
Validity	format ผิดที่สาขา	High	RTP
Uniqueness	ซ้ำ ทำให้ลบไม่ครบ	High	RTP
Completeness	บางรายไม่มีเบอร์	Medium	Monitor
Accuracy	เบอร์ผิดคน	Medium	Monitor
Timeliness	เบอร์เก่าไม่อัปเดต	Low	Accept
Consistency	ไม่กระทบการใช้งาน	Low	Accept

ชุดข้อมูลลูกค้า (CUSTOMER INFORMATION)

คุณลักษณะ (Dimension)	เกณฑ์ที่กำหนด (Threshold)
Accuracy	≥ 99%
Completeness	≥ 95%
Consistency	≥ 98%
Timeliness	≥ 95%
Relevancy	≥ 95%
Availability	≥ 99.5%

Dataset Name	Data Field (CDE)	Dimension	Threshold (%)	Measurement Method	Data Owner
Customer Information	Customer ID	Accuracy	99	Check uniqueness and valid format	Customer Service
Customer Information	Full Name	Completeness	97	Non-null, no placeholder values	Customer Service
Customer Information	Phone Number	Consistency	98	Format validation and duplication check	Customer Service
Customer Information	Email	Availability	99.5	Accessible and verified delivery	IT
Policy Information	Policy Number	Accuracy	99	Cross-check with issuance system	Underwriting
Policy Information	Policy Type	Consistency	98	Standard naming convention	Product Management
Policy Information	Effective Date	Timeliness	95	Date falls within valid range	Underwriting
Premium Data	Premium Amount	Accuracy	99	Match business logic and finance rules	Finance
Premium Data	Payment Status	Completeness	96	Non-null, status exists in master list	Finance
Claim Data	Claim Number	Accuracy	99	Unique ID format and no duplication	Claims Department
Claim Data	Claim Amount	Completeness	95	Non-null, valid currency format	Claims Department
Claim Data	Claim Status	Consistency	97	Matches predefined status values	Claims Department
Claim Data	Claim Date	Timeliness	95	Reported within defined SLA	Claims Department

DATA QUALITY MEASUREMENT



Institute of
Internal Auditors
Thailand

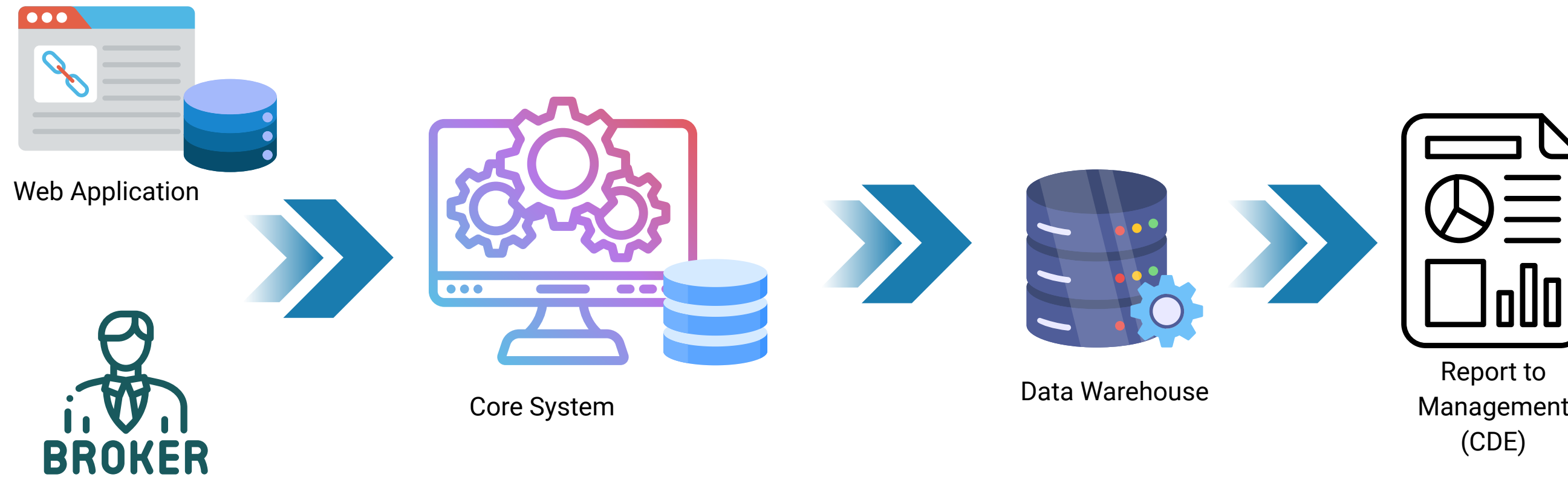


ชุดข้อมูล	CDE	DQ Dimension	Minimum Quality Standard	Owner	ระดับคุณภาพเป้าหมาย	คุณภาพที่วัดได้ (ปัจจุบัน)	สถานะ
ข้อมูลลูกค้า	เบอร์มือถือ	Validity	ต้องอยู่ในรูปแบบ +66XXXXXXXXX เท่านั้น	ฝ่ายลูกค้าสัมพันธ์	99.5%	94.1%	ต่ำกว่าเกณฑ์
ข้อมูลลูกค้า	เบอร์มือถือ	Completeness	ลูกค้าที่ใช้บริการออนไลน์ต้องมีเบอร์ทุกราย	ฝ่ายลูกค้าสัมพันธ์	100.0%	99.8%	เฝ้าระวัง
ข้อมูลลูกค้า	เบอร์มือถือ	Uniqueness	1 เบอร์ผูกได้ไม่เกิน 3 บัญชี	ฝ่ายลูกค้าสัมพันธ์	100.0%	97.3%	ต่ำกว่าเกณฑ์
ข้อมูลพนักงาน	เลขบัตรประชาชน	Uniqueness	ต้องไม่ซ้ำกันในระบบ	ฝ่ายทรัพยากรบุคคล	100.0%	100.0%	ผ่านเกณฑ์
ข้อมูลพนักงาน	เลขบัตรประชาชน	Validity	13 หลัก และผ่านการตรวจ check digit	ฝ่ายทรัพยากรบุคคล	100.0%	99.9%	เฝ้าระวัง
ข้อมูลลูกค้า	ที่อยู่จัดส่ง	Completeness	ต้องมีจังหวัดและรหัสไปรษณีย์ครบทุกรายการ	ฝ่ายปฏิบัติการ	99.0%	91.4%	ต่ำกว่าเกณฑ์
ข้อมูลลูกค้า	ที่อยู่จัดส่ง	Validity	รหัสไปรษณีย์ต้องตรงกับจังหวัด	ฝ่ายปฏิบัติการ	98.0%	96.2%	ต่ำกว่าเกณฑ์
ข้อมูลลูกค้า	ที่อยู่จัดส่ง	Timeliness	ทบทวนความถูกต้องอย่างน้อยทุก 24 เดือน	ฝ่ายปฏิบัติการ	95.0%	88.5%	ต่ำกว่าเกณฑ์

WHERE TO MEASURE?

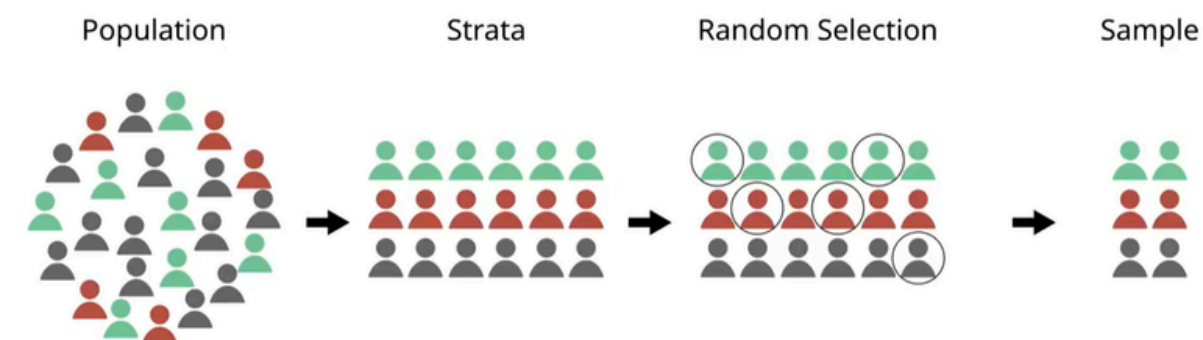
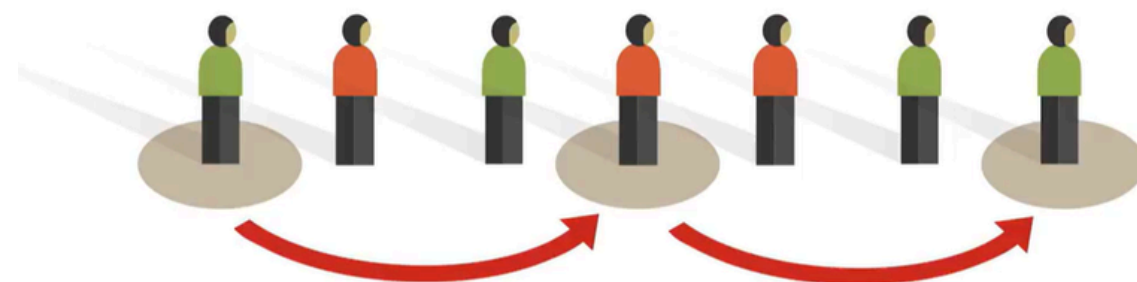


Institute of
Internal Auditors
Thailand



Stratified Sampling

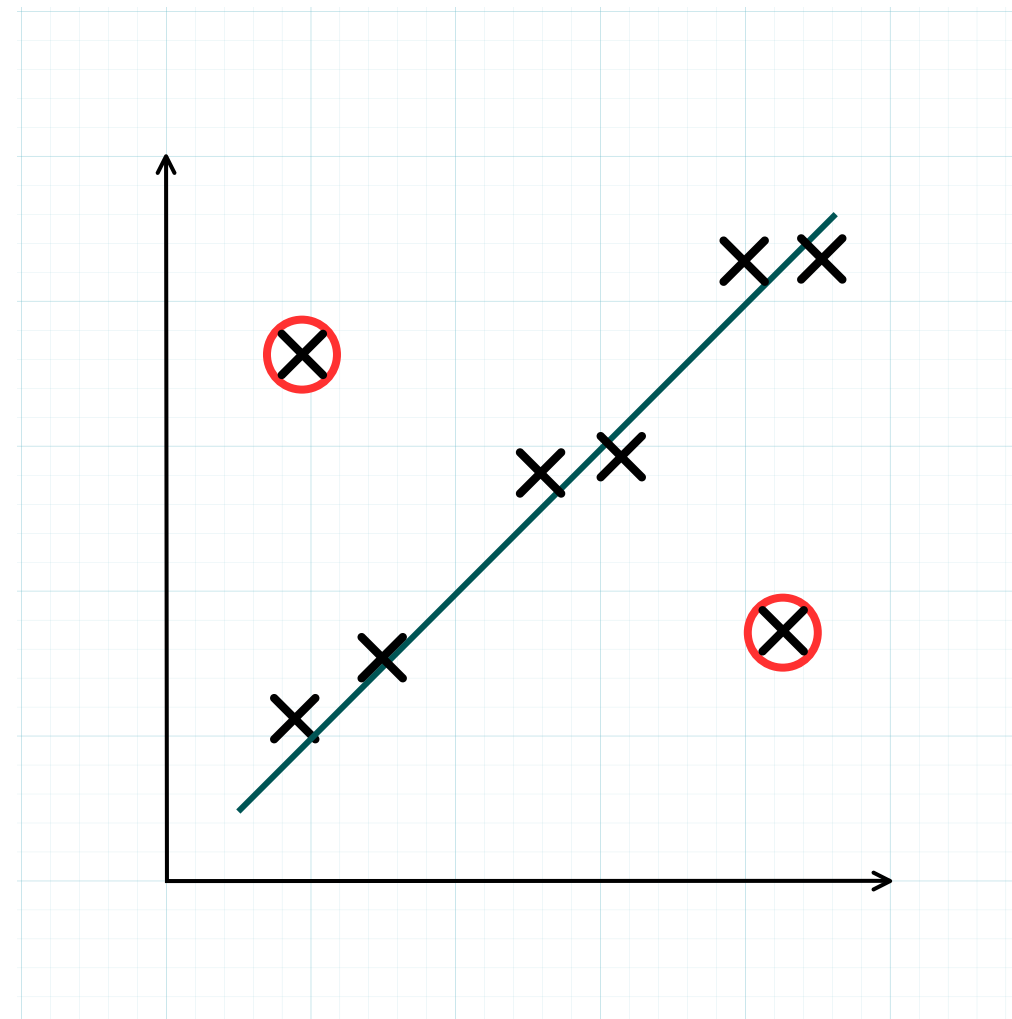
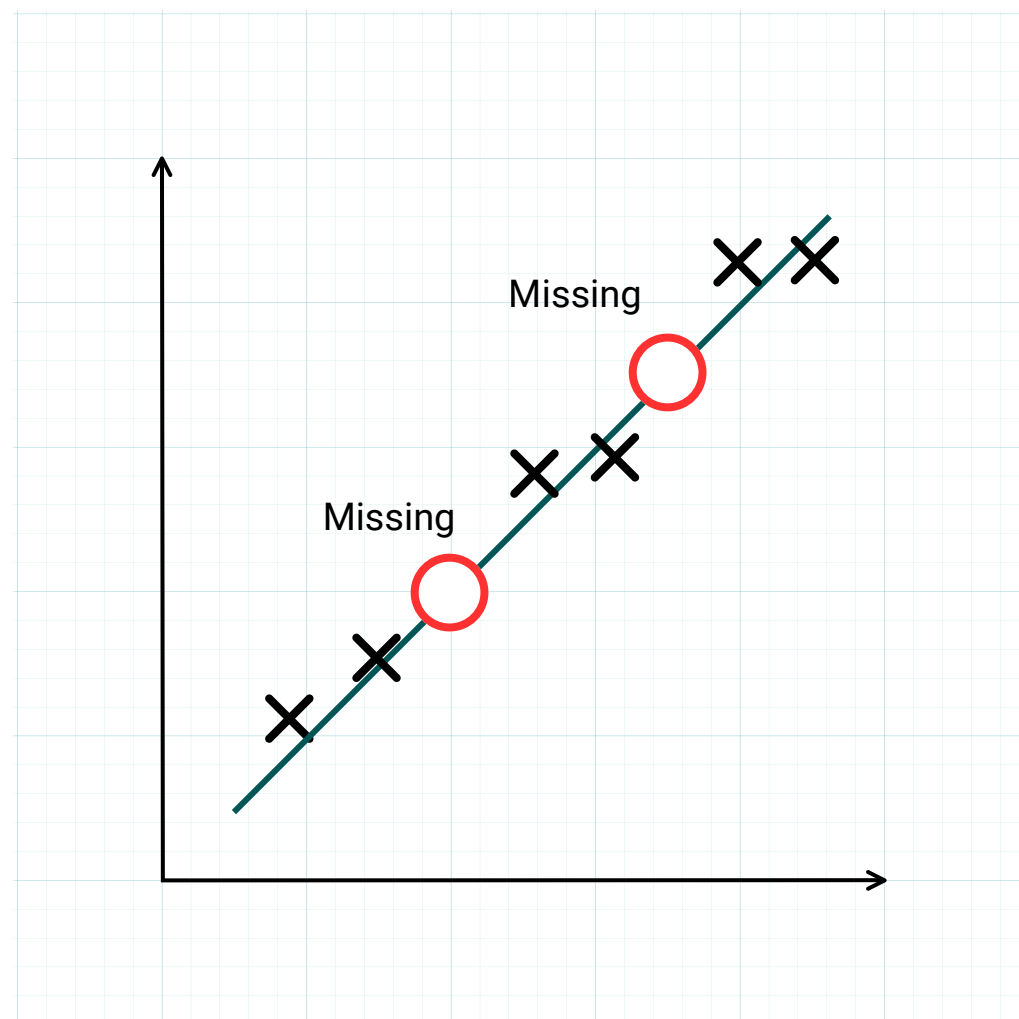
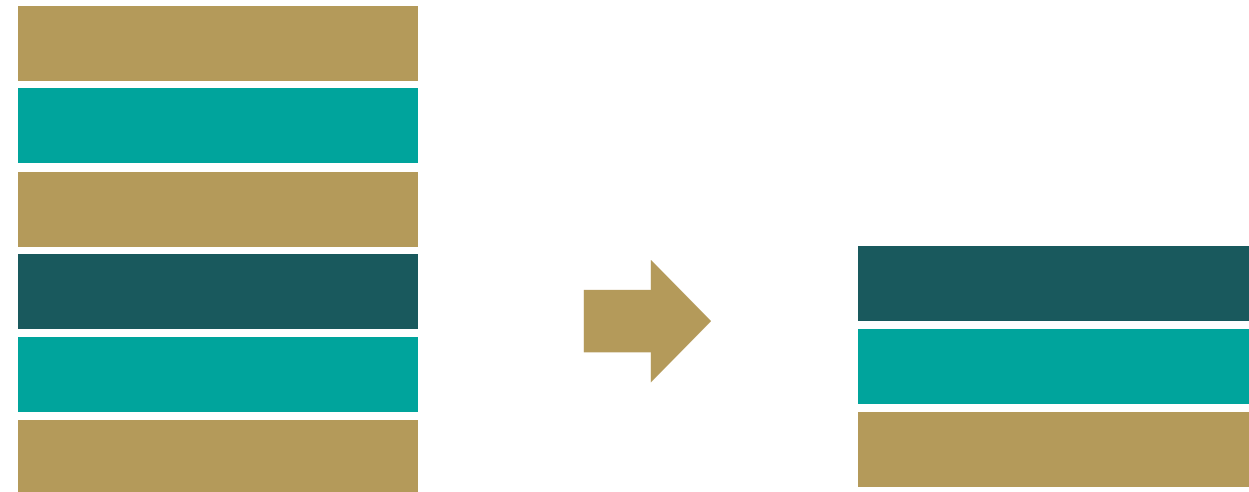
Systematic sampling



DATA QUALITY IMPROVEMENT



Institute of
Internal Auditors
Thailand



A group of five people (three men and two women) and three humanoid robots are gathered around a large, circular, glowing blue table. The table displays various data visualizations, including bar charts, line graphs, and network diagrams. The people are dressed in business attire, and the robots are sleek, white, and blue. The setting is a modern, brightly lit room with white walls and a large window in the background. The overall atmosphere is professional and high-tech.

AI / Privacy / Data Gov



Contact Us



+66 2 231 8488 (Direct line)



+66 82 459 0459



roujkun@iconicadvisory.co.th



www.iconicadvisory.co.th



92 Central Park Offices, Room No. 3521, Level 35
Rama IV Road, Silom, Bangrak, Bangkok 10500