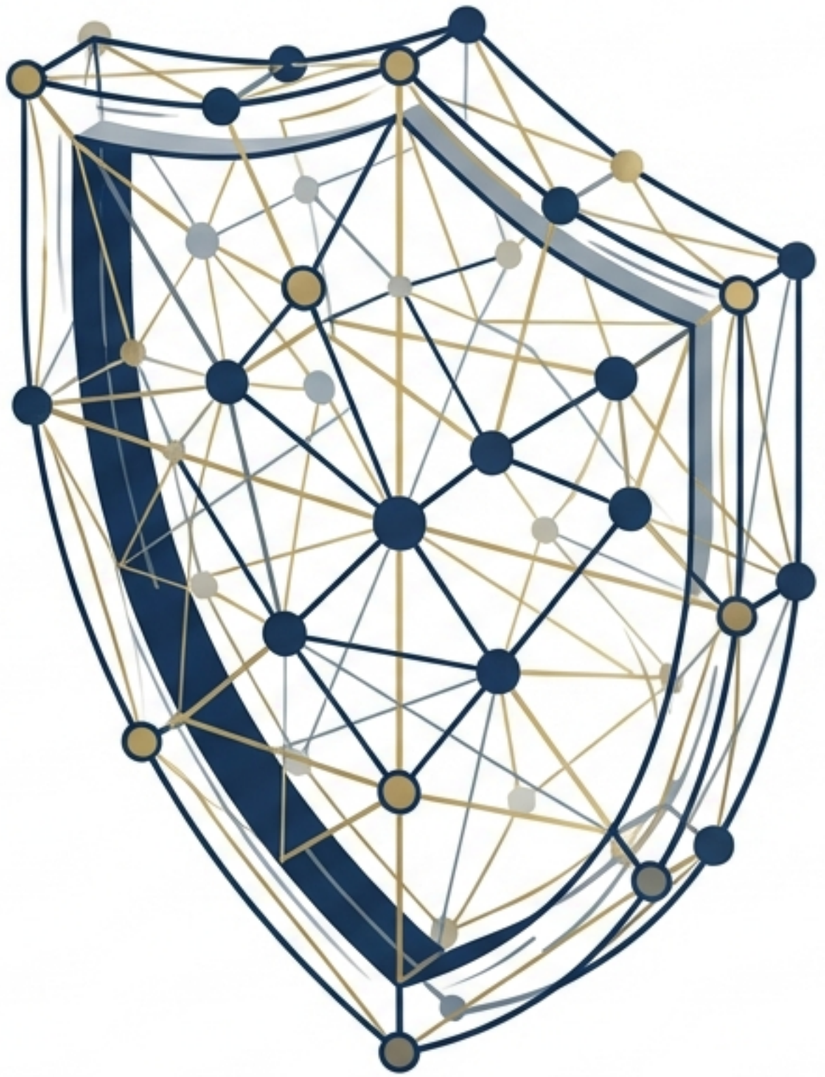
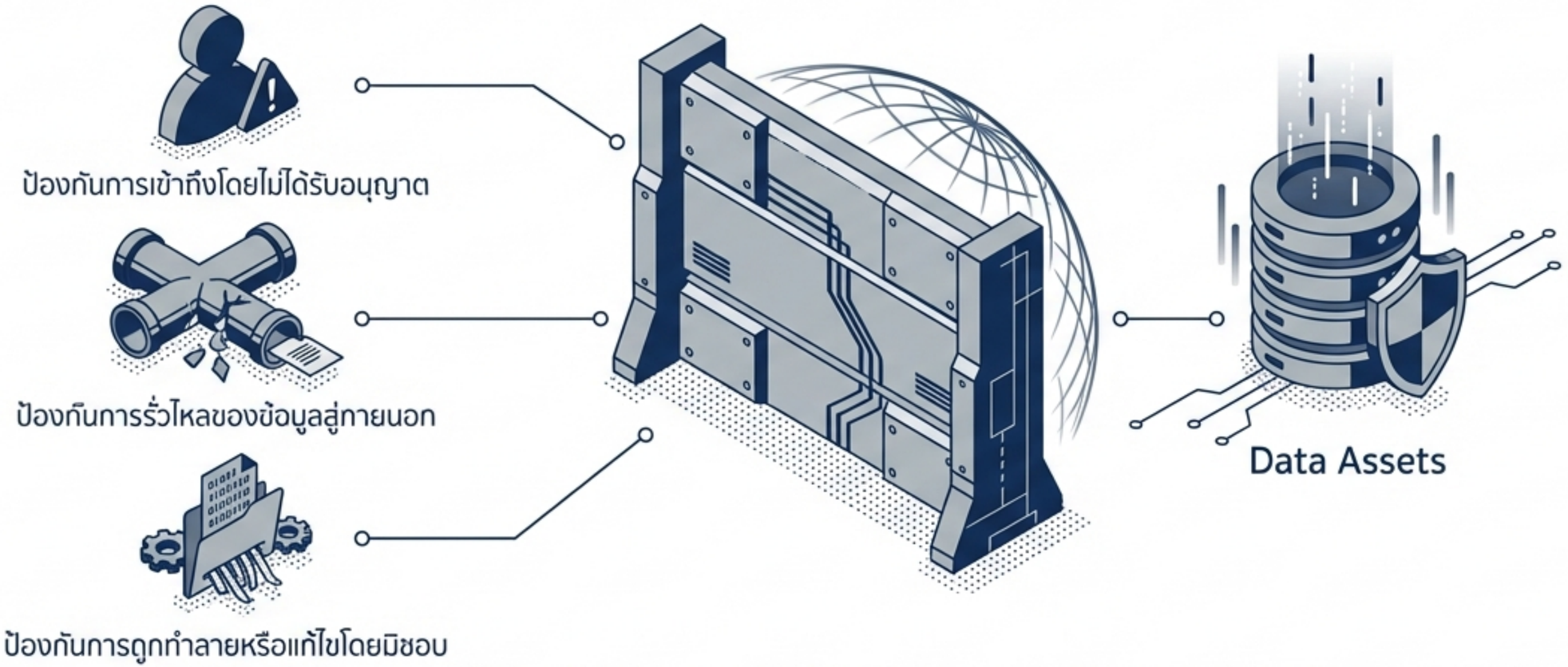
ความมั่นคงปลอดภัยของข้อมูล (Data Security)

การปกป้องทรัพย์สินที่มีค่าที่สุดขององค์กรในยุคดิจิทัล



DAMA SAUDI

นิยาม: ความมั่นคงปลอดภัยของข้อมูลคืออะไร?



ครอบคลุมวงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่การจัดเก็บ การใช้งาน ไปจนถึงการทำลาย

ความจำเป็นเชิงกลยุทธ์: กฎหมายและธุรกิจ

กฎหมาย (Legal & Compliance)

- **การปฏิบัติตามกฎหมาย:** เพื่อให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ของไทย และมาตรฐานสากลเช่น GDPR
- **Accountability:** องค์กรต้องมีความรับผิดชอบในการจัดการข้อมูลส่วนบุคคลอย่างโปร่งใส

ธุรกิจ (Business Value)

- **ความลับทางธุรกิจ:** รักษาความได้เปรียบในการแข่งขัน (Competitive Advantage) โดยการปกป้องข้อมูลความลับและทรัพย์สินทางปัญญา
- **Trust:** สร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรทางธุรกิจ

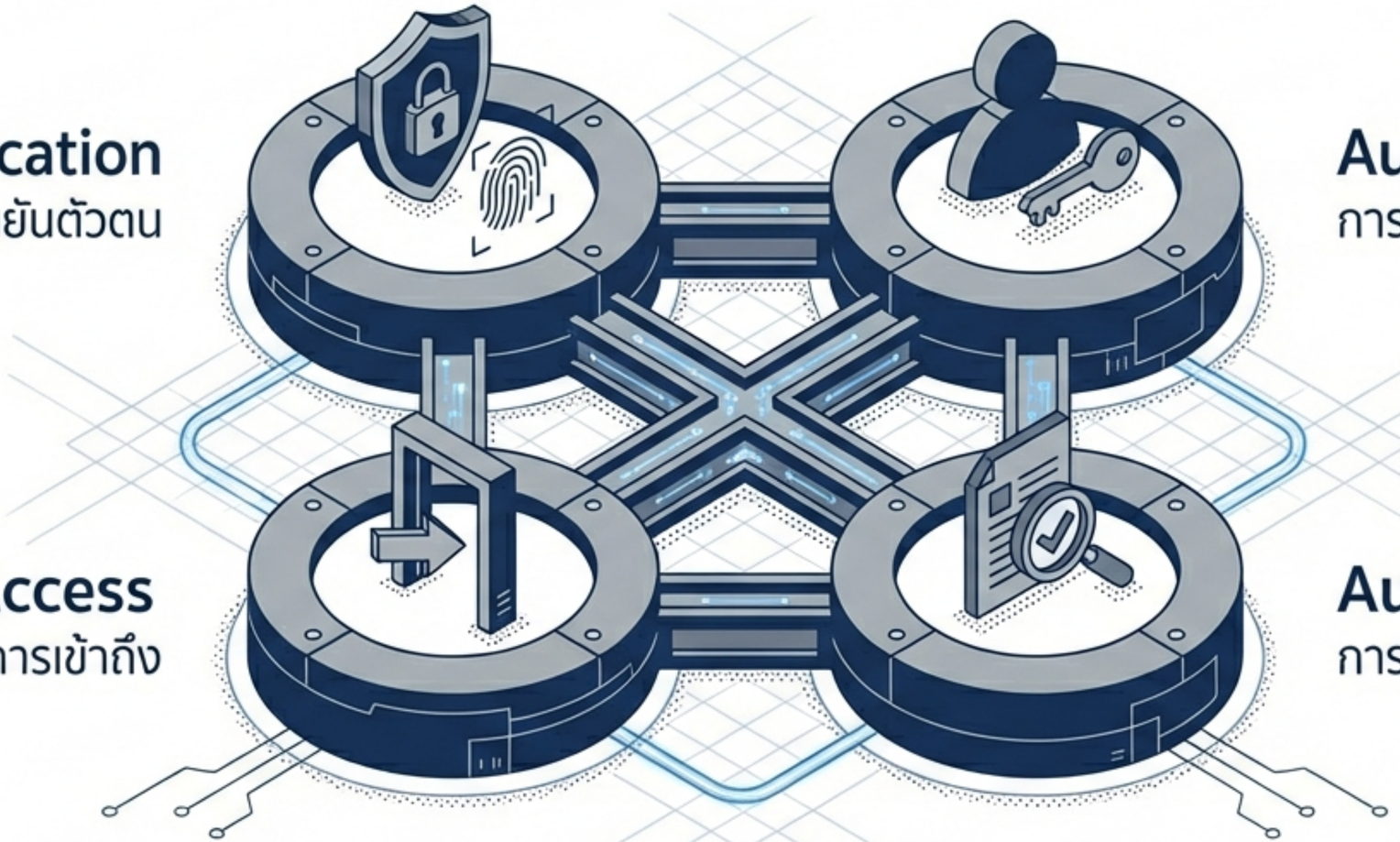
Competitive Advantage

DAMA SAUDI

หัวใจสำคัญของการจัดการ: หลักการ 4 A’s

Authentication
การยืนยันตัวตน

Authorization
การกำหนดสิทธิ์



Access
การเข้าถึง

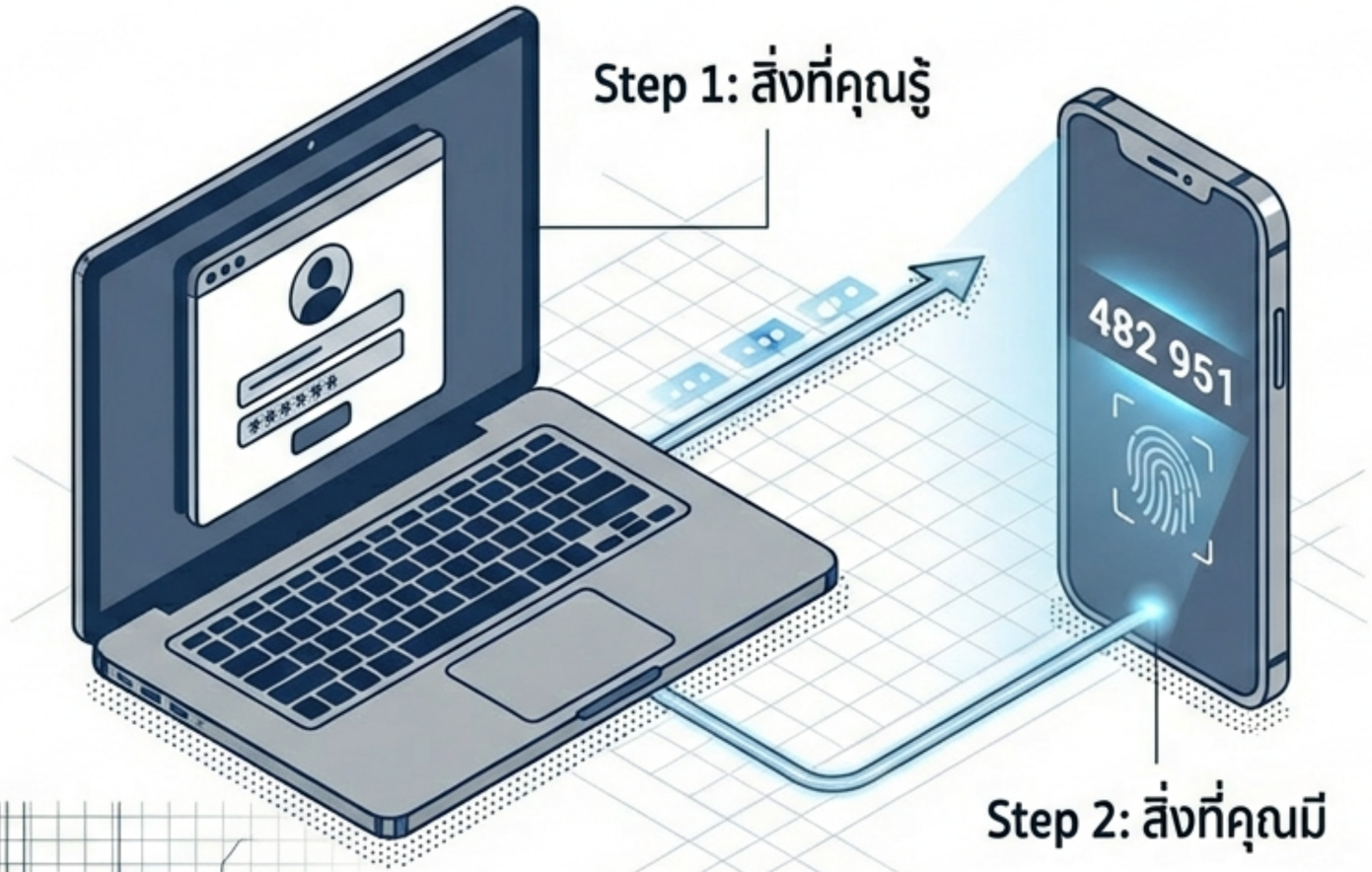
Audit
การตรวจสอบ

***หมายเหตุ:** Availability (ความพร้อมใช้งาน) ไม่จัดอยู่ในกลุ่ม 4 A's ของความปลอดภัยข้อมูลตามหลักการนี้*

DAMA SAUDI

1. Authentication: การยืนยันตัวตน

กระบวนการตรวจสะบว่าผู้ขอใช้ระบบเป็นบุคคลนั้นจริงหรือไม่ ก่อนที่จะอนุญาตให้เข้าสู่ระบบ



2-Factor Authentication (2FA)

เพิ่มความปลอดภัยอีกระดับด้วยการใช้การยืนยัน 2 ขั้นตอน:

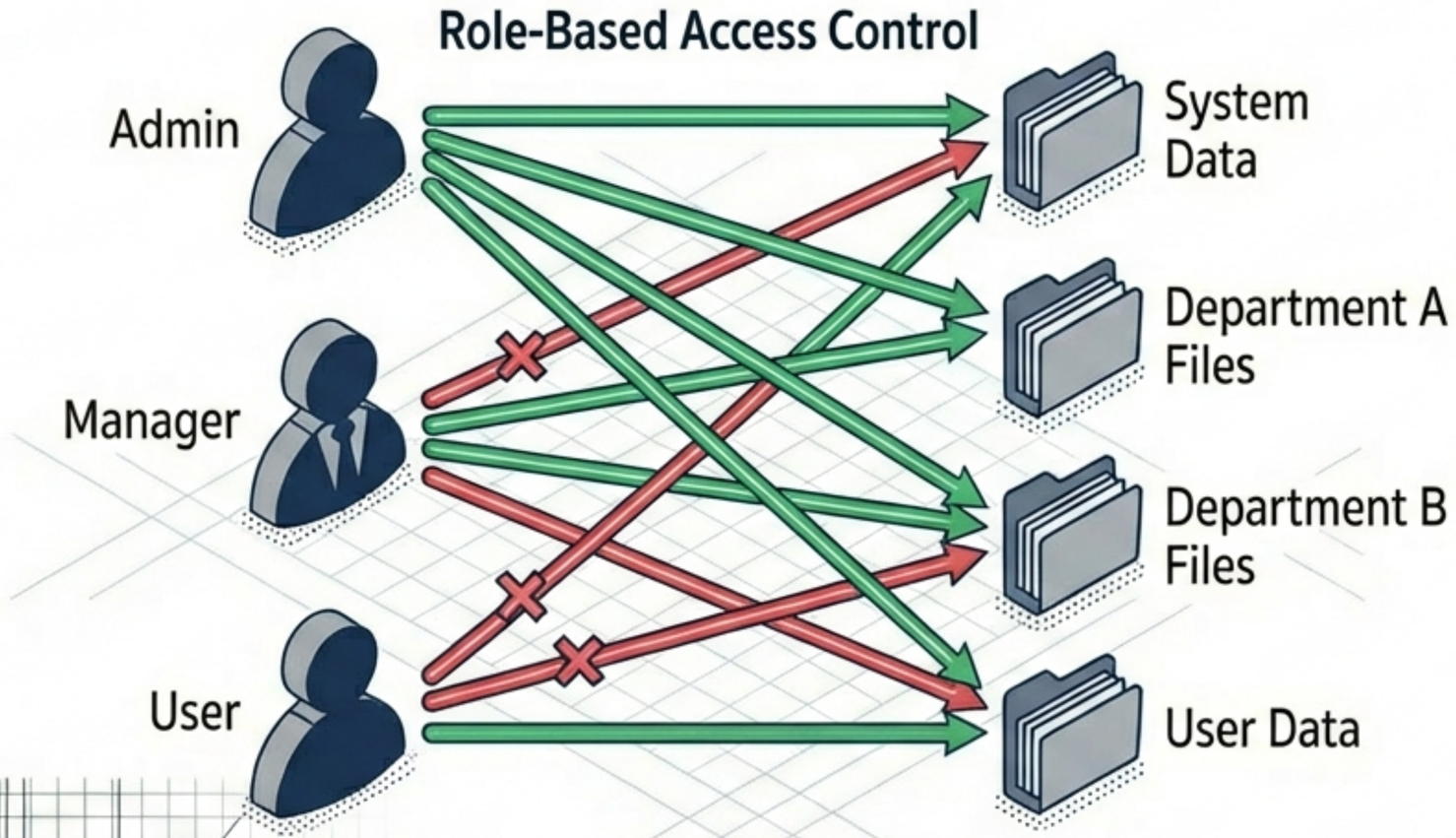
1. **สิ่งที่คุณรู้**
   (Username & Password)

2. **สิ่งที่คุณมี**
   (Code from Authentication App หรือ SMS)

DAMA SAUDI

2. Authorization: การกำหนดสิทธิ์การใช้งาน

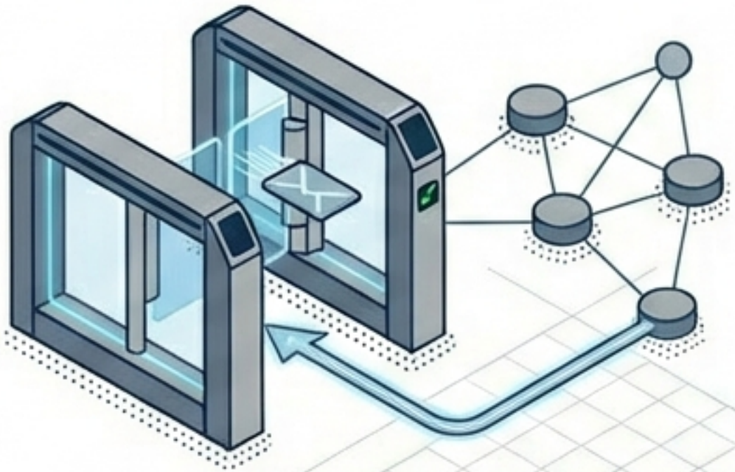
การกำหนดขอบเขตอำนาจหน้าที่ของผู้ใช้งานหลังจากผ่านการยืนยันตัวตนแล้ว



Key Concepts

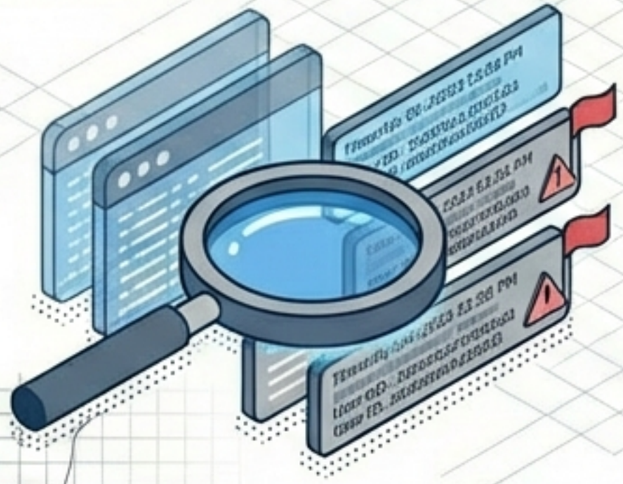
- **Privilege Management:** กำหนดสิทธิ์ตามหน้าที่งาน (Role-based access)
- **Granular Control:** ควบคุมสิทธิ์ละเอียดถึงระดับ การอ่าน (Read), การแก้ไข (Write), หรือ การลบ (Delete)

3. Access & 4. Audit: การควบคุมและตรวจสอบ



A. Access (การเข้าถึง)

- ควบคุมจุดสัมผัสข้อมูล (Data Touch Points) ในกระบวนการทำงานทางธุรกิจ
- ต้องมั่นใจว่าการเข้าถึงผ่านช่องทางต่างๆ มีความปลอดภัย



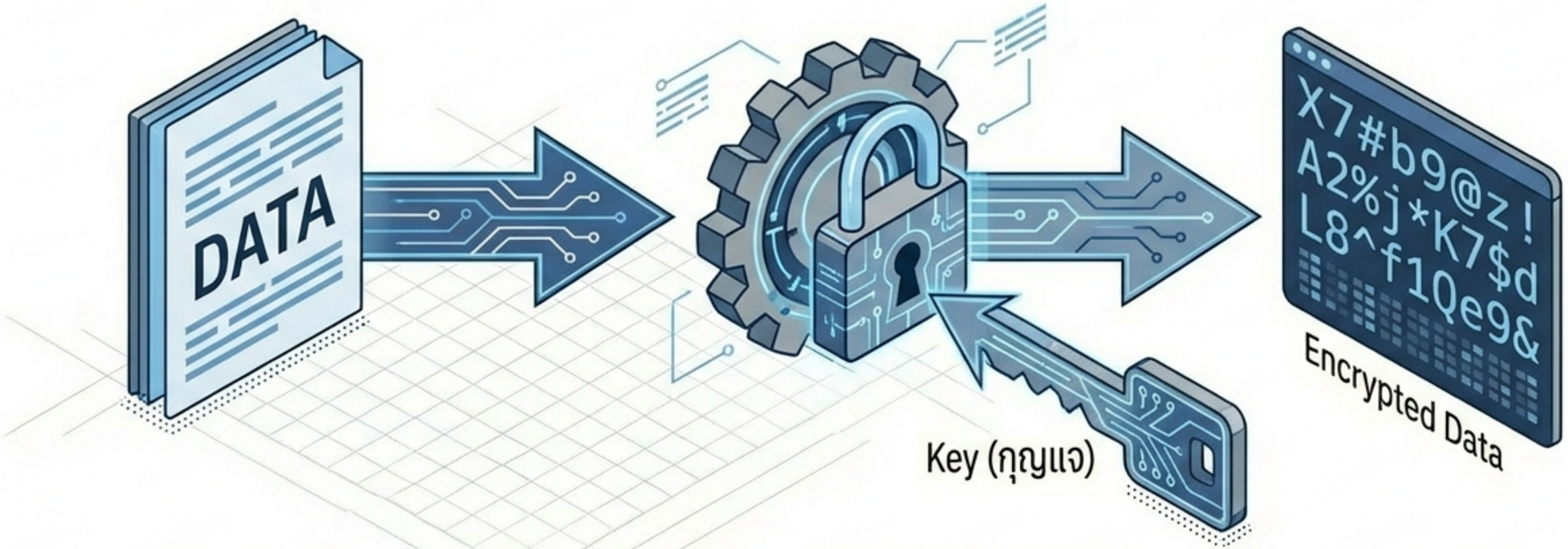
B. Audit (การตรวจสอบ)

- Usage Logs: การบันทึกประวัติการใช้งานเพื่อตรวจสอบย้อนกลับ
- Detection: ใช้สำหรับตรวจจับพฤติกรรมที่ผิดปกติหรือการเข้าถึงข้อมูลโดยมิชอบของพนักงาน (Inappropriate access)

DAMA SAUDI

กลไกทางเทคนิค: การเข้ารหัสข้อมูล (Encryption)

กระบวนการแปลงข้อความธรรมดา (Plain Text) ให้เป็นรหัสที่ซับซ้อน (Complex Codes) เพื่อซ่อนข้อมูลสำคัญ



ข้อมูลที่ถูกเข้ารหัสจะอยู่ในรูปแบบที่อ่านไม่ได้ และต้องใช้ 'กุญแจ' (Key)
ที่ถูกต้องเท่านั้นในการถอดรหัสเพื่อนำกลับมาใช้งาน

สถานะของการเข้ารหัส: จัดเก็บและส่งต่อ

1. At Rest (ขณะจัดเก็บ)

- การเข้ารหัสข้อมูลที่บันทึกอยู่ในฐานข้อมูล ฮาร์ดไดรฟ์ หรืออุปกรณ์พกพา
- ป้องกันข้อมูลหากอุปกรณ์ถูกขโมยหรือเจาะระบบ

2. In Transit (ขณะส่งต่อ)

- การเข้ารหัสข้อมูลขณะเดินทางผ่านเครือข่าย (Network)
- HTTPS: มาตรฐานที่ช่วยให้มั่นใจว่าการสื่อสารระหว่างเบราว์เซอร์และเว็บไซต์ถูกเข้ารหัสและปลอดภัย

ความแตกต่างของนโยบายความปลอดภัย

Data Security Policy
นโยบายความปลอดภัยข้อมูล

- เน้นที่ ‘ตัวข้อมูล’ (Data-centric)
- มีความละเอียดสูง (Granular) กำหนดวิธีจัดการข้อมูลแต่ละประเภท/ชั้นความลับ

IT Security Policy
นโยบายความปลอดภัยไอที

- เน้นภาพรวมของโครงสร้างพื้นฐาน (Infrastructure)
- ครอบคลุมความปลอดภัยของเครือข่าย (Network) และอุปกรณ์

DAMA SAUDI

บทบาทและความรับผิดชอบ (Roles & Responsibilities)

Data Owner (เจ้าของข้อมูล)

- ผู้บริหารระดับสูงที่รับผิดชอบหลัก (Accountable) ต่อข้อมูล
- ตัดสินใจเรื่องสิทธิ์การเข้าถึงและความเสี่ยง

Data Steward (ผู้ดูแลข้อมูล)

- จำแนกประเภทข้อมูล (Data Classification) ตามระดับความลับ
- ร่วมมือกับทีม Compliance เพื่อบังคับใช้นโยบายความปลอดภัย

Data Users (ผู้ใช้งานข้อมูล)

- ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัย

DAMA SAUDI

บทสรุปสาระสำคัญ

คืออะไร: การปกป้องข้อมูลจากการเข้าถึง การรั่วไหล และการทำลายโดยไม่ได้รับอนุญาต

ความจำเป็น: ปฏิบัติตามกฎหมาย (PDPA/GDPR) และรักษาความลับทางธุรกิจ

หลักการ 4 A’s: Authentication, Authorization, Access, Audit

การเข้ารหัส (Encryption): ปกป้องข้อมูลทั้งขณะจัดเก็บ (At Rest) และขณะส่งต่อ (In Transit)

ความมั่นคงปลอดภัยของข้อมูลคือกุญแจสำคัญสู่ความยั่งยืนขององค์กร