

บทที่ 1 ความหมาย บทบาท ความสำคัญ และวิวัฒนาการของความมั่นคง

รายวิชา: SEM1201 การบริหารและการจัดการความมั่นคง (Introduction to Security Management)

ผู้บรรยาย: พศ.ดร.หทัยพันธุ์ สุนทรพิพิธ



ความมั่นคงคือรากฐานของความสงบเรียบร้อยและการพัฒนา

วัตถุประสงค์การเรียนรู้



อธิบายความหมาย
ของความมั่นคงจาก
มุมมองทางวิชาการ
และวิชาชีพที่
หลากหลาย



ทำความเข้าใจบริบท
ของความมั่นคงใน
มิติการเมือง
กายภาพ และไซเบอร์



วิเคราะห์บทบาทแ
ละความสำคัญขอ
งการจัดการความ
มั่นคงในองค์กร



ทบทวนวิวัฒนาการ
ทางประวัติศาสตร์
และกลยุทธ์การ
ป้องกันจากอดีตถึง
ปัจจุบัน

เข้าใจรากฐานเพื่อประยุกต์ใช้ในโลกแห่งความเป็นจริง

ความรู้เบื้องต้นเกี่ยวกับการจัดการความมั่นคง



ความมั่นคงมุ่งเน้นการสร้างสภาพแวดล้อมที่คาดเดาได้และปลอดภัย

นิยามความหมายของความมั่นคง

พจนานุกรม

อิสระจากอันตราย ความกลัว
และความวิตกกังวล (Merriam-Webster);
การป้องกันการโจรกรรม (Collins)

นักวิชาการ

สภาพแวดล้อมที่ปลอดภัย
ดำเนินชีวิตได้โดยไม่หยุดชะงัก
(Fischer et al., 2018)

ภาครัฐ

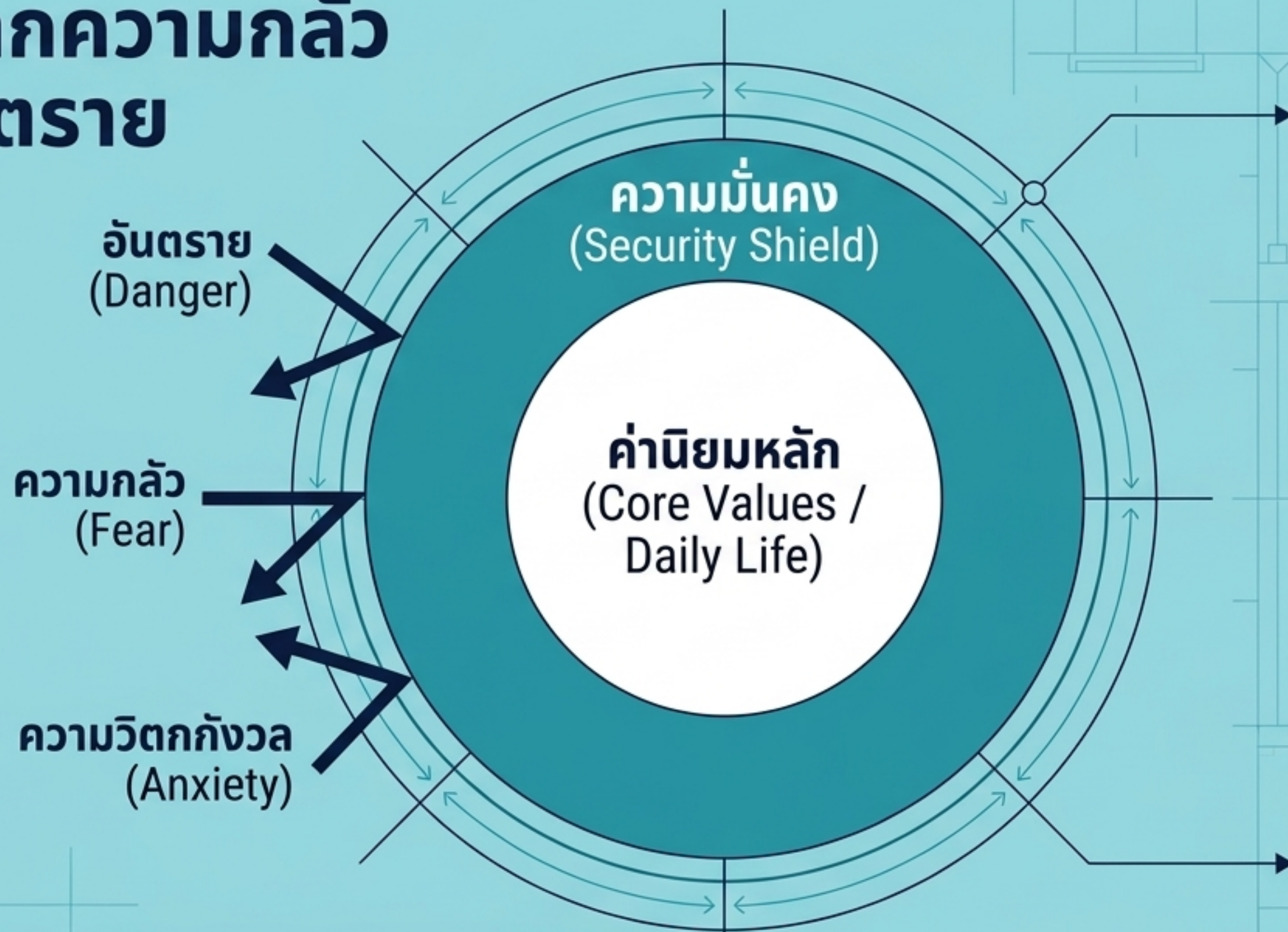
การปกป้องอธิปไตยและการอยู่รอดของรัฐ
(Bodunde et al., 2014)

ภาคธุรกิจ

การปกป้องบุคคล ทรัพย์สิน และข้อมูล
เพื่อป้องกันการสูญเสีย
(Craighead, 2009)

นิยามความมั่นคงเปลี่ยนไปตามมุมมองและบริบทของผู้ใช้งาน

อิสระจากความกลัว และอันตราย



หัวใจสำคัญคือสถานะ
ความปลอดภัยทางจิตใจ
และการใช้ชีวิต

การปกป้องให้พ้นจาก
ความกลัว ความกดขี่
และความสูญเสีย

มุ่งรักษาค่านิยมหลัก
ของสังคมพร้อมกับ
กำจัดภัยคุกคาม

ทำให้กิจกรรมในชีวิต
ประจำวันดำเนินต่อไป
ได้โดยไม่หยุดชะงัก
(Fischer et al., 2018)

ความมั่นคงเริ่มต้นที่ความรู้สึกปลอดภัยทางจิตใจ

ความมั่นคงในฐานะสหวิทยาการ

The Blueprint of Protection

ไม่มีคำนิยามที่เป็นสากลเพียงหนึ่งเดียว
(ASIS International, 2003)

บูรณาการความรู้ทั้งการเมือง
กฎหมาย เทคโนโลยี และสังคมวิทยา

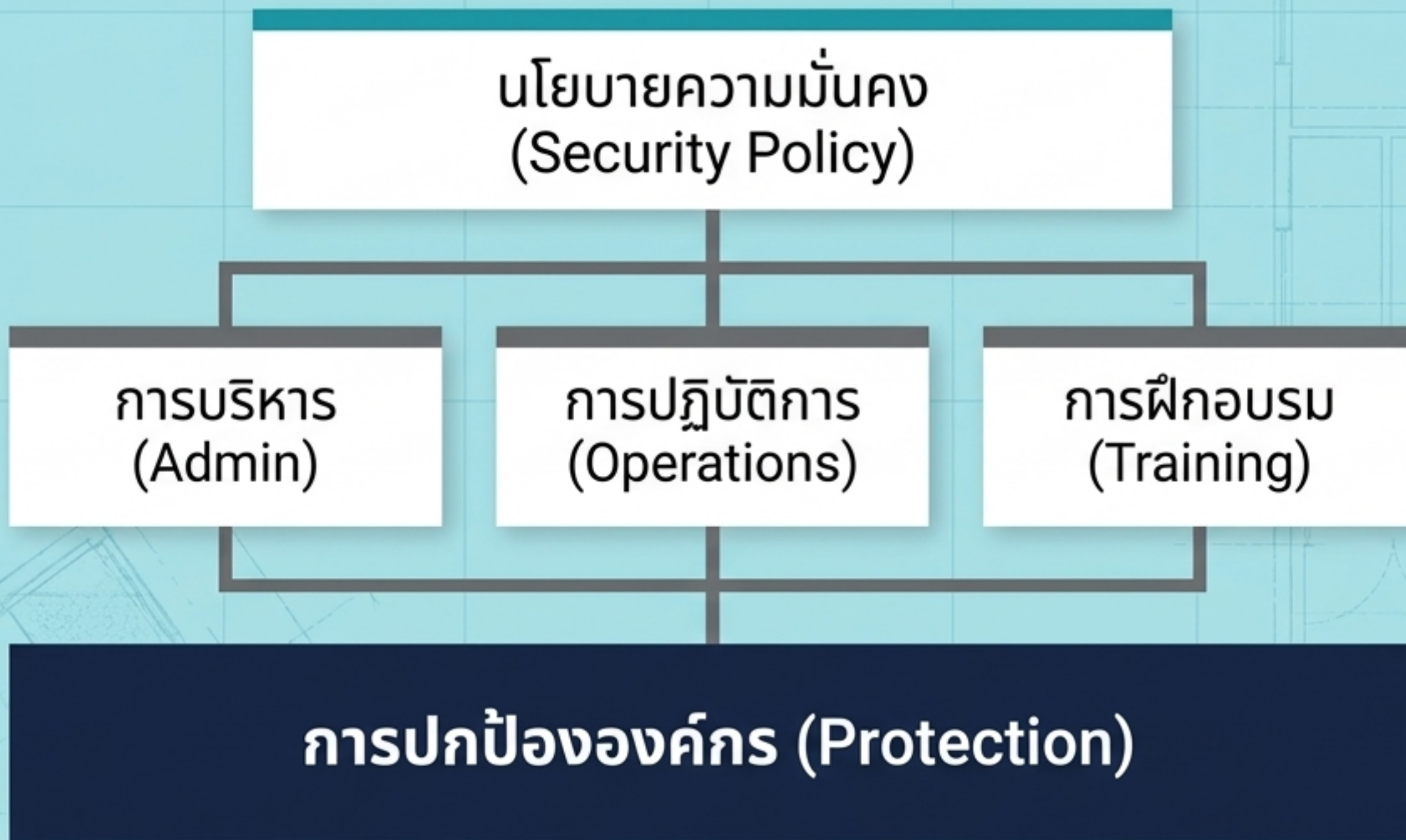
ต้องปรับตัวตามเวลา สถานที่
และการเปลี่ยนแปลงของโลก

ครอบคลุมตั้งแต่การป้องกันประเทศไป
จนถึงการป้องกันอาชญากรรมและการ
จัดการความเสี่ยง (Brooks, 2009)



ความมั่นคงไม่ใช่เรื่องของทหารหรือตำรวจเพียงอย่างเดียว
แต่เป็นสหวิทยาการ

ขอบเขตของการจัดการความมั่นคง



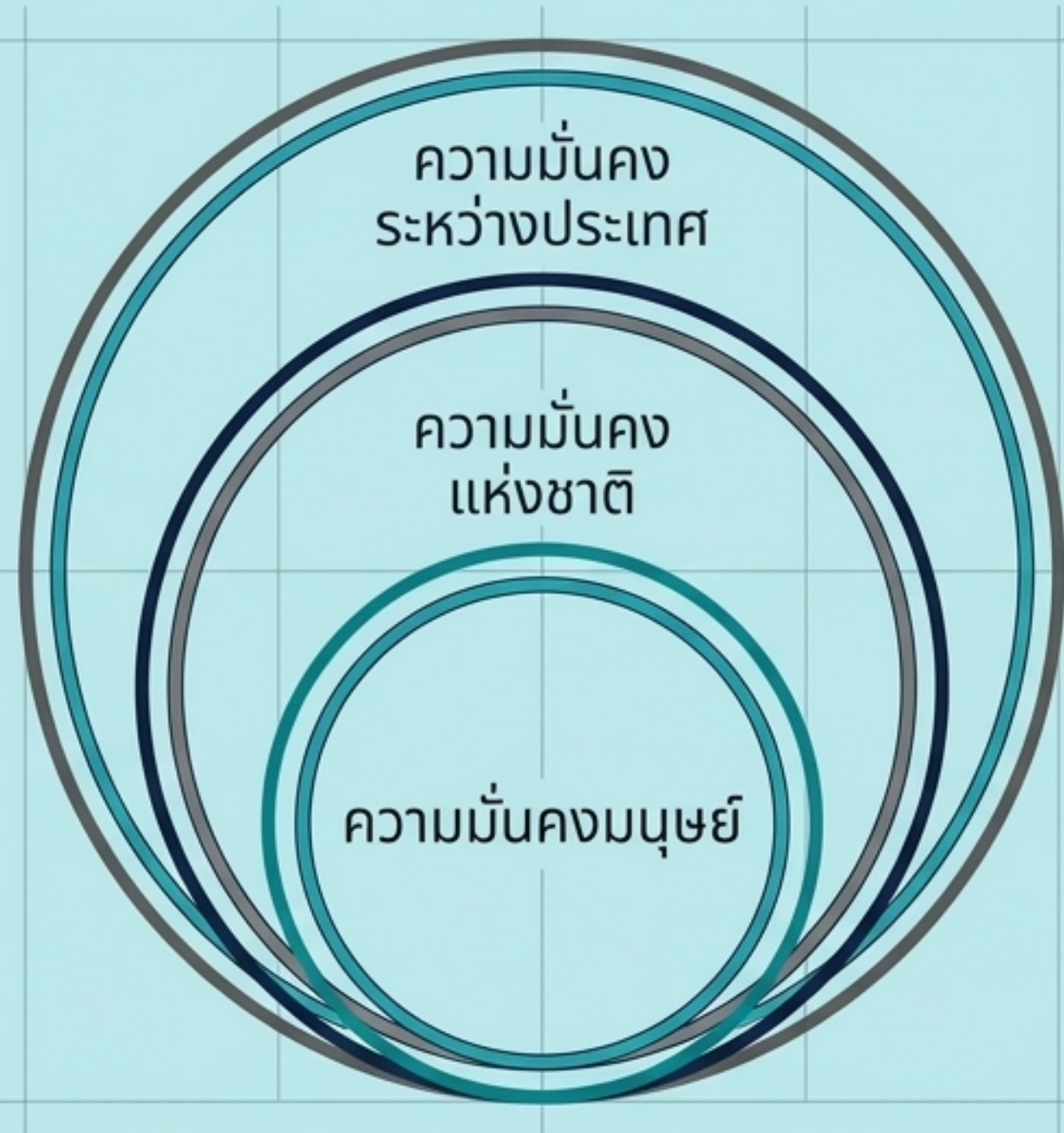
การควบคุมทรัพยากรขององค์กรเพื่อส่งมอบหน้าที่รักษาความปลอดภัย

ต้องใช้กลยุทธ์การป้องกันที่หลากหลาย (เช่น เจ้าหน้าที่, การควบคุมการเข้าถึง, การสืบสวน)

เป้าหมายคือการปกป้ององค์กรและสร้างผลตอบแทนจากการลงทุน (ROI) สูงสุด

การจัดการที่ดีเปลี่ยนนโยบายให้กลายเป็นการปฏิบัติที่ปกป้ององค์กร

บริบททางการเมืองของความมั่นคง



ความมั่นคงแห่งชาติ:

ปกป้องอธิปไตย สถาบันหลัก
และความมั่นคงสาธารณะของรัฐ

ความมั่นคงระหว่างประเทศ:

ความร่วมมือผ่านสนธิสัญญา
(เช่น UN, ASEAN) เพื่อความอยู่รอดร่วมกัน

ความมั่นคงมนุษย์:

ปกป้องศักดิ์ศรีความเป็นมนุษย์ เสรีภาพ
และความต้องการขั้นพื้นฐานให้พ้นจากความกลัว

รัฐบาลปกป้องอธิปไตย แต่ความมั่นคงมนุษย์ปกป้องศักดิ์ศรี

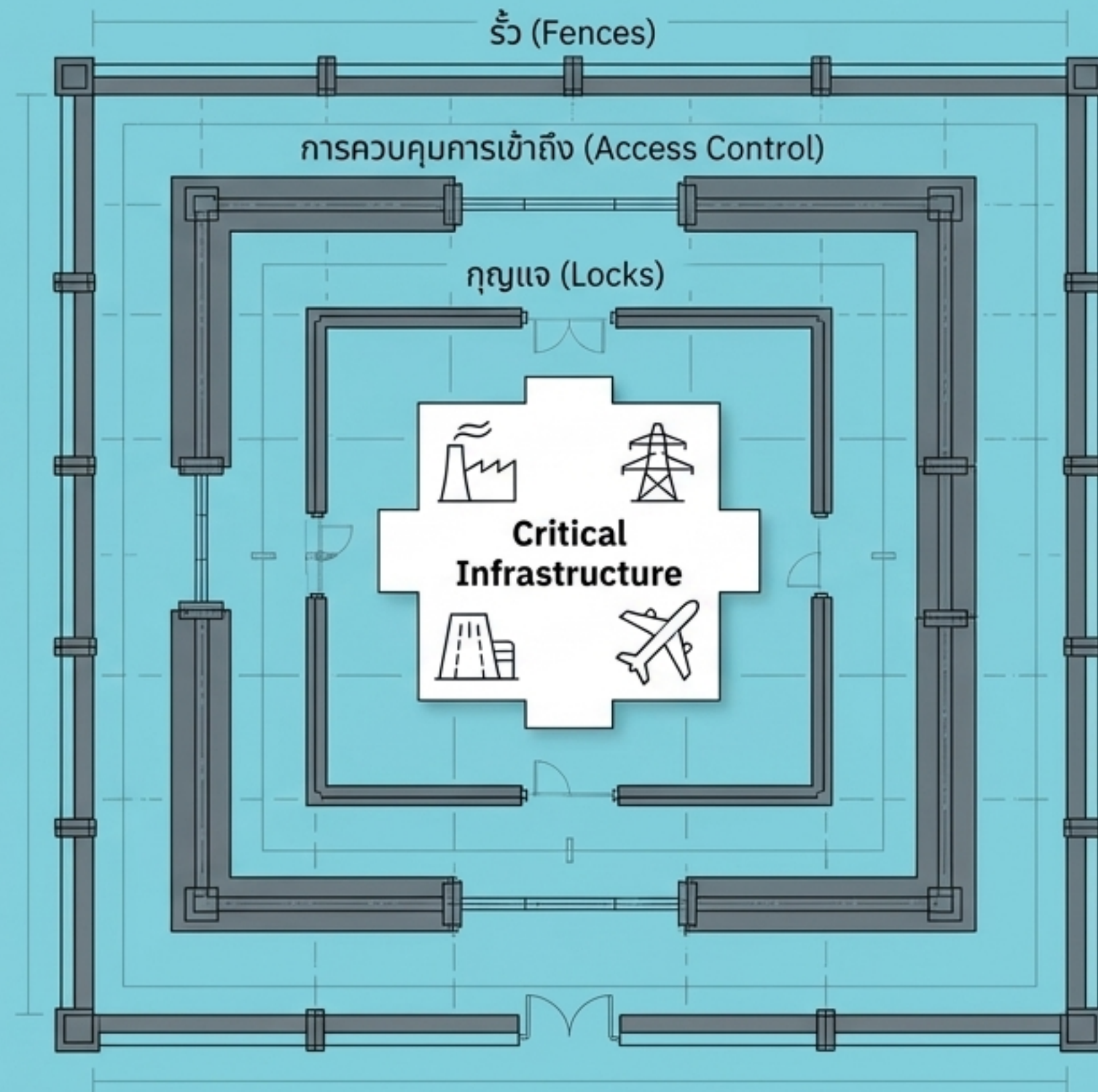
บริบททางกายภาพและ โครงสร้างพื้นฐาน

ความมั่นคงทางกายภาพ

มาตรการที่จับต้องได้เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม หรือการก่อวินาศกรรม

ความมั่นคงโครงสร้างพื้นฐาน

การปกป้องระบบหลักที่หล่อเลี้ยงประเทศ (เช่น ท่าอากาศยาน ระบบไฟฟ้า เขื่อน) การจำกัดช่องโหว่เพื่อป้องกันการก่อการร้าย และผลกระทบต่อประชาชนวงกว้าง



โครงสร้างพื้นฐานที่ปลอดภัยคือกระดูกสันหลังของประเทศ

บริบทองค์กร ชายแดน และทางทะเล



ความมั่นคงองค์กร

การบรรเทาความเสี่ยงและจัดการภัยคุกคามเพื่อความอยู่รอดทางธุรกิจ



ความมั่นคงชายแดน

การควบคุมและตรวจสอบการเคลื่อนย้ายของบุคคลและสินค้าข้ามพรมแดน



ความมั่นคงทางทะเล

การปกป้องเรือและน่านน้ำจากโจรสลัด การค้ามนุษย์ และมลพิษ

ความมั่นคงต้องครอบคลุมทุกอาณาบริเวณของการดำเนินธุรกิจและรัฐ

บริบททางไซเบอร์และสารสนเทศ

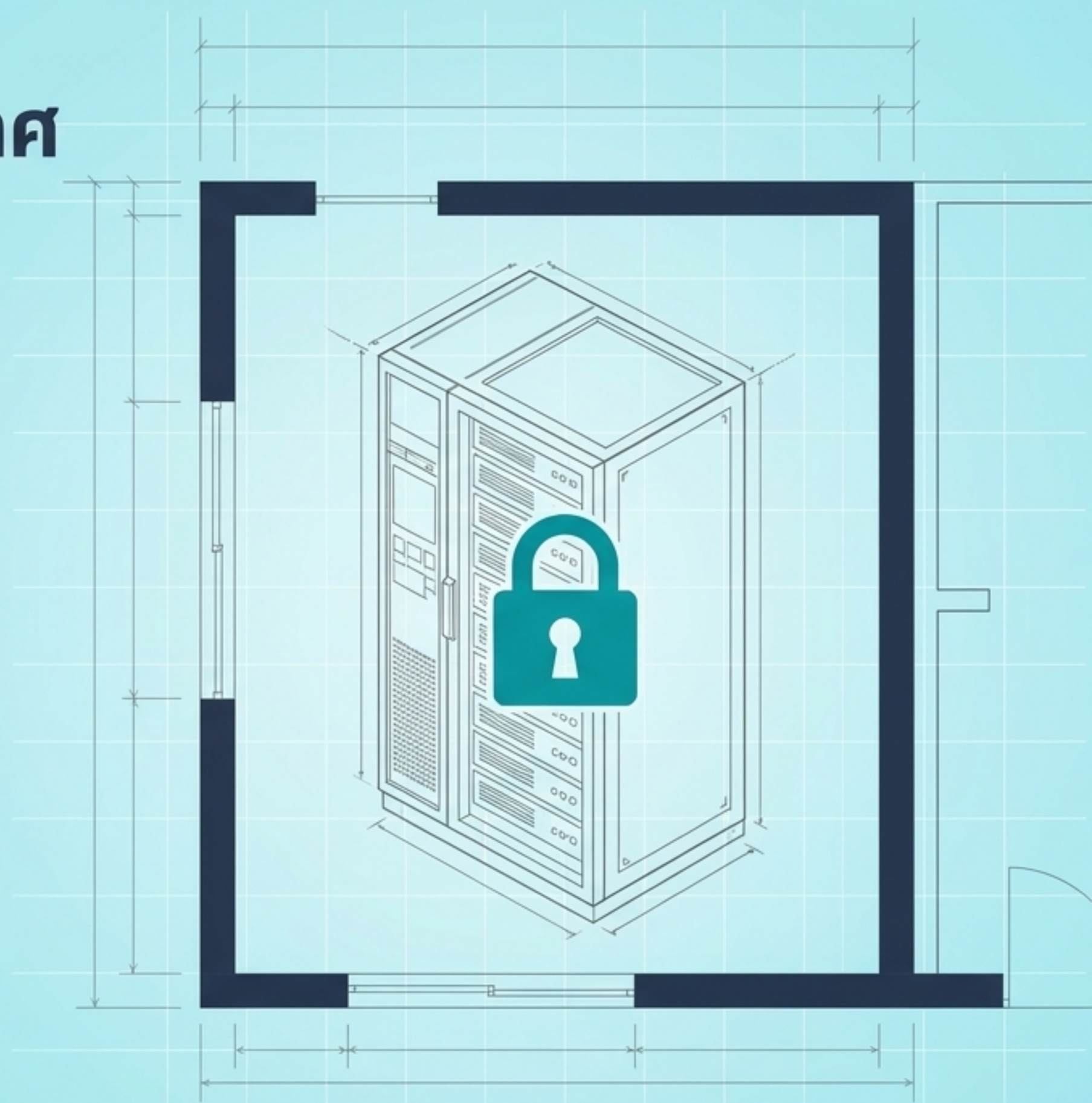
ความมั่นคงทางไซเบอร์

การปกป้องฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่าย
จากการโจมตีหรือการหยุดชะงัก

ความมั่นคงทางข้อมูล

การควบคุมการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
การเปิดเผย หรือการทำลายข้อมูล

ต้องการการฝึกอบรมข้ามสายงานระหว่างผู้เชี่ยวชาญ
ด้าน IT และความมั่นคงทางกายภาพ (Purpura, 2018)



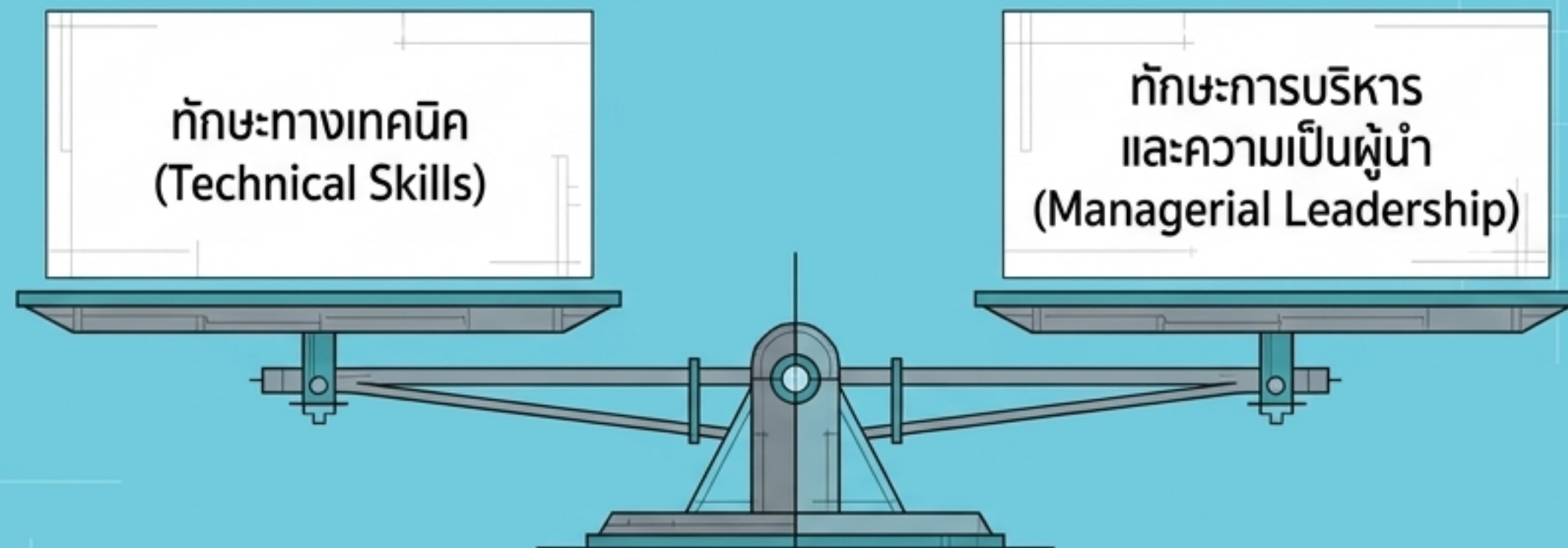
ข้อมูลเป็นทรัพย์สินที่มีค่าที่สุดในศตวรรษที่ 21

เปรียบเทียบบริบทหลักของความมั่นคง

บริบท (Context)	เป้าหมาย (Referent Object)	ภัยคุกคามหลัก (Main Threat)	มาตรการป้องกัน (Measure)
แห่งชาติ (National)	รัฐ	การสูญเสียอธิปไตย	กองทัพ, ตำรวจ
มนุษย์ (Human)	ปัจเจกบุคคล	การละเมิดสิทธิ, ความยากจน	กฎหมาย, สวัสดิการ
องค์กร (Corporate)	ธุรกิจ, ทรัพย์สิน	การโจรกรรม, การฟ้องร้อง	รปภ., นโยบาย
ไซเบอร์ (Cyber)	ข้อมูล, เครือข่าย	แฮกเกอร์, ไวรัส	ไฟร์วอลล์, การเข้ารหัส

เข้าใจเป้าหมาย (Referent Object) เพื่อเลือกเครื่องมือป้องกันที่ถูกต้อง

บทบาทพื้นฐานของการจัดการความมั่นคง



ความเป็นผู้นำและการประสานงานร่วมกับทุกภาคส่วนในองค์กร

การสร้างสมดุลระหว่างความรู้ทางเทคนิคและทักษะการบริหารจัดการ

ดูแลให้การดำเนินงานต่อเนื่องโดยมีข้อขัดข้องน้อยที่สุด

บรรเทาความเสียหายจากการสูญเสียทางกายภาพและลดความเสี่ยงทางกฎหมาย (Land et al., 2014)

ผู้จัดการความมั่นคงคือสะพานเชื่อมระหว่างเทคนิคและวิสัยทัศน์องค์กร

เป้าหมายการปกป้อง 4 ประการ



ความปลอดภัยสร้างความไว้วางใจ และความไว้วางใจเพิ่มผลผลิต

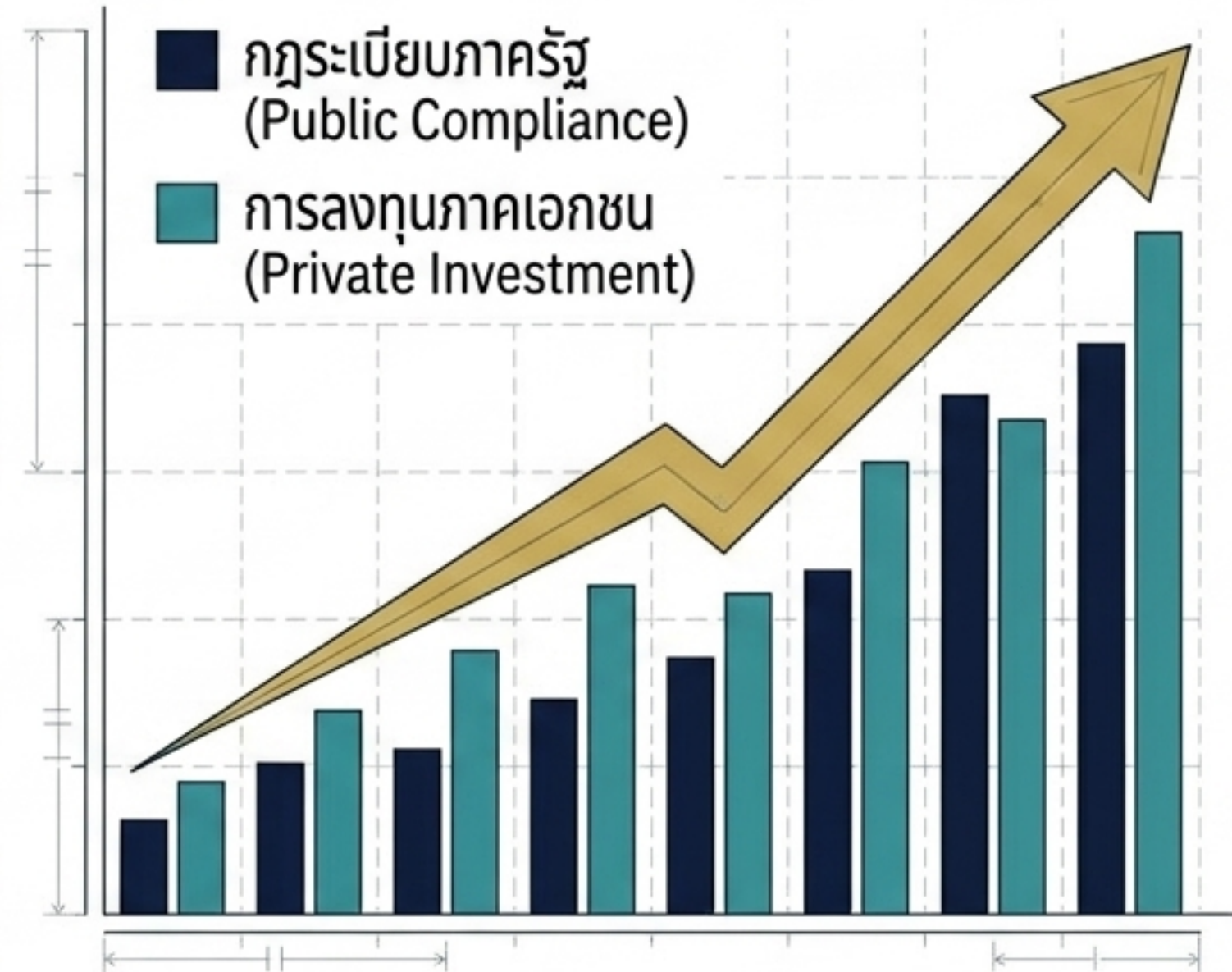
ความสำคัญต่อภาครัฐและเอกชน

งบประมาณด้านความมั่นคงทั่วโลก
เพิ่มสูงขึ้นอย่างต่อเนื่อง

ขับเคลื่อนโดยข้อกำหนดทางกฎหมาย
มาตรฐานประกันภัย และหุ้นส่วนธุรกิจ

ลดต้นทุนแฝงจากการเปลี่ยนทรัพย์สิน
ที่สูญหายและการถูกฟ้องร้อง

ความต้องการฮาร์ดแวร์ ซอฟต์แวร์ และบุคลากร
ที่ผ่านการฝึกอบรมเพิ่มขึ้นอย่างรวดเร็ว
(Land et al., 2014)



ความมั่นคงไม่ใช่ค่าใช้จ่าย แต่เป็นการลงทุนเพื่อลดความเสี่ยง

ระเบียบวิธีและนโยบายความมั่นคง



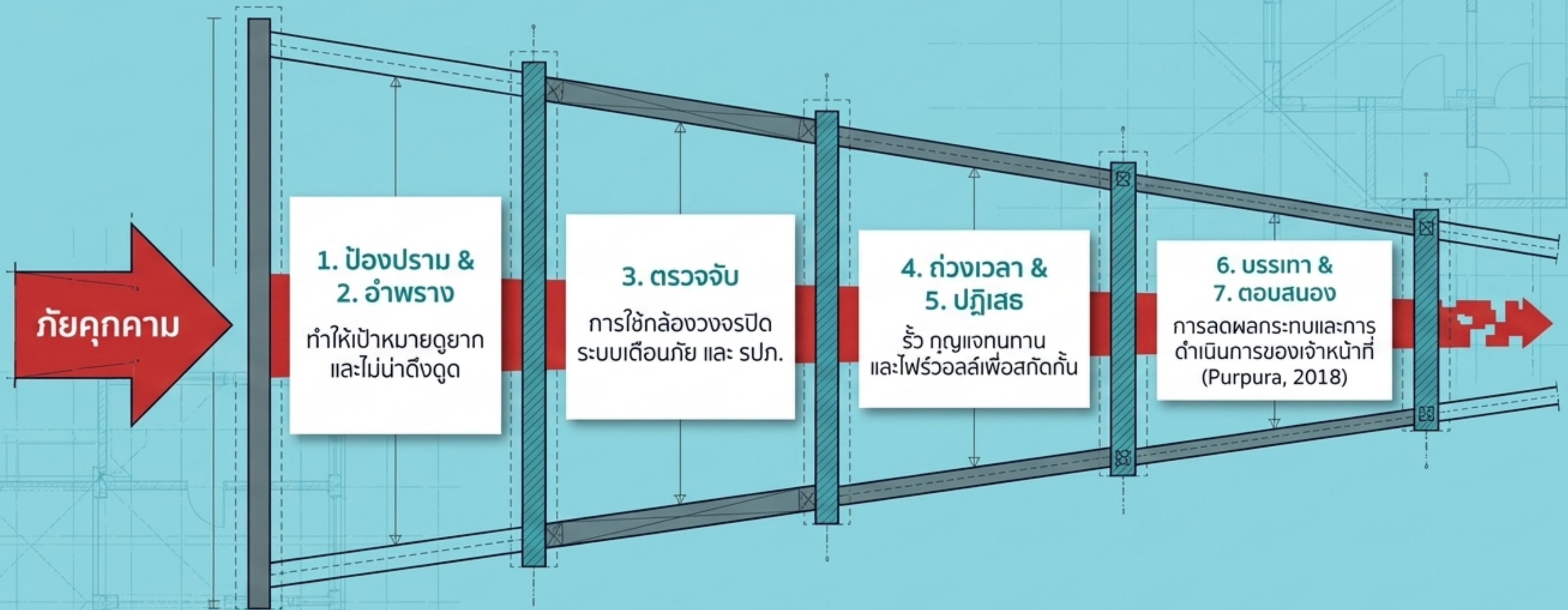
พัฒนาจากกฎหมาย หลักการ
และตระหนักรู้ทางปรัชญา

ตัวอย่าง:
การป้องกันอาชญากรรมผ่าน
การออกแบบสิ่งแวดล้อม
(CPTED)

ใช้การสำรวจอาคารสถานที่
(Security Survey) เพื่อ
ระบุจุดอ่อนและวางแผน

การออกแบบสภาพแวดล้อมที่ดีสามารถยับยั้งอาชญากรรมได้

กลยุทธ์การป้องกัน 7 ประการ



กลยุทธ์ที่ดีต้องเริ่มจากการป้องกันปรามและจบที่การบรรเทาความเสียหาย

ต้นกำเนิดทางประวัติศาสตร์

ยุคกลาง

ปราสาทที่มีคูน้ำ,
ระบบ Tithing/Shire,
กฎบัตรแมกนาคาร์ตา (ค.ศ. 1215)
กำหนดกระบวนการยุติธรรม



ยุคโบราณ

กำแพงเมืองจีน,
กฎหมายฮัมมูราบี
(กฎหมายลายลักษณ์
อักษรฉบับแรก),
ทหารองครักษ์โรมัน



ยุคก่อนประวัติศาสตร์

มนุษย์ทำใช้สิ่งกีดขวาง
ทางธรรมชาติและการ
ป้องกันแบบซ้ำซ้อน
(ไฟ, สุนัข)



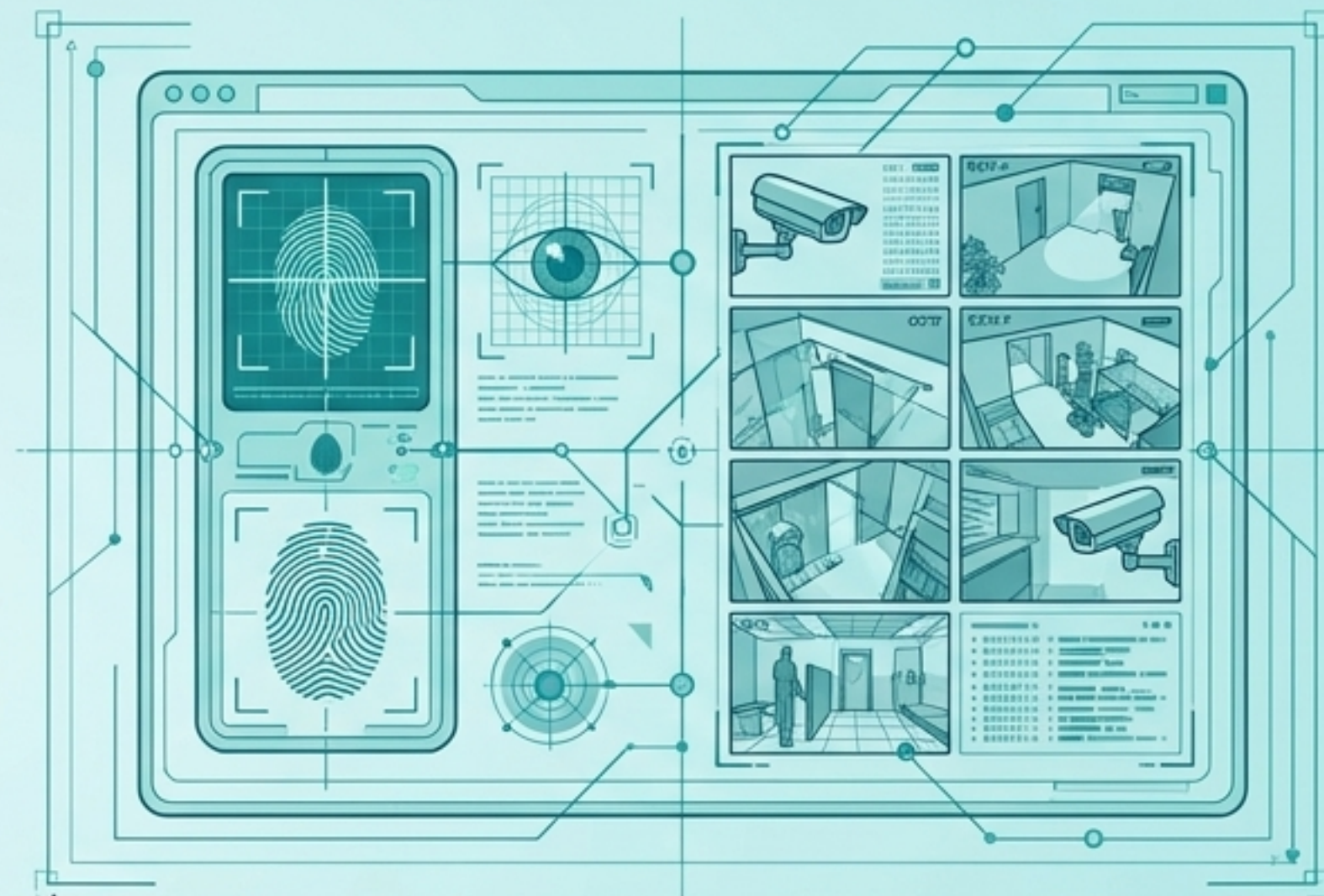
กลยุทธ์ "การป้องกันหลายชั้น"
ถูกใช้มาตั้งแต่ยุคก่อนประวัติศาสตร์

สู่ยุคความมั่นคงสมัยใหม่และเทคโนโลยี



ปฏิวัติอุตสาหกรรม: การเติบโตของความมั่นคงเอกชน (Bow Street Runners, Pinkerton, Wells Fargo, ADT)

เซอร์โรเบิร์ต พีล (Sir Robert Peel): ผู้ก่อตั้งกองกำลังตำรวจอาชีพแห่งลอนดอน ("Bobbies")



ศตวรรษที่ 20-21: การเปลี่ยนผ่านสู่เทคโนโลยีเทรอนิกส์, อาชญากรรมไซเบอร์ และการต่อต้านการก่อการร้ายหลังเหตุการณ์ 9/11

เทคโนโลยีเปลี่ยนรูปแบบอาชญากรรม
จึงต้องเปลี่ยนรูปแบบการป้องกัน

บทสรุปและกิจกรรมทบทวน

สรุป:

ความมั่นคงเป็นสหวิทยาการที่มุ่งปกป้องบุคคล
ทรัพย์สิน และสร้างสภาพแวดล้อมที่คาดเดาได้

คำถาม 1: ความมั่นคงเอกชนและความมั่นคง
สาธารณะในประเทศไทยแตกต่างกันอย่างไร?

คำถาม 2: ผู้จัดการความมั่นคงในยุคไซเบอร์
ควรมีทักษะอะไรบ้าง?



ให้นักศึกษาจับคู่และระบุภัย
คุกคามในมหาวิทยาลัย
พร้อมเสนอมาตรการป้องกัน
1 วิธีตามกลยุทธ์ 7 ประการ