สรุปคู่มือ
การควบคุมภายใน
มหาวิทยาลัยแม่โจ้

สื่อสารถ่ายทอดคู่มือกระบวนการจัดวางการควบคุมภายใน เพื่อใช้เป็นแนวทางในการปฏิบัติงานให้เป็นไปรูปแบบและทิศทางเดียวกันทั่วทั้งองค์กร

ฉบับถ่ายทอดสู่การปฏิบัติ

การจัดวางการควบคุมภายใน

ให้ทุกส่วนงาน/หน่วยงาน “เข้าใจง่าย • ทำได้จริง • มีหลักฐาน • ติดตามต่อเนื่อง”

Internal Control Deployment – MJU 2570

1 เริ่มจาก “งานจริง”

เลือกพันธกิจ/กระบวนงานสำคัญ กำหนดวัตถุประสงค์ให้ชัด แล้วจึงมองความเสี่ยง

2 ควบคุม “ตรงสาเหตุ”

ไม่ใช่เพิ่มเอกสาร แต่กำหนดวิธีป้องกัน ตรวจพบ หรือแก้ไขที่ทำได้จริง

3 พิสูจน์ด้วย “หลักฐาน”

ระบุผู้รับผิดชอบ ความถี่ หลักฐาน และประเมินว่าความเสี่ยงลดลงจริงหรือไม่

เป้าหมาย: การควบคุมภายในเป็นส่วนหนึ่งของงานประจำ ไม่ใช่งานเอกสารปลายปี

เข้าใจก่อนเริ่ม: การควบคุมภายในคืออะไร?

สร้างความเชื่อมั่นอย่างสมเหตุสมผลต่อการบรรลุวัตถุประสงค์ 3 ด้าน

1 การดำเนินงาน

ทำงานได้ผล มีประสิทธิภาพ ประหยัด คุ้มค่า และดูแลทรัพยากร

2 การรายงาน

ข้อมูลถูกต้อง ครบถ้วน เชื่อถือได้ โปร่งใส และทันเวลา

3 การปฏิบัติตาม

ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ นโยบาย และหลักธรรมาภิบาล

หลักคิดสำคัญ

- เป็นส่วนหนึ่งของงานประจำ ไม่ใช่ทำเพื่อรายงานเท่านั้น
- ออกแบบบนพื้นฐานความเสี่ยง (Risk-based)
- ผู้บริหาร + เจ้าของกระบวนงาน + ผู้ปฏิบัติ รับผิดชอบร่วมกัน
- **การมีระเบียบ/คู่มือ ≠ การควบคุมมีประสิทธิผล ต้องมีการปฏิบัติและหลักฐาน**

SIPOC+ กระบวนการจัดวางการควบคุมภายใน

มหาวิทยาลัยแม่โจ้

สร้างความเชื่อมั่นอย่างสมเหตุสมผลต่อการบรรลุวัตถุประสงค์ 3 ด้าน: การดำเนินงาน • การรายงาน • การปฏิบัติตาม

Supplier (ผู้ส่งมอบข้อมูล/ทรัพยากร)

- หน่วยงานภายในมหาวิทยาลัย (คณะ, วิทยาลัย, สำนัก, สถาบัน, กอง, ศูนย์)
- หน่วยงานกำกับดูแลภายนอก (สป.อว., สตง., ป.ป.ช., กกต., ฯลฯ)
- ผู้มีส่วนได้ส่วนเสีย (นักศึกษา, ผู้ปกครอง, บุคลากร, พันธมิตรทางวิชาการ/ธุรกิจ)
- ระบบสารสนเทศ/ฐานข้อมูล งบประมาณ, การเงิน, บุคลากร, พัสดุ, ทรัพย์สิน, งานวิจัย
- กฎหมาย ระเบียบ ข้อบังคับ นโยบาย และมาตรฐานที่เกี่ยวข้อง
- นโยบายและยุทธศาสตร์ของมหาวิทยาลัย
- ข้อมูลผภาพแวดล้อมภายใน-ภายนอก (SWOT, PESTLE, Benchmark)

Input (ข้อมูลนำเข้า)

- ข้อมูลสภาพแวดล้อมภายในและภายนอก
- นโยบายและยุทธศาสตร์มหาวิทยาลัย
- ข้อมูลทะเบียนความเสี่ยง (Risk Register)
- ข้อมูลการเงิน บุคลากร โครงสร้างพื้นฐาน
- กฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานที่เกี่ยวข้อง
- ความคาดหวัง/ความต้องการของผู้มีส่วนได้ส่วนเสีย
- ข้อมูลผลการดำเนินงานในอดีต (KPI, KRI, Audit, Incident)

Process (กระบวนการ)

1. **กำหนดบริบทและวัตถุประสงค์**
   กำหนดขอบเขต ผู้รับผิดชอบ กฎหมาย/ข้อกำหนด วัตถุประสงค์ และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
2. **วิเคราะห์กระบวนงานและระบุความเสี่ยง**
   วิเคราะห์ขั้นตอนงาน จุดเสี่ยง สาเหตุ ผลกระทบ และการควบคุมที่มีอยู่เดิม
3. **ประเมินความเสี่ยง**
   ประเมินโอกาส (Likelihood) และผลกระทบ (Impact) ประเมินประสิทธิผลการควบคุม และความเสี่ยงคงเหลือ (Residual Risk)
4. **ออกแบบการควบคุม**
   กำหนดมาตรการควบคุมเพิ่มเติม เพื่อลด/ป้องกัน/ตรวจพบ กำหนดผู้รับผิดชอบ ความถี่ และหลักฐาน (Evidence)
5. **นำไปใช้และติดตาม**
   ดำเนินการควบคุมตามแผน เก็บหลักฐาน ติดตามตัวชี้วัด (KRI) และประเมินประสิทธิผล
6. **รายงานผลและปรับปรุง**
   รายงานต่อผู้บริหาร ระบุข้อบกพร่อง วิเคราะห์สาเหตุ (RCA) กำหนดแผนปรับปรุง (CAPA) และติดตามจนปิดประเด็น

Output (ผลลัพธ์)

- รายงานการควบคุมภายใน (แบบ ปค.5)
- ทะเบียนความเสี่ยงที่ปรับปรุง (Risk Register)
- แผน/มาตรการควบคุม และแนวทางตอบสนองความเสี่ยง
- KPI/KRI สำหรับติดตามความเสี่ยงสำคัญ
- การสื่อสารและสร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสีย
- ข้อมูลสำหรับการตัดสินใจและการกำกับดูแล

Customer (ผู้รับผลลัพธ์)

- ผู้บริหารมหาวิทยาลัย และคณะกรรมการ
- หน่วยงานภายในมหาวิทยาลัย (คณะ, สำนัก, กอง, ศูนย์)
- หน่วยงานกำกับดูแลภายนอก
- นักศึกษา บุคลากร ผู้ปกครอง ผู้รับบริการ
- ชุมชน สังคม และพันธมิตร
- มหาวิทยาลัยแม่โจ้ สู่เป้าหมายอย่างยั่งยืน

เส้นเรื่อง การควบคุมภายใน

ภารกิจ/วัตถุประสงค์ (ต้องบรรลุให้ได้) → ความเสี่ยง (อะไรอาจเกิดขึ้น) → การควบคุม (เราทำอะไรเพื่อจัดการ) → ผลการดำเนินงานและหลักฐาน (ทำแล้วเกิดผลอะไร) → ผลประเมิน (ควบคุมได้ผลหรือไม่) → ความเสี่ยงคงเหลือ (ยังเหลืออะไร) → การปรับปรุง (ทำอะไรเพิ่ม)

หลักคิดสำคัญ

- ✓ ควบคุมภายในเป็นส่วนหนึ่งของงานประจำ
- ✓ ออกแบบบนพื้นฐานความเสี่ยง (Risk-based)
- ✓ ผู้บริหารกำกับดูแล เจ้าของกระบวนงานเป็นเจ้าภาพ
- ✓ มีหลักฐาน = ทำจริง วัดผลได้

ตัวชี้วัดตาม (Lagging Indicators)

- จำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง
- ร้อยละของความเสี่ยงระดับสูง/สูงมาก ที่มีการตอบสนองแล้วเสร็จ
- ระยะเวลาเฉลี่ยในการตอบสนองต่อความเสี่ยงระดับสูง

ตัวชี้วัดนำ (Leading Indicators)

- ร้อยละความครบถ้วนของการระบุความเสี่ยงก่อนรอบประเมิน
- จำนวนข้อเสนอแนะ/มาตรการควบคุมใหม่
- ร้อยละการสื่อสารนโยบายความเสี่ยงถึงหน่วยงาน

การจัดการความรู้ (KM)

- สรุปบทเรียนจากเหตุการณ์ความเสี่ยง
- คู่มือ/แนวทางการควบคุมภายใน
- แหล่งเรียนรู้ (Infographic, Dashboard, Quick Guide, Template)

การบูรณาการและนวัตกรรม

- ใช้ AI/Analytics วิเคราะห์แนวโน้มความเสี่ยง
- เชื่อมโยง Risk Register กับยุทธศาสตร์และตัวชี้วัดระดับมหาวิทยาลัย
- Dashboard ติดตาม KPI/KRI แบบเรียลไทม์
- ระบบแจ้งเตือนความเสี่ยงสำคัญอัตโนมัติ

เป้าหมาย เชื่อมโยง Risk Register กับ KPI/KRI ≥ 80%

ภาพรวม 6 ขั้นตอน: จาก “ภารกิจ” สู่ “การควบคุมที่ใช้ได้จริง”

ใช้วงจรนี้กับทุกกระบวนงานหลักและกระบวนงานสนับสนุน

1 กำหนดบริบท

วัตถุประสงค์ • ขอบเขต • กฎหมาย • ผู้รับผิดชอบ

2 วิเคราะห์กระบวนงาน

ขั้นตอน • จุดเสี่ยง • สาเหตุ • ผลกระทบ • การควบคุมเดิม

3 ประเมินความเสี่ยง

L × I • ประสิทธิผลการควบคุม • Residual Risk

4 ออกแบบการควบคุม

Control Gap • ผู้รับผิดชอบ • ความถี่ • หลักฐาน • KRI

5 นำไปใช้และติดตาม

ปฏิบัติจริง • เก็บหลักฐาน • ทดสอบประสิทธิผล • ประเมินซ้ำ

6 รายงานและปรับปรุง

ข้อบกพร่อง • RCA/CAPA • ติดตามปิดประเด็น • ส่งต่อปีถัดไป

จำง่าย: Objective → Risk → Control → Evidence → Residual Risk → Improve

ขั้นตอน 1–2: เริ่มจากวัตถุประสงค์และ “งานจริง”

อย่าเริ่มจากการคิดความเสี่ยงลอย ๆ ให้เริ่มจากสิ่งที่หน่วยงานต้องทำให้สำเร็จ

1 STEP 1 กำหนดบริบทและวัตถุประสงค์

ถาม 5 คำถาม
- ภารกิจ/งานนี้ทำเพื่ออะไร?
- ผลลัพธ์หรือเป้าหมายคืออะไร?
- มีกฎหมาย/ข้อกำหนดอะไร?
- ใครเป็น Process Owner / Control Owner?
- จะวัดความสำเร็จด้วยอะไร?

2 STEP 2 วิเคราะห์กระบวนงานและระบุความเสี่ยง

วาด Flow ตั้งแต่ต้นจนจบ แล้วมองแต่ละจุดว่า
- อะไรอาจผิดพลาด/ล่าช้า/ไม่ครบถ้วน?
- เกิดจากสาเหตุอะไร? กระทบอะไร?
- มี Fraud / IT / PDPA / Continuity หรือไม่?
- ตอนนี้ควบคุมอย่างไร?

ตัวอย่าง: “การจัดซื้อจัดจ้าง”

วัตถุประสงค์: จัดซื้อถูกต้อง โปร่งใส และแล้วเสร็จตามแผน

ความเสี่ยง: เอกสารไม่ครบ/ล่าช้า → โครงการและการเบิกจ่ายไม่เป็นไปตามแผน

เขียนความเสี่ยงให้เห็น “เหตุการณ์ + ผลต่อวัตถุประสงค์”

ไม่ใช่: “บุคลากรไม่พอ”
ควรเป็น: “การตรวจเอกสารอาจล่าช้า ทำให้การจัดซื้อไม่แล้วเสร็จตามแผน”

ขั้นตอน 3: ประเมินความเสี่ยงและคัดเลือกประเด็นสำคัญ

ประเมินก่อนควบคุม → ดูประสิทธิผลการควบคุมเดิม → ประเมินความเสี่ยงคงเหลือ

1–4 ต่ำ
ติดตามตามงานปกติ

5–9 ปานกลาง
ทบทวน/ติดตามโดยผู้รับผิดชอบ

10–15 สูง
ต้องจัดทำ/ปรับปรุงการควบคุม

16–25 สูงมาก
รีบจัดการและรายงานผู้บริหาร

เกณฑ์คัดเลือกเพื่อจัดวาง/ปรับปรุง

- Residual Risk ≥ 11 คะแนน ให้พิจารณาเป็นลำดับแรก
- ต้องดู “นัยสำคัญ + ประสิทธิผลการควบคุม” ร่วมด้วย
- ต่ำกว่า 11 ก็เลือกได้ หากเกี่ยวกับกฎหมาย/ทุจริต/ความปลอดภัย/สิทธิผู้รับบริการ/การเงิน/PDPA/ชื่อเสียง
- ไม่ต้องฝืนเลือกให้ครบ 3 ประเด็น

คำถามตัดสินใจ 3 ข้อ

1) ถ้าเกิดขึ้น กระทบวัตถุประสงค์สำคัญหรือไม่?
2) การควบคุมที่มีอยู่ “ออกแบบดี + ทำจริง + มีหลักฐาน” หรือไม่?
3) หลังควบคุมแล้ว ความเสี่ยงยังสูงเกินยอมรับหรือไม่?

ถ้า “ใช่” → ต้องจัดวาง/ปรับปรุงการควบคุม

ขั้นตอน 4: ออกแบบกิจกรรมควบคุมให้ “ตรงสาเหตุ”

กิจกรรมควบคุมที่ดีต้องบอกได้ว่า ใครทำ • ทำอะไร • เมื่อไร • อย่างไร • มีหลักฐานอะไร

ป้องกัน | Preventive

ป้องกันก่อนเกิด เช่น แบ่งแยกหน้าที่ ตรวจคุณสมบัติก่อนอนุมัติ

ตรวจพบ | Detective

ค้นหาความผิดปกติ เช่น กระทบยอด สอบทาน Exception/Log

แก้ไข | Corrective

แก้ปัญหาและไม่ให้เกิดซ้ำ เช่น RCA, CAPA, ปรับขั้นตอน

Control Design Checklist

- ✓ ตรงกับ “สาเหตุ” ของความเสี่ยง
- ✓ ระบุ Control Owner และผู้สอบทาน/อนุมัติ
- ✓ กำหนดความถี่/ระยะเวลาให้ชัด
- ✓ มีหลักฐานตรวจสอบย้อนกลับได้
- ✓ คุ้มค่าและทำได้จริง ไม่สร้างภาระเกินจำเป็น
- ✓ มีตัวชี้วัด/KRI และแผนเพิ่ม หาก Residual Risk ยังสูง

ตัวอย่างทำจริง: จากความเสี่ยง → การควบคุม → หลักฐาน

ตัวอย่างกระบวนงานจัดซื้อจัดจ้าง เพื่อเห็นความเชื่อมโยงแบบครบวงจร

วัตถุประสงค์	จัดซื้อถูกต้อง โปร่งใส และแล้วเสร็จตามแผน
ความเสี่ยง	เอกสารไม่ครบ/ล่าช้า ทำให้โครงการและเบิกจ่ายไม่เป็นไปตามแผน
การควบคุมเดิม	แผนจัดซื้อ + Checklist + สอบทานก่อนอนุมัติ + รายงานสถานะ
ผลประเมิน	ปฏิบัติไม่สม่ำเสมอ ไม่มีระบบแจ้งเตือน เอกสารถูกส่งกลับหลายครั้ง
การปรับปรุง	**Dashboard ติดตาม · ตรวจ TOR ล่วงหน้า · แจ้งเตือน 15/30 วัน · รายงานรายการล่าช้ารายเดือน**
หลักฐาน	Dashboard/รายงานสถานะ · Checklist ที่ลงนาม · Log แจ้งเตือน · รายงานต่อหัวหน้าส่วนงาน

หลักคิด: “ทำครบกิจกรรม” ยังไม่พอ — ต้องพิสูจน์ว่าการควบคุมทำงานและช่วยลดความเสี่ยง

ขั้นตอน 5–6: นำไปใช้ ติดตาม ประเมิน และปรับปรุง

ประสิทธิผล = ออกแบบเหมาะสม + ปฏิบัติจริงอย่างต่อเนื่อง + ทำงานร่วมกัน

1 Present

มีการออกแบบไว้จริง
- ขั้นตอน/ผู้รับผิดชอบชัด
- ครอบคลุมความเสี่ยงสำคัญ
- ไม่ใช่มีเพียงเอกสาร

2 Functioning

ทำจริงตามที่กำหนด
- ความถี่ครบ
- มีหลักฐาน
- ตรวจสอบย้อนกลับได้

3 Operating Together

ระบบทำงานเชื่อมกัน
- ป้องกัน/ตรวจพบ/แก้ไข
- Residual Risk ลดลง
- บรรลุวัตถุประสงค์

เมื่อพบข้อบกพร่อง

ระบุปัญหา → วิเคราะห์สาเหตุ (RCA) → กำหนด Corrective/Preventive Action (CAPA) → ผู้รับผิดชอบ/กำหนดเสร็จ → ติดตามจนพิสูจน์ว่าปิดได้

เหตุร้ายแรง / ทุจริต / ฝ่าฝืนกฎหมาย / ข้อมูลรั่วไหล / Cyber / เกิน Risk Tolerance → รายงานทันที ไม่รอรอบ 6 หรือ 12 เดือน

Workflow ผ่านระบบ ICS: ใครทำอะไร เมื่อไร?

วงจรประจำปีของส่วนงาน/หน่วยงาน ตั้งแต่เริ่มจัดวางจนถึงรายงานระดับมหาวิทยาลัย

1. มอบหมายผู้รับผิดชอบ
2. ทบทวนข้อมูลเดิม
3. วิเคราะห์ภารกิจ/ความเสี่ยง
4. จัดวางกิจกรรมควบคุม
5. ปฏิบัติจริง + หลักฐาน
6. **รายงาน 6 เดือน**
7. ทบทวนกลางปี
8. **ประเมิน 12 เดือน / ปค.5**
9. ประเมิน 5 องค์ประกอบ / ปค.4
10. ผู้บริหารรับรอง
11. มหาวิทยาลัยวิเคราะห์
12. จัดทำ ปค.1 ระดับมหาวิทยาลัย
13. ส่งต่อประเด็นปีถัดไป

ICS = ศูนย์กลางข้อมูล · เชื่อมความเสี่ยง → การควบคุม → ผลติดตาม → แผนปรับปรุง

แบบฟอร์มที่ต้องเชื่อมโยงกัน: กรอกครั้งเดียว คิดต่อเนื่อง

ข้อมูลต้องเล่าเรื่องเดียวกันตั้งแต่ภารกิจจนถึงการปรับปรุง

IC-MJU-01

วิเคราะห์ภารกิจ/กระบวนงาน
ความเสี่ยง + การควบคุมเดิม
คัดเลือกประเด็นสำคัญ

→

ปค.5

ติดตามผล 6/12 เดือน
ประเมินการควบคุม
Residual Risk + ปรับปรุง

→

ปค.4

ประเมินภาพรวมระบบ
5 องค์ประกอบ COSO
จุดแข็ง/ข้อบกพร่อง

→

ปค.1

รับรองผลการประเมิน
สรุปความเพียงพอ
เปิดเผยประเด็นที่ยังต้องปรับปรุง

เส้นเรื่องที่ต้อง “ตรงกัน”

ภารกิจ → วัตถุประสงค์ → ความเสี่ยง → การควบคุม → ผลการดำเนินงาน → ผลประเมิน → ความเสี่ยงคงเหลือ → การปรับปรุง

ผู้บริหารส่วนงานต้องสอบทานความครบถ้วน ถูกต้อง สอดคล้อง สมเหตุสมผล และหลักฐาน ก่อนรับรองใน ICS

วิธีกรอกรายงาน

ความเชื่อมโยงการกรอกแบบรายงานการควบคุมภายใน

เสี่ยงอะไร › ควบคุมอย่างไร › ทำแล้วเกิดผลอะไร › ได้ผลหรือไม่ › ยังเหลือความเสี่ยงอะไร › ต้องปรับปรุงอะไร › ใครรับผิดชอบเสร็จเมื่อใด

คอลัมน์	คำถามที่ต้องตอบ	แนวทางเขียนให้ใช้ได้จริง
(2) ความเสี่ยง	อะไรอาจผิดพลาดหรือทำให้วัตถุประสงค์ไม่บรรลุ?	เขียน “เหตุการณ์ความเสี่ยง” ให้ชัดเจน
(3) การควบคุมภายในที่มีอยู่	เรามีวิธีป้องกัน/ตรวจสอบอย่างไร?	ระบุวิธีที่ใช้จริง เช่น Checklist • แบ่งแยกหน้าที่ • อนุมัติ • สอบทาน • แจ้งเตือน
(4) ผลการดำเนินงาน	รอบนี้ทำอะไร และเกิดผลอย่างไร?	เขียนทั้ง “สิ่งที่ทำ + ผลที่เกิด” พร้อมข้อมูล/หลักฐาน
(5) การประเมินผลการควบคุม	การควบคุมได้ผลจริงหรือไม่?	ประเมินว่าสามารถ ป้องกัน • ตรวจพบ • แก้ไข และลดความเสี่ยงได้เพียงใด
(6) ความเสี่ยงที่ยังมีอยู่	หลังควบคุมแล้ว ยังอาจผิดพลาดอะไร?	ระบุเฉพาะ Residual Risk / ช่องว่างที่ยังเหลือ ไม่คัดลอกความเสี่ยงเดิมทั้งประโยค
(7) การปรับปรุงการควบคุม	ต้องทำอะไรเพิ่ม?	มาตรการใหม่ต้องตอบตรงกับความเสี่ยงใน (6) และติดตามผลได้
(8) ผู้รับผิดชอบ/กำหนดเสร็จ	ใครทำ และเสร็จเมื่อใด?	ระบุ Owner หลัก + วัน/เดือน/ปี หรือช่วงเวลาที่ชัดเจน

หลักคิด: ทุกคอลัมน์ต้องเชื่อมกันเป็นเหตุเป็นผล (2) → (3) → (4) → (5) → (6) → (7) → (8) และต้องมีหลักฐานรองรับ

Checklist ก่อนกดส่ง: 10 ข้อที่ช่วยลดการแก้กลับ

ใช้เป็นรายการตรวจคุณภาพข้อมูลของส่วนงาน/หน่วยงาน

1. วัตถุประสงค์เขียนเป็น “ผลลัพธ์ที่ต้องการ” ชัดเจน
2. ความเสี่ยงเชื่อมโยงกับวัตถุประสงค์ ไม่ใช่เพียงปัญหาทั่วไป
3. ระบุสาเหตุและผลกระทบพอให้เลือกการควบคุมได้
4. ประเมิน L × I และ Residual Risk อย่างมีเหตุผล
5. การควบคุมตรงสาเหตุและทำได้จริง
6. ระบุ Owner / ความถี่ / ระยะเวลา / หลักฐาน
7. มี KRI/ตัวชี้วัดที่สะท้อนความเสี่ยงหรือผลของการควบคุม
8. **ผลประเมินอ้างอิงหลักฐาน ไม่ใช้เพียง % ความสำเร็จกิจกรรม**
9. **ปค.5 / ปค.4 / ปค.1 สอดคล้องกับข้อมูลจัดวาง**
10. **ประเด็นค้าง/ข้อบกพร่องสำคัญถูกส่งต่อและติดตามจนปิด**

สรุป: ทำให้การควบคุมภายใน “มีชีวิต” ในงานประจำ

เป้าหมายไม่ใช่แบบฟอร์มที่ครบ แต่คือความเสี่ยงที่ถูกจัดการและงานที่บรรลุวัตถุประสงค์

1
เริ่มจากงาน
Objective & Process

2
มองความเสี่ยง
Risk & Root Cause

3
ควบคุมตรงจุด
Control Design

4
ทำจริงมีหลักฐาน
Implement & Evidence

5
ประเมินผล
Residual Risk

6
ปรับปรุงต่อเนื่อง
Improve

3 คำถามก่อนจบทุกปี

ความเสี่ยงลดลงหรือยัง?

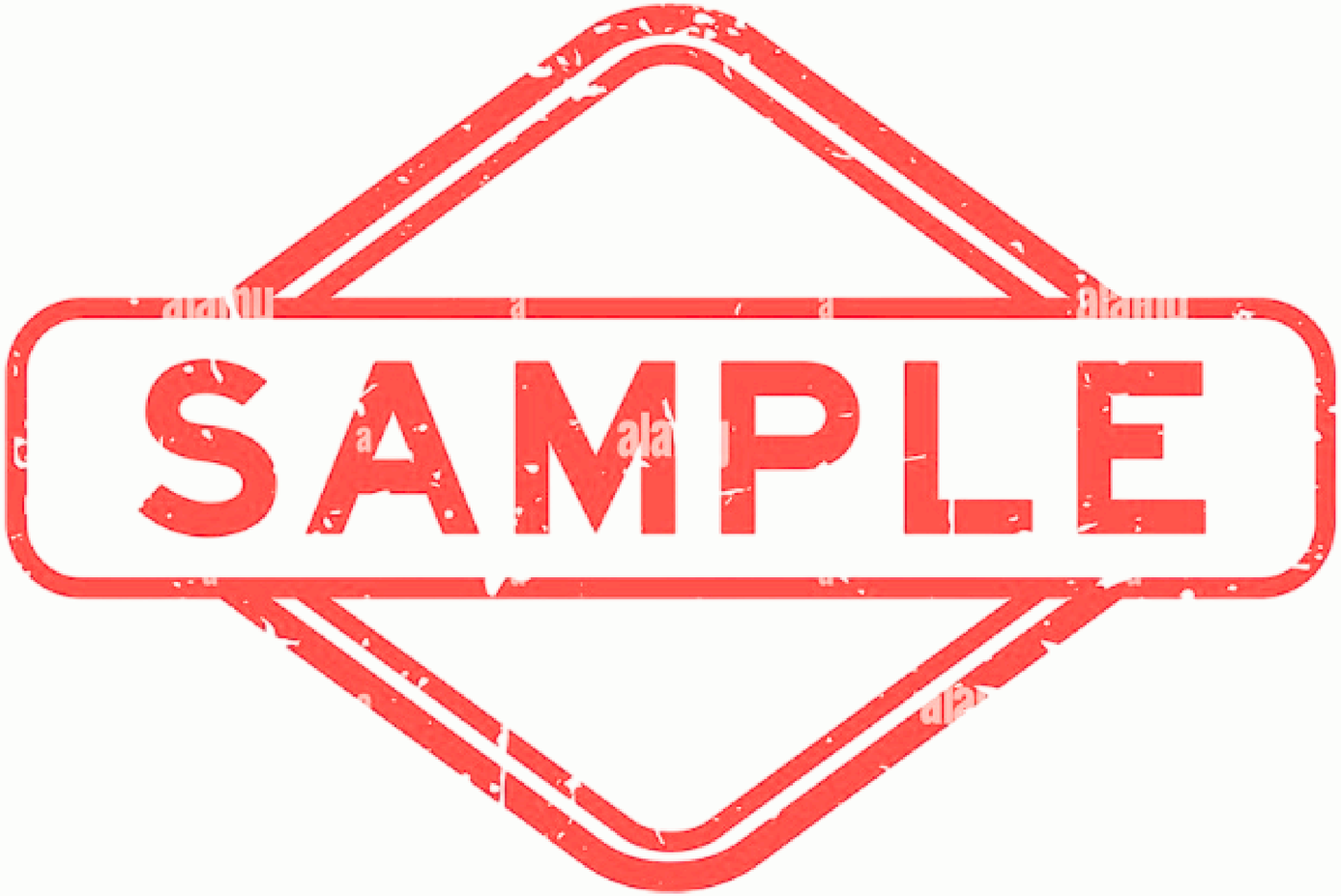
ดู Residual Risk + เหตุการณ์จริง + KRI

การควบคุมทำงานจริงไหม?

ดูหลักฐาน + ความสม่ำเสมอ + ผลลัพธ์

ต้องปรับอะไรต่อ?

RCA/CAPA + ประเด็นค้าง + บริบทใหม่


SAMPLE

ตัวอย่างการควบคุมภายใน — จากความเสี่ยงสู่การควบคุมที่ใช้ได้จริง

ใช้เป็นตัวอย่างประกอบการกรอก IC-MJU-01 และการรายงานผล 6/12 เดือน

วัตถุประสงค์	ความเสี่ยง	การควบคุมที่มีอยู่	ผล/หลักฐาน	ประเมินผล	Residual Risk	ปรับปรุง

หลักของการควบคุมที่ดี

- ตอบตรงกับสาเหตุ/ความเสี่ยง ไม่ใช่เพียงระบุกิจกรรมทั่วไป
- ระบุผู้ทำ ผู้สอบทาน ความถี่ และหลักฐานได้
- แยก Preventive / Detective / Corrective ตามวัตถุประสงค์
- ประเมินผลจากหลักฐานและผลลัพธ์ ไม่ใช้คำว่า “ดำเนินการแล้ว” อย่างเดียว

สิ่งที่ไม่ควรใช้เป็น Control เพียงลำพัง

- “มีคณะกรรมการ” แต่ไม่ระบุว่าตรวจอะไร/ตัดสินใจอย่างไร
- “กำชับ/แจ้งเวียน” โดยไม่มีการตรวจสอบความเข้าใจหรือการปฏิบัติ
- “ประชุมติดตาม” แต่ไม่มีเกณฑ์ สถานะ และการแก้ไข
- มาตรการที่ยังไม่เริ่มดำเนินการ ไม่ควรใช้ลด Residual Risk ปัจจุบัน

คำถามก่อนยืนยันว่าควบคุมได้ผล

- ออกแบบเพียงพอหรือไม่? (Design)
- นำไปปฏิบัติจริงหรือไม่? (Implementation)
- ทำงานสม่ำเสมอและลดความเสี่ยงจริงหรือไม่? (Effectiveness)
- มีหลักฐานตรวจสอบย้อนกลับได้หรือไม่?

ตัวอย่าง 1 | การจัดซื้อจัดจ้าง

(1) วัตถุประสงค์: จัดซื้อถูกต้อง โปร่งใส ทันเวลา และได้พัสดุตรงความต้องการ

(2) ความเสี่ยง
• การกำหนด TOR/คุณลักษณะหรือเอกสารจัดซื้ออาจไม่ครบถ้วน ทำให้ล่าช้า/ผิดระเบียบ

(3) การควบคุมที่มีอยู่
• Checklist เอกสารก่อนเสนออนุมัติ
• แยกผู้จัดทำ–ผู้ตรวจสอบ–ผู้อนุมัติ
• สอบทาน TOR/ราคากลางตามเกณฑ์
• บันทึกผลการตรวจและเก็บหลักฐานในระบบ

(4) ผลการดำเนินงาน / หลักฐาน
• ตรวจ 50 รายการ พบเอกสารไม่ครบ 3 รายการ และแก้ไขก่อนอนุมัติทั้งหมด

(5) ประเมินผลการควบคุม
• ประเมิน Design + Implementation + Effectiveness
• สรุปว่า “เพียงพอ/ควรปรับปรุง” พร้อมเหตุผลจากหลักฐาน

(6) ความเสี่ยงที่ยังมีอยู่
• ยังเสี่ยงจากการตีความข้อกำหนดเฉพาะกรณีและการเปลี่ยนแปลงระเบียบ

(7) การปรับปรุงการควบคุม
• จัดทำ Knowledge Base/FAQ + ทบทวน Checklist เมื่อกฎหมายเปลี่ยน + กำหนดผู้เชี่ยวชาญให้คำปรึกษา

หลักการ: คอลัมน์ (7) ต้องตอบตรงกับความเสี่ยงคงเหลือใน (6) และกำหนด Owner + กำหนดเสร็จในคอลัมน์ (8)

ตัวอย่าง 2 | การรับนักศึกษา

(1) วัตถุประสงค์: รับสมัครและยืนยันสิทธิ์ถูกต้อง ครบถ้วน ทันตามปฏิทิน

(2) ความเสี่ยง

• ข้อมูลผู้สมัคร/คุณสมบัติอาจตรวจสอบไม่ครบ ทำให้รับผู้ไม่มีคุณสมบัติหรือเกิดข้อร้องเรียน

(3) การควบคุมที่มีอยู่

• ระบบตรวจสอบข้อมูลบังคับกรอก
• Checklist คุณสมบัติรายหลักสูตร
• ผู้ตรวจสอบคนที่ 2 สำหรับกรณีเงื่อนไขพิเศษ
• รายงาน Exception ก่อนประกาศผล

(4) ผลการดำเนินงาน / หลักฐาน

• พบ Exception 8 ราย ตรวจสอบซ้ำและแก้ไขก่อนประกาศผล 8 ราย

(5) ประเมินผลการควบคุม

• ประเมิน Design + Implementation + Effectiveness
• สรุปว่า “เพียงพอ/ควรปรับปรุง” พร้อมเหตุผลจากหลักฐาน

(6) ความเสี่ยงที่ยังมีอยู่

• กรณีเอกสารจากภายนอกหรือเงื่อนไขเทียบโอนยังมีความคลาดเคลื่อนได้

(7) การปรับปรุงการควบคุม

• กำหนดเกณฑ์ Exception กลาง + Digital Verification + Log การอนุมัติกรณีพิเศษ

หลักการ: คอลัมน์ (7) ต้องตอบตรงกับความเสี่ยงคงเหลือใน (6) และกำหนด Owner + กำหนดเสร็จในคอลัมน์ (8)

ตัวอย่าง 3 | การบริหารโครงการวิจัย

(1) วัตถุประสงค์: ใช้งบวิจัยถูกต้องตามสัญญาและเงื่อนไขแหล่งทุน

(2) ความเสี่ยง
• การเบิกจ่ายอาจไม่เป็นไปตามหมวด/ระยะเวลา/เงื่อนไข ทำให้ถูกเรียกคืนเงิน

(3) การควบคุมที่มีอยู่
• Checklist เงื่อนไขทุนก่อนเบิก
• Budget Control เทียบสัญญา
• ผู้รับผิดชอบตรวจเอกสารก่อนส่งการเงิน
• แจ้งเตือนวันสิ้นสุดโครงการ/งวดเงิน

(4) ผลการดำเนินงาน / หลักฐาน
• ตรวจ 30 โครงการ พบรายการเสี่ยง 4 รายการ และแก้ไขก่อนเบิกจ่าย

(5) ประเมินผลการควบคุม
• ประเมิน Design + Implementation + Effectiveness
• สรุปว่า “เพียงพอ/ควรปรับปรุง” พร้อมเหตุผลจากหลักฐาน

(6) ความเสี่ยงที่ยังมีอยู่
• การเปลี่ยนแปลงกิจกรรม/งบระหว่างโครงการอาจไม่ได้รับอนุมัติก่อนดำเนินการ

(7) การปรับปรุงการควบคุม
• Workflow ขออนุมัติเปลี่ยนแปลงก่อนใช้จ่าย + Dashboard แจ้งเตือนเงื่อนไขสำคัญ

หลักการ: คอลัมน์ (7) ต้องตอบตรงกับความเสี่ยงคงเหลือใน (6) และกำหนด Owner + กำหนดเสร็จในคอลัมน์ (8)

ตัวอย่าง 4 | ข้อมูลส่วนบุคคล/PDPA

(1) วัตถุประสงค์: ใช้และเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นและมีฐานกฎหมาย

(2) ความเสี่ยง
• อาจเก็บ/ส่งข้อมูลเกินความจำเป็นหรือส่งผิดผู้รับ ทำให้เกิดเหตุละเมิดข้อมูล

(3) การควบคุมที่มีอยู่
• กำหนดสิทธิ์เข้าถึงตามหน้าที่
• ตรวจผู้รับก่อนส่งข้อมูล
• ใช้ช่องทางที่กำหนดและเข้ารหัสเมื่อเหมาะสม
• ทบทวนสิทธิ์และบันทึกเหตุการณ์

(4) ผลการดำเนินงาน / หลักฐาน
• ทบทวนสิทธิ์ครบทุกบัญชี พบสิทธิ์เกินจำเป็น 6 บัญชีและยกเลิกแล้ว

(5) ประเมินผลการควบคุม
• ประเมิน Design + Implementation + Effectiveness
• สรุปว่า “เพียงพอ/ควรปรับปรุง” พร้อมเหตุผลจากหลักฐาน

(6) ความเสี่ยงที่ยังมีอยู่
• ยังเสี่ยงจาก Human Error และไฟล์ที่ส่งนอกระบบ

(7) การปรับปรุงการควบคุม
• DLP/Warning ก่อนส่ง + Quarterly Access Review + Incident Drill + Awareness เฉพาะกลุ่ม

หลักการ: คอลัมน์ (7) ต้องตอบตรงกับความเสี่ยงคงเหลือใน (6) และกำหนด Owner + กำหนดเสร็จในคอลัมน์ (8)

ตัวอย่าง 5 | การเงินและรายได้

(1) วัตถุประสงค์: บันทึกรายรับครบถ้วน ถูกต้อง และกระทบยอดได้

(2) ความเสี่ยง
• รายรับอาจบันทึกผิดบัญชี/ไม่ครบ ทำให้ข้อมูลการเงินคลาดเคลื่อน

(3) การควบคุมที่มีอยู่
• แบ่งแยกผู้รับเงิน–บันทึก–กระทบยอด
• กระทบยอดรายวัน/รายเดือน
• Exception Report รายการค้าง
• หัวหน้างานสอบทานและลงนาม

(4) ผลการดำเนินงาน / หลักฐาน
• กระทบยอด 100% พบรายการค้าง 5 รายการ ปิดได้ 4 รายการ เหลือ 1 รายการรอตรวจสอบ

(5) ประเมินผลการควบคุม
• ประเมิน Design + Implementation + Effectiveness
• สรุปว่า “เพียงพอ/ควรปรับปรุง” พร้อมเหตุผลจากหลักฐาน

(6) ความเสี่ยงที่ยังมีอยู่
• รายการเชื่อมต่อข้ามระบบอาจตกหล่นหรือจับคู่ไม่สำเร็จ

(7) การปรับปรุงการควบคุม
• Automated Reconciliation + Aging Dashboard + SLA ปิด Exception

หลักการ: คอลัมน์ (7) ต้องตอบตรงกับความเสี่ยงคงเหลือใน (6) และกำหนด Owner + กำหนดเสร็จในคอลัมน์ (8)

ตัวอย่าง 6 | ระบบสารสนเทศและบริการ

(1) วัตถุประสงค์: ระบบสำคัญพร้อมใช้งานและกู้คืนได้ภายในเวลาที่กำหนด

(2) ความเสี่ยง
• ระบบอาจหยุดชะงักจากความขัดข้อง/การเปลี่ยนแปลงระบบ ทำให้บริการหยุด

(3) การควบคุมที่มีอยู่
• Change Approval ก่อนขึ้นระบบจริง
• Backup ตามรอบและทดสอบ Restore
• Monitoring/Alert ระบบสำคัญ
• Incident Response + DR Procedure

(4) ผลการดำเนินงาน / หลักฐาน
• เกิด Incident 2 ครั้ง กู้คืนภายใน SLA ทั้ง 2 ครั้ง; Restore Test ผ่านตามแผน

(5) ประเมินผลการควบคุม
• ประเมิน Design + Implementation + Effectiveness
• สรุปว่า “เพียงพอ/ควรปรับปรุง” พร้อมเหตุผลจากหลักฐาน

(6) ความเสี่ยงที่ยังมีอยู่
• Single Point of Failure และการพึ่งพาผู้ให้บริการภายนอกบางระบบ

(7) การปรับปรุงการควบคุม
• Redundancy สำหรับระบบสำคัญ + Vendor SLA Review + DR Drill แบบ End-to-End

หลักการ: คอลัมน์ (7) ต้องตอบตรงกับความเสี่ยงคงเหลือใน (6) และกำหนด Owner + กำหนดเสร็จในคอลัมน์ (8)