LIB-SOP-B03-2570.md



Add new file
jeerapol kumkeam authored just now

LIB-SOP-B03-2570.md 27.54 KiB

เอกสารมาตรฐานการปฏิบัติงาน (SOP) ฉบับเต็ม

รหัสเอกสาร: LIB-SOP-B03-2570
ชื่อเอกสาร: การบริหารความเสี่ยงและความต่อเนื่องทางธุรกิจ (Risk Management & Business Continuity)
เวอร์ชัน: 1.0
วันที่บังคับใช้: 1 ตุลาคม 2569
วันที่ทบทวนถัดไป: 1 ตุลาคม 2570 (หรือเมื่อ发生重大事件/มีการเปลี่ยนแปลงบริบทองค์กรอย่างมีนัยสำคัญ)
Process Owner: คณะทำงานบริหารความเสี่ยงและความต่อเนื่องทางธุรกิจ (Risk & BCP Committee) โดยมีหัวหน้าฝ่ายแผนงานและประกันคุณภาพ (นางสาวอรนุช ใดงาม) เป็นเลขานุการคณะทำงาน และผู้อำนวยการสำนักฯ เป็นประธาน
เชื่อมโยงยุทธศาสตร์: Library 5.0 • ยุทธศาสตร์ที่ 1 (Efficient Management) • TQA หมวด 6.2 (Operational Effectiveness & Resilience) • Enterprise Priority 5 (Standardized & Resilient Operations) • SWOT (T1, T4, W1)

1. วัตถุประสงค์ (Outcome-Based Objective)

เพื่อสร้างวัฒนธรรมการบริหารความเสี่ยงเชิงรุก (Proactive Risk Management) และเตรียมความพร้อมในการรับมือกับภาวะวิกฤต (Resilience) ให้สำนักหอสมุดกลางสามารถ **"คาดการณ์ ป้องกัน ตอบสนอง และฟื้นฟู"** การดำเนินงานได้อย่างรวดเร็ว ปลอดภัย และต่อเนื่อง มุ่งเน้นผลลัพธ์ที่วัดได้ ได้แก่ **การไม่มีอุบัติการณ์รุนแรง (Zero Major Disruption), การลดเวลาในการฟื้นฟูระบบ (RTO) ลง ≥20%, และการครอบคลุมของแผน BCP ในกระบวนการสำคัญ 100%** สอดคล้องกับวิสัยทัศน์ Library 5.0 ที่ต้องมีความยืดหยุ่นและพร้อมรับการเปลี่ยนแปลง

2. ขอบเขต (Scope)

ครอบคลุมการบริหารความเสี่ยงและการวางแผนความต่อเนื่องทางธุรกิจ (BCP) ใน 5 มิติหลัก (COSO ERM Framework) ทั่วทั้งองค์กรและทุกวิทยาเขต:

1. **Strategic Risk:** ความเสี่ยงเชิงยุทธศาสตร์ (เช่น การเปลี่ยนแปลงเทคโนโลยี, งบประมาณ, นโยบายมหาวิทยาลัย)
2. **Operational Risk:** ความเสี่ยงด้านการปฏิบัติการ (เช่น ระบบล่ม, กระบวนการผิดพลาด, บุคลากรลาออก)
3. **Financial Risk:** ความเสี่ยงทางการเงิน (เช่น ฐานข้อมูลขึ้นราคา, อัตราแลกเปลี่ยน)
4. **Compliance & Legal Risk:** ความเสี่ยงด้านกฎหมายและกฎระเบียบ (เช่น PDPA, ลิขสิทธิ์, มาตรฐาน Green)
5. **Cybersecurity & Physical Safety:** ความปลอดภัยทางไซเบอร์และกายภาพ (เช่น Ransomware, ไฟไหม้, น้ำท่วม, อุบัติเหตุ)

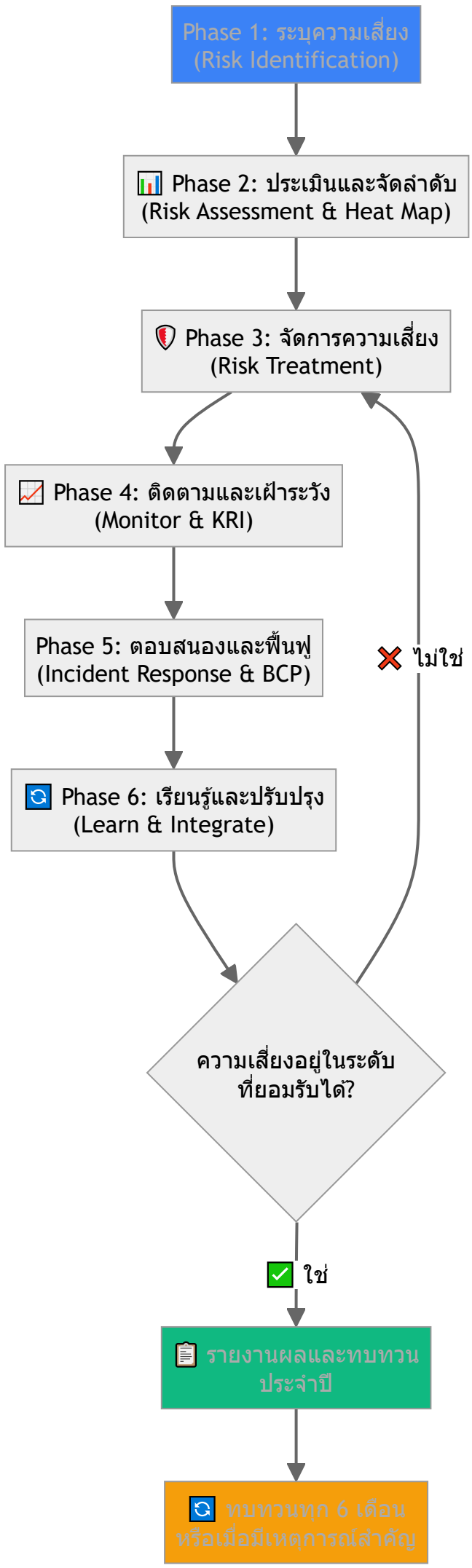
3. คำจำกัดความ (Definitions)

คำศัพท์	นิยาม
Risk Appetite	ระดับความเสี่ยงที่องค์กรยอมรับได้ในการมุ่งสู่เป้าหมาย
Risk Register	ทะเบียนความเสี่ยง ที่ระบุรายละเอียด การประเมิน และแผน mitigating
Likelihood (L)	โอกาสเกิดความเสี่ยง (1-5)
Impact (I)	ผลกระทบหากเกิดความเสี่ยง (1-5)
Risk Score	L × I (ใช้จัดระดับ ต่ำ/ปานกลาง/สูง/วิกฤต)
BCP (Business Continuity Plan)	แผนความต่อเนื่องทางธุรกิจ สำหรับกระบวนการสำคัญเมื่อเกิดเหตุวิกฤต
RTO (Recovery Time Objective)	เวลาเป้าหมายในการฟื้นฟูระบบ/กระบวนการให้กลับมาใช้งานได้
RPO (Recovery Point Objective)	จุดข้อมูลย้อนหลังสูงสุดที่ยอมรับได้หากข้อมูลสูญหาย
KRI (Key Risk Indicator)	ตัวชี้วัดความเสี่ยงล่วงหน้า (Early Warning Sign)
Incident / Near Miss	เหตุการณ์ที่เกิดขึ้นแล้ว / เหตุการณ์เกือบเกิด (ใช้เรียนรู้ได้)

4. บทบาทและหน้าที่ (Roles & Responsibilities)

บทบาท	หน้าที่ความรับผิดชอบ
ประธานคณะทำงาน (ผู้อำนวยการ)	อนุมัติ Risk Appetite, BCP, และตัดสินใจในภาวะวิกฤตระดับองค์กร
เลขานุการ (หน.ฝ่ายแผนงาน/QA)	ประสานงาน รวบรวม Risk Register จัดอบรม และติดตามความคืบหน้า
Risk Owner (Process Owner ของแต่ละ SOP)	ระบุ ประเมิน และ mitigating ความเสี่ยงในกระบวนการที่ตนเองรับผิดชอบ
Risk Champion (ตัวแทนแต่ละฝ่าย)	เป็นจุดติดต่อ เฝ้าระวัง KRI และรายงาน Near Miss/Incident ในฝ่ายตนเอง
บุคลากรทุกคน	ปฏิบัติตามมาตรการควบคุม แจ้งเหตุผิดปกติ และเข้าร่วมอบรม/ซ้อมแผน

5. ขั้นตอนการดำเนินงาน (Procedure)



Phase 1: ระบุความเสี่ยง (Risk Identification) - ทุกต้นปี/เมื่อมีเปลี่ยนแปลง

1. ทบทวนบริบทองค์กร (SWOT/TOWS, TQA OFI, VOC, Audit Findings)
2. ระบุความเสี่ยงใหม่ที่เกิดขึ้น (Emerging Risks) เช่น AI Hallucination, IoT Vulnerability, PDPA Breach
3. Risk Owner แต่ละกระบวนการบันทึกเข้า **Risk Register กลาง**

Phase 2: ประเมินและจัดลำดับ (Risk Assessment)

1. ประเมิน **Likelihood (L)** และ **Impact (I)** ระดับ 1-5
2. คำนวณ **Risk Score (L×I)** และจัดระดับ:
   - 🔴 **วิกฤต (15-25):** ต้องจัดการทันที รายงานผู้อำนวยการ
   - 🟠 **สูง (8-14):** ต้องมีแผนจัดการชัดเจน ติดตามรายเดือน
   - 🟡 **ปานกลาง (4-7):** จัดการตามปกติ ติดตามรายไตรมาส
   - 🟢 **ต่ำ (1-3):** ยอมรับและเฝ้าระวัง
3. สร้าง **Risk Heat Map** ขององค์กร

Phase 3: จัดการความเสี่ยง (Risk Treatment)

เลือกกลยุทธ์สำหรับความเสี่ยงระดับ "สูง" และ "วิกฤต":

- **Avoid (หลีกเลี่ยง):** หยุดกิจกรรมที่เสี่ยงเกินไป
- **Reduce/Mitigate (ลด/ควบคุม):** สร้างมาตรการควบคุม (Control) เช่น SOP-A03 (Cybersecurity), SOP-A04 (Safety)
- **Transfer (โอนย้าย):** ทำประกันภัย หรือ Outsource
- **Accept (ยอมรับ):** ยอมรับความเสี่ยงในระดับที่จัดการได้ พร้อมแผนเผชิญเหตุ

Phase 4: ติดตามและเฝ้าระวัง (Monitor & KRI)

1. กำหนด **KRI (Key Risk Indicator)** สำหรับความเสี่ยงสำคัญ (เช่น จำนวน Failed Login Attempts, จำนวนระบบที่ Patch ล่าช้า)
2. Risk Champion รายงานสถานะ KRI และ Near Miss ทุกเดือน
3. อัปเดต Risk Register ทุก 6 เดือน

Phase 5: ตอบสนองและฟื้นฟู (Incident Response & BCP)

1. สำหรับกระบวนการสำคัญ (Key Processes) ต้องมี **BCP** ที่ระบุ RTO/RPO
2. ซ้อมแผน BCP (Tabletop Exercise หรือ Full Drill) อย่างน้อยปีละ 1 ครั้ง (เช่น ซ้อมแผน Ransomware, ซ้อมแผนไฟไหม้)
3. เมื่อเกิด Incident จริง: เปิดใช้ Incident Response Plan → กู้คืนระบบ → สื่อสารกับผู้มีส่วนได้ส่วนเสีย

Phase 6: เรียนรู้และปรับปรุง (Learn & Integrate)

1. ทำ **Root Cause Analysis (RCA)** หลังเกิด Incident ทุกครั้ง
2. นำบทเรียนที่ได้ไปปรับปรุง SOP ที่เกี่ยวข้อง และบันทึกเข้า **ONE Improvement Portfolio (SOP-C02)**
3. แชร์ Lesson Learned ผ่าน Knowledge Sharing Day

6. ตัวชี้วัดกระบวนการ (Process KPIs) - LeTCI Framework

KPI Name	นิยาม (Definition)	สูตรคำนวณ (Formula)	ค่าเป้าหมาย (Target)	แหล่งข้อมูล (Data Source)	ความถี่
Critical Risk Mitigation Rate	ร้อยละของความเสี่ยงระดับวิกฤต/สูงที่มีแผนจัดการและดำเนินการตามแผน	(ความเสี่ยงที่มีแผนจัดการ / ความเสี่ยงวิกฤต+สูงทั้งหมด) × 100	**100%**	Risk Register	ราย 6 เดือน
BCP Coverage	ร้อยละของกระบวนการสำคัญที่มีแผน BCP ที่อัปเดตแล้ว	(กระบวนการที่มี BCP / กระบวนการสำคัญทั้งหมด) × 100	**100%**	BCP Register	รายปี
BCP Drill Completion	ร้อยละของการซ้อมแผน BCP ตามกำหนดการ	(ครั้งที่ซ้อมจริง / ครั้งที่วางแผน) × 100	**100%**	Drill Report	รายปี
Incident Response Time	เวลาเฉลี่ยในการตอบสนองต่อ Incident วิกฤตตั้งแต่รับแจ้งจนถึงเริ่มกู้คืน	ผลรวมเวลาตอบสนอง / จำนวน Incident	**≤ 30 นาที**	Incident Log	รายเดือน
Near Miss Reporting Rate	จำนวน Near Miss ที่ถูกรายงานและนำไปปรับปรุง (แสดงถึงวัฒนธรรมความปลอดภัย)	นับจำนวน Near Miss ที่ปิดบทเรียนได้	**เพิ่มขึ้น ≥10%/ปี**	Near Miss Log	รายปี
Risk Awareness Training	ร้อยละของบุคลากรที่ผ่านการอบรม Risk/Cybersecurity/BCP	(ผู้ผ่านอบรม / บุคลากรทั้งหมด) × 100	**100%**	Training Log	รายปี

7. ตัวอย่างทะเบียนความเสี่ยง (Risk Register Example)

ID	ความเสี่ยง (Risk)	L	I	Score	ระดับ	กลยุทธ์	มาตรการควบคุม (Control)	Risk Owner
R-01	**Ransomware / Data Breach** (T1)	3	5	15	🔴 วิกฤต	Reduce	SOP-A03 (Zero Trust, Backup 3-2-1, Pen Test), อบรม Phishing	IT (จีระพล)
R-02	**ระบบ Sierra/Smart Room ล่มช่วง Peak**	3	4	12	🟠 สูง	Reduce	SOP-A03 (Uptime ≥99.9%, HA System), Manual Backup Plan	IT (จีระพล)
R-03	**ฐานข้อมูลอิเล็กทรอนิกส์ขึ้นราคา >15%** (T3)	4	4	16	🔴 วิกฤต	Reduce/Accept	SOP-A02 (Usage+Cost+Need, Negotiate, Open Access)	วิเคราะห์ฯ (กนกพรรณ)
R-04	**AI Jinny X ให้ข้อมูลผิด (Hallucination)**	3	3	9	🟠 สูง	Reduce	SOP-A03 (RAG with verified sources, User feedback loop)	IT (ยุทธชัย)
R-05	**บุคลากรหลักลาออก/เกษียณ สูญเสีย Tacit Knowledge**	3	4	12	🟠 สูง	Reduce	SOP-B02 (KM, OPL, Succession Plan, Cross-training)	HR-KM (อรนุช)
R-06	**ผู้ใช้ลื่นล้ม/อุบัติเหตุในพื้นที่**	2	4	8	🟠 สูง	Reduce	SOP-A04 (Daily Inspection, Warning Signs, Thermography)	อาคาร (สรณ์พงษ์)

8. เอกสารและบันทึกที่เกี่ยวข้อง (Documents & Records)

รหัสเอกสาร	ชื่อเอกสาร	หน้าที่จัดเก็บ	ระยะเวลาจัดเก็บ
LIB-FM-RM-001	แบบฟอร์ม Risk Register และ Risk Heat Map	ฝ่ายแผนงาน/QA	5 ปี
LIB-FM-RM-002	แบบฟอร์ม BCP (Business Continuity Plan)	ฝ่ายแผนงาน/QA	5 ปี (หลังหมดอายุแผน)
LIB-FM-RM-003	แบบฟอร์ม Incident Report & RCA	ฝ่ายที่เกี่ยวข้อง	5 ปี
LIB-FM-RM-004	แบบฟอร์ม Near Miss Report	ฝ่ายที่เกี่ยวข้อง	3 ปี
LIB-FM-RM-005	แบบบันทึกการซ้อมแผน BCP (Drill Report)	ฝ่ายแผนงาน/QA	5 ปี
LIB-RPT-RM-001	รายงานการบริหารความเสี่ยงประจำปี	ฝ่ายแผนงาน/QA	5 ปี
LIB-POL-RM-001	นโยบายการบริหารความเสี่ยงและ BCP	ฝ่ายแผนงาน/QA	ตลอดอายุ

9. ประวัติการแก้ไข (Revision History)

เวอร์ชัน	วันที่	รายละเอียดการแก้ไข	ผู้จัดทำ	ผู้อนุมัติ
1.0	01/10/2569	จัดทำฉบับแรก เพื่อรองรับ Library 5.0, TQC 2570 และ Enterprise Priority 5	คณะทำงานยุทธศาสตร์	รศ.ดร.พยุง มีสัจ

💡 คำแนะนำสำหรับ Process Owner (คณะทำงานบริหารความเสี่ยง) ในการนำ SOP นี้ไปใช้จริง:

1. **เปลี่ยนจาก "เอกสารเพื่อตรวจประเมิน" เป็น "เครื่องมือตัดสินใจ":** Risk Register ไม่ควรเป็นไฟล์ Excel ที่เปิดเฉพาะตอนจะส่ง TQA แต่ควรเป็น **Dashboard ที่ผู้บริหารเปิดดูทุกเดือน** เพื่อตัดสินใจจัดสรรงบประมาณ (เช่น งบ Cybersecurity, งบสำรองฐานข้อมูล)
2. **เน้น Near Miss มากกว่า Incident:** วัฒนธรรมองค์กรที่แข็งแกร่งคือวัฒนธรรมที่ **"กล้ารายงานเกือบพลาด"** อย่าลงโทษคนที่รายงาน Near Miss แต่ให้รางวัล เพราะนั่นคือโอกาสในการป้องกัน Incident จริง
3. **BCP ต้อง "ทดสอบ" เท่านั้นถึงจะเชื่อถือได้:** แผน BCP ที่ไม่เคยซ้อม = ไม่มีแผน การทำ Tabletop Exercise (นั่งคุยจำลองสถานการณ์) ใช้เวลาแค่ 2 ชม. แต่ได้ผลดีกว่าแผนหนา 100 หน้า
4. **เชื่อมโยงกับ ONE Improvement Portfolio:** เมื่อความเสี่ยงเกิดขึ้นจริง หรือมาตรการควบคุมล้มเหลว ต้องส่งต่อเข้า SOP-C02 ทันที เพื่อปิดวงจร PDCA
5. **Risk Owner คือ Process Owner:** อย่าตั้งคนใหม่มาทำ Risk Management ให้ Process Owner ของ SOP-A01 ถึง A07 เป็น Risk Owner ของกระบวนการตัวเอง เพราะเขารู้ลึกที่สุด

การเชื่อมโยงกับเกณฑ์ TQA และห้องสมุดดีเด่น (Evidence Packaging)

TQA Band 3

- **หมวด 6.2 (การปฏิบัติการ):** SOP นี้คือหลักฐานหลักของ "Operational Resilience" แสดงถึง Risk Register, BCP, Incident Response และ KRI
- **หมวด 2 (กลยุทธ์):** การบริหาร Strategic Risk (เช่น การเปลี่ยนแปลงเทคโนโลยี T4, งบประมาณ T3)
- **หมวด 7.2 (ผลลัพธ์):** KPI เรื่อง Incident Response Time, BCP Drill Completion, Zero Major Disruption

ห้องสมุดดีเด่น 2569

- **ตัวชี้วัด 1.1 (การบริหารสมัยใหม่):** การบริหารความเสี่ยงเชิงรุก การใช้ KRI และ Dashboard
- **ตัวชี้วัด 3.1 (ระบบดิจิทัล):** มาตรการ Cybersecurity และ BCP ของระบบดิจิทัล

Library 5.0

- **Standardized & Resilient Operations:** SOP นี้ตอบโจทย์ Enterprise Priority 5 โดยตรง
- **Sustainable & Resilient:** การเตรียมพร้อมรับมือภาวะวิกฤตทั้งทางกายภาพและดิจิทัล

🔗 การเชื่อมโยงกับ SOP อื่น

SOP ที่เชื่อมโยง	ลักษณะการเชื่อมโยง
SOP-A03 (Digital System)	รับผิดชอบ Cybersecurity Risk, System Downtime Risk, BCP ของระบบดิจิทัล
SOP-A04 (Facilities)	รับผิดชอบ Physical Safety Risk, Environmental Risk, BCP ของอาคาร
SOP-B01 (One Data)	รับผิดชอบ Data Loss Risk, PDPA Compliance Risk
SOP-C02 (ONE Improvement Portfolio)	รับ OFI ที่เกิดจาก Incident หรือ Risk ที่จัดการไม่ได้ เพื่อปิดวงจรปรับปรุง
ทุก SOP-A (Core Processes)	Process Owner ของแต่ละ SOP คือ Risk Owner ที่ต้องระบุความเสี่ยงในกระบวนการตนเอง

ตัวอย่าง Dashboard สำหรับติดตาม SOP-B03

```
┌─────────────────────────────────────────────────────────┐
│  RISK MANAGEMENT & RESILIENCE DASHBOARD                 │
│  สำนักหอสมุดกลาง มจพ. | Library 5.0                     │
├─────────────────────────────────────────────────────────┤
│  🔴 Critical Risks Mitigated: 100% ✅ (Target 100%)     │
│  🟠 High Risks with Action Plan: 100% ✅ (Target 100%)  │
│  📋 BCP Coverage (Key Processes): 100% ✅ (Target 100%) │
│  🚨 BCP Drill Completion: 100% ✅ (Target 100%)         │
│  ⏱️ Incident Response Time: 22 นาที ✅ (Target ≤30 นาที) │
│  🔔 Near Miss Reported & Learned: 14 เรื่อง ✅ (Target ≥10) │
│  🛡️ Risk/Cybersecurity Training: 100% ✅ (Target 100%)  │
│  📉 Major Disruption Incidents: 0 ครั้ง ✅ (Target 0)   │
└─────────────────────────────────────────────────────────┘
```

> **เอกสารนี้จัดทำในรูปแบบ Markdown รองรับ GitLab Native Rendering**
> **เวอร์ชัน:** 1.0 (Risk Management & Business Continuity SOP) | **วันที่:** 28 กันยายน 2569
> **ผู้จัดทำ:** คณะทำงานยุทธศาสตร์ สำนักหอสมุดกลาง มจพ.
> **Process Owner:** คณะทำงานบริหารความเสี่ยง (เลขานุการ: น.ส.อรนุช ใดงาม)
> **ผู้อนุมัติ:** รศ.ดร.พยุง มีสัจ (ผู้อำนวยการ)
> **การทบทวนถัดไป:** 1 ตุลาคม 2570

🎯 ข้อความปิดท้าย

> *"การบริหารความเสี่ยงไม่ใช่การ 'กลัวปัญหา' แต่คือการ 'เตรียมพร้อมให้ดีที่สุด' เพื่อให้องค์กรสามารถก้าวไปข้างหน้าได้อย่างมั่นใจ แม้ในสภาวะที่ไม่แน่นอน นี่คือเกราะป้องกันที่ทำให้ Library 5.0 ยั่งยืนและพร้อมรับมือกับทุกความท้าทาย"*

✅ สรุปความคืบหน้าชุด SOP

รหัส	ชื่อ SOP	สถานะ
LIB-SOP-A01-2570 ถึง A07-2570	กระบวนการหลัก (7 ฉบับ)	✅ เสร็จสมบูรณ์
LIB-SOP-B01-2570	One Data One Truth	✅ เสร็จสมบูรณ์
LIB-SOP-B02-2570	พัฒนาบุคลากรและ KM	✅ เสร็จสมบูรณ์
LIB-SOP-B03-2570	**บริหารความเสี่ยง**	✅ **เสร็จสมบูรณ์ (ฉบับนี้)**
LIB-SOP-B04-2570	บริหารงบประมาณและจัดซื้อสีเขียว	⏳ รอ
LIB-SOP-B05-2570	สื่อสารองค์กรและการตลาด	⏳ รอ
LIB-SOP-C01-2570	วัดผลและรายงานผล	⏳ รอ
LIB-SOP-C02-2570	ONE Improvement Portfolio	⏳ รอ
LIB-SOP-C03-2570	ทบทวนโดยผู้บริหาร	⏳ รอ

หากท่านต้องการให้ผมจัดทำ **SOP ฉบับถัดไป (B04-B05 หรือ C01-C03)** หรือ **แบบฟอร์ม Risk Register / BCP Template** แจ้งได้เลยครับ! 📊