ตัวอย่าง Activity 2: Risk Assessment & Mitigation Planning

รายละเอียดกิจกรรม

ชื่อ: Risk Assessment & Mitigation Workshop

ระยะเวลา: 20 นาที

เป้าหมาย: ระบุความเสี่ยง ให้คะแนน และวางแผนบรรเทา

จำนวนคน: 4-6 คนต่อกลุ่ม

Output: Risk Register + Mitigation Plan

ส่วนที่ 1: ระดมความคิดความเสี่ยง

Brainstorming Process

กระบวนการ

1. ทีมนั่งเป็นวงกลม
2. นึกความเสี่ยงที่อาจเกิด (อะไรอาจผิดได้?)
3. เขียนลงบนกระดาษ Sticky Notes (1 ความเสี่ยง = 1 Note)
4. วาง Note ไว้บนกระดาน
5. ไม่ต้องมี Filter ในตอน Brainstorming
6. Quantity > Quality (ปริมาณ > คุณภาพ)

Time Box: 7 นาที

- First 3 min: Silent Individual Thinking
- Next 4 min: Group Discussion & Consolidation

ตัวอย่างความเสี่ยง (สำหรับ ShopEase)

BRAINSTORMED RISKS (ตัวอย่าง 12 ความเสี่ยง)

1. Payment Gateway Integration ขัดข้อง
2. Database Corruption / Data Loss
3. Server ล่มเหลว (ในวันเปิดตัว)
4. ความเสี่ยงด้าน Security (SQL Injection, XSS)
5. Scope Creep (ขยายขอบเขต)
6. Niwat (Key Developer) ลาออก
7. Requirement ไม่ชัดเจน / เปลี่ยนแปลง
8. API Third-party ขัดข้อง (Payment/SMS/Email)
9. Performance ล้ม (ช้า/Timeout)
10. Testing ตกหล่น (Quality Problem)
11. Cloud Provider Outage (AWS Down)
12. Customer Adoption Low (ไม่มีใครใช้)

Tip:

- ประกอบด้วย Technical + Business + Team Risks
- ไม่ต้องรอให้ Reality Complete
- ลองคิด "กรณีร้ายแรง" (Worst Case)

ตัวอย่างความเสี่ยง (สำหรับ MediBook)

BRAINSTORMED RISKS (ตัวอย่าง 14 ความเสี่ยง)

1. HIS/Hospital System Integration ขัดข้อง
2. PDPA Data Privacy Compliance Issue
3. Patient Data Breach / Hacking
4. AI Recommendation Model ผิด / ไม่ถูกต้อง
5. Doctor Adoption Resistance (ไม่อยากใช้)
6. Patient Adoption Low (ไม่มีใครบุ๊ก)
7. Load Test Failure (System ขัด at 500 users)
8. Hospital IT Support ไม่เข้าใจ
9. ข้อมูลผู้ป่วยไม่ครบถ้วน
10. Scheduling Algorithm Bug (Double-booking)
11. Payment Gateway ขัดข้อง
12. Somsak (Lead Dev) ลาออก
13. Regulatory Approval Delayed
14. Machine Learning Data Quality (ต้องมี 100k records)

Tip:

- Domain-specific Risks (Medical, Privacy, Compliance)
- Integration Risks (HIS Connection)
- Adoption Risks (Doctor + Patient)
- Regulatory Risks (Thai Healthcare Law)

ส่วนที่ 2: ให้คะแนนความเสี่ยง (7 นาที)

Scoring Matrix

Risk Scoring Method:

Score = Probability × Impact

Probability (ความเป็นไปได้)

1 = Very Low (< 10%) - หากเกิด 1 ใน 100 ครั้ง

2 = Low (10-30%) - อาจเกิด แต่ไม่น่า

3 = Medium (30-50%) - อาจเกิดได้เป็นโอกาส

4 = High (50-70%) - น่าจะเกิดแน่นอน

5 = Very High (> 70%) - แทบจะแน่นอน

Impact (ผลกระทบ)

1 = Negligible (ไม่มีผลกระทบต่อ Project)

2 = Minor (ผลกระทบเล็กน้อย ขยายเวลา < 1 วัน)

3 = Moderate (ผลกระทบปานกลาง ขยายเวลา 1-3 วัน)

4 = Major (ผลกระทบใหญ่ ขยายเวลา 1-2 สัปดาห์)

5 = Critical (ผลกระทบร้ายแรง ขยายเวลา > 2 สัปดาห์)

Risk Color Coding:

🔴 RED (20-25): Critical - ต้องจัดการทันที

🟠 ORANGE (12-19): High - ต้องเตรียมการบรรเทา

🟡 YELLOW (6-11): Medium - ติดตาม

🟢 GREEN (1-5): Low - บันทึกไว้เท่านั้น

ตัวอย่างการให้คะแนน (ShopEase)

📋 RISK SCORING EXAMPLE

Risk #1: Payment Gateway Integration ขัดข้อง

```
├─ Probability: 4 (High 50-70%)
│  (Payment APIs มีหลาย version + supplier support ช้า)
│
├─ Impact: 5 (Critical)
│  (ไม่สามารถเก็บเงินได้ = Revenue 0 = Project Fail)
│
├─ Score: 4 × 5 = 20 🔴 RED
│
└─ Reason: "Payment is core feature - if fails, no revenue"
```

Risk #2: Scope Creep

```
├─ Probability: 5 (Very High 70%+)
│  (Investors always want more features)
│
├─ Impact: 4 (Major)
│  (Timeline +2-4 weeks = miss deadline)
│
├─ Score: 5 × 4 = 20 🔴 RED
│
└─ Reason: "Historical: 80% of projects have scope creep"
```

Risk #3: Niwat (Key Lead Dev) ลาออก

```
├─ Probability: 2 (Low 10-30%)
│  (เงินเดือนดี ทำงานสนุก)
│
├─ Impact: 5 (Critical)
│  (ไม่มี Lead Developer = everything stops)
│
├─ Score: 2 × 5 = 10 🟡 YELLOW
│
└─ Reason: "Unlikely but catastrophic if happens"
```

Risk #4: API Third-party Outage

```
├─ Probability: 2 (Low 10-30%)
│  (AWS/Stripe are reliable)
│
├─ Impact: 3 (Moderate)
│  (Users can't pay temporarily but service recovers)
│
├─ Score: 2 × 3 = 6 🟡 YELLOW
│
└─ Reason: "Low probability but has happened before"
```

Risk #5: Performance Issues (Slow/Timeout)

```
├─ Probability: 3 (Medium 30-50%)
│  (E-commerce sites often face scaling issues)
│
├─ Impact: 3 (Moderate)
│  (Users frustrated but service works)
│
├─ Score: 3 × 3 = 9 🟡 YELLOW
│
└─ Reason: "Common issue but manageable"
```

Risk #6: Security Breach / Data Leak

```
├─ Probability: 2 (Low 10-30%)
│  (Good security practices + audits)
│
├─ Impact: 5 (Critical)
│  (Legal fine + reputation damage + trust loss)
│
├─ Score: 2 × 5 = 10 🟡 YELLOW
│
└─ Reason: "Unlikely with proper security but catastrophic"
```

Risk #7: Customer Adoption Low

```
├─ Probability: 3 (Medium 30-50%)
│  (Market uncertainty + competition)
│
├─ Impact: 4 (Major)
│  (Revenue < forecast + extend runway)
│
├─ Score: 3 × 4 = 12 🟠 ORANGE
│
└─ Reason: "Common startup risk"
```

Risk #8: Database Corruption / Data Loss

```
├─ Probability: 1 (Very Low < 10%)
│  (Modern databases have backup)
│
├─ Impact: 5 (Critical)
│  (All data gone = restart from scratch)
│
├─ Score: 1 × 5 = 5 🟢 GREEN
│
└─ Reason: "Unlikely with modern infrastructure"
```

SORTED BY SCORE (Highest First)

1. Payment Gateway	20	🔴 RED
2. Scope Creep	20	🔴 RED
3. Customer Adoption Low	12	🟠 ORANGE
4. Security Breach	10	🟡 YELLOW
5. Key Dev Turnover	10	🟡 YELLOW
6. Performance Issues	9	🟡 YELLOW
7. API Outage	6	🟡 YELLOW
8. Database Corruption	5	🟢 GREEN

(+ 4 more minor risks)

ACTION: Focus on Top 5 for mitigation planning

ตัวอย่างการให้คะแนน (**MediBook)**

RISK SCORING EXAMPLE

Risk #1: HIS Integration ขัดข้อง

```
├─ Probability: 3 (Medium 30-50%)
│  (Each hospital has different system)
│
├─ Impact: 5 (Critical)
│  (Cannot read schedule = pilot fails)
│
├─ Score: 3 × 5 = 15 🔴 RED
│
└─ Reason: "Integration complexity + Hospital IT support variability"
```

Risk #2: PDPA/Healthcare Compliance Issue

```
├─ Probability: 2 (Low 10-30%)
│  (Proper planning + legal review)
│
├─ Impact: 5 (Critical)
│  (Fine 5M+ baht + deployment blocked + reputational damage)
│
├─ Score: 2 × 5 = 10 🔴 RED
│
└─ Reason: "Healthcare is heavily regulated"
```

Risk #3: Doctor Adoption Resistance

```
├─ Probability: 4 (High 50-70%)
│  (Doctors resistant to new tech)
│
├─ Impact: 4 (Major)
│  (System not used = project fails)
│
├─ Score: 4 × 4 = 16 🔴 RED
│
└─ Reason: "Change management is hard in healthcare"
```

Risk #4: AI Model Accuracy Poor

```
├─ Probability: 2 (Low 10-30%)
│  (Good ML team + sufficient training data)
│
├─ Impact: 3 (Moderate)
│  (Feature not trusted but system works)
│
├─ Score: 2 × 3 = 6 🟡 YELLOW
│
└─ Reason: "Manageable with good model validation"
```

```
Risk #5: Load Test Failure
├─ Probability: 2 (Low 10-30%)
│  (Good infrastructure + testing)
│
├─ Impact: 4 (Major)
│  (System crashes + pilot fails)
│
├─ Score: 2 × 4 = 8 🟡 YELLOW
│
└─ Reason: "Preventable with early testing"
```

Risk #6: Patient Data Breach

```
├─ Probability: 1 (Very Low < 10%)
│  (Security audit + encryption)
│
├─ Impact: 5 (Critical)
│  (Legal consequences + trust loss)
│
├─ Score: 1 × 5 = 5 🟢 GREEN
│
└─ Reason: "Unlikely with proper security"
```

Risk #7: Lead Dev Turnover

```
├─ Probability: 1 (Very Low < 10%)
│  (Good compensation + career growth)
│
├─ Impact: 5 (Critical)
│  (Architecture knowledge loss)
│
├─ Score: 1 × 5 = 5 🟢 GREEN
│
└─ Reason: "Unlikely but catastrophic"
```

SORTED BY SCORE (Highest First):

1. Doctor Adoption Resistance	16	🔴 RED
2. HIS Integration Failure	15	🔴 RED
3. PDPA Compliance Issue	10	🔴 RED
4. Load Test Failure	8	🟡 YELLOW
5. AI Model Accuracy Poor	6	🟡 YELLOW
6. Data Breach	5	🟢 GREEN
7. Key Dev Turnover	5	🟢 GREEN

(+ 7 more risks)

ACTION: Focus on Top 5 for mitigation planning

ส่วนที่ 3: วางแผนบรรเทา (**6** นาที)

Mitigation Strategy Format

📋 FOR EACH TOP 5 RISK

1. Risk Description
   └ What could go wrong?

2. Probability Assessment
   └ 1-5 rating + reason

3. Impact Assessment
   └ 1-5 rating + reason

4. Mitigation Strategy (วิธีป้องกัน)
   └ Preventive Actions (ทำตอนนี้)
   └ Detective Actions (ตรวจจับเร็ว)
   └ Corrective Actions (แก้เมื่อเกิด)

5. Responsibility
   └ Who owns this?

6. Timeline
   └ When to start mitigation?

7. Status Tracking
   └ How to monitor?

ตัวอย่างแผนบรรเทา (ShopEase)

🛡️ RISK MITIGATION PLAN:

═══

1. RISK: Payment Gateway Integration ขัดข้อง

Severity: 🔴 RED (Score: 20)
Details
- Probability: 4/5 (High) - APIs have version changes
- Impact: 5/5 (Critical) - No revenue if payment fails
- Worst Case: System live but can't take payments

MITIGATION STRATEGY

PREVENTIVE ACTIONS (ทำตั้งแต่ตอนนี้)

1. Early Integration Testing
   - Start payment integration in Week 4
   - Not wait until Week 7
   - Document API changes
2. Mock Payment Gateway
   - Build mock API server
   - Test all scenarios (success/fail/timeout)
   - No need for real Stripe credentials
3. Multiple Payment Providers
   - Primary: Stripe (International)
   - Backup: Omise (Thailand)
   - Fallback: Manual Bank Transfer
   - Never depend on single provider
4. API Version Strategy
   - Use stable API versions (not beta)
   - Monitor for deprecations
   - Test 6 months before upgrade

DETECTIVE ACTIONS (ตรวจจับปัญหาเร็ว)

1. Automated Testing
   - Daily payment test (small amount)
   - Alert if payment fails
2. Integration Tests
   - End-to-end test (full checkout)
   - Run before every deploy
3. Staging Verification
   - Test in staging before production
   - Use real API but test account

CORRECTIVE ACTIONS (แก้เมื่อเกิด)

1. Failover to Backup Provider
   - Automatic switch in 5 seconds
   - No downtime
2. Manual Payment Process
   - Customer provides bank details
   - Human operator processes

3. Communication Plan
   - Alert customer within 1 minute
   - Update status every 15 minutes
   - Target resolution: 2 hours

Owner: Siam (Lead Developer)

Timeline
- Week 2: Research multiple providers
- Week 3: Implement mock API
- Week 4: Integrate primary provider
- Week 5: Add backup provider
- Week 6: Load testing

Success Criteria
- ✓ Payment works 99.9% uptime
- ✓ Failover works in < 5 seconds
- ✓ Manual fallback tested
- ✓ No revenue loss > 5 minutes

---

2. RISK: Scope Creep (ขยายขอบเขต)

Severity: 🔴 RED (Score: 20)
Details:
- Probability: 5/5 (Very High) - Investors always want more
- Impact: 4/5 (Major) - Extends timeline 2-4 weeks
- Pattern: 80% of projects have scope creep

MITIGATION STRATEGY
PREVENTIVE ACTIONS
1. Fixed Scope Agreement
   - Signed by Investor + Team
   - Clear MVP vs. Phase 2
   - Cannot change without formal approval
2. Prioritization Matrix (MoSCoW)
   - MUST Have: Login, Browse, Cart, Checkout (16 stories)
   - SHOULD Have: Reviews, Recommendations (8 stories)
   - COULD Have: Admin Dashboard, Analytics (5 stories)
   - WON'T Have in Phase 1: Loyalty, Gamification (defer)
3. Change Control Process
   - Any new requirement → formal request
   - Assess: Effort + Timeline Impact
   - Get sign-off from Investor + Team
   - Add to Phase 2 backlog (not Phase 1)
4. Feature Freeze Dates
   - Week 2: No new features added
   - Week 5: No more changes to MVP
   - Only bug fixes after Week 5

DETECTIVE ACTIONS

1. Weekly Scope Review
   - Track added/removed features
   - Flag any scope changes
   - Report to Investor
2. Backlog Monitoring
   - Count total stories
   - Monitor for additions
   - Alert if > 10% increase

CORRECTIVE ACTION

1. Negotiate Trade-offs
   - "If we add this feature, we must remove that one"
   - Show impact on timeline
   - Let stakeholder decide
2. Phase 2 Backlog
   - Collect all "nice-to-have" features
   - Plan for Phase 2 (Month 2)
   - Show roadmap to Investor

Owner: Somchai (Scrum Master)

Timeline:

- Week 1: Finalize MVP scope
- Week 1: Sign scope agreement
- Weekly: Scope review meeting

Success Criteria:

✓ No scope creep > 10%
✓ All changes go through formal process
✓ Phase 1 delivers on time
✓ Phase 2 planned by Week 5

---

3. RISK: Customer Adoption Low

Severity: 🟠 ORANGE (Score: 12)

Details:

- Probability: 3/5 (Medium) - Market uncertainty
- Impact: 4/5 (Major) - Revenue shortfall
- Historical: 60% of new platforms under-perform

MITIGATION STRATEGY

PREVENTIVE ACTIONS

1. Market Research (Week 1)
   - Survey 50 target sellers
   - Understand pain points
   - Validate product-market fit
2. Beta Testing Program
   - Week 13: Launch with 100 early adopters

- Get feedback early
- Iterate based on feedback

3. Go-to-Market Strategy
   - Partner with fashion influencers
   - Offer first month free
   - Seller incentive: 0% commission
4. Onboarding Program
   - Video tutorials (5 min)
   - Live training sessions
   - 1-on-1 support for first week

DETECTIVE ACTIONS

1. KPI Monitoring
   - Track: # of signups, active sellers, GMV
   - Week 1 target: 50 sellers
   - Week 4 target: 200 sellers
2. Feedback Collection
   - Weekly surveys
   - NPS score tracking
   - Support ticket analysis

CORRECTIVE ACTIONS

1. If adoption < 30 sellers by Week 2
   - Pivot to B2B approach
   - Contact department stores directly
2. If adoption is low
   - Reduce commission fee
   - Add new seller segments
   - Increase marketing budget

Owner: Niwat (Product Owner)

Timeline:
- Week 1: Market research
- Week 13: Beta launch
- Week 14: Monitor daily
- Week 15: Analyze & adjust

Success Criteria:
✓ 500 sellers by end of Month 1
✓ 10,000 products listed
✓ $10,000 GMV by Week 16

---

4. RISK: Key Team Member (Dev) Turnover
Severity: 🟡 YELLOW (Score: 10)
Details:
- Probability: 2/5 (Low) - Good compensation
- Impact: 5/5 (Critical) - Architecture knowledge lost
- Pattern: Tech teams lose 1-2 people/year

MITIGATION STRATEGY

PREVENTIVE ACTIONS

1. Competitive Compensation
   - Salary at market rate 75th percentile
   - Performance bonus (equity)
   - Professional development budget
2. Knowledge Transfer
   - Pair programming daily
   - Document architecture
   - Code review process
   - Wiki for design decisions
3. Team Culture
   - Regular 1-on-1s (2x/month)
   - Career path discussion
   - Feedback mechanism
4. Cross-Training
   - Have 2 developers for each critical system
   - Avoid single points of failure

DETECTIVE ACTIONS

1. Sentiment Monitoring
   - Watch for disengagement
   - Ask "How are you feeling?"
   - Early warning signs
2. Knowledge Audit
   - Who knows what?
   - Document critical paths
   - Identify knowledge gaps

CORRECTIVE ACTIONS

1. If Someone Resigns
   - 2-week knowledge transfer
   - Pair with incoming developer
   - Document lessons learned
2. If Knowledge Gap Exists
   - Hire contractor
   - Accelerate training of backup dev

Owner: Niwat (PO) + Somchai (PM)

Timeline

- Week 1: Finalize team structure
- Ongoing: Monthly 1-on-1s
- Week 8: Knowledge audit

Success Criteria

✓ Team retention 100% through Phase 1
✓ Critical knowledge documented
✓ No single points of failure
✓ Smooth knowledge transfer process

---

5. RISK: Security Breach / Data Leak
Severity: 🟡 YELLOW (Score: 10)
Details:
- Probability: 2/5 (Low) - Good security practices
- Impact: 5/5 (Critical) - Legal fine + reputation
- Pattern: E-commerce targets for hackers

MITIGATION STRATEGY

PREVENTIVE ACTIONS

1. Security by Design
   - Encrypt passwords (bcrypt)
   - HTTPS everywhere
   - Input validation
   - SQL injection prevention
2. Code Review
   - All code reviewed by 2 people
   - Focus on security issues
   - Use security checklist
3. Third-party Security Audit
   - Week 4: Initial audit
   - Fix critical issues
   - Week 8: Final audit before launch
   - Cost: ~100,000 baht
4. Compliance
   - OWASP Top 10 compliance
   - Penetration testing
   - Regular vulnerability scan

DETECTIVE ACTIONS

1. Monitoring
   - Intrusion detection system
   - Log anomalies
   - Alert on suspicious activity
2. Regular Testing
   - Monthly penetration tests
   - Quarterly security audit
   - Continuous vulnerability scanning

CORRECTIVE ACTIONS

1. If Breach Detected
   - Immediate containment
   - Investigate root cause
   - Notify customers within 24 hours
   - Report to regulators
2. Post-Incident
   - Patch vulnerability
   - Review security practices
   - Update documentation

Owner: Siam (Lead Dev) + Security Firm

Timeline

- Week 2: Security design review
- Week 4: Initial audit
- Week 8: Final audit
- Ongoing: Monthly monitoring

Success Criteria

✓ OWASP compliance 100%
✓ Audit pass with 0 critical issues
✓ No breaches during 12-month period
✓ Customer trust score > 4.5/5

ตัวอย่างแผนบรรเทา (MediBook)

RISK MITIGATION PLAN

---

1. RISK: HIS Integration ขัดข้อง

Severity: 🔴 RED (Score: 15)

MITIGATION STRATEGY

PREVENTIVE ACTIONS

1. Early Integration Planning (Week 2)
   - Meet Hospital IT team
   - Understand their system (HL7, API, Direct)
   - Get access to dev/staging environment
2. Integration Test Harness
   - Build mock HIS API
   - Test appointment booking
   - Simulate edge cases
3. Multiple Integration Approaches
   - Primary: REST API (if available)
   - Secondary: HL7 protocol
   - Fallback: Manual import/export
4. API Documentation
   - Request detailed API docs
   - Document expected responses
   - Create integration guide

CORRECTIVE ACTIONS

1. If Integration Fails
   - Fallback to manual process
   - Data import via CSV/Excel
   - Staff enters appointments manually
2. Extended Timeline
   - Build workaround
   - Plan IT team training
   - Delay pilot by 1-2 weeks

Owner: Somsak (Lead Dev)

Success Criteria

✓ HIS integration tested by Week 9
✓ Fallback process documented
✓ Hospital IT trained
✓ Zero downtime during pilot

---

2. RISK: PDPA/Healthcare Compliance Issue

Severity: 🔴 RED (Score: 10)

MITIGATION STRATEGY

PREVENTIVE ACTIONS

1. Legal Review (Week 2)
   - Healthcare lawyer consultation
   - Understand PDPA requirements
   - Privacy impact assessment
2. Privacy Design
   - Encrypt patient data at rest
   - Encrypt in transit (HTTPS + SSL)
   - Minimal data collection
   - Clear data retention policy
3. Compliance Framework
   - Data protection officer assigned
   - Privacy policy documented
   - Consent form for patients
   - Incident response plan
4. Professional Audit (Week 4)
   - Third-party PDPA audit
   - Penetration testing
   - Fix issues before pilot

DETECTIVE ACTIONS

1. Regular Audits
   - Quarterly PDPA audit
   - Annual security assessment

CORRECTIVE ACTIONS

1. If Compliance Gap Found
   - Immediate remediation
   - Update privacy practices
   - Notify affected parties

Owner: Dr. Kawin + Legal Team

Success Criteria:

✓ PDPA compliance 100%
✓ Audit pass before pilot
✓ No regulatory issues during year 1
✓ Patient trust score > 4.7/5

---

3. RISK: Doctor Adoption Resistance

Severity: 🔴 RED (Score: 16)

MITIGATION STRATEGY

PREVENTIVE ACTIONS

1. Co-Design Process (Week 1-3)
   - Interview 20 doctors
   - Understand workflow

- Design with doctors (not for)
- Iterate on prototypes

2. User Testing
   - Test with target doctors
   - Get feedback early
   - Iterate design
3. Change Management Plan
   - Hospital leadership endorsement
   - Doctor champion identification
   - Incentive structure (bonus for use)
   - Communication plan
4. Training Program
   - 3-hour hands-on training
   - Detailed user manual
   - Video tutorials
   - Live Q&A sessions
5. On-site Support
   - 2 support staff during pilot
   - Real-time help
   - Issue resolution same-day

DETECTIVE ACTIONS

1. Usage Monitoring
   - Track doctor login rate
   - Monitor appointment booking
   - NPS score tracking
2. Feedback Collection
   - Weekly check-ins
   - Suggestion box
   - Monthly focus groups

CORRECTIVE ACTIONS

1. If Adoption < 50% by Week 11
   - Additional training
   - 1-on-1 coaching
   - Incentive increase
2. If Specific Issues Found
   - Rapid fix
   - Deploy update same week
   - Get user feedback

Owner: Dr. Kawin (PO) + Anucha (PM)

Success Criteria

✓ Doctor usage rate > 70% by Week 12
✓ Booking accuracy > 95%
✓ Doctor satisfaction > 4.5/5
✓ Successful pilot transition to Phase 2

Risk Register Template

Output Format

📋 RISK REGISTER (Excel/Google Sheet)

ID	Risk Description	Prob	Impact	Score	Owner	Mitigation
R1	Payment Integration	4/5	5/5	20 🔴	Siam	Dual provider
R2	Scope Creep	5/5	4/5	20 🔴	Somchai	Change ctrl
R3	Adoption Low	3/5	4/5	12 🟠	Niwat	Go-to-market
R4	Team Turnover	2/5	5/5	10 🟡	Niwat	Knowledge xfer
R5	Security Breach	2/5	5/5	10 🟡	Siam	Security audit
...	...	...	...	...	...	...

Additional Columns

- Detection Method (How to identify if risk occurs?)
- Contingency (What if mitigation fails?)
- Status (Open / Monitoring / Mitigated / Closed)
- Review Date (When to re-assess?)

🎓 Learning Outcomes

นักศึกษาสามารถ:

☑ Identify Project Risks
- ✓ Technical risks
- ✓ Business risks
- ✓ Team/People risks
- ✓ External/Third-party risks

☑ Assess Risk Severity
- ✓ Probability (1-5 scale)
- ✓ Impact (1-5 scale)
- ✓ Risk Score calculation
- ✓ Prioritization (Top 5)

☑ Develop Mitigation Strategies
- ✓ Preventive actions
- ✓ Detective actions
- ✓ Corrective actions
- ✓ Contingency plans

☑ Create Risk Register
- ✓ Document risks
- ✓ Track ownership
- ✓ Monitor status
- ✓ Review regularly

☑ Communicate Risk Management
- ✓ Explain to stakeholders
- ✓ Escalate when needed
- ✓ Update team on changes
