W01 Work -- Quality Risk Cards

Submission context

- Project/team: ScamGuard
- Proposal/SRS source + version: INPUTS/requirements-srs/05_Software_Requirement_Specification.md v1.0 (August 23, 2026)
- Authors: Panuwat Takham
- Peer reviewer: Ekkphan Thotsatisangsan
- Review date/commit: 2026-08-25 / faf6911

> ทำ 3-5 cards โดยคัดลอกหัวข้อ Card เพิ่มตามจำนวนจริง

Card QR-01

Field	Team record
Requirement/feature/stakeholder source	FR-ANALYSIS-02: Visual Analysis (Image Forgery + AI-Gen Detection), NFR-05: Model Performance (Accuracy >= 85%) -- SRS v1.0, Section 2.3 and Section 3
Situation/context	ผู้ใช้งานทั่วไป (ST01) อัปโหลดรูปภาพที่สงสัยว่าถูกตัดต่อ (เช่น สลิปโอนเงินปลอม) เข้าสู่ระบบเพื่อรับผลประเมินความเสี่ยง โดยระบบต้องรัน ELA Preprocessing, PSCC-Net + SegFormer Model และ AI-Gen Detection Model ผ่าน ONNX Runtime
Quality risk statement	เมื่อโมเดล AI ตรวจจับการตัดต่อไม่ถึงเป้า Accuracy/F1/Precision/Recall >= 85% บน Testing Set (1,000 ภาพ, 50% real / 50% fake) อาจเกิด False Negative (ภาพปลอมแต่ระบบบอกว่าจริง) ทำให้ผู้ใช้หลงเชื่อสลิปปลอมและสูญเสียทรัพย์สิน หรือเกิด False Positive (ภาพจริงแต่ระบบบอกว่าปลอม) ทำให้เกิดความไม่เชื่อมั่นในระบบ
Quality concern	Functional suitability, Reliability
Impact and rationale	นี่คือฟังก์ชันหลักของระบบ (C-01 ใน PROJECT.md) หากผลลัพธ์ผิดพลาดบ่อย แอปพลิเคชันจะหมดความน่าเชื่อถือ ผู้ใช้จะไม่กลับมาใช้ซ้ำ และ OBJ-02 (ใช้ Deep Learning ตรวจการตัดต่อ) จะไม่บรรลุเป้าหมาย นอกจากนี้ visual_score มีน้ำหนัก 45% ในสูตร Risk Score และมี Special Rule ว่าถ้า visual_score >= 80 ให้ grade เป็น High ทันที ดังนั้นความผิดพลาดของโมเดลส่งผลกระทบทั้งต่อ grade และ risk score สุดท้าย
Verification question/action	1. โมเดล PSCC-Net + SegFormer ถูก train, evaluate บน dataset ที่สมดุล (50/50) หรือไม่ 2. มี Confusion Matrix, Classification Report (Accuracy, Precision, Recall, F1) ที่วัดได้จริงบน Testing Set 1,000 ภาพ หรือไม่ 3. ไฟล์ .onnx ที่ deploy ตรงกับ version ที่ผ่านการ evaluate หรือไม่
Validation question/action	1. เมื่อผู้ใช้จริงอัปโหลดสลิปปลอมที่พบบ่อยในไทย (เช่น สลิป K-Bank, SCB ที่แก้ไขจำนวนเงิน) ระบบให้ risk_grade = High จริงหรือไม่ 2. เมื่อผู้

Field	Team record
	ใช้อัปโหลดรูปภาพจริงที่ไม่ถูกแก้ไข ระบบให้ risk_grade = Low จริงหรือไม่
Planned evidence	1. Model evaluation report (Confusion Matrix, Classification Report) บน Testing Set 1,000 ภาพ 2. Test case results สำหรับ AC-1 ถึง AC-5 ของ FR-ANALYSIS-02 3. UAT scenario ทดสอบกับสลิปปลอมจริงและรูปจริง
Evidence status	Not Ready
Evidence path/owner/next action	Owner: Panuwat / Next action: ต้องรอจน model training เสร็จ และ testing set ถูกจัดเตรียม จึงจะสามารถรัน evaluation ได้

Card QR-02

Field	Team record
Requirement/feature/stakeholder source	FR-XAI-01: Grad-CAM Heatmap Generation & Display, NFR-06: Usability & Explainability -- SRS v1.0, Section 2.4 and Section 3
Situation/context	ผู้ใช้งานทั่วไป (ST01) ที่ไม่มีพื้นฐานเทคนิคดูผลการวิเคราะห์ภาพบนหน้าจอมือถือ ระบบแสดง Heatmap ซ้อนทับภาพต้นฉบับ (Overlay) โดยใช้ Color Map: แดง = เสี่ยงสูง, เหลือง = ปานกลาง, เขียว = ปลอดภัย พร้อม Toggle On/Off และ Opacity Slider (0-100%)
Quality risk statement	เมื่อ Grad-CAM Heatmap แสดงจุดสีแดงผิดตำแหน่ง (ไม่ตรงกับบริเวณที่ถูกตัดต่อจริง) หรือสี/ระดับความเข้มไม่ชัดเจนบนหน้าจอมือถือขนาดเล็ก อาจทำให้ผู้ใช้ตีความผิด (เช่น เข้าใจว่าบริเวณปลอดภัยคือจุดเสี่ยง) ส่งผลให้เป้าหมาย Heatmap Comprehension >= 80% และ Satisfaction >= 4.00/5.00 จากผู้ทดสอบ 100 คนไม่ผ่าน
Quality concern	Usability, Explainability (XAI)
Impact and rationale	C-02 และ C-08 ใน PROJECT.md ระบุว่า Heatmap คือตัวสร้างความโปร่งใสให้ระบบ หาก >= 80% ของผู้ทดสอบตอบคำถาม 4 ข้อ (Q1: สีแดงหมายถึงอะไร, Q2: สีแดง vs สีเขียว, Q3: Likert ความมั่นใจ, Q4: เข้าใจโดยไม่ต้องมีผู้เชี่ยวชาญ) ไม่ได้ตามเป้า จะถือว่า OBJ-04 (Heatmap Understanding) ล้มเหลว นอกจากนี้ อาจารย์ที่ปรึกษา (ST03) ต้องการเห็น testability และ explainability ที่วัดได้
Verification question/action	1. Grad-CAM implementation ใช้ layer ที่ถูกต้องจากโมเดล PSCC-Net + SegFormer หรือไม่ 2. Color Map (red/yellow/green) ถูก render ตามข้อกำหนดใน SRS หรือไม่ 3. Toggle Button, Opacity Slider (0-100%) ทำงานตามที่ระบุใน AC-2, AC-3, AC-4 หรือไม่
Validation question/action	1. ผู้ใช้ที่ไม่มีพื้นฐานเทคนิคตอบคำถาม Scenario-based 4 ข้อได้ถูก >= 80% หรือไม่ (NFR-06 AC-2) 2. Heatmap ช่วยให้ผู้ใช้ตัดสินใจเชื่อ/ไม่เชื่อภาพได้ดีขึ้นจริงหรือไม่ (วัดจาก Likert >= 4.00)

Field	Team record
Planned evidence	1. Grad-CAM output comparison: จับคู่ heatmap กับ ground-truth mask ของภาพตัดต่อ 2. UI test สำหรับ Toggle/Opacity Slider บน Android 3. UAT questionnaire results (100 ผู้ทดสอบ, 4 คำถาม)
Evidence status	Not Ready
Evidence path/owner/next action	Owner: Panuwat, Ekkphan / Next action: ต้องรอ Grad-CAM implementation เสร็จ, UI ถูกพัฒนา, และแบบสอบถาม UAT ถูกออกแบบ

Card QR-03

Field	Team record
Requirement/feature/stakeholder source	NFR-01: Performance -- Response Time, NFR-02: Scalability (100 concurrent users), FR-SCAN-03: Cache & Process -- SRS v1.0, Section 3
Situation/context	ผู้ใช้อัปโหลดภาพใหม่ (Cache Miss) ระบบต้องรัน Multi-layer Analysis Pipeline แบบขนาน: OCR/NLP (Surya-OCR), Visual Analysis (PSCC-Net + SegFormer via ONNX), Reverse Image Search (Google Vision API) แล้วรวม Weighted Risk Score ทั้งหมดต้องตอบกลับภายใน P50 <= 15s, P95 <= 25s สำหรับภาพใหม่ และ P95 <= 3s สำหรับ Cache Hit
Quality risk statement	เมื่อ pipeline วิเคราะห์ภาพใหม่ใช้เวลาเกิน 25 วินาที (P95) หรือ Google Vision API ตอบกลับช้า/ล่ม หรือ GPU inference ใช้เวลาเกิน 10 วินาที/ภาพ อาจทำให้ผู้ใช้เห็นหน้า Loading นานเกินไปจนปิดแอป ไม่กลับมาใช้ซ้ำ และเมื่อมีผู้ใช้พร้อมกัน 100 คน ระบบอาจล่มหรือมี Error Rate > 1%
Quality concern	Performance efficiency, Reliability
Impact and rationale	C-03, C-06, C-07 ใน PROJECT.md ครอบคลุมปัญหานี้ ระบบพึ่งพาบริการภายนอก (Google Vision API) ที่อาจล่มได้ และต้องใช้ GPU ซึ่งเป็นทรัพยากรจำกัด หากไม่มี pHash Cache ช่วย Server อาจ Overload นอกจากนี้ เป้าหมาย Uptime >= 99.5% (NFR-03) จะไม่ผ่านหากระบบล่มบ่อย
Verification question/action	1. Pipeline ถูกออกแบบให้รัน OCR, Visual, Source analysis แบบขนาน (parallel) จริงหรือไม่ 2. pHash Cache ใน Redis ถูก implement พร้อม TTL 30 วันตาม FR-SCAN-03 หรือไม่ 3. Fallback logic เมื่อ Google Vision API down (source_score = 50, source_status = "unavailable") ถูก implement ตาม FR-ANALYSIS-03 AC-4 หรือไม่
Validation question/action	1. Load test ด้วย 100 concurrent users ผ่านเป้า Cache Hit avg <= 5s, Cache Miss avg <= 20s, Error Rate < 1% หรือไม่ (NFR-02 AC-1) 2. ผู้ใช้จริงรู้สึกว่าเวลารอยอมรับได้หรือไม่

Field	Team record
Planned evidence	1. Load test report (JMeter/Locust) ทดสอบ 100 concurrent users 2. Response time measurements (P50, P95, P99) จาก API monitoring 3. GPU vs CPU inference time benchmark 4. Google Vision API fallback test results
Evidence status	Not Ready
Evidence path/owner/next action	Owner: Panuwat / Next action: ต้องรอจน Backend API, AI Inference Service, และ Redis Cache ถูกพัฒนาเสร็จจึงจะ run load test ได้

Card QR-04

Field	Team record
Requirement/feature/stakeholder source	FR-PDPA-01: Consent Management (2-level consent), NFR-04: Security -- SRS v1.0, Section 2.6 and Section 3
Situation/context	ผู้ใช้สมัครสมาชิกครั้งแรก ระบบต้องแสดง Consent Screen ที่แยก System Consent (บังคับ) กับ Research Consent (ไม่บังคับ) ออกจากกัน บันทึก consent_logs (user_id, consent_type, is_granted, created_at) และรองรับการถอน Research Consent ภายหลัง รวมถึง Right to Access (ดูข้อมูลส่วนตัว, consent logs)
Quality risk statement	เมื่อ Consent Screen ไม่แยก System Consent กับ Research Consent ออกจากกันอย่างชัดเจน หรือระบบไม่บันทึก consent_logs พร้อม timestamp หรือผู้ใช้ไม่สามารถถอน Research Consent ได้ อาจทำให้ระบบละเมิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ส่งผลให้สถาบันการศึกษาและทีมพัฒนาเผชิญความเสี่ยงทางกฎหมาย
Quality concern	Security, Compliance (PDPA)
Impact and rationale	C-04 ใน PROJECT.md ระบุว่านี่คือข้อกำหนดทางกฎหมายที่สำคัญมาก ต่างจาก quality concern อื่นที่กระทบแค่ usability หรือ performance ความล้มเหลวในจุดนี้มีผลทางกฎหมาย ข้อมูลที่ระบบจัดเก็บ (อีเมล, รหัสผ่าน hashed, รูปภาพที่อาจมีข้อมูลใบหน้าหรือข้อมูลทางการเงิน) อยู่ภายใต้ PDPA ทั้งหมด
Verification question/action	1. Consent Screen แสดง 2 ระดับ (System = บังคับ, Research = ไม่บังคับ) แยกกันชัดเจนหรือไม่ 2. API endpoint PUT /consent/research รองรับ is_granted: false (ถอนความยินยอม) ตาม FR-PDPA-01 AC-3 หรือไม่ 3. consent_logs table มี fields ครบ (user_id, consent_type, is_granted, created_at) ตาม SRS หรือไม่ 4. Data retention policy (ลบ scan/images หลัง 1 ปี, cron daily 02:00) ถูก implement หรือไม่
Validation question/action	1. ผู้ใช้จริงเข้าใจความแตกต่างระหว่าง System Consent กับ Research Consent หรือไม่ 2. เมื่อผู้ใช้ถอน Research Consent แล้ว ข้อมูลของผู้ใช้ถูกปฏิบัติตามที่สัญญาไว้จริงหรือไม่
Planned evidence	1. UI test: Consent Screen แสดง 2 checkbox แยกกัน พร้อมคำอธิบาย 2. API test: POST /register ด้วย system_consent=false ต้องถูก reject

Field	Team record
	3. API test: PUT /consent/research ด้วย is_granted=false ต้อง return 200 4. Database check: consent_logs มี record ครบตาม flow 5. Data retention cron job test
Evidence status	Not Ready
Evidence path/owner/next action	Owner: Panuwat, Ekkphan / Next action: ต้องรอจน Mobile App consent screen และ Backend API consent endpoints ถูกพัฒนาเสร็จ

Card QR-05

Field	Team record
Requirement/feature/stakeholder source	FR-ANALYSIS-01: Textual Analysis (OCR + NLP) -- SRS v1.0, Section 2.3
Situation/context	ระบบรับภาพที่อาจมีข้อความภาษาไทย (เช่น สลิปโอนเงิน, โฆษณาหลอกลวง) เข้าสู่ Surya-OCR เพื่อสกัดข้อความ จากนั้นใช้ RegEx + NLP ตรวจจับคำหลอกลวง (เช่น "กู้เงินด่วน", "โบนัสพิเศษ", "ถอนยอด") แล้วคำนวณ text_score (น้ำหนัก 25% ของ Risk Score สุดท้าย)
Quality risk statement	เมื่อ OCR สกัดข้อความภาษาไทยจากภาพได้ต่ำกว่าเป้า >= 80% accuracy (เนื่องจากฟอนต์บิดเบี้ยว, พื้นหลังรบกวน, ลายน้ำ, หรือข้อความเขียนด้วยมือในสลิป) ทำให้คำหลอกลวงถูกพลาดหรือสกัดผิด ส่งผลให้ text_score คลาดเคลื่อน และ Risk Score สุดท้ายต่ำกว่าที่ควร (เช่น สลิปปลอมที่มีคำว่า "โอนสำเร็จ" ถูกสกัดเป็นคำอื่น) ทำให้ผู้ใช้ได้รับผลประเมินที่ผิดพลาด
Quality concern	Functional suitability
Impact and rationale	C-05 ใน PROJECT.md ระบุว่าหาก OCR สกัดคำผิดพลาดจะทำให้การคำนวณคะแนนความเสี่ยงคลาดเคลื่อน OCR ภาษาไทยมีความยากเฉพาะ (ไม่มีช่องว่างระหว่างคำ, สระลอย, วรรณยุกต์, ฟอนต์หลากหลาย) text_score มีน้ำหนัก 25% ในสูตร Risk Score สุดท้าย หากเป็น 0 ผิดพลาด (ทั้งที่ภาพมีคำหลอกลวง) จะทำให้ risk_score ลดลง 25 คะแนนจากที่ควรจะได้
Verification question/action	1. Surya-OCR ถูก configure ให้รองรับภาษาไทยอย่างถูกต้องหรือไม่ 2. RegEx/NLP keyword list ครอบคลุมคำหลอกลวงที่พบบ่อยในบริบทไทยหรือไม่ 3. สูตร S_text = (keyword_count x severity_weight) / max_possible_score x 100 ถูก implement ตรงตาม SRS หรือไม่
Validation question/action	1. เมื่อป้อนสลิปโอนเงินจริงของธนาคารไทย (K-Bank, SCB, Bangkok Bank) ที่มีข้อความ ระบบสกัดข้อความได้ถูกต้อง >= 80% หรือไม่ (FR-ANALYSIS-01 AC-1) 2. เมื่อป้อนภาพโฆษณาหลอกลวงที่มีคำ "กู้เงินด่วน" ระบบตรวจจับและคำนวณ text_score ถูกต้องหรือไม่
Planned evidence	1. OCR accuracy test: เปรียบเทียบ OCR output กับ ground-truth text บนชุดภาพตัวอย่าง 2. Keyword detection test: ทดสอบ RegEx/NLP กับภาพที่มีคำหลอกลวงที่รู้จัก 3. text_score calculation test ตาม AC-4 ของ FR-ANALYSIS-01

Field	Team record
Evidence status	Not Ready
Evidence path/owner/next action	Owner: Panuwat / Next action: ต้องรอจน OCR engine (Surya-OCR) ถูก integrate กับ API และจัดเตรียมชุดภาพทดสอบภาษาไทย

Peer check and revision

Check	Result / comment	Revision made / open action
ทุก card trace ไปยัง source จริงได้	ผ่าน -- ทั้ง 5 cards อ้าง FR/NFR ID ที่ตรงกับ SRS v1.0 (FR-ANALYSIS-02, FR-XAI-01, NFR-01, NFR-02, FR-SCAN-03, FR-PDPA-01, NFR-04, FR-ANALYSIS-01, NFR-05, NFR-06) ตรวจสอบแล้วทุก ID มีอยู่จริงในเอกสาร	ไม่มี
risk statement มี event/condition และ impact	ผ่าน -- ทุก card ใช้โครงสร้าง "เมื่อ...[condition]...อาจเกิด...[event]...ทำให้...[impact]" ไม่มีคำกว้างอย่าง "คุณภาพต่ำ" หรือ "ระบบไม่ดี" โดยไม่มีรายละเอียด	ไม่มี
V&V action ตอบ risk ไม่ใช่คำกว้าง	ผ่าน -- Verification ระบุ artifact/process ที่ตรวจได้ (เช่น Confusion Matrix, Classification Report, consent_logs table fields) และ Validation ระบุสถานการณ์จริง (เช่น สลิป K-Bank/SCB, ผู้ทดสอบ 100 คน)	ไม่มี
evidence status เป็นความจริง	ผ่าน -- ทั้ง 5 cards ระบุ Not Ready ซึ่งตรงกับสถานะจริง (โครงงานอยู่ในขั้น Requirements/SRS ยังไม่มี implementation) ไม่มี card ใดอ้างผลทดสอบหรือ log ที่ยังไม่เกิดขึ้น	ไม่มี

Team conclusion

- Critical risk/feature ที่เลือกไป Week 02: QR-01 (AI Model Accuracy) / เป็นหัวใจหลักของระบบ visual_score มีน้ำหนักสูงสุด (45%) ในสูตร Risk Score และมี Special Rule ที่ override grade ได้ หากโมเดลล้มเหลว ระบบทั้งหมดจะไม่มีคุณค่า จึงเหมาะเป็น critical slice สำหรับวาง Project Quality Route Map ตั้งแต่ Requirements -> Design -> Implement -> Test -> Decision
- สิ่งที่ยังไม่รู้และ owner: 1. Model training dataset ยังไม่เสร็จสมบูรณ์ (Owner: Panuwat) 2. OCR engine (Surya-OCR) ยังไม่ได้ benchmark กับภาษาไทยในบริบทสลิปธนาคาร (Owner: Panuwat) 3. UAT questionnaire ยังไม่ได้ออกแบบรายละเอียด (Owner: Ekkphan)
- AI Use Declaration: WEEKS/week-01/work/ai-use-declaration.md