Cyber Resilience ของ FFIEC กับ สถาบันการเงิน US

ในโลกการเงินยุคดิจิทัลที่ขับเคลื่อนด้วยเทคโนโลยีอย่างไม่หยุดนิ่ง ภัยคุกคามทางไซเบอร์ได้กลายเป็นหนึ่งในความเสี่ยงสำคัญที่สถาบันการเงินไม่อาจมองข้ามอีกต่อไป ประเทศสหรัฐอเมริกาในฐานะหนึ่งในผู้นำด้านการกำกับดูแล ได้ให้ความสำคัญกับการสร้าง "ความยืดหยุ่นทางไซเบอร์" (Cyber Resilience) ผ่านการดำเนินการของ **FFIEC** (Federal Financial Institutions Examination Council) ซึ่งเป็นองค์กรที่ทำหน้าที่ประสานความร่วมมือระหว่างหน่วยงานกำกับดูแลหลายภาคส่วน บทบาทของ FFIEC จึงไม่ได้จำกัดแค่การออกแนวทางเท่านั้น แต่ยังรวมถึงการสร้างกรอบการทำงานร่วมกันที่เป็นระบบ เพื่อให้สถาบันการเงินทุกขนาดสามารถรับมือกับความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

FFIEC (Federal Financial Institutions Examination Council) จึงกลายเป็นกลไกสำคัญในการกำกับดูแลและควบคุม Cyber Resilience ของสถาบันการเงินในสหรัฐอเมริกา โดยไม่แยกการดำเนินงานเป็นส่วน ๆ อย่างอิสระ แต่เลือกใช้แนวทาง “การบูรณาการ” ซึ่งเน้นการทำงานร่วมกันระหว่างหน่วยงานสมาชิกภายใต้กรอบเดียวกัน นี่คือจุดเด่นที่ช่วยให้การกำกับดูแลมีเอกภาพ และสามารถปรับตัวตอบสนองต่อภัยคุกคามที่ซับซ้อนและเปลี่ยนแปลงตลอดเวลาได้อย่างทันการณ์

FFIEC คืออะไร?

FFIEC คือสภาที่ประกอบด้วยหน่วยงานกำกับดูแลสถาบันการเงินของรัฐบาลกลางสหรัฐฯ 5 แห่ง ได้แก่:

- Board of Governors of the Federal Reserve System (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Consumer Financial Protection Bureau (CFPB)
- State Liaison Committee (SLC) (เป็นตัวแทนของหน่วยงานกำกับดูแลของรัฐ)

บทบาทหลักของ FFIEC คือการกำหนดมาตรฐานและแนวปฏิบัติที่สอดคล้องกันสำหรับการตรวจสอบและกำกับดูแลสถาบันการเงิน เพื่อส่งเสริมความปลอดภัย ความมั่นคง และการคุ้มครองข้อมูลลูกค้า

วิธีกำกับและควบคุม Cyber Resilience ของ FFIEC

FFIEC ใช้แนวทางที่ครอบคลุมและเป็นองค์รวมในการส่งเสริม Cyber Resilience ซึ่งสามารถแบ่งออกเป็นองค์ประกอบหลักๆ ได้ดังนี้:

1. **การออกแนวทางและมาตรฐาน (Issuing Guidance and Standards):**
    - **FFIEC Cybersecurity Assessment Tool (CAT):** เป็นเครื่องมือหลักที่ FFIEC พัฒนาขึ้นเพื่อช่วยให้สถาบันการเงินสามารถประเมินความเสี่ยงด้านไซเบอร์และระดับความพร้อมด้านความปลอดภัยทางไซเบอร์ของตนเองได้ CAT ประกอบด้วย 2 ส่วนหลักคือ:
        - **Inherent Risk Profile (โปรไฟล์ความเสี่ยงโดยธรรมชาติ):** ช่วยให้สถาบันการเงินระบุระดับความเสี่ยงที่เกิดจากลักษณะทางธุรกิจ เทคโนโลยี และการเชื่อมต่อต่างๆ ก่อนที่จะมีการควบคุมใดๆ โดยประเมินจาก 5 หมวดหมู่:
            - Technologies and Connection Types (ประเภทเทคโนโลยีและการเชื่อมต่อ)
            - Delivery Channels (ช่องทางการส่งมอบบริการ)
            - Online/Mobile Products and Technology Services (ผลิตภัณฑ์และบริการเทคโนโลยีออนไลน์/มือถือ)
            - Organizational Characteristics (ลักษณะองค์กร)
            - External Threats (ภัยคุกคามภายนอก)
        - **Cybersecurity Maturity (ระดับความพร้อมด้านความปลอดภัยทางไซเบอร์):** ประเมินความสามารถของสถาบันในการจัดการความเสี่ยงด้านไซเบอร์ โดยมี 5 ระดับ (Baseline, Evolving, Intermediate, Advanced, Innovative) ครอบคลุมหลายโดเมน เช่น:
            - Cybersecurity Governance (ธรรมาภิบาลความปลอดภัยทางไซเบอร์)
            - Risk Management and Oversight (การบริหารความเสี่ยงและการกำกับดูแล)

        - Threat Intelligence and Collaboration (ข่าวกรองภัยคุกคามและการทำงานร่วมกัน)
        - Cybersecurity Controls (การควบคุมความปลอดภัยทางไซเบอร์)
        - External Dependency Management (การจัดการการพึ่งพาภายนอก)
        - Cyber Incident Management and Resilience (การจัดการเหตุการณ์ไซเบอร์และความยืดหยุ่น)
    - **FFIEC IT Examination Handbook:** เป็นชุดเอกสารคู่มือที่ให้คำแนะนำแก่ผู้ตรวจสอบเกี่ยวกับประเด็นต่างๆ ด้านเทคโนโลยีสารสนเทศ รวมถึงความปลอดภัยทางไซเบอร์ ซึ่งเป็นพื้นฐานสำหรับการตรวจสอบสถาบันการเงิน
    - **Advisories and Joint Statements:** FFIEC และหน่วยงานสมาชิกมักออกประกาศและแถลงการณ์ร่วมกันเพื่อแจ้งเตือนเกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นใหม่ และให้คำแนะนำในการจัดการความเสี่ยง
2. **การตรวจสอบและกำกับดูแล (Examination and Supervision):**
    - **การประเมินความเสี่ยงและระดับความพร้อม:** ผู้ตรวจสอบของหน่วยงานสมาชิก FFIEC จะใช้ CAT และแนวทางอื่นๆ ในการประเมินโปรไฟล์ความเสี่ยงโดยธรรมชาติและระดับความพร้อมด้านความปลอดภัยทางไซเบอร์ของสถาบันการเงิน
    - **การกำหนดแนวทางแก้ไข:** หากพบช่องโหว่หรือจุดอ่อน ผู้ตรวจสอบจะทำงานร่วมกับสถาบันการเงินเพื่อกำหนดแผนการแก้ไขและปรับปรุง
    - **การติดตามและประเมินผล:** หน่วยงานกำกับดูแลจะติดตามความคืบหน้าของสถาบันในการแก้ไขปัญหาที่ระบุ และอาจมีการตรวจสอบติดตามผลเพื่อให้แน่ใจว่าเป็นไปตามข้อแนะนำ
3. **การส่งเสริมการแลกเปลี่ยนข้อมูลและการทำงานร่วมกัน (Promoting Information Sharing and Collaboration):**
    - **FS-ISAC (Financial Services Information Sharing and Analysis Center):** FFIEC สนับสนุนให้สถาบันการเงินเข้าร่วมและใช้ประโยชน์จากแพลตฟอร์มการแบ่งปันข้อมูล

ภัยคุกคาม เช่น FS-ISAC เพื่อให้ได้รับข้อมูลข่าวสารล่าสุดเกี่ยวกับภัยคุกคามและแนวทางการป้องกัน

- **Public-Private Partnerships:** FFIEC และหน่วยงานสมาชิกทำงานร่วมกับภาคเอกชนเพื่อพัฒนาแนวทางและเครื่องมือในการรับมือกับภัยคุกคามไซเบอร์ที่ซับซ้อนขึ้น

4. **การเน้นย้ำถึงบทบาทของคณะกรรมการและผู้บริหาร (Emphasis on Board and Management Oversight):**
    - FFIEC เน้นย้ำถึงความสำคัญของการมีธรรมาภิบาลความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง โดยคณะกรรมการและผู้บริหารระดับสูงต้องมีส่วนร่วมอย่างแข็งขันในการกำกับดูแลความเสี่ยงด้านไซเบอร์ กำหนดกลยุทธ์ และจัดสรรทรัพยากรที่เพียงพอ
5. **การพัฒนาบุคลากรและความตระหนัก (Workforce Development and Awareness):**
    - ส่งเสริมให้สถาบันการเงินลงทุนในการพัฒนาทักษะและความรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากร และสร้างวัฒนธรรมองค์กรที่ตระหนักถึงความเสี่ยงด้านไซเบอร์

"อิสรภาพ" คำว่า "อิสรภาพ" ในบริบทของ FFIEC ไม่ได้หมายถึงการแยกขาดจากกันอย่างสมบูรณ์ แต่หมายถึง:

- **อิสระในการประเมินและตัดสินใจของสถาบันการเงิน:** FFIEC CAT เป็นเครื่องมือที่สถาบันการเงินสามารถนำไปใช้ในการประเมินตนเอง (self-assessment) เพื่อทำความเข้าใจสถานะความปลอดภัยทางไซเบอร์ของตนเอง สถาบันการเงินมีอิสระในการเลือกวิธีการและเครื่องมือที่เหมาะสมกับขนาดและความซับซ้อนขององค์กร เพื่อให้สามารถบรรลุเป้าหมายด้าน Cyber Resilience
- **ความยืดหยุ่นในการประยุกต์ใช้:** แม้ว่า FFIEC จะออกแนวทาง แต่สถาบันการเงินมีความยืดหยุ่นในการปรับใช้แนวทางเหล่านั้นให้เข้ากับลักษณะเฉพาะและความเสี่ยงของตนเอง โดยคำนึงถึงหลักการของ "สัดส่วนความเหมาะสม" (proportionality) คือ ยิ่งมีความเสี่ยงมากเท่าไหร่ การควบคุมก็ควรจะเข้มงวดมากขึ้นเท่านั้น
- **บทบาทอิสระของผู้ตรวจสอบภายใน/ภายนอก:** FFIEC เน้นย้ำถึงความสำคัญของการตรวจสอบและทดสอบที่เป็นอิสระ (independent testing) เช่น การเจาะระบบ (penetration testing) และการตรวจสอบช่องโหว่ (vulnerability scanning) รวมถึงการตรวจสอบโดยหน่วยงานภายในหรือ

ภายนอกที่เป็นอิสระ เพื่อให้มั่นใจว่าการควบคุมความปลอดภัยทางไซเบอร์มีประสิทธิภาพและเป็นไปตามนโยบายและมาตรฐานที่กำหนดไว้

โดยสรุปแล้ว FFIEC ไม่ได้ "แบ่ง" การควบคุม Cyber Resilience ออกเป็นส่วนที่แยกเป็นอิสระ แต่เป็นการสร้างกรอบการทำงานที่แข็งแกร่งและสอดคล้องกัน ซึ่งสนับสนุนให้สถาบันการเงินมี "อิสระ" ในการบริหารจัดการความเสี่ยงของตนเองภายใต้แนวทางที่ชัดเจนและมีการกำกับดูแลอย่างต่อเนื่องจากหน่วยงานสมาชิก

เพื่อให้เห็นภาพชัดเจนขึ้นว่า FFIEC Cybersecurity Assessment Tool (CAT) ถูกนำไปใช้ปฏิบัติอย่างไร ผมขอยกตัวอย่างสถานการณ์ของ **ธนาคารชุมชนขนาดเล็กแห่งหนึ่งในสหรัฐอเมริกา** ที่ชื่อว่า "เฟิร์สต์ คอมมูนิตี้ แบงก์" (First Community Bank) ให้ศึกษากันครับ

กรณีศึกษา: เฟิร์สต์ คอมมูนิตี้ แบงก์ กับ FFIEC CAT

ข้อมูลเบื้องต้นของธนาคาร:

- **ขนาด:** ธนาคารชุมชนขนาดเล็ก มีสาขาไม่มากนัก
- **บริการ:** เน้นบริการธนาคารพื้นฐาน เช่น บัญชีเงินฝาก, สินเชื่อขนาดเล็ก, ตู้ ATM, และมีบริการธนาคารออนไลน์ขั้นพื้นฐาน (เช่น การตรวจสอบยอดคงเหลือ, การโอนเงินภายใน)
- **เทคโนโลยี:** ใช้ระบบ Core Banking จากผู้ให้บริการภายนอก, มีเว็บไซต์ธนาคาร, และมีแอปพลิเคชันมือถือแบบพื้นฐาน
- **บุคลากร:** มีทีม IT ขนาดเล็ก ไม่มีผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์โดยเฉพาะ

ขั้นตอนการประยุกต์ใช้ FFIEC CAT

1. การประเมินโปรไฟล์ความเสี่ยงโดยธรรมชาติ (Inherent Risk Profile)

เฟิร์สต์ คอมมูนิตี้ แบงก์ จะเริ่มจากการประเมินว่าธุรกิจและเทคโนโลยีของพวกเขามีความเสี่ยงด้านไซเบอร์โดยธรรมชาติในระดับใด ก่อนที่จะพิจารณามาตรการควบคุมใดๆ

- **Technologies and Connection Types (ประเภทเทคโนโลยีและการเชื่อมต่อ):**
    - มีเครือข่ายภายในองค์กร, มีการเชื่อมต่ออินเทอร์เน็ตสำหรับลูกค้าและพนักงาน

- มีการใช้ Wi-Fi ในสำนักงาน
- มีการเชื่อมต่อกับผู้ให้บริการ Core Banking และผู้ให้บริการแอปพลิเคชันมือถือผ่าน VPN
- **ผลการประเมิน: Minimal Inherent Risk** (ความเสี่ยงน้อย) เนื่องจากไม่มีเทคโนโลยีซับซ้อนมากนัก และการเชื่อมต่อส่วนใหญ่ผ่านช่องทางที่มีการรักษาความปลอดภัยเบื้องต้น

- **Delivery Channels (ช่องทางการส่งมอบบริการ):**
  - ตู้ ATM (มีจำนวนน้อย)
  - เว็บไซต์ธนาคาร (มีฟังก์ชันจำกัด)
  - แอปพลิเคชันมือถือ (มีฟังก์ชันจำกัด)
  - **ผลการประเมิน: Minimal Inherent Risk** (ความเสี่ยงน้อย) เพราะช่องทางที่ให้บริการมีจำกัดและไม่ได้ซับซ้อนมาก

- **Online/Mobile Products and Technology Services (ผลิตภัณฑ์และบริการเทคโนโลยีออนไลน์/มือถือ):**
  - บริการดูยอดเงิน, โอนเงินระหว่างบัญชีตัวเอง, ชำระบิล (ขั้นพื้นฐาน)
  - ไม่มีบริการที่ซับซ้อน เช่น การโอนเงินระหว่างประเทศจำนวนมาก หรือการซื้อขายหุ้นออนไลน์
  - **ผลการประเมิน: Minimal Inherent Risk** (ความเสี่ยงน้อย) เพราะผลิตภัณฑ์และบริการออนไลน์ไม่หลากหลายและไม่เกี่ยวข้องกับการทำธุรกรรมมูลค่าสูงที่ซับซ้อน

- **Organizational Characteristics (ลักษณะองค์กร):**
  - จำนวนพนักงานน้อย, พนักงานไอทีมีจำกัด
  - ไม่มีผู้เชี่ยวชาญด้านความปลอดภัยโดยตรง
  - **ผลการประเมิน: Moderate Inherent Risk** (ความเสี่ยงปานกลาง) เนื่องจากทรัพยากรบุคคลและความเชี่ยวชาญด้านความปลอดภัยมีจำกัด ซึ่งอาจเป็นช่องโหว่ได้

- **External Threats (ภัยคุกคามภายนอก):**

- โดยทั่วไป ธนาคารทุกแห่งเผชิญกับภัยคุกคาม เช่น ฟิชชิ่ง, มัลแวร์, DDoS
- ยังไม่เคยตกเป็นเป้าหมายของการโจมตีขนาดใหญ่
- **ผลการประเมิน: Moderate Inherent Risk** (ความเสี่ยงปานกลาง) เพราะภัยคุกคามไซเบอร์มีอยู่จริงและพัฒนาอย่างต่อเนื่อง แม้ธนาคารจะขนาดเล็กก็ยังเป็นเป้าหมายได้

สรุปโปรไฟล์ความเสี่ยงโดยธรรมชาติ (Inherent Risk Profile): Minimal to Moderate Inherent Risk (โดยรวมอยู่ในระดับน้อยถึงปานกลาง)

2. การประเมินระดับความพร้อมด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Maturity)

หลังจากทราบโปรไฟล์ความเสี่ยงแล้ว เฟิร์สต์ คอมมูนิตี้ แบงก์ จะประเมินว่ามาตรการควบคุมที่มีอยู่มีความพร้อมในระดับใดในแต่ละโดเมน โดยมี 5 ระดับ (Baseline, Evolving, Intermediate, Advanced, Innovative)

- **Domain 1: Cyber Risk Management and Oversight (ธรรมาภิบาลและการกำกับดูแลความเสี่ยงไซเบอร์)**
  - **การปฏิบัติที่มีอยู่:** มีนโยบายความปลอดภัยข้อมูลเบื้องต้น, มีการทบทวนโดยผู้บริหารปีละครั้ง, มีการจัดสรรงบประมาณ IT แต่ไม่มีงบเฉพาะด้านไซเบอร์
  - **ระดับความพร้อม: Baseline** (ขั้นพื้นฐาน) - มีนโยบายและการกำกับดูแลขั้นต้น แต่ยังขาดการบูรณาการและความชัดเจน
- **Domain 2: Threat Intelligence and Collaboration (ข่าวกรองภัยคุกคามและการทำงานร่วมกัน)**
  - **การปฏิบัติที่มีอยู่:** พนักงาน IT ติดตามข่าวสารด้านความปลอดภัยจากแหล่งสาธารณะทั่วไป, ไม่ได้เข้าร่วม FS-ISAC หรือเครือข่ายแบ่งปันข้อมูลภัยคุกคามเฉพาะอุตสาหกรรม
  - **ระดับความพร้อม: Baseline** (ขั้นพื้นฐาน) - มีการรับรู้ภัยคุกคามเบื้องต้น แต่ขาดแหล่งข้อมูลเชิงลึกและการทำงานร่วมกับภายนอก
- **Domain 3: Cybersecurity Controls (การควบคุมความปลอดภัยไซเบอร์)**
  - **การปฏิบัติที่มีอยู่:** มี Firewall, Antivirus, มีการสำรองข้อมูล, มีการอัปเดตระบบปฏิบัติการและซอฟต์แวร์ตามปกติ, มีการควบคุมการเข้าถึงระบบแบบพื้นฐาน

- **ระดับความพร้อม: Evolving** (กำลังพัฒนา) - มีการควบคุมพื้นฐานที่ดี แต่ยังขาดการควบคุมที่ซับซ้อนขึ้น เช่น การจัดการช่องโหว่เชิงรุก หรือการตรวจจับการบุกรุกขั้นสูง

- **Domain 4: External Dependency Management (การจัดการการพึ่งพาภายนอก)**
    - **การปฏิบัติที่มีอยู่:** มีสัญญาบริการกับผู้ให้บริการ Core Banking และแอปพลิเคชันมือถือ, มีการทบทวนสัญญาเป็นประจำ, แต่ยังไม่มีการประเมินความปลอดภัยของผู้ให้บริการอย่างละเอียด
    - **ระดับความพร้อม: Baseline** (ขั้นพื้นฐาน) - มีการจัดการสัญญา แต่ยังขาดการตรวจสอบความปลอดภัยของบุคคลที่สามอย่างเข้มงวด

- **Domain 5: Cyber Incident Management and Resilience (การจัดการเหตุการณ์ไซเบอร์และความยืดหยุ่น)**
    - **การปฏิบัติที่มีอยู่:** มีแผนการกู้คืนระบบจากภัยพิบัติ (DRP) ทั่วไป, มีทีม IT ที่รับผิดชอบในการตอบสนองเหตุการณ์ แต่ยังไม่มีแผนรับมือเหตุการณ์ไซเบอร์โดยเฉพาะที่ทดสอบอย่างสม่ำเสมอ
    - **ระดับความพร้อม: Evolving** (กำลังพัฒนา) - มีแผนรองรับภัยพิบัติ แต่ยังไม่เฉพาะเจาะจงและทดสอบเรื่องภัยไซเบอร์อย่างเพียงพอ

ผลลัพธ์และการนำไปปฏิบัติ

เมื่อเปรียบเทียบ **Inherent Risk Profile (Minimal to Moderate)** กับ **Cybersecurity Maturity (ส่วนใหญ่อยู่ที่ Baseline และ Evolving)** เฟิร์สต์ คอมมูนิตี้ แบงก์ พบว่า:

- **ช่องว่าง (Gaps):** ระดับความพร้อมด้านความปลอดภัยยังไม่สอดคล้องกับระดับความเสี่ยงโดยธรรมชาติ โดยเฉพาะในด้านการกำกับดูแล, ข่าวกรองภัยคุกคาม, และการจัดการความสัมพันธ์กับบุคคลภายนอก ธนาคารมีความเสี่ยงที่จะไม่สามารถรับมือกับภัยคุกคามที่ซับซ้อนขึ้นได้
- **ข้อเสนอแนะสำหรับการปรับปรุง:**
    1. **ยกระดับธรรมาภิบาล:**
        - จัดตั้งคณะทำงานด้านความปลอดภัยไซเบอร์เฉพาะกิจ
        - กำหนดนโยบายความปลอดภัยไซเบอร์ที่ชัดเจนและครอบคลุม

- จัดให้มีการฝึกอบรมด้านความตระหนักรู้ด้านไซเบอร์สำหรับพนักงานทุกคนอย่างสม่ำเสมอ

2. **เสริมสร้างข่าวกรองภัยคุกคาม:**
    - พิจารณาเข้าร่วม FS-ISAC หรือแหล่งข้อมูลข่าวกรองภัยคุกคามที่น่าเชื่อถือ
    - ลงทุนในเครื่องมือหรือบริการที่ช่วยในการรวบรวมและวิเคราะห์ข้อมูลภัยคุกคาม
3. **ปรับปรุงการควบคุม:**
    - พิจารณาการนำระบบ SIEM (Security Information and Event Management) มาใช้เพื่อรวบรวมและวิเคราะห์ Log การใช้งาน
    - ดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) และการทดสอบการเจาะระบบ (Penetration Testing) โดยผู้เชี่ยวชาญภายนอกอย่างน้อยปีละครั้ง
4. **ยกระดับการจัดการบุคคลภายนอก:**
    - สร้างกระบวนการประเมินความปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Third-Party Risk Assessment) ที่เข้มงวดขึ้น
    - กำหนดข้อกำหนดด้านความปลอดภัยไซเบอร์ในสัญญาอย่างชัดเจน
5. **พัฒนาการจัดการเหตุการณ์:**
    - พัฒนากระบวนการตอบสนองเหตุการณ์ไซเบอร์ (Cyber Incident Response Plan) โดยเฉพาะ
    - จัดการฝึกซ้อมแผน (Tabletop Exercise) เพื่อทดสอบประสิทธิภาพของแผนและบทบาทของทีมงานอย่างน้อยปีละครั้ง

บทบาทของ "อิสรภาพ" ในการปฏิบัติ:

- **ความยืดหยุ่นในการนำไปใช้:** FFIEC CAT ไม่ได้บังคับให้ธนาคารต้องมี "ระดับ Innovative" ในทุกโดเมน ธนาคารสามารถตัดสินใจเองได้ว่าจะยกระดับความพร้อมไปถึงระดับใด โดยพิจารณาจากขนาด, ความซับซ้อน, และโปรไฟล์ความเสี่ยงของตนเอง

- **การประเมินตนเอง:** ธนาคารมีอิสระในการใช้ CAT เป็นเครื่องมือในการประเมินตนเอง และใช้ผลลัพธ์เพื่อขับเคลื่อนการปรับปรุงภายในโดยไม่ต้องรอการตรวจสอบจากหน่วยงานกำกับดูแลเสมอไป
- **การปรับปรุงอย่างต่อเนื่อง:** CAT เป็นเครื่องมือที่ใช้ในการประเมินซ้ำได้ ทำให้ธนาคารสามารถติดตามความคืบหน้าของตนเองในการปรับปรุง Cyber Resilience ได้อย่างอิสระและต่อเนื่อง

ด้วยตัวอย่างนี้ ผมหวังว่าจะช่วยให้เข้าใจถึงวิธีการนำ FFIEC CAT ไปใช้ในการปฏิบัติเพื่อประเมินและปรับปรุง Cyber Resilience ของสถาบันการเงินได้ชัดเจนยิ่งขึ้นนะครับ

สำหรับการกำกับและควบคุม Cyber Resilience ของธนาคารขนาดใหญ่ในสหรัฐอเมริกา FFIEC (Federal Financial Institutions Examination Council) และหน่วยงานกำกับดูแลสมาชิก (เช่น FRB, FDIC, OCC) จะมีแนวทางที่เข้มงวดและซับซ้อนกว่าธนาคารขนาดเล็กมาก เนื่องจากความซับซ้อนของโครงสร้างองค์กร เทคโนโลยี และปริมาณข้อมูลที่ธนาคารขนาดใหญ่จัดการ รวมถึงบทบาทสำคัญต่อระบบเศรษฐกิจโดยรวม

แม้ว่า FFIEC Cybersecurity Assessment Tool (CAT) จะเป็นเครื่องมือพื้นฐานที่ธนาคารทุกขนาดสามารถใช้ได้ แต่ธนาคารขนาดใหญ่จะก้าวข้ามไปใช้กรอบการทำงานด้านความปลอดภัยไซเบอร์ที่เป็นที่ยอมรับในระดับสากล เช่น **NIST Cybersecurity Framework (CSF) 2.0** ซึ่ง FFIEC ก็สนับสนุนให้ธนาคารหันมาใช้มากขึ้น และยังรวมไปถึงมาตรฐานอื่นๆ เช่น ISO/IEC 27001 หรือ Center for Internet Security (CIS) Controls

ตัวอย่าง: การกำกับ / ควบคุม Cyber Resilience ของธนาคารขนาดใหญ่ (กรณีสมมติ: "โกลบอล แบงก์ คอร์ป" - Global Bank Corp)

ข้อมูลเบื้องต้นของธนาคาร:

- **ขนาด:** ธนาคารขนาดใหญ่ระดับโลก ให้บริการเต็มรูปแบบ (ค้าปลีก, พาณิชย์, วาณิชธนกิจ, การลงทุน, การบริหารความมั่งคั่ง)
- **โครงสร้าง:** มีการดำเนินงานในหลายประเทศ, มีบริษัทย่อยจำนวนมาก, มีระบบเทคโนโลยีที่ซับซ้อนและหลากหลาย (Legacy systems, Cloud-native, FinTech integrations)
- **บุคลากร:** มีทีมงานด้าน IT และ Cybersecurity ขนาดใหญ่ พร้อมผู้เชี่ยวชาญเฉพาะทางจำนวนมาก

1. การประเมินความเสี่ยงและกำหนดโปรไฟล์ความเสี่ยง (Inherent Risk Profile & Continuous Risk Assessment)

ธนาคารขนาดใหญ่จะไม่ได้ใช้ FFIEC CAT ในการประเมิน Inherent Risk Profile เพียงอย่างเดียว แต่จะใช้ **กรอบการบริหารความเสี่ยงแบบองค์รวม (Enterprise Risk Management - ERM)** ที่บูรณาการความเสี่ยงด้านไซเบอร์เข้าไปในทุกมิติของธุรกิจ

- **การระบุความเสี่ยงเชิงลึก:**
    - **การวิเคราะห์สินทรัพย์วิกฤต (Critical Asset Identification):** ระบุและจัดลำดับความสำคัญของข้อมูล ลูกค้า ระบบ และบริการที่สำคัญที่สุด (เช่น ระบบชำระเงิน, ข้อมูลส่วนบุคคลลูกค้า, ระบบซื้อขายหลักทรัพย์)
    - **การวิเคราะห์ภัยคุกคาม (Threat Intelligence & Analysis):**
        - มีทีม **Threat Intelligence** โดยเฉพาะที่รวบรวมข้อมูลจากแหล่งต่างๆ (FS-ISAC, หน่วยงานรัฐ, บริษัทรักษาความปลอดภัยชั้นนำ, Dark Web) เพื่อวิเคราะห์แนวโน้มภัยคุกคาม การโจมตีแบบ Zero-day และกลุ่มผู้บุกรุก (APT groups) ที่อาจเป็นเป้าหมาย
        - ใช้ **AI/ML** เพื่อตรวจจับรูปแบบภัยคุกคามและพฤติกรรมที่ผิดปกติ
    - **การประเมินช่องโหว่ (Vulnerability Management):** ดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) อย่างต่อเนื่องและการทดสอบการเจาะระบบ (Penetration Testing) ที่ซับซ้อน ทั้งภายในและภายนอก (Red Teaming, Purple Teaming) ครอบคลุมทุกระบบ รวมถึง Cloud และ Mobile Applications
    - **การประเมินความเสี่ยงบุคคลที่สาม (Third-Party Risk Management - TPRM):**
        - มีกระบวนการประเมินความเสี่ยงไซเบอร์ของผู้ให้บริการภายนอก (Vendors) และพันธมิตรทางธุรกิจที่เข้มงวดมาก ตั้งแต่การคัดเลือกผู้ให้บริการไปจนถึงการตรวจสอบและประเมินผลอย่างต่อเนื่อง
        - กำหนดข้อกำหนดด้านความปลอดภัยไซเบอร์ในสัญญา (SLA) ที่เข้มงวด

- **การจัดหมวดหมู่ความเสี่ยง:** มีการจำแนกความเสี่ยงออกเป็นระดับละเอียด (เช่น High, Medium, Low) และอาจใช้ **การประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Assessment)** โดยประเมินเป็นมูลค่าทางการเงินที่อาจเสียหาย (เช่น Loss Event Frequency x Loss Magnitude) เพื่อให้ผู้บริหารระดับสูงและคณะกรรมการสามารถเข้าใจผลกระทบทางธุรกิจได้ชัดเจน

โปรไฟล์ความเสี่ยงโดยธรรมชาติของ Global Bank Corp: โดยทั่วไปจะอยู่ในระดับ **"Significant" ถึง "Most" Inherent Risk** เนื่องจากมีบริการที่หลากหลาย, เทคโนโลยีซับซ้อน, มีการเชื่อมต่อจำนวนมาก และเป็นเป้าหมายหลักของการโจมตีไซเบอร์

2. การยกระดับความพร้อมด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Maturity - NIST CSF 2.0 / ISO 27001)

ธนาคารขนาดใหญ่จะตั้งเป้าที่ระดับความพร้อมที่สูงกว่า Baseline มาก โดยอาจเทียบเคียงกับระดับ **"Advanced" หรือ "Innovative"** ตามแนวคิดของ FFIEC CAT แต่จะใช้กรอบการทำงานที่ละเอียดกว่า เช่น NIST CSF 2.0 ซึ่งมี 6 ฟังก์ชันหลัก: Govern, Identify, Protect, Detect, Respond, Recover

- **Govern (ธรรมาภิบาล):**
    - **คณะกรรมการและผู้บริหาร:** คณะกรรมการธนาคารมีคณะอนุกรรมการด้านความเสี่ยงด้านเทคโนโลยีและไซเบอร์โดยเฉพาะ มีการประชุมและรายงานผลเป็นประจำ
    - **นโยบายและกลยุทธ์:** มีนโยบายความปลอดภัยไซเบอร์ระดับองค์กรที่ครอบคลุมทุกบริษัทย่อยและทุกภูมิภาค รวมถึงกลยุทธ์ด้านความปลอดภัยไซเบอร์ที่สอดคล้องกับกลยุทธ์ทางธุรกิจ
    - **งบประมาณและทรัพยากร:** จัดสรรงบประมาณมหาศาลและบุคลากรผู้เชี่ยวชาญเฉพาะทาง (เช่น CISO, Chief Privacy Officer, Incident Response Team, Red Team, Security Architects)
- **Identify (ระบุ):**
    - **การบริหารสินทรัพย์:** มีระบบ Asset Management ที่ละเอียดอ่อนเพื่อระบุและจัดประเภทสินทรัพย์ทั้งหมด (ฮาร์ดแวร์, ซอฟต์แวร์, ข้อมูล, Cloud instances) พร้อมกำหนดเจ้าของสินทรัพย์

    - **การบริหารความเสี่ยง:** ใช้แพลตฟอร์ม GRC (Governance, Risk, and Compliance) ขนาดใหญ่เพื่อรวมการประเมินความเสี่ยง, การควบคุม, การตรวจสอบ และการรายงานผล
    - **การบริหารความรู้:** มีฐานข้อมูลความรู้เกี่ยวกับช่องโหว่, ภัยคุกคาม, และมาตรการป้องกันที่ทันสมัย
- **Protect (ป้องกัน):**
    - **การควบคุมการเข้าถึง (Access Control):** ใช้ Zero Trust Architecture, Multi-Factor Authentication (MFA) สำหรับการเข้าถึงทุกระดับ, มีระบบ Identity and Access Management (IAM) และ Privileged Access Management (PAM) ที่ซับซ้อน
    - **การป้องกันข้อมูล (Data Protection):** ใช้ Data Loss Prevention (DLP) solution, การเข้ารหัสข้อมูล (Encryption) ทั้ง In-transit และ At-rest สำหรับข้อมูลสำคัญทุกประเภท
    - **ความปลอดภัยเครือข่าย:** Next-Gen Firewalls, Intrusion Prevention Systems (IPS), Segmentation เครือข่ายอย่างละเอียด, Micro-segmentation สำหรับ Workloads ที่สำคัญ
    - **ความปลอดภัยแอปพลิเคชัน:** Secure Software Development Life Cycle (SSDLC), Static/Dynamic Application Security Testing (SAST/DAST)
- **Detect (ตรวจจับ):**
    - **SIEM/SOAR:** มีระบบ Security Information and Event Management (SIEM) และ Security Orchestration, Automation, and Response (SOAR) ที่รวบรวม Log จากทุกระบบทั่วโลก พร้อมทีม SOC (Security Operations Center) ที่ทำงาน 24/7
    - **Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR):** ติดตั้งบน Endpoint ทุกตัวเพื่อตรวจจับกิจกรรมที่ผิดปกติ
    - **Threat Hunting:** มีทีมงาน Threat Hunter ที่ค้นหาภัยคุกคามเชิงรุกภายในเครือข่าย
- **Respond (ตอบสนอง):**
    - **แผนรับมือเหตุการณ์ไซเบอร์ (Incident Response Plan - IRP):** มี IRP ที่ละเอียดอ่อนครอบคลุมสถานการณ์หลากหลาย (Ransomware, Data Breach, DDoS) พร้อมการกำหนดบทบาทหน้าที่และกระบวนการที่ชัดเจน

- **การฝึกซ้อม:** จัดการฝึกซ้อมแผนรับมือเหตุการณ์ไซเบอร์ (Tabletop Exercises, Simulation Exercises) อย่างสม่ำเสมอ ทั้งภายในและร่วมกับหน่วยงานภาครัฐและอุตสาหกรรม
- **Forensics:** มีความสามารถในการสืบสวนทางดิจิทัล (Digital Forensics) ภายในองค์กร หรือใช้บริการจากผู้เชี่ยวชาญภายนอกที่พร้อมตลอดเวลา

- **Recover (กู้คืน):**
  - **Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP):** มี BCP/DRP ที่ซับซ้อน เพื่อให้มั่นใจว่าบริการสำคัญสามารถกู้คืนและดำเนินงานต่อได้ในเวลาที่กำหนด (RTO/RPO) แม้เกิดการโจมตีไซเบอร์รุนแรง
  - **Immutable Backups:** มีการสำรองข้อมูลสำคัญแบบ Immutable เพื่อป้องกันการแก้ไขหรือลบโดยผู้โจมตี
  - **การทดสอบการกู้คืน:** ทดสอบแผน BCP/DRP และการกู้คืนข้อมูลอย่างสม่ำเสมอในสภาพแวดล้อมจำลอง

3. บทบาทของหน่วยงานกำกับดูแล (FFIEC Member Agencies)

สำหรับธนาคารขนาดใหญ่ หน่วยงานกำกับดูแลจะไม่เพียงแค่ใช้ FFIEC CAT เพื่อประเมินเท่านั้น แต่จะทำการตรวจสอบเชิงลึกและเข้มงวดมากขึ้น:

- **การตรวจสอบเฉพาะทาง:** ส่งผู้ตรวจสอบที่มีความเชี่ยวชาญด้านไซเบอร์โดยเฉพาะเข้าตรวจสอบอย่างละเอียด รวมถึงการทบทวนเอกสาร, การสัมภาษณ์บุคลากร, การทดสอบระบบ และการทบทวนผลการทดสอบการเจาะระบบ
- **การติดตามอย่างใกล้ชิด:** มีการติดตามสถานะความเสี่ยงและมาตรการป้องกันอย่างต่อเนื่องผ่านการรายงานผลและข้อมูลที่ธนาคารส่งให้
- **การออกคำสั่งกำกับ (Supervisory Orders):** หากพบช่องโหว่หรือความบกพร่องที่สำคัญ อาจมีการออกคำสั่งกำกับให้ธนาคารแก้ไขภายในระยะเวลาที่กำหนด ซึ่งอาจรวมถึงการปรับโครงสร้าง, การลงทุนในเทคโนโลยี, หรือการเปลี่ยนแปลงบุคลากร

- **การสนับสนุนการทำงานร่วมกัน:** ส่งเสริมและอาจบังคับให้ธนาคารขนาดใหญ่เข้าร่วมแพลตฟอร์มการแลกเปลี่ยนข้อมูลภัยคุกคาม เช่น FS-ISAC และการฝึกซ้อมร่วมกับภาครัฐ (เช่น "Cyber Storm" Exercise)

"อิสรภาพ" ในบริบทของธนาคารขนาดใหญ่

ในขณะที่ธนาคารขนาดใหญ่ถูกกำกับดูแลอย่างเข้มงวด แต่ก็ยังมี "อิสรภาพ" ในด้านต่างๆ:

- **อิสระในการเลือก Framework/Solution:** ธนาคารมีอิสระในการเลือกกรอบการทำงานด้านความปลอดภัยไซเบอร์ (เช่น NIST CSF, ISO 27001) และโซลูชันเทคโนโลยีที่เหมาะสมที่สุดกับโครงสร้างและกลยุทธ์ของตนเอง ตราบใดที่ยังคงบรรลุเป้าหมายด้าน Cyber Resilience ตามที่หน่วยงานกำกับดูแลคาดหวัง
- **นวัตกรรมและเทคโนโลยีใหม่:** ธนาคารมีอิสระในการทดลองและนำเทคโนโลยีใหม่ๆ (เช่น AI/ML, Quantum Computing) มาใช้ในการป้องกันภัยคุกคาม หรือปรับปรุงประสิทธิภาพการดำเนินงาน โดยต้องมีการประเมินความเสี่ยงและมีมาตรการควบคุมที่เหมาะสมรองรับ
- **การจัดการความเสี่ยงแบบปรับตัว (Adaptive Risk Management):** ด้วยภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา ธนาคารขนาดใหญ่มีอิสระในการปรับเปลี่ยนกลยุทธ์และมาตรการป้องกันได้อย่างรวดเร็ว โดยอาศัยข้อมูลเชิงลึกจากทีม Threat Intelligence และการประเมินความเสี่ยงอย่างต่อเนื่อง
- **การบริหารจัดการภายใน:** หน่วยงานกำกับดูแลจะเน้นที่ผลลัพธ์และความสามารถในการจัดการความเสี่ยงของธนาคารเป็นหลัก ไม่ได้เข้ามาสั่งการในทุกรายละเอียดของวิธีการดำเนินการ ธนาคารมีอิสระในการจัดโครงสร้างทีมงาน, กำหนดกระบวนการภายใน, และจัดสรรงบประมาณอย่างมีประสิทธิภาพตามดุลยพินิจของตนเอง

สรุปได้ว่า สำหรับธนาคารขนาดใหญ่ การกำกับดูแล Cyber Resilience เป็นเรื่องที่ซับซ้อนและครอบคลุมทุกมิติ โดยเน้นที่การมีกรอบการบริหารความเสี่ยงที่แข็งแกร่ง, การลงทุนในเทคโนโลยีและบุคลากรระดับสูง, และความสามารถในการตอบสนองและกู้คืนจากเหตุการณ์ไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ ในขณะเดียวกันก็ยังคงมี "อิสรภาพ" ในการนำแนวทางและเทคโนโลยีมาปรับใช้ให้เหมาะสมกับบริบทและความซับซ้อนขององค์กรตนเอง ภายใต้การกำกับดูแลที่เข้มงวด

การบริหารความเสี่ยงที่เชื่อถือได้ด้วย GRC: แนวทางจาก FFIEC สำหรับองค์กรการเงิน

ในบริบทของสถาบันการเงิน การบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบ (Governance, Risk, and Compliance: GRC) ถือเป็นกลไกสำคัญในการสร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร โดยเฉพาะอย่างยิ่งในยุคที่ภัยคุกคามด้านไซเบอร์มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งในบริบทที่จะกล่าวถึงนี้เป็นแนวทางที่ผมชอบและใช้มานานแล้วจนกระทั่งปัจจุบัน เพราะเข้าใจได้ง่ายและสามารถนำมาประยุกต์ใช้ในทุกระดับของกระบวนการกำกับและการบริหารในภาครัฐและภาคเอกชนได้อย่างกว้างขวาง

แม้ว่า **FFIEC (Federal Financial Institutions Examination Council)** จะไม่ได้จัดทำคู่มือ GRC แบบเฉพาะเจาะจง แต่ก็ได้ให้แนวทางการกำกับดูแลที่ครอบคลุมในหลายด้าน ซึ่งสามารถนำมาบูรณาการเข้ากับโครงสร้าง GRC ขององค์กรได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในประเด็นที่เกี่ยวข้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และความปลอดภัยทางไซเบอร์ (Cybersecurity)

FFIEC เน้นให้สถาบันการเงินมีกรอบการบริหารความเสี่ยงที่แข็งแกร่ง และส่งเสริมการใช้ GRC Platform หรือ GRC Solution เป็นเครื่องมือในการสนับสนุนการประเมิน การควบคุม การตรวจสอบ และการรายงาน เพื่อให้สอดคล้องกับข้อกำหนดและความคาดหวังของหน่วยงานกำกับดูแล

ต่อไปนี้คือคำแนะนำทั่วไปที่ FFIEC เน้นย้ำเกี่ยวกับการบริหารความเสี่ยง การควบคุม การตรวจสอบ และการรายงาน ซึ่งสถาบันการเงินสามารถใช้เป็นแนวทางในการพัฒนาระบบ GRC ที่เชื่อถือได้:

1. การบริหารความเสี่ยง (Risk Assessment and Management):

- **การประเมินความเสี่ยงอย่างต่อเนื่อง:** FFIEC คาดหวังให้สถาบันการเงินดำเนินการประเมินความเสี่ยงอย่างสม่ำเสมอและต่อเนื่อง ไม่ใช่แค่ทำครั้งเดียวแล้วจบไป การประเมินนี้ควรรวมถึง:
    - **การระบุสินทรัพย์ (Asset Identification):** ระบุและจัดหมวดหมู่สินทรัพย์ข้อมูลและระบบเทคโนโลยีสารสนเทศทั้งหมด รวมถึงเจ้าของสินทรัพย์นั้นๆ
    - **การระบุภัยคุกคาม (Threat Identification):** ระบุภัยคุกคามทั้งภายในและภายนอกที่อาจส่งผลกระทบต่อสินทรัพย์ (เช่น มัลแวร์, ฟิชชิ่ง, DDoS, การโจมตีแบบ Zero-day, ภัยคุกคามจากบุคคลภายใน)
    - **การระบุช่องโหว่ (Vulnerability Identification):** ระบุจุดอ่อนในระบบ กระบวนการ หรือบุคลากรที่อาจถูกใช้ประโยชน์จากภัยคุกคาม

    - **การวิเคราะห์ผลกระทบ (Impact Analysis):** ประเมินผลกระทบที่อาจเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง (ทางการเงิน, ชื่อเสียง, การดำเนินงาน, กฎระเบียบ)
    - **การวิเคราะห์โอกาส (Likelihood Analysis):** ประเมินความเป็นไปได้ที่ภัยคุกคามจะใช้ช่องโหว่เพื่อส่งผลกระทบต่อสินทรัพย์
- **การจัดทำทะเบียนความเสี่ยง (Risk Register):** ต้องมีระบบกลาง (เช่น ใน GRC Platform) เพื่อบันทึก จัดการ และติดตามความเสี่ยงทั้งหมด รวมถึงการกำหนดเจ้าของความเสี่ยง (Risk Owner) และสถานะการแก้ไข
- **การใช้กรอบการทำงาน:** FFIEC สนับสนุนให้ใช้กรอบการทำงานที่เป็นที่ยอมรับ เช่น NIST Cybersecurity Framework (CSF) ซึ่งช่วยในการจัดหมวดหมู่และจัดการความเสี่ยงด้านไซเบอร์อย่างเป็นระบบ (แม้ FFIEC CAT จะถูกยกเลิกในเดือนสิงหาคม 2025 แต่แนวคิดหลักยังคงมีความสำคัญ)
- **การประเมินความเสี่ยงของบุคคลที่สาม (Third-Party Risk Management):** เป็นส่วนสำคัญที่ FFIEC เน้นย้ำอย่างมาก ธนาคารต้องมีกระบวนการที่เข้มงวดในการประเมินและบริหารความเสี่ยงที่เกิดจากผู้ให้บริการภายนอก (vendors) รวมถึงการตรวจสอบสถานะด้านความปลอดภัยของผู้ให้บริการอย่างละเอียดและต่อเนื่อง

2. การควบคุม (Controls Implementation and Management):

- **การนำมาตรการควบคุมมาใช้:** สถาบันการเงินต้องนำมาตรการควบคุมที่เหมาะสมมาใช้เพื่อลดความเสี่ยงที่ระบุ โดย FFIEC IT Examination Handbook มีรายละเอียดเกี่ยวกับมาตรการควบคุมในด้านต่างๆ เช่น:
    - **การควบคุมการเข้าถึง (Access Controls):** การยืนยันตัวตน (Authentication), การให้สิทธิ์ (Authorization), การจัดการสิทธิ์พิเศษ (Privileged Access Management - PAM)
    - **ความปลอดภัยเครือข่าย (Network Security):** Firewall, Intrusion Detection/Prevention Systems (IDS/IPS), การแบ่งส่วนเครือข่าย (Network Segmentation)
    - **การป้องกันข้อมูล (Data Protection):** การเข้ารหัสข้อมูล (Encryption), Data Loss Prevention (DLP)

    - **ความปลอดภัยแอปพลิเคชัน (Application Security):** Secure Software Development Life Cycle (SSDLC), การทดสอบความปลอดภัยแอปพลิเคชัน
    - **การจัดการช่องโหว่ (Vulnerability Management):** การสแกนช่องโหว่, การทดสอบการเจาะระบบ (Penetration Testing)

- **การตรวจสอบประสิทธิภาพของการควบคุม (Control Effectiveness Testing):** ต้องมีการตรวจสอบและทดสอบมาตรการควบคุมอย่างสม่ำเสมอเพื่อให้แน่ใจว่ามาตรการเหล่านั้นมีประสิทธิภาพตามที่คาดหวัง
- **การจัดการการเปลี่ยนแปลง (Change Management):** ต้องมีกระบวนการจัดการการเปลี่ยนแปลงระบบและแอปพลิเคชันที่รัดกุม เพื่อลดความเสี่ยงจากการเปลี่ยนแปลงที่ไม่ได้ควบคุม

3. การตรวจสอบ (Auditing):

- **การตรวจสอบภายในที่เป็นอิสระ (Independent Internal Audit):** FFIEC คาดหวังให้สถาบันการเงินมีฟังก์ชันการตรวจสอบภายในที่แข็งแกร่งและเป็นอิสระ โดยผู้ตรวจสอบภายในควร:
    - มีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงด้าน IT และ Cybersecurity อย่างลึกซึ้ง
    - ดำเนินการตรวจสอบตามแผนการตรวจสอบที่อิงตามความเสี่ยง (Risk-Based Audit Plan)
    - ประเมินความเพียงพอและประสิทธิภาพของการควบคุมภายในด้าน IT และ Cybersecurity
    - ระบุจุดอ่อน, เสนอข้อเสนอแนะในการปรับปรุง, และติดตามการแก้ไขให้แล้วเสร็จ
- **การตรวจสอบภายนอก (External Audit/Assurance):** สถาบันการเงินควรพิจารณาให้มีการตรวจสอบจากผู้ตรวจสอบภายนอกหรือได้รับรายงานการรับรอง (เช่น SOC 1, SOC 2) โดยเฉพาะอย่างยิ่งสำหรับผู้ให้บริการเทคโนโลยีภายนอก เพื่อให้มั่นใจในความปลอดภัยและการควบคุมของบุคคลที่สาม

4. การรายงาน (Reporting):

- **การรายงานต่อคณะกรรมการและผู้บริหารระดับสูง:** GRC Platform ควรสามารถสร้างรายงานที่เข้าใจง่ายสำหรับคณะกรรมการและผู้บริหารระดับสูง โดยเน้นที่:
    - **โปรไฟล์ความเสี่ยงโดยรวมขององค์กร (Overall Risk Profile):** สถานะความเสี่ยงในปัจจุบันและแนวโน้ม

- **ช่องโหว่และจุดอ่อนที่สำคัญ (Key Vulnerabilities and Gaps):** ระบุปัญหาเร่งด่วนที่ต้องแก้ไข
- **สถานะการปฏิบัติตามข้อกำหนด (Compliance Status):** ประเมินว่าองค์กรปฏิบัติตามกฎระเบียบและแนวทางของ FFIEC ได้ดีเพียงใด
- **ผลการตรวจสอบและการแก้ไข (Audit Findings and Remediation Status):** ความคืบหน้าในการแก้ไขข้อบกพร่องที่พบจากการตรวจสอบ
- **ดัชนีชี้วัดความเสี่ยงหลัก (Key Risk Indicators - KRIs) และดัชนีชี้วัดประสิทธิภาพหลัก (Key Performance Indicators - KPIs) ด้านความปลอดภัยไซเบอร์:** เพื่อติดตามสถานะและแนวโน้มของความปลอดภัย

- **การรายงานเหตุการณ์ (Incident Reporting):** มีกระบวนการรายงานเหตุการณ์ด้านไซเบอร์ที่ชัดเจนและทันท่วงทีไปยังผู้บริหารและหน่วยงานกำกับดูแลตามที่กำหนด
- **การรายงานสำหรับการตรวจสอบ (Audit-Ready Reporting):** GRC Solution ควรช่วยในการรวบรวมหลักฐานและจัดทำรายงานที่พร้อมสำหรับการตรวจสอบโดยหน่วยงานกำกับดูแล ทำให้กระบวนการตรวจสอบมีประสิทธิภาพมากขึ้น

FFIEC และ GRC Tools/Platforms

แม้ FFIEC จะไม่บังคับใช้แพลตฟอร์ม GRC เฉพาะ แต่ก็สนับสนุนการใช้เทคโนโลยีเพื่อช่วยในการจัดการความเสี่ยงและการปฏิบัติตามข้อกำหนด แพลตฟอร์ม GRC ที่ดีควรมีคุณสมบัติดังนี้:

- **การรวมศูนย์ข้อมูล:** รวบรวมข้อมูลความเสี่ยง, การควบคุม, การตรวจสอบ, และนโยบายไว้ในที่เดียว
- **การทำให้เป็นมาตรฐาน:** ช่วยให้กระบวนการประเมินและการจัดการเป็นไปตามมาตรฐานที่กำหนด
- **ระบบอัตโนมัติ (Automation):** ช่วยให้การรวบรวมข้อมูล, การประเมิน, การติดตาม, และการสร้างรายงานเป็นไปโดยอัตโนมัติ ลดภาระงานด้วยมือ
- **การวิเคราะห์และการแสดงผล (Analytics and Dashboards):** นำเสนอข้อมูลในรูปแบบที่เข้าใจง่ายผ่าน Dashboard และรายงานที่ปรับแต่งได้

- **การเชื่อมโยงกับ Frameworks:** สามารถเชื่อมโยงการควบคุมและกิจกรรมต่างๆ เข้ากับกรอบการทำงานเช่น NIST CSF หรือมาตรฐานอื่นๆ เพื่อช่วยในการแสดงหลักฐานการปฏิบัติตามข้อกำหนด

ข้อควรทราบ: FFIEC CAT จะถูก **"ยกเลิก" (sunset)** ในวันที่ 31 สิงหาคม 2568 (2025) โดย FFIEC สนับสนุนให้สถาบันการเงินหันไปใช้กรอบการทำงานที่เป็นที่ยอมรับในระดับสากลมากขึ้น เช่น NIST CSF 2.0 ซึ่งเน้นผลลัพธ์ (outcome-based) มากกว่าการประเมินระดับความพร้อม (maturity-level assessment) การเปลี่ยนผ่านนี้จะยิ่งเน้นความสำคัญของการมีระบบ GRC ที่ยืดหยุ่นและบูรณาการ เพื่อรองรับการบริหารความเสี่ยงและการปฏิบัติตามข้อกำหนดที่เปลี่ยนแปลงไป

ดังนั้น การบริหารความเสี่ยงด้วย GRC ที่เชื่อถือได้ตามคำแนะนำของ FFIEC คือการสร้างระบบที่ครอบคลุมและต่อเนื่องในการระบุ ประเมิน ควบคุม ตรวจสอบ และรายงานความเสี่ยงด้านไซเบอร์ โดยอาศัยเทคโนโลยี GRC เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการปฏิบัติตามกฎระเบียบ

สรุป FFIEC ไม่ได้ให้คู่มือ GRC แบบเฉพาะเจาะจง แต่ให้แนวทางที่สำคัญในด้านการบริหารความเสี่ยง การควบคุม การตรวจสอบ และการรายงาน ที่สามารถนำไปบูรณาการเข้ากับระบบ GRC ขององค์กรอย่างมีประสิทธิภาพ การนำ GRC Platform มาใช้ควบคู่จะช่วยเพิ่มขีดความสามารถในการบริหารความเสี่ยง และทำให้องค์กรสามารถตอบสนองต่อการเปลี่ยนแปลงของภัยไซเบอร์และข้อกำหนดได้อย่างยั่งยืน