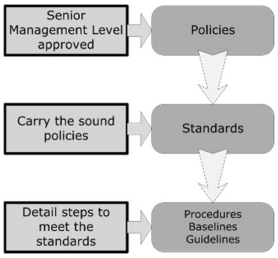
Computer Security Information Security & Risk Management

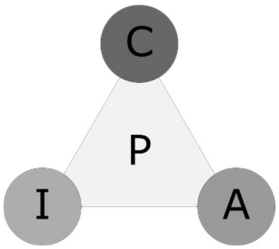
Core Principles ในด้านความปลอดภัยของคอมพิวเตอร์และการจัดการความเสี่ยงเป็นหลักการหรือแนวทางที่สำคัญในการดำเนินงานในระบบสารสนเทศและเทคโนโลยีข้อมูลสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งประกอบไปด้วยหลักการสำคัญต่อไปนี้:

- **Confidentiality (ความลับ):** หลักการนี้หมายถึงการรักษาความลับของข้อมูล ในระบบคอมพิวเตอร์และเครือข่าย การรักษาความลับมักจะเกี่ยวข้องกับการใช้เทคนิคการเข้ารหัสข้อมูลเพื่อป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตเข้าถึงข้อมูลเชิงลึกขององค์กรหรือผู้ใช้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลนั้น ตัวอย่างเช่นการใช้รหัสผ่านและการเข้ารหัสข้อมูล
- **Integrity (ความคงสภาพ):** หลักการนี้หมายถึงการรักษาความถูกต้องและความเชื่อถือได้ของข้อมูลในระบบคอมพิวเตอร์ ซึ่งการรักษาความคงสภาพข้อมูลมักจะใช้เทคนิคต่าง ๆ เช่นการใช้เช็คซัม (checksums) หรือเซ็นเชียลดิจิตอล (digital signatures) เพื่อตรวจสอบว่าข้อมูลยังคงเป็นไปตามรูปแบบและค่าที่คาดหวังไว้โดยไม่มีการแก้ไขหรือบิดเบือน.
- **Availability (ความพร้อมใช้งาน):** หลักการนี้หมายถึงการรักษาความพร้อมใช้งานของระบบคอมพิวเตอร์และข้อมูล หมายความว่าระบบคอมพิวเตอร์และข้อมูลต้องมีความพร้อมใช้งานสูงตลอดเวลา โดยไม่เป็นผลกระทบต่อการเข้าถึงข้อมูลหรือการใช้งานระบบ ตัวอย่างเช่นการใช้เทคนิคการสำรองข้อมูล (backup) เพื่อให้สามารถกู้คืนข้อมูลที่สูญหายหรือเสียหายได้ การใช้งานระบบเครือข่ายที่มีความเสถียรสูง เป็นต้น.
- **Privacy (ความเป็นส่วนตัว):** หลักการนี้เน้นความเป็นส่วนตัวของข้อมูลส่วนบุคคล คือการรักษาความลับและความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่เกี่ยวข้อง หรือมีผลต่อบุคคลที่เกี่ยวข้องกับข้อมูลนั้น หมายความว่าองค์กรหรือบุคคลที่เกี่ยวข้องต้องปฏิบัติตามกฎหมายและนโยบายที่เกี่ยวข้องในการรักษาความเป็นส่วนตัวของข้อมูลที่ได้รับจากผู้ใช้หรือผู้ส่งมา

Management Governance (การบริหารการปกครอง) คือกระบวนการและโครงสร้างที่ใช้ในการดำเนินการและควบคุมกิจกรรมต่าง ๆ เพื่อให้ระบบสารสนเทศและการจัดการความเสี่ยงในองค์กรมีความปลอดภัย การบริหารการปกครองรวมถึงการกำหนดนโยบายและกระบวนการที่เกี่ยวข้อง เพื่อให้ผู้บริหารและเจ้าหน้าที่สามารถดำเนินการตรวจสอบ ติดตาม และควบคุมการดำเนินงานในด้านความปลอดภัยได้อย่างมีประสิทธิภาพและต่อเนื่อง

- **Policies (นโยบาย):** เป็นคำสั่งหรือแนวทางที่กำหนดโดยองค์กรเพื่อกำหนดกรอบและกฎเกณฑ์ในการดำเนินการ นโยบายเกี่ยวกับความปลอดภัยและการจัดการความเสี่ยงอาจประกอบด้วยกฎระเบียบในการใช้ระบบ การเข้าถึงข้อมูล การใช้งานอุปกรณ์ หรือการจัดการอื่น ๆ ที่เกี่ยวข้องกับความปลอดภัย
- **Standards (มาตรฐาน):** เป็นกลไกที่ใช้ในการกำหนดและรวบรวมเกณฑ์หรือข้อกำหนดที่เกี่ยวข้องกับความปลอดภัย มาตรฐานช่วยกำหนดสิ่งที่ควรทำหรือไม่ควรทำเพื่อรักษาความปลอดภัยและป้องกันความเสี่ยง ตัวอย่างเช่นมาตรฐานการเข้ารหัสข้อมูล มาตรฐานการรักษาความลับ หรือมาตรฐานการสำรองข้อมูล
- **Procedures (กระบวนการ):** เป็นคำแนะนำหรือคำแนะนำที่อธิบายขั้นตอนการดำเนินงานที่เฉพาะเจาะจงและละเอียดอย่างชัดเจน กระบวนการระบุวิธีการทำงานเฉพาะที่ต้องปฏิบัติในการดำเนินการปฏิบัติงานเพื่อรักษาความปลอดภัย การกระทำและการปฏิบัติตามกระบวนการช่วยให้เจ้าหน้าที่สามารถปฏิบัติงานได้อย่างสอดคล้องและมีประสิทธิภาพ
- **Baselines (เกณฑ์หลัก):** เป็นเกณฑ์ที่ใช้เป็นพื้นฐานในการตรวจสอบความปลอดภัยและการประเมินความเสี่ยง โดยเกณฑ์หลักเป็นเกณฑ์ที่กำหนดระดับขั้นต่ำของการรักษาความปลอดภัย ส่วนใหญ่จะรวมถึงการกำหนดค่าตั้งต้นที่มีความปลอดภัยและการป้องกันความเสี่ยงเช่นการกำหนดค่าความยากต่อการเจาะของรหัสผ่านหรือการกำหนดการปรับปรุงซอฟต์แวร์เป็นระยะเวลาที่กำหนด
- **Guidelines (แนวปฏิบัติ):** เป็นแนวทางหรือคำแนะนำที่มีประโยชน์ในการดำเนินงานและการปฏิบัติตามเพื่อรักษาความปลอดภัย แนวปฏิบัติช่วยให้ผู้ใช้หรือเจ้าหน้าที่มีแนวทางในการดำเนินงานที่ถูกต้องและปลอดภัยตามหลักการ องค์กรส่วนมากจะมีนวัตกรรมที่จะช่วยในการดำเนินงานและการรักษาความปลอดภัย เช่น คำแนะนำเกี่ยวกับการใช้งานอุปกรณ์ต่าง ๆ และโปรแกรมป้องกันไวรัส การแนะนำเกี่ยวกับการกำหนดรหัสผ่านที่แข็งแกร่งหรือการแนะนำเกี่ยวกับการเก็บรักษาและการทำลายข้อมูลที่ไม่ได้ใช้แล้ว เป็นต้น





Audit Frameworks (เฟรมเวิร์กการตรวจสอบ) คือโครงสร้างหรือกรอบงานที่ใช้ในการดำเนินการตรวจสอบระบบสารสนเทศและความปลอดภัยขององค์กร เฟรมเวิร์กการตรวจสอบช่วยให้ผู้ตรวจสอบสามารถกำหนดแนวทางการตรวจสอบ วิธีการวิเคราะห์ และตรวจสอบความเสี่ยงได้อย่างเน้นที่โดยมีวัตถุประสงค์เพื่อการประเมินความเสี่ยง การควบคุมและการปรับปรุงระบบสารสนเทศและการจัดการความเสี่ยงในองค์กร

- **ISACA - COBIT (Information Systems Audit and Control Association - Control Objectives for Information and Related Technologies)** เป็นกรอบงานที่ถูกพัฒนาขึ้นโดยองค์กร ISACA เพื่อสนับสนุนการตรวจสอบระบบสารสนเทศและการควบคุมในองค์กร มีเป้าหมายในการจัดเตรียมและให้คำแนะนำเกี่ยวกับการดำเนินงานและการควบคุมที่มีเสถียรภาพสูงในระบบสารสนเทศ โดยมีคำแนะนำเกี่ยวกับกระบวนการทางธุรกิจและเทคโนโลยีที่สอดคล้องกัน
- **AXELOS - ITIL (Information Technology Infrastructure Library)** เป็นกรอบงานที่พัฒนาขึ้นโดย AXELOS เพื่อการบริหารจัดการบริการทางเทคโนโลยีสารสนเทศในองค์กร ITIL เป็นคอลเลกชันของความรู้และประสบการณ์ที่ดีที่สุดในด้านการจัดการและให้บริการทางเทคโนโลยีสารสนเทศ มีเป้าหมายในการปรับปรุงคุณภาพการให้บริการและการปรับปรุงกระบวนการทางธุรกิจที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศในองค์กร
- **ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Commission 27001)** เป็นมาตรฐานสากลที่เกี่ยวข้องกับการจัดการความปลอดภัยของข้อมูลในองค์กร มาตรฐานนี้กำหนดข้อกำหนดและแนวทางเพื่อสนับสนุนการบริหารจัดการความปลอดภัยของข้อมูลอย่างมีประสิทธิภาพและยั่งยืน โดยมีเนื้อหาที่สำคัญเช่น การตรวจสอบความปลอดภัยของข้อมูล การบริหารความเสี่ยง การกำหนดนโยบายความปลอดภัย การเข้าถึงข้อมูล และการจัดการเหตุการณ์ความเสี่ยง

Organizational Behavior (พฤติกรรมองค์กร) เป็นการศึกษาและวิเคราะห์พฤติกรรมที่เกิดขึ้นในองค์กร ศึกษาเกี่ยวกับความเชื่อมั่น การมีส่วนร่วม ความสัมพันธ์ระหว่างบุคคล การควบคุมและการจัดการองค์กร เพื่อเข้าใจและปรับปรุงการทำงานภายในองค์กร

- **Organizational Structure & Environment (โครงสร้างและสภาพแวดล้อมขององค์กร)** คือการออกแบบและการจัดวางโครงสร้างองค์กร รวมถึงความสัมพันธ์ระหว่างส่วนประกอบต่าง ๆ ในองค์กร ส่วนการสร้างสภาพแวดล้อมจะเกี่ยวข้องกับปัจจัยภายนอกที่ส่งผลต่อการดำเนินงานขององค์กร
- **Best Practices (ปฏิบัติที่ดีที่สุด)** คือเทคนิคหรือวิธีการที่ได้รับการยอมรับและถือเป็นมาตรฐานสูงสุดในวงการ มักเกี่ยวข้องกับวิธีการที่ถูกต้องและมีประสิทธิภาพในการดำเนินงานหรือการจัดการในองค์กร
- **Hiring (การสรรหาบุคคลเข้าทำงาน)** คือกระบวนการในการคัดเลือกและเลือกบุคคลที่เหมาะสมเพื่อเข้าทำงานในองค์กร รวมถึงการประกาศรับสมัคร

สัมภาษณ์ และการตรวจสอบข้อมูลเพื่อให้ได้คนที่มีความสามารถและประสบการณ์ที่เหมาะสม

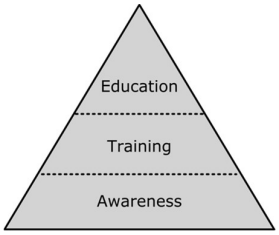
- **Job Rotation (การเปลี่ยนงานหรือการโรเทต)** คือกระบวนการที่พนักงานจะถูกย้ายไปตำแหน่งงานต่าง ๆ ในองค์กรเพื่อให้พนักงานได้สัมผัสและเรียนรู้การทำงานในบทบาทและส่วนต่าง ๆ ขององค์กร เป้าหมายของการโรเทตงานคือการพัฒนาทักษะและความสามารถของพนักงาน ส่งเสริมการทำงานที่หลากหลายและการเข้าใจทั้งกระบวนการภายในองค์กร
- **Separation of Duties (การแยกหน้าที่)** เป็นหลักการที่บังคับให้หน้าที่และสิทธิ์การดำเนินการที่สำคัญในองค์กรถูกแบ่งแยกออกเพื่อลดความเสี่ยงในการทุจริต โดยให้มีคนหลายคนทำหน้าที่ต่าง ๆ และตรวจสอบงานของกันและกัน
- **Least Privilege (Need to Know) (การให้สิทธิ์ขั้นต่ำ)** หรือหลักการ "ต้องการทราบเพียงสิ่งที่จำเป็น" หมายถึงการให้สิทธิ์แก่ผู้ใช้งานเพียงในขอบเขตและระดับที่จำเป็นสำหรับการทำงานที่ต้องทำ โดยเพื่อป้องกันความเสี่ยงและการแอบแฝงในการเข้าถึงข้อมูลและระบบที่ไม่เกี่ยวข้องกับงานของผู้ใช้งาน
- **Job Position Sensitivity (ความละเอียดอ่อนในตำแหน่งงาน)** เป็นค่าความลับและความเป็นส่วนตัวของข้อมูลหรือสิ่งที่มีค่าที่เกี่ยวข้องกับตำแหน่งงานในองค์กร ซึ่งตำแหน่งงานบางตำแหน่งอาจมีความสำคัญและความลับมากกว่าอื่น ๆ

Security-related Units

- **CEO / Board of Directors (กรรมการผู้บริหาร / คณะกรรมการบริษัท)** เป็นหน่วยงานที่มีอำนาจสูงสุดในองค์กร มีบทบาทในการตัดสินใจเกี่ยวกับนโยบายทั่วไปและกำหนดทิศทางและยุทธศาสตร์ในด้านต่าง ๆ ขององค์กร
- **CIO / IT dept. (ผู้อำนวยการเทคโนโลยีสารสนเทศ / แผนกเทคโนโลยีสารสนเทศ)** เป็นหน่วยงานที่รับผิดชอบในการดูแลและบริหารจัดการเทคโนโลยีสารสนเทศภายในองค์กร รวมถึงการพัฒนาและดูแลระบบสารสนเทศที่ใช้งานในองค์กร
- **HR / Legal dept. (แผนกทรัพยากรบุคคล / แผนกทนายความ)** เป็นหน่วยงานที่รับผิดชอบในการจัดการทรัพยากรบุคคลขององค์กร รวมถึงการจัดการเรื่องทางกฎหมายที่เกี่ยวข้องกับองค์กร
- **Internal Audit dept. (แผนกตรวจสอบภายใน)** เป็นหน่วยงานที่รับผิดชอบในการตรวจสอบและประเมินประสิทธิภาพของระบบความคุ้มครองและการควบคุมภายในองค์กร เพื่อให้มั่นใจว่ากระบวนการทำงานและการดำเนินงานเป็นไปตามมาตรฐานและนโยบายที่กำหนดไว้
- **Corporate Security Guards (หน่วยงานรักษาความปลอดภัยขององค์กร)** เป็นหน่วยงานที่มีหน้าที่รักษาความปลอดภัยในพื้นที่ภายในและรอบองค์กรณ์องค์กร ปฏิบัติหน้าที่เฝ้าระวังความเสี่ยงที่อาจเกิดขึ้น เช่น การรักษาความปลอดภัยในอาคาร การควบคุมการเข้าออก และการดูแลทรัพย์สินขององค์กร
- **(Chief) Information Security Officer ((หัวหน้า) ผู้ดูแลความปลอดภัยข้อมูล)** เป็นบทบาทหรือตำแหน่งงานที่รับผิดชอบในการดูแลและจัดการความปลอดภัยข้อมูลภายในองค์กร รวมถึงการให้คำปรึกษาและพัฒนานโยบายความปลอดภัยที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศในองค์กร

Security Courses

- **Awareness (การเข้าใจและตระหนักในเรื่องความปลอดภัย)**: หัวข้อนี้เน้นให้คนทั่วไปในองค์กรเข้าใจและตระหนักถึงความสำคัญของความปลอดภัยข้อมูลและประเด็นที่เกี่ยวข้อง เช่น การรู้จักภัยคุกคามทางไซเบอร์, การรับรู้เกี่ยวกับการโจมตีทางไซเบอร์, และนโยบายความปลอดภัยขององค์กร
- **Training (การฝึกอบรม)**: หัวข้อนี้เน้นให้ความรู้และทักษะทางเทคนิคเฉพาะที่เกี่ยวข้องกับความปลอดภัย มักเป็นการฝึกทักษะเชิงปฏิบัติ เช่น การใช้งานระบบความปลอดภัย, การตรวจสอบความปลอดภัยของเครื่องมือเทคโนโลยี, หรือการตอบสนองต่อเหตุการณ์ความเสี่ยงทางความปลอดภัย
- **Education (การศึกษา)**: หัวข้อนี้เน้นให้ความรู้ทางทฤษฎีและความเข้าใจทางกลยุทธ์เกี่ยวกับความปลอดภัย ระดับการศึกษาสูงขึ้น เช่น หลักสูตรปริญญาตรีหรือปริญญาโทที่เกี่ยวข้องกับความปลอดภัยข้อมูลและการจัดการความเสี่ยงทางความปลอดภัย



Risk Management (การจัดการความเสี่ยง) เป็นกระบวนการที่ใช้ในการรับรู้และประเมินความเสี่ยงที่อาจเกิดขึ้นและมีการวางแผนเพื่อจัดการกับความเสี่ยงให้เหมาะสม โดยมุ่งเน้นการลดความเสี่ยงหรือการควบคุมความเสี่ยงให้มีผลกระทบต่อองค์กรในระดับที่ยอมรับได้

Concepts (แนวความคิด): เป็นแนวความคิดและหลักการในการจัดการความเสี่ยง เช่น การรับรู้ความเสี่ยง, การวัดและประเมินความเสี่ยง, การวางแผนการจัดการความเสี่ยง และการติดตามและประเมินผลการจัดการความเสี่ยง

- **Qualitative Assessments (การประเมินความเสี่ยงแบบคุณภาพ)**: เป็นกระบวนการในการประเมินความเสี่ยงโดยใช้การประเมินแบบทั่วไป โดยไม่ใช้ตัวเลขหรือข้อมูลที่เป็นเชิงปริมาณ การประเมินความเสี่ยงแบบคุณภาพใช้เกณฑ์หรือมาตรฐานที่กำหนดเพื่อแยกแยะความเสี่ยงเป็นระดับต่าง ๆ เช่น ความน่าจะเป็นของเหตุการณ์เสี่ยงและผลกระทบที่เกิดขึ้น
- **Quantitative Assessments (การประเมินความเสี่ยงแบบปริมาณ)**: เป็นกระบวนการในการประเมินความเสี่ยงโดยใช้ข้อมูลที่เป็นเชิงปริมาณ เพื่อให้สามารถวัดและคำนวณความเสี่ยงอย่างชัดเจน โดยการใช้ตัวเลขหรือข้อมูลที่แท้จริงเพื่อประเมินความน่าจะเป็นของเหตุการณ์เสี่ยงและผลกระทบที่อาจเกิดขึ้น การประเมินแบบปริมาณช่วยให้องค์กรทราบถึงความรุนแรงของความเสี่ยง และสามารถทำเปรียบเทียบความเสี่ยงที่ต่างกันได้อย่างชัดเจน

Principles (หลักการ): เป็นหลักและแนวทางในการจัดการความเสี่ยงที่เกี่ยวข้องกับการรับรู้และการวางแผน หลักการเหล่านี้สามารถรวมถึงการหลีกเลี่ยงความเสี่ยง (Avoidance), การโอนความเสี่ยง (Transfer), การบรรเทาความเสี่ยง (Mitigation), การยอมรับความเสี่ยง (Acceptance) และการรับผิดชอบความเสี่ยง (Ownership) เพื่อให้การจัดการความเสี่ยงเป็นไปตามแผนและเป้าหมายที่กำหนด

- **Avoidance (การหลีกเลี่ยง)**: หมายถึงการตัดสินใจในการละเว้นหรือปฏิเสธกิจกรรมหรือสถานการณ์ที่มีความเสี่ยงสูงโดยตรง หรือการใช้วิธีการทางธุรกิจที่ไม่ต้องมีความเสี่ยง เพื่อลดความเสี่ยงให้องค์กร
- **Transfer (การโอนความเสี่ยง)**: หมายถึงการโอนความเสี่ยงจากองค์กรหนึ่งไปยังองค์กรอื่น โดยอาจเป็นการซื้อประกันหรือการทำสัญญากับบุคคลหรือองค์กรภายนอกเพื่อรับผิดชอบความเสี่ยงแทน
- **Mitigation (การบรรเทาความเสี่ยง)**: หมายถึงการนำเสนอและดำเนินการเพื่อลดหรือควบคุมความเสี่ยงให้มีผลกระทบน้อยลง โดยใช้มาตรการที่เหมาะสม เช่น การใช้เทคโนโลยีที่ปลอดภัยมากขึ้นหรือการใช้นโยบายและกระบวนการที่เหมาะสมในการจัดการความเสี่ยง
- **Acceptance (การยอมรับความเสี่ยง)**: เป็นหลักการที่องค์กรยอมรับความเสี่ยงที่เกิดขึ้นและไม่มีการดำเนินการใด ๆ เพื่อจัดการหรือลดความเสี่ยงนั้น ๆ ในบางกรณี การยอมรับความเสี่ยงสามารถเกิดขึ้นเมื่อความเสี่ยงมีระดับต่ำหรือมีผลกระทบน้อย และการรับรู้ความเสี่ยงนั้นเป็นสิ่งที่องค์กรต้องพิจารณาและตัดสินใจว่าจะรับรู้และยอมรับความเสี่ยงดังกล่าวหรือไม่
- **Ownership (การรับผิดชอบความเสี่ยง)**: เป็นหลักการที่กำหนดให้บุคคลหรือหน่วยงานในองค์กรรับผิดชอบในการจัดการความเสี่ยงในพื้นที่หนึ่ง ๆ โดยผู้รับผิดชอบจะต้องมีความรับผิดชอบในการระบุความเสี่ยง เลือกวิธีการจัดการความเสี่ยงที่เหมาะสม และติดตามผลการจัดการความเสี่ยง

Risk Assessment (การประเมินความเสี่ยง): เป็นกระบวนการที่ใช้ในการตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นในองค์กร โดยการระบุและวิเคราะห์ข้อมูลเพื่อระบุความเสี่ยงที่เป็นไปได้ตามสถานการณ์ที่มีอยู่ การ

ประเมินความเสี่ยงช่วยให้องค์กรรับรู้และเข้าใจความเสี่ยงที่เกี่ยวข้องกับทรัพยากรและกิจกรรมขององค์กร

- **Identify Vulnerabilities (การระบุจุดอ่อน):** เป็นกระบวนการในการตรวจหาและระบุจุดอ่อนหรือช่องโหว่ที่อาจทำให้เกิดความเสี่ยงหรือปัญหาในระบบหรือกระบวนการที่องค์กรใช้งาน การระบุจุดอ่อนช่วยให้องค์กรสามารถดำเนินการป้องกันและเสริมความมั่นคงปลอดภัยของระบบได้
- **Identify Threats (การระบุความเสี่ยง):** เป็นกระบวนการในการระบุและกำหนดความเสี่ยงที่เกิดจากสิ่งที่อาจก่อให้เกิดความเสียหายหรือผลกระทบต่อองค์กร เช่น ความเสี่ยงจากการโจมตีด้านความปลอดภัยของข้อมูล การระบุความเสี่ยงช่วยให้องค์กรรับรู้และเข้าใจถึงตัวอันตรายที่อาจเกิดขึ้นและสามารถวางแผนการป้องกันได้
- **Likelihood (ความน่าจะเป็น):** เป็นการประเมินค่าความน่าจะเป็นที่เหตุการณ์เสี่ยงจะเกิดขึ้นหรือเกิดปัญหาในอนาคต โดยการใช้ข้อมูลที่มีอยู่ เช่น ประวัติการเกิดเหตุการณ์ที่คล้ายกันในอดีต และปัจจัยอื่น ๆ เช่น สภาพแวดล้อม ประสบการณ์ทางวิชาชีพ และข้อมูลสถิติ เพื่อให้สามารถประเมินได้ว่าเหตุการณ์เสี่ยงเหล่านั้นเป็นไปได้ในระดับใด การประเมินความน่าจะเป็นช่วยให้องค์กรสามารถกำหนดลำดับความสำคัญของเหตุการณ์เสี่ยง และจัดสรรทรัพยากรในการจัดการความเสี่ยงได้อย่างเหมาะสม
- **Impact (ผลกระทบ):** เป็นการประเมินระดับของผลกระทบที่อาจเกิดขึ้นหากเกิดเหตุการณ์เสี่ยงหรือเหตุการณ์ที่ผิดปกติ เช่น การสูญเสียข้อมูลที่มีความสำคัญ การขาดทุนการเงิน หรือการเสียชื่อเสียงขององค์กร เพื่อให้สามารถวิเคราะห์ความรุนแรงของความเสี่ยงได้อย่างถูกต้องและรับมือกับผลกระทบที่เป็นไปได้
- **RISK (ความเสี่ยง):** เป็นผลลัพธ์ที่ได้จากการประเมินความเสี่ยง ซึ่งรวมถึงความน่าจะเป็นของเหตุการณ์เสี่ยงและผลกระทบที่เกิดขึ้น ความเสี่ยงที่มีระดับสูงและมีผลกระทบมากอาจต้องการการจัดการและการบริหารความเสี่ยงที่เข้มข้นมากขึ้น
- **Countermeasure (มาตรการป้องกันและแก้ไข):** เป็นมาตรการหรือกลยุทธ์ที่ใช้เพื่อลดหรือป้องกันความเสี่ยงที่เกิดขึ้นหรือลดผลกระทบที่เกิดขึ้น อาจเป็นการดำเนินการป้องกันก่อนเกิดเหตุการณ์เสี่ยงหรือกำหนดมาตรการแก้ไขเมื่อเกิดเหตุการณ์เสี่ยงแล้ว
- **Valuation (การประเมินมูลค่า):** เป็นกระบวนการที่ใช้ในการประเมินมูลค่าหรือค่าใช้จ่ายที่เกี่ยวข้องกับการจัดการความเสี่ยง โดยการนำเสนอข้อมูลที่เกี่ยวข้องเช่น ค่าสูญเสียที่อาจเกิดขึ้นหากเกิดเหตุการณ์เสี่ยง เปรียบเทียบกับค่าใช้จ่ายในการบรรลุเป้าหมายการจัดการความเสี่ยง เพื่อให้สามารถตัดสินใจเกี่ยวกับการลงทุนและการจัดสรรทรัพยากรเพื่อการจัดการความเสี่ยงให้เหมาะสม

Ethics & Professionals

Who watches the Watchmen? (ใครจะดูแลผู้ดูแล?): เป็นคำถามที่ยกขึ้นเพื่อสะท้อนถึงความสำคัญของการตรวจสอบและกำกับผู้ดูแลระบบหรือบุคคลที่มีอำนาจในการควบคุมและดูแลความปลอดภัย คำถามนี้เตือนให้ระวังไม่ให้ผู้ดูแลระบบหลุดพ้นจากการตรวจสอบและการควบคุม และให้มีการตรวจสอบและสมดุลย์ของอำนาจในการดูแลเพื่อป้องกันการละเมิดความเป็นธรรม

Code of Conduct (กฎเกณฑ์การปฏิบัติ): เป็นเอกสารที่กำหนดจรรยาบรรณและค่านิยมที่ผู้มีส่วนเกี่ยวข้องต้องปฏิบัติตามในการดำเนินงานหรือการปฏิบัติตามบทบัญญัติทางวิชาชีพ โดยมักใช้ในบริบทของอาชีพที่เกี่ยวข้องกับความรับผิดชอบทางสังคม ความเป็นธรรม และการกระทำที่ถูกต้อง

Put the right MAN on the right JOB at the right TIME with the right TOOLS! (ใส่คนที่เหมาะสมลงไปทำงานที่เหมาะสมในเวลาที่เหมาะสมพร้อมกับใช้เครื่องมือที่เหมาะสม!): เป็นคำกล่าวที่เน้นความสำคัญของการเลือกคนที่เหมาะสมและที่เหมาะสมในตำแหน่งงานที่เหมาะสมในเวลาที่เหมาะสม และให้มีเครื่องมือที่เหมาะสมเพื่อให้ผู้ที่ได้รับมอบหมายมีความสามารถในการดำเนินงาน

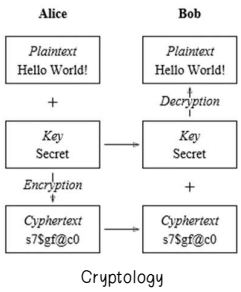
Certifications (การรับรองความรู้และความเชี่ยวชาญ): เป็นการรับรองว่าบุคคลได้ผ่านการศึกษาและทดสอบความรู้และทักษะทางวิชาชีพในด้านที่เกี่ยวข้องกับความปลอดภัยและการบริหารจัดการเทคโนโลยีสารสนเทศ การรับรองมีหลายองค์กรที่เชื่อถือได้ เช่น (ISC)2 CISSP (Certified Information Systems Security Professional), EC-Council CEH (Certified Ethical Hacker), ISACA CISM (Certified Information Security Manager), SANS GIAC (Global Information Assurance Certification) เป็นต้น การรับรองความรู้และความเชี่ยวชาญในระดับนี้ช่วยให้บุคคลสามารถพัฒนาทักษะและเสริมความเชี่ยวชาญในด้านความปลอดภัยได้ และเป็นการยืนยันว่าบุคคลนั้นเป็นผู้เชี่ยวชาญในด้านนั้นตามมาตรฐานที่กำหนดไว้

"Security is a process,
not a product."
-- Bruce Schneier
Computer Security and Privacy Specialist

Computer Security Cryptography (1/3)

The Protection (การป้องกัน): เป็นกระบวนการหรือมาตรการที่ใช้เพื่อป้องกันความเสี่ยงและการบุกรุกที่อาจเกิดขึ้นต่อระบบหรือข้อมูลที่มีความเป็นค่า

- **Time VS Value (เวลาเทียบกับมูลค่า):** เป็นการพิจารณาว่าเราควรลงทุนเวลาและทรัพยากรใดในการป้องกันและรักษาความปลอดภัยให้เหมาะสมกับมูลค่าและความสำคัญของทรัพยากรที่ต้องการปกป้อง
- **Direct benefits (ประโยชน์โดยตรง):** เป็นประโยชน์ที่ได้รับโดยตรงจากการดำเนินการป้องกันความเสี่ยงและการบุกรุก เช่น ป้องกันการสูญเสียข้อมูล ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต หรือป้องกันการบุกรุกลักลอบ
- **Confuse unauthorized people (สับสนบุคคลที่ไม่ได้รับอนุญาต):** เป็นกระบวนการที่ใช้เพื่อสร้างความสับสนและยากต่อการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต
- **Confirm authorized people (ยืนยันบุคคลที่ได้รับอนุญาต):** เป็นกระบวนการที่ใช้เพื่อตรวจสอบและยืนยันตัวตนของบุคคลที่ได้รับอนุญาตให้เข้าถึงข้อมูลหรือระบบ
- **Indirect benefits (ประโยชน์ทางอ้อม):** เป็นประโยชน์ที่ได้รับผลทางอ้อมจากการดำเนินการป้องกันความเสี่ยง เช่น การตรวจสอบความถูกต้องของข้อมูล การยืนยันตัวตนของผู้ใช้ ซึ่งส่งผลให้เกิดความเชื่อถือ
- **Integrity checking (การตรวจสอบความถูกต้อง): เป็น** กระบวนการที่ใช้เพื่อตรวจสอบและรักษาความถูกต้องของข้อมูล โดยตรวจสอบว่าข้อมูลยังคงไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- **Authentication (การยืนยันตัวตน):** เป็นกระบวนการที่ใช้ในการตรวจสอบและยืนยันตัวตนของผู้ใช้หรืออุปกรณ์ โดยใช้วิธีต่างๆ เช่น รหัสผ่าน เครื่องหมายเซสชัน หรือเทคโนโลยีการรู้จักตัวตน เพื่อให้มั่นใจว่าผู้เข้าถึงหรืออุปกรณ์ที่เชื่อถือได้



Cryptology

Cryptology

- **คริปโทกราฟี (Cryptography)** เป็นการปฏิบัติและการศึกษาเกี่ยวกับการซ่อนข้อมูล โดยใช้เทคนิคและวิธีการต่างๆ เพื่อทำให้ข้อมูลเป็นความลับและป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

- **การวิเคราะห์คริปโทกราฟี (Cryptanalysis)** เป็นการศึกษาเกี่ยวกับวิธีการในการรับรู้ความหมายของข้อมูลที่ถูกเข้ารหัส โดยการศึกษาและวิเคราะห์เทคนิคและวิธีการต่างๆ เพื่อให้สามารถแก้ไขหรือเข้าใจข้อมูลที่ถูกเข้ารหัสได้

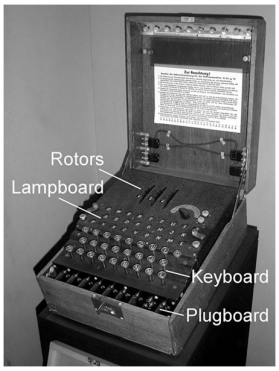
Classic Cryptos

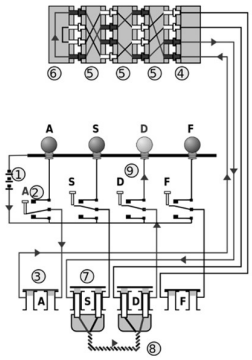
Scytale

Caesar Cipher

Classic Crypto Device

Enigma Machine





Modern Cryptos

Symmetric/Secret Key Cryptography

Decipher() = Encipher()-1

DES (p{64}:k{56})

3DES (p{64}:k{112|168})

c = E(D(E(p,k1),k2),k3)

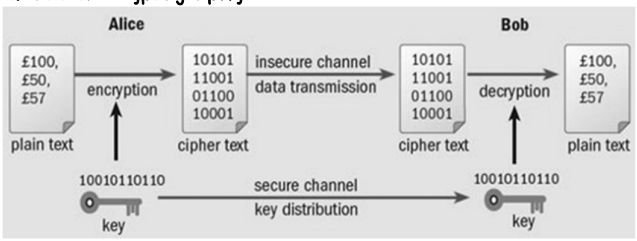
p = D(E(D(c,k3),k2),k1)

AES (p{128}:k{128|192|256})

Asymmetric/Public Key Cryptography

Physical Crypto

Quantum Cryptography

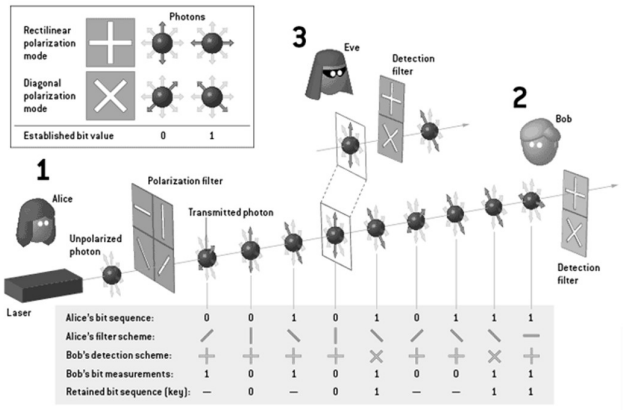


Quantum Key Distribution (QKD)

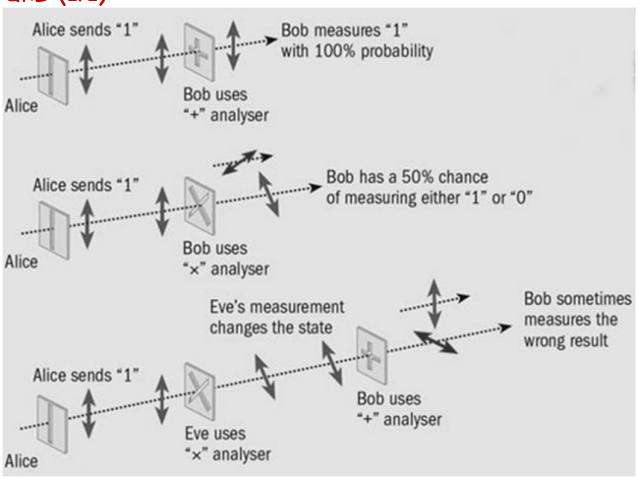
Polarization of Photon

No-cloning theorem

QKD (1/2)



QKD (2/2)



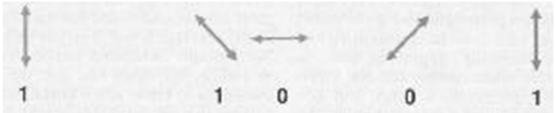
Alice sends

Bob chooses

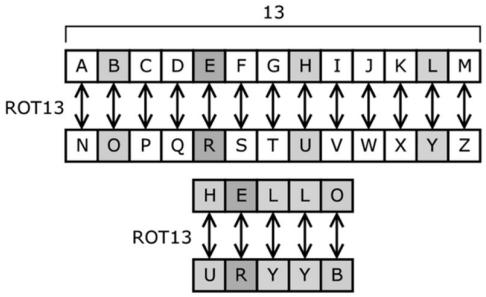
Bob gets

Bob and Alice exchange

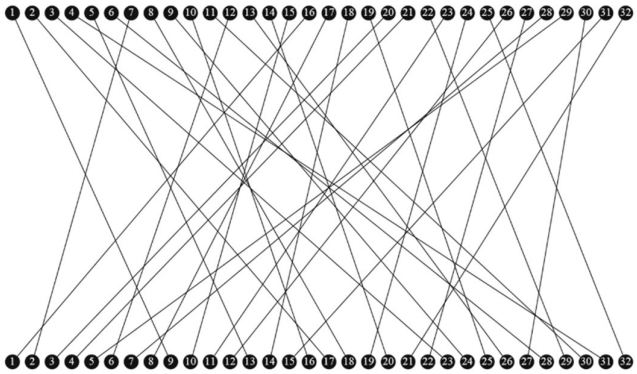
They share



Substitution Cipher



Permutation Cipher

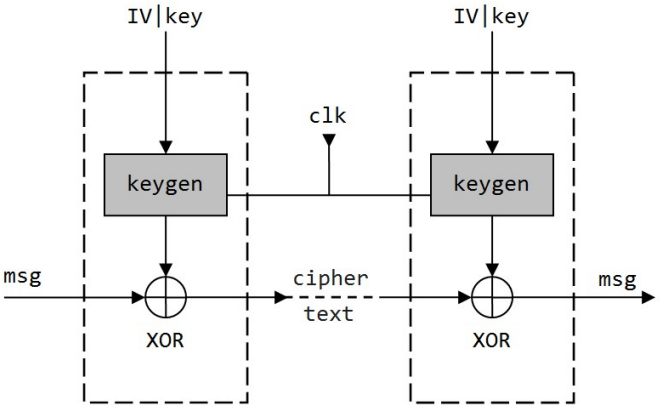


One-Time Pad

	H	E	L	L	O	**message**
	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	message (as numbers)
+	**24 (Y)**	**12 (M)**	**2 (C)**	**18 (S)**	**11 (L)**	**key**
=	31	16	13	29	25	message + key
=	5 (F)	16 (Q)	13 (N)	3 (D)	25 (Z)	message + key (mod 26)
	F	Q	N	D	Z	→ **ciphertext**

	F	Q	N	D	Z	**ciphertext**
	5 (F)	16 (Q)	13 (N)	3 (D)	25 (Z)	ciphertext (as numbers)
-	**24 (Y)**	**12 (M)**	**2 (C)**	**18 (S)**	**11 (L)**	**key**
=	-19	4	11	-15	14	ciphertext - key
=	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	ciphertext - key (mod 26)
	H	E	L	L	O	→ **message**

Stream Cipher



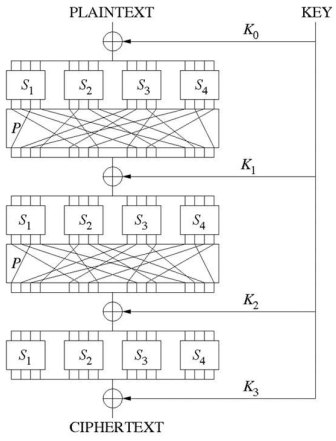
Block Cipher

|pil=|K0..nl=|cil

KEY gives K0 .. Kn

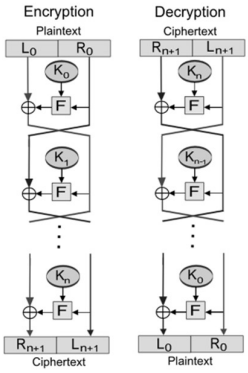
Sx are substitutions

P is permutation



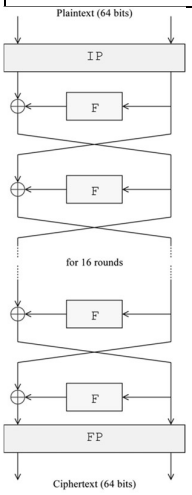
Feistel Cipher

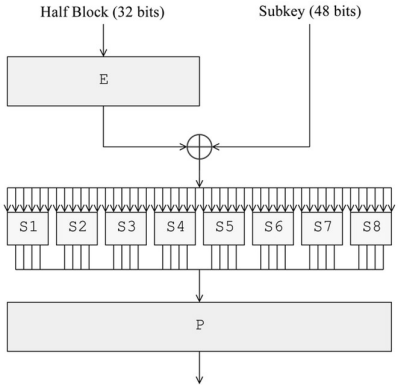
Encipher	Decipher
p = L0 | R0	c = Rn+1 | Ln+1
Li+1 = Ri	Ri = Li+1
Ri+1 = Li ⊕ F(Ri,Ki)	Li = Ri+1 ⊕ F(Li+1,Ki)



DES

DES : Overall (1/3)	DES : Feistel Function (2/3)
|Data| = 64 bits	Expansion
|Key| = 56 bits (why?)	32-bits TO 48-bits
IP = FP^{-1}	S-$Box_{1..8}$
	6-bits TO 4-bits





DES : Key Schedule (3/3)

Key & Subkeys

PC1

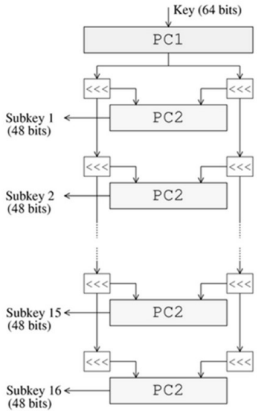
64-bits TO 56-bits

56-bits TO two 28-bits

PC2

28-bits TO 24-bits

Two 24-bits TO 48-bits



DES (Data Encryption Standard) ไม่เป็นระบบการเข้ารหัสที่ปลอดภัย เนื่องจาก..

- ความยาวของคีย์ 56 บิตสั้นเกินไป! ความยาวคีย์ของ DES เป็น 56 บิตซึ่งถือว่าสั้นเกินไปในปัจจุบัน ทำให้ง่ายต่อการโจมตีแบบค้นพบคีย์ (brute-force attack) และการโจมตีแบบรู้คีย์บางส่วน (known-plaintext attack)
- การมีส่วนร่วมของ NSA ในการออกแบบ S-Box: นักวิเคราะห์ความปลอดภัยได้พบว่า NSA เข้ามามีส่วนร่วมในการออกแบบ S-Box ใน DES ซึ่งเป็นส่วนที่ทำหน้าที่ในกระบวนการเข้ารหัส การมีส่วนร่วมของ NSA ก่อให้เกิดความคิดสงสัยเกี่ยวกับความปลอดภัยและความเชื่อถือใน DES

ดังนั้น.. เราจะรอดอยู่ได้อย่างไร?

- ความยาวของคีย์ที่เหมาะสม: เพื่อป้องกันการโจมตีแบบค้นพบคีย์ ควรใช้คีย์ที่มีความยาวใหญ่พอที่จะยากต่อการค้นพบคีย์ โดยในปัจจุบันคีย์ที่มีความยาว 128 บิตหรือมากกว่าจะถือว่าปลอดภัยอย่างมั่นคง
- เลือกใช้ระบบการเข้ารหัสที่เป็นที่เชื่อถือได้: การเลือกใช้ระบบการเข้ารหัสที่ผ่านการตรวจสอบและเชื่อถือได้ เช่น AES (Advanced Encryption Standard) ที่ใช้คีย์ความยาว 128, 192, หรือ 256 บิต เป็นต้น

Computer Security Cryptography (2/3)

Triple Data Encryption Algorithm

3DES / Triple DES / Triple DEA / TDEA

$c = E(D(E(p,k_1),k_2),k_3)$

$p = D(E(D(c,k_3),k_2),k_1)$

If $k_1 \neq k_2 \neq k_3$ then it's 168-bits.

If $k_1 \neq k_2$ but $k_1 = k_3$ then it's 112-bits.

Advanced Encryption Standard

1977 – DES

1998 – 3DES

2001 – AES

By NIST, not NSA (?)

Derived from Square Cipher (1997)

Final round (Speed/Space vs Strength)

MARS, RC6, Twofish, Serpent, and Rijndael

Vincent Rijmen and Joan Daemen from BE

p{128}:k{128|192|256}

AES in big picture

AES-128

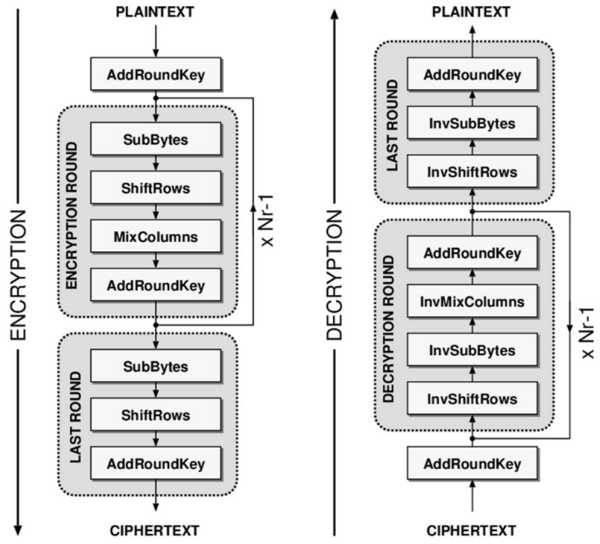
- 10 rounds

AES-192rounds

- 12 rounds

AES-256

- 14 rounds



Block Ciphers and ...

- **Padding:** การเติมข้อมูลในบล็อกเพื่อให้ขนาดของบล็อกเหมาะสมกับการใช้งานของระบบการเข้ารหัสแบบบล็อกไซเฟอร์ ซึ่งใช้เพื่อให้ข้อมูลมีความยาวที่ถูกต้องตามข้อกำหนด
- **Modes of Operation:** วิธีการใช้งานระบบการเข้ารหัสแบบบล็อกไซเฟอร์ในการปรับปรุงความปลอดภัยและการใช้งาน มีหลายโหมด เช่น ECB (Electronic Codebook), CBC (Cipher Block Chaining), CTR (Counter), เป็นต้น
- **Initialization Vector (IV):** ข้อมูลที่ถูกนำมาใช้ในกระบวนการเข้ารหัสแบบบล็อกไซเฟอร์เพื่อกำหนดสถานะเริ่มต้นของการเข้ารหัสในแต่ละบล็อก มีไว้เพื่อป้องกันการเข้ารหัสแบบซ้ำซ้อน
- **Message Integrity Code (MIC):** รหัสความถูกต้องของข้อมูล (MIC) เป็นรหัสที่สร้างขึ้นเพื่อตรวจสอบความถูกต้องและไม่ถูกแก้ไขของข้อมูล ใช้ในการรักษาความความปลอดภัยของข้อมูลที่ถูกส่งหรือเก็บรักษา
- **Message Authentication Code (MAC):** รหัสการตรวจสอบของข้อความ (MAC) เป็นรหัสที่สร้างขึ้นเพื่อตรวจสอบความถูกต้องและความสมบูรณ์ของข้อความ ใช้ในการรับรองความปลอดภัยและความน่าเชื่อถือของข้อมูล

Byte Padding

ANSI X.923

... | DD DD DD DD DD DD DD DD | DD DD DD DD 00 00 00 04 |
... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD DD 01 |

PKCS#7 (RFC 5652)

... | DD DD DD DD DD DD DD DD | DD DD DD DD 04 04 04 04 |
... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD DD 01 |

ISO/IEC 7816-4

... | DD DD DD DD DD DD DD DD | DD DD DD DD 80 00 00 00 |
... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD DD 80 |

Zero padding

... | DD DD DD DD DD DD DD DD | DD DD DD DD 00 00 00 00 |
... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD DD 00 |

What if data blocks are ...

Case #1

... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD DD DD |

Case #2

... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD 04 04 |
... | DD DD DD DD DD DD DD DD | DD DD DD DD DD DD DD 01 |
... | DD DD DD DD DD DD DD DD | 00 00 00 00 00 00 00 00 |

Modes of Operation

Electronic codebook (ECB): ECB เป็นโหมดการทำงานของระบบการเข้ารหัสแบบบล็อกไซเฟอร์ที่แต่ละบล็อกข้อมูลถูกเข้ารหัสโดยตัวเข้ารหัสเดียวกัน การใช้ ECB อาจทำให้เกิดปัญหาความปลอดภัยเนื่องจากข้อมูลที่เหมือนกันจะถูกเข้ารหัสในลักษณะที่เหมือนกันเช่นกัน

Cipher-block chaining (CBC): CBC เป็นโหมดการทำงานของระบบการเข้ารหัสแบบบล็อกไซเฟอร์ที่ข้อมูลของแต่ละบล็อกถูกผ่านกระบวนการ XOR กับบล็อกก่อนหน้าเพื่อเพิ่มความสุ่มในการเข้ารหัส โดยต้องใช้ Initialization Vector (IV) เพื่อกำหนดสถานะเริ่มต้นของกระบวนการ

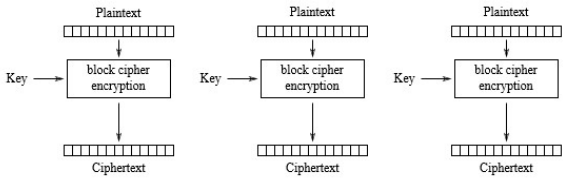
Cipher feedback (CFB): CFB เป็นโหมดการทำงานของระบบการเข้ารหัสแบบบล็อกไซเฟอร์ที่ใช้ผลลัพธ์ของการเข้ารหัสก่อนหน้าเป็นตัวเข้ารหัสสำหรับบล็อกถัดไป โดยอาจใช้ในการเข้ารหัสและถอดรหัสบล็อกเดียวหรือบล็อกหลายๆ บล็อก

Output feedback (OFB): OFB เป็นโหมดการทำงานของระบบการเข้ารหัสแบบบล็อกไซเฟอร์ที่ใช้ผลลัพธ์ของการเข้ารหัสก่อนหน้าเป็นตัวกำหนดสำหรับการทำ XOR กับข้อมูลที่จะถูกเข้ารหัส โดยไม่ต้องใช้การเข้ารหัสและถอดรหัสบล็อกในลำดับต่อเนื่อง

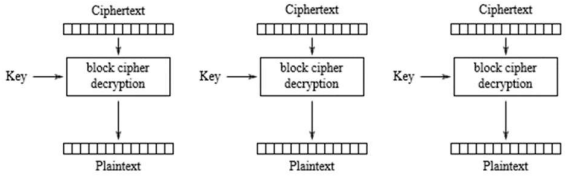
Counter (CTR): CTR เป็นโหมดการทำงานของระบบการเข้ารหัสแบบบล็อกไซเฟอร์ที่ใช้การเพิ่มค่า Counter แทนการใช้ IV ในการกำหนดสถานะ

เริ่มต้นของการเข้ารหัส โดยบล็อกที่จะถูกเข้ารหัสจะถูกนำไป XOR กับค่า Counter ที่ถูกเพิ่มขึ้นเรื่อยๆ ในลำดับเพื่อให้ได้ผลลัพธ์ของการเข้ารหัส

Electronic codebook (ECB)

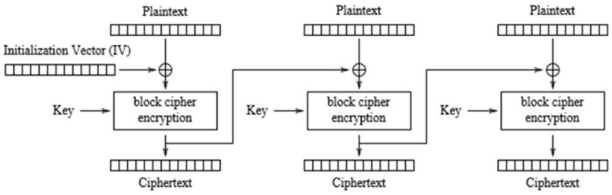


Electronic Codebook (ECB) mode encryption

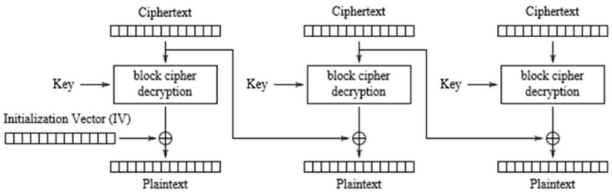


Electronic Codebook (ECB) mode decryption

Cipher-block chaining (CBC)

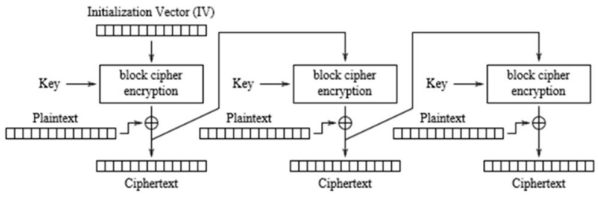


Cipher Block Chaining (CBC) mode encryption

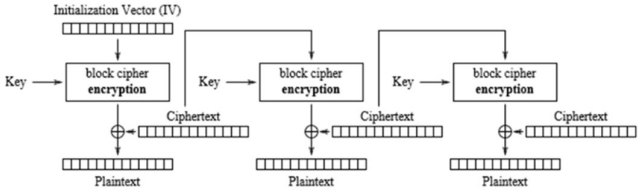


Cipher Block Chaining (CBC) mode decryption

Cipher feedback (CFB)

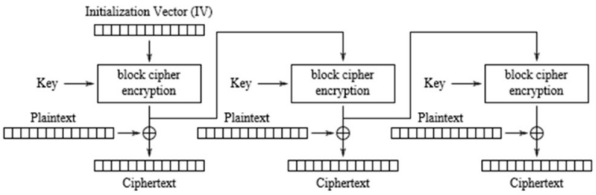


Cipher Feedback (CFB) mode encryption

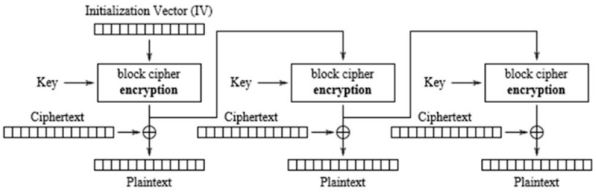


Cipher Feedback (CFB) mode decryption

Output feedback (OFB)

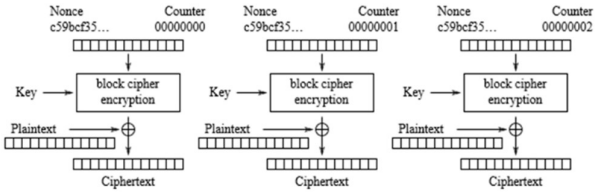


Output Feedback (OFB) mode encryption

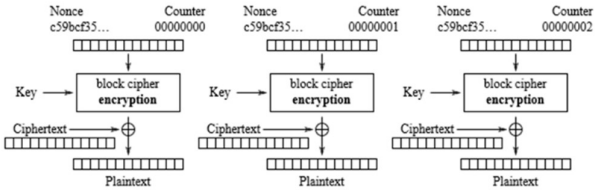


Output Feedback (OFB) mode decryption

Counter (CTR)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Initialization Vector (IV)

Random Block

- Lack of any pattern
- Be sent along with Ciphertext blocks

Random Number Generator (RNG)

- True Random (Physical Methods)
  - Noise
  - Entropy
- Pseudo Random (Computational Methods)
  - PRNG
  - Seed

IV-like

Cryptographic nonce

- Arbitrary number used only once in a cryptographic communication to prevent the Replay Attacks

Salt

- Short additional data for one-way function to defend against the Dictionary Attacks and the Pre-computed Table Attacks

Message Integrity Code (MIC)

MIC = H(m); H() is cryptographic hash function which is

Infeasible to generate a message that has a given hash (Pre-image Resistance; One-Way)

Infeasible to modify a message without changing the hash (Second pre-image Resistance; Strong Avalanche)

Infeasible to find two different messages with the same hash. (Strong Collision Resistance)

Cryptographic hash functions

SHA-1

160-bit MIC

SHA-256

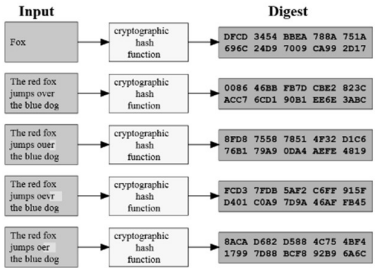
256-bit MIC

SHA3-512

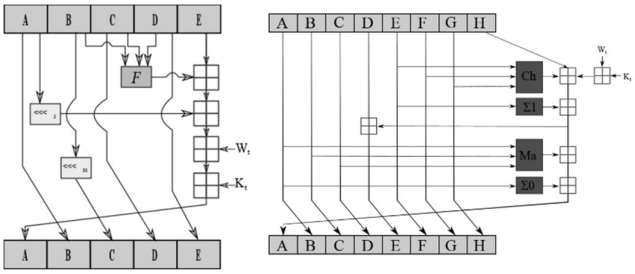
512-bit MIC

MIC ~ Digest

MIC ~ MD



SHA-1 vs SHA2

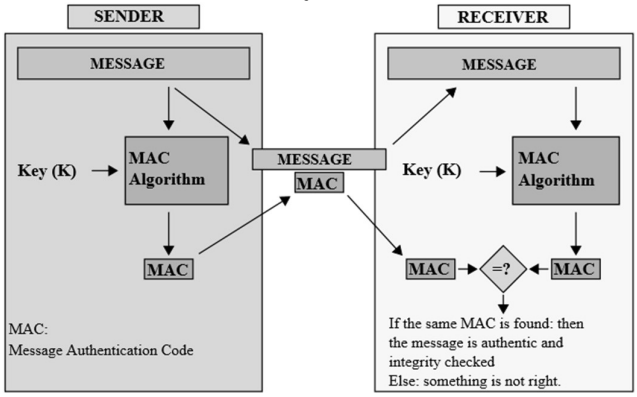


Wt = message word of round t

Kt = constant of round t

Message Authentication Code (MAC)

MAC = H(m,K); K is the MIC guardian

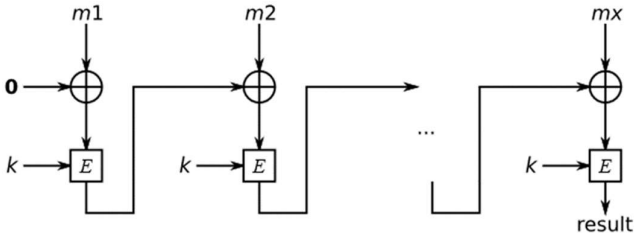


MAC functions

HMAC(K,m)

H((K □ opad)IH((K □ ipad)Im))

CMAC or CBC-MAC



Computer Security Cryptography (3/3)

Key Distribution Problems

Too many parties = Too many keys

Key Distribution Center ... how to trust?

Secure communication w/ strangers?

Public Key Cryptography

Number Theory (ทฤษฎีจำนวน): เป็นสาขาของคณิตศาสตร์ที่ศึกษาเกี่ยวกับคุณสมบัติและความสัมพันธ์ของจำนวนเต็ม

Modular Arithmetic (การเลขานิยามแบบโมดูลาร์): เป็นการดำเนินการทางคณิตศาสตร์ที่เกี่ยวข้องกับการหาเศษของการหาร

Prime numbers (จำนวนเฉพาะ): เป็นจำนวนเต็มที่มีเพียงสองจำนวนที่หารลงตัวคือ 1 และตัวเอง

RSA: RSA เป็นระบบการเข้ารหัสและถอดรหัสแบบกุญแจสาธารณะ ที่ใช้คู่ของกุญแจ (กุญแจสาธารณะและกุญแจส่วนตัว) เพื่อเข้ารหัสและถอดรหัสข้อมูล

Encryption/Decryption (การเข้ารหัส/การถอดรหัส): เป็นกระบวนการในการเปลี่ยนแปลงข้อมูลให้เป็นรูปแบบที่เข้ารหัสหรือถอดรหัสได้

Digital Signatures (ลายเซ็นดิจิตอล): เป็นวิธีการที่ใช้ในการยืนยันความถูกต้องและความเป็นจริงของข้อมูลหรือเอกสารที่ส่งหรือรับผ่านทางอินเทอร์เน็ต โดยใช้คู่ของกุญแจ (กุญแจสาธารณะและกุญแจส่วนตัว)

Modular Arithmetic

n e Z^+, n >= 2

x e Z

x modulo n

x mod n

x (mod n)

x (mod 12)

0 = 12 = 24 = 36 ...

1 = 13 = 25 = 37 ...

-1 = 11, -2 = 10, -3 = 9 ...

Modular Addition:

x + y (mod 10)

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Modular Addition: Additive Inverse

x + (-x) = 0 (mod n)

4 + (6) = 0 (mod 10)

EnKey=4, DeKey=6

Encipher: m+4 = c (mod 10)

Decipher: c+6 = m (mod 10)

Sound? Indeed

Safe? Definitely NOT

Modular Multiplication: x □ y(mod 10)

.	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	2	3	2	1

Modular Multiplication: Multiplicative Inverse

x . (x-1) = 1 (mod n)

7 .(3) = 1 (mod 10)

EnKey=7, DeKey=3

Encipher: m.7 = c (mod 10)

Decipher: c.3 = m (mod 10)

Sound? Useable Keys = {1, 3, 7, 9}

Safe? Nope – Euclid's Algorithm

Relatively Prime and o (n)

Relatively primes to n have multiplicative inverse (mod n)

GCD(x, n) = 1; x < n

1, 3, 7, and 9 are relatively prime to 10

Totient function: o(n)

|{x e Z^+ ^ x<n | GCD(x,n)=1}|

o(10) = |{1,3,7,9}| = 4

If n is prime, □(n) = |{1,2,3,…,n-1}| = n-1

If p and q are prime and n=pq,

o(pq) =|{1,2,…,(pq)-1}|=pq-(p+q-1)=(p-1)(q-1)

Modular Exponentiation: x^y (mod 10)

x^y	0	1	2	3	4	5	6	7	8	9	10	11	12
0		0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	6	2	4	8	6	2	4	8	6
3	1	3	9	7	1	3	9	7	1	3	9	7	1
4	1	4	6	4	6	4	6	4	6	4	6	4	6
5	1	5	5	5	5	5	5	5	5	5	5	5	5
6	1	6	6	6	6	6	6	6	6	6	6	6	6
7	1	7	9	3	1	7	9	3	1	7	9	3	1
8	1	8	4	2	6	8	4	2	6	8	4	2	6
9	1	9	1	9	1	9	1	9	1	9	1	9	1

Modular Exponentiation: Useful properties

xy (mod n) != xy+n (mod n)

xy (mod n) = x(y mod o(n)) (mod n)

n must be square free!

y = 1 (mod o(n))

RSA: Rivest, Shamir, Adleman

Choose distinct prime numbers p and q

n = pq

o(n) = (p-1)(q-1)

Choose e then d (w/ some conditions)

e . d = 1 (mod o(n))

e is public key exponent

d is private key exponent

As x^ed = x (mod n) and m<n

Encipher: c □ me (mod n) <e,n> is public key

Decipher: m □ cd (mod n) <d,n> is private key

Encryption/Decryption

Alice has

<e,n> as PUBLIC key and announces it

<d,n> as PRIVATE key and keeps it secret

Bob wants to send m to Alice securely

Bob uses Alice's PUBLIC key to encipher

Alice gets the ciphertext from Bob

Alice uses Alice's PRIVATE key to decipher

Digital Signatures

Alice wants to sign digital content then send to Bob

Alice computes MD from that content

Alice signs MD with her own PRIVATE key

Bob gets the digital content from Alice

Bob computes MD' from received content

Bob computes MD from signed MD with Alice's PUBLIC key

Bob compares MD with MD'

The Solutions

- PKI (Public Key Infrastructure) (พื้นฐานสาธารณะ):
เป็นโครงสร้างระบบที่ใช้ในการจัดการกุญแจสาธารณะและใบรับรองดิจิทัล ซึ่งมุ่งเน้นในการให้บริการที่เกี่ยวข้องกับการเข้ารหัสและเอกสารดิจิทัล

- Certificates (ใบรับรองดิจิทัล):
เป็นข้อมูลที่เก็บรวบรวมข้อมูลประจำตัวของผู้ใช้และกุญแจสาธารณะ เพื่อให้ผู้ใช้สามารถยืนยันตัวตนและให้ความเชื่อถือในการสื่อสารอิเล็กทรอนิกส์

- CA (Certificate Authority) (หน่วยความปลอดภัย):
เป็นองค์กรหรือบริษัทที่มีหน้าที่ออกใบรับรองดิจิทัล ซึ่งตรวจสอบและรับรองตัวตนของผู้ใช้และองค์กร

- Root CA (Root Certificate Authority) (หน่วยความปลอดภัยราก):
เป็น CA ระดับสูงสุดในโครงสร้าง PKI ซึ่งออกใบรับรองดิจิทัลสำหรับ Intermediate CA และองค์กรอื่น ๆ

- Intermediate CA (Intermediate Certificate Authority) (หน่วยความปลอดภัยระหว่าง):
เป็น CA ระดับกลางที่รับรองใบรับรองดิจิทัลสำหรับองค์กรและบุคคล

- CRL (Certificate Revocation List) (รายการการเพิกถอนใบรับรอง):
เป็นรายการที่บอกถึงใบรับรองดิจิทัลที่ถูกเพิกถอนและไม่ถูกยอมรับในระบบ PKI

Computer Security Physical Security

Threat Types (ประเภทของความเสี่ยง): เป็นการแบ่งประเภทของความเสี่ยงที่อาจเกิดขึ้นต่อระบบหรือข้อมูล

- Environmental Threats (ความเสี่ยงจากสิ่งแวดล้อม):
เป็นความเสี่ยงที่เกิดจากสิ่งแวดล้อมรอบตัว เช่น น้ำ/ความชื้น ฝุ่น อุณหภูมิ แหล่งจ่ายพลังงาน/การกระพริบแสงสายฟ้า

- Water / Humidity (น้ำ/ความชื้น): ความเสี่ยงที่เกิดจากน้ำหรือความชื้นที่สามารถทำให้ระบบหรืออุปกรณ์เสียหาย

- Dust (ฝุ่น): ความเสี่ยงที่เกิดจากฝุ่นที่สามารถเข้าสะดุดเข้าสู่ระบบหรืออุปกรณ์และทำให้เกิดความเสียหาย

- Temperature (อุณหภูมิ): ความเสี่ยงที่เกิดจากอุณหภูมิที่ไม่เหมาะสมสำหรับระบบหรืออุปกรณ์และอาจทำให้เกิดความเสียหาย

- Power Source / Lightning (แหล่งจ่ายพลังงาน/การกระพริบแสงสายฟ้า): ความเสี่ยงที่เกิดจากปัญหาที่เกี่ยวข้องกับแหล่งจ่ายพลังงานหรือการกระพริบแสงสายฟ้า อาจทำให้ระบบไฟฟ้าเสียหายหรือข้อมูลสูญหาย

- Human Life FIRST, Computers LATER! (ชีวิตมนุษย์มาก่อน, คอมพิวเตอร์หลัง): เป็นคติที่เน้นความสำคัญของชีวิตมนุษย์เป็นหลักในการจัดการความเสี่ยง

- Malicious Threats (ความเสี่ยงที่เกิดจากการทรมาน): เป็นความเสี่ยงที่เกิดจากการทรมานที่ตั้งใจเพื่อทำความเสียหายต่อระบบหรือองค์กร

- Physical Attack (site/building) (การโจมตีทางกายภาพ (สถานที่/อาคาร)): ความเสี่ยงที่เกิดจากการโจมตีทางกายภาพต่อที่ตั้งหรืออาคารที่มีความสำคัญสำหรับระบบหรือองค์กร

- Sabotage (การทำลายตามหากำลังงาน): ความเสี่ยงที่เกิดจากการทำลายหรือยึดครองแหล่งกำลังงานของระบบหรือองค์กร

- Vandalism (การทำลายทรัพย์สิน): ความเสี่ยงที่เกิดจากการทำลายทรัพย์สินต่างๆ ของระบบหรือองค์กร เช่น เครื่องจักร อุปกรณ์ต่างๆ

- **Arson (การลักไฟ):** ความเสี่ยงที่เกิดจากการลักไฟที่สามารถทำลายระบบหรืออาคารขององค์กร
- **Theft (การโจรกรรม):** ความเสี่ยงที่เกิดจากการโจรกรรมทรัพย์สินหรือข้อมูลที่สำคัญของระบบหรือองค์กร

Small Devices, BIG Problems! (อุปกรณ์เล็ก ปัญหาใหญ่): การเน้นความสำคัญของอุปกรณ์เล็กๆ ที่อาจเป็นตัวที่สร้างปัญหาใหญ่ในระบบ

- **Accidental Threats (ความเสี่ยงที่เกิดจากการไม่ได้ตั้งใจ):** เป็นความเสี่ยงที่เกิดขึ้นจากความไม่ระมัดระวังหรือความผิดพลาดที่เกิดขึ้นโดยไม่ได้ตั้งใจ
- **Insiders' Ignorance (ความไม่รู้ของบุคคลภายใน):** ความเสี่ยงที่เกิดจากความไม่รู้หรือความไม่เข้าใจที่เกิดขึ้นกับบุคคลที่เป็นส่วนหนึ่งขององค์กร
- **Outsiders' Mistake (ความผิดพลาดของบุคคลภายนอก):** ความเสี่ยงที่เกิดจากความผิดพลาดที่เกิดขึ้นกับบุคคลภายนอกที่มีความเกี่ยวข้องกับองค์กร
- **Expect the Unexpected! (คาดการณ์สิ่งที่ไม่คาดคิด):** การเตรียมตัวเผื่อความเป็นไปได้ที่ไม่คาดคิดเพื่อเตรียมรับมือกับสถานการณ์ที่อาจเกิดขึ้นได้

Site Location

Standalone VS Shared (ตั้งเอง VS แบ่งใช้ร่วมกับผู้อื่น): เลือกตั้งสถานที่เป็นแบบตั้งเองหรือแบ่งใช้ร่วมกับผู้อื่น

Rural VS Urban (ชนบท VS เมือง): เลือกตั้งสถานที่ในพื้นที่ชนบทหรือในเมือง

Natural Disaster & Civil Chaos (ภัยธรรมชาติและความวุ่นวายทางการปกครอง): พิจารณาความเสี่ยงจากภัยธรรมชาติ เช่น ภัยพิบัติธรรมชาติ และความวุ่นวายทางการปกครอง

Infrastructure & Emergency (สาธารณูปโภคและสถานการณ์ฉุกเฉิน): พิจารณาสถานการณ์สาธารณูปโภคและความพร้อมในกรณีฉุกเฉิน

Layered Defense Model (โมเดลการป้องกันแบบชั้น):

Outermost perimeter (เขตเส้นขนานนอกสุด): เป็นชั้นความปลอดภัยที่ตั้งอยู่ภายนอกสุดของระบบ มีบทบาทในการกรองและป้องกันการเข้าถึงจากภายนอก

Inner perimeters (เขตเส้นขนานภายใน): เป็นชั้นความปลอดภัยที่ตั้งอยู่ภายในเขตเส้นขนานนอกสุด มีบทบาทในการควบคุมและกำกับการเข้าถึงในเขตภายในระบบ

Restricted areas (พื้นที่ที่มีการจำกัด): เป็นชั้นความปลอดภัยที่จำกัดการเข้าถึงในพื้นที่ที่มีความสำคัญสูง อาจเป็นการใช้มาตรการเข้ารหัสหรือการตรวจสอบและติดตามกิจกรรม

Wireless (การเชื่อมต่อแบบไร้สาย): เป็นแง่มุมที่ต้องคำนึงถึงในเรื่องความปลอดภัยเมื่อมีการใช้เทคโนโลยีการเชื่อมต่อแบบไร้สาย ต้องมีการใช้เทคนิคและมาตรการที่เหมาะสมเพื่อป้องกันการบุกรุกหรือการดักรับข้อมูล

Procedural Controls (การควบคุมแบบกระบวนการ):

Guard Posts (จุดควบคุม): เป็นจุดที่ตั้งคนรักษาการความปลอดภัยซึ่งมีหน้าที่ควบคุมการเข้า-ออกของบุคคลหรือรถยนต์ที่สถานที่ มักมีการตรวจสอบและบันทึกข้อมูลเกี่ยวกับผู้เข้า-ออก

Visitors (ผู้มาเยือน): มีการควบคุมการเข้าถึงของผู้มาเยือน เช่น ต้องลงทะเบียน เวลาเข้าออก และมีการจำกัดสิทธิ์การเข้าถึงในบริเวณที่จำกัด

Deliveries (incoming & outgoing) (การจัดส่งสินค้า (ขาเข้าและขาออก)): มีการควบคุมและตรวจสอบการจัดส่งสินค้าที่เข้า-ออกขององค์กร เพื่อให้มั่นใจว่าสินค้าที่เข้า-ออกเป็นไปตามกฎระเบียบและมีความปลอดภัย

Infrastructure Support Systems (ระบบสนับสนุนโครงสร้างพื้นฐาน):

Health and Safety legislation (กฎหมายเกี่ยวกับสุขภาพและความปลอดภัย): มีการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับสุขภาพและความปลอดภัยเพื่อให้สถานที่มีการทำงานที่ปลอดภัยและเป็นสุขภาพสำหรับพนักงาน

Power / UPS / RFI (พลังงาน / ระบบสำรอง / การรบกวนคลื่นวิทยุ): มีการจัดการและสนับสนุนระบบพลังงาน รวมถึงระบบสำรอง (UPS) และการรบกวนคลื่นวิทยุ (RFI) เพื่อให้มีการจ่ายไฟต่อเนื่องและป้องกันการรบกวนทางไฟฟ้า

HVAC: Heating, Ventilation, Air-Con (ระบบทำความร้อน, ระบบระบายอากาศ, ระบบปรับอากาศ): มีการใช้ระบบทำความร้อน, ระบบระบายอากาศ, และระบบปรับอากาศ เพื่อให้สถานที่มีสภาพแวดล้อมที่เหมาะสมสำหรับการทำงานและสื่อสาร

Emergency SHUTDOWN (การปิดระบบฉุกเฉิน): มีการกำหนดและฝึกฝนกระบวนการปิดระบบในกรณีฉุกเฉิน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในสถานการณ์ฉุกเฉิน

Fire – Prevention / Detection / Suppression (การป้องกัน / ตรวจจับ / ปราบไฟ): มีการใช้มาตรการป้องกันไฟไหม้, ระบบตรวจจับไฟไหม้, และระบบปราบไฟไหม้ เพื่อลดความเสี่ยงจากเหตุการณ์ไฟไหม้

Boundary Protection (การป้องกันขอบเขต): มีการกำหนดและติดตั้งมาตรการป้องกันขอบเขตของสถานที่ เช่น ผนังกั้น, ประตูเข้า-ออก เพื่อความปลอดภัยและการควบคุมการเข้าถึงสถานที่

Walls (ผนังกั้น): มีการติดตั้งผนังกั้นเพื่อกำหนดขอบเขตและป้องกันการเข้าถึงที่ไม่เหมาะสม

Entry & Exit points (จุดเข้า-ออก): มีการกำหนดจุดเข้า-ออกที่มีการควบคุมเพื่อรักษาความปลอดภัย และมีการตรวจสอบผู้เข้า-ออกเพื่อให้เข้าถึงเฉพาะบุคคลที่มีสิทธิ์

Building Entry Points

Keys and Locking Systems

Walls, Doors, and Windows

- Door Design / Materials
- Window Glass / Types

Access Controls

- Tokens / PIN / Bio

CCTV

PHY IDS

Portable Devices and Assets

Information Protection and Management Services

Managed Services

- Outsourcing services

Audits, Exercises, and Testing

Vulnerability and Penetration Tests

- Social engineering / Challenging

Maintenance and Service Issues

Education / Training / Awareness ...

DNS :

ระบบชื่อโดเมน (Domain Name System : DNS) เป็นระบบการตั้งชื่อแบบลำดับชั้นที่ใช้กับทุกเอกลักษณ์ที่เชื่อมต่อกับอินเทอร์เน็ตหรือเครือข่ายส่วนตัว เช่น อุปกรณ์หรือบริการเทคโนโลยีทำหน้าที่เป็นสื่อกลางระหว่างผู้ใช้และเว็บเบราว์เซอร์ ซึ่งโดยปกติแล้วจะทำงานร่วมกับแม่แบบชื่อโดเมนที่น่าจดจำในขณะที่ IP addresses ใช้เพื่อสื่อสารกับบริการอื่น ๆ ผ่านอินเทอร์เน็ต ด้วยเหตุนี้ DNS จึงไม่จำเป็นต้องให้ผู้ใช้จดจำ IP addresses ที่ไม่ซ้ำกัน ซึ่งมักถูกเรียกว่า "สมุดโทรศัพท์ของอินเทอร์เน็ต" DNS ช่วยให้ผู้ใช้สามารถจำที่อยู่เว็บไซต์ได้ เช่น www.itpro.co.uk แทนที่จะเป็นจำนวนชุดหมายเลข ตัวคั่นด้วยจุดในกรณีของ IPv4 หรือเครื่องหมายทวิภาคในกรณีของ IPv6

Port scanning :

Port scanning คือกระบวนการที่ใช้ในการติดต่อไปที่Portของ TCP หรือ UDP ของเครื่องเป้าหมายและมีจุดประสงค์เพื่อตรวจสอบเพื่อหาบริการที่ระบบรอรับการเชื่อมต่อหรืออยู่ในสถานะที่ให้บริการโดยมีจุดประสงค์อื่น ๆ ดังนี้

- ค้นหาserviceที่ทำงานอยู่บนProtocol TCP หรือ UDP ว่ามีServicesไหนทำงานอยู่ เช่น http ที่port 80 เป็นต้น
- ค้นหาประเภทของระบบปฏิบัติการ(OS) ที่อยู่บนเครื่องเป้าหมาย
- ค้นหาApplicationที่ทำงานบนเครื่องเป้าหมาย เช่น

Indicators of Compromise (IOCs) หมายถึงข้อมูลหรือสัญญาณที่เกี่ยวข้องกับการโจมตีหรือกิจกรรมที่เป็นอันตรายที่อาจเกิดขึ้น ซึ่งสามารถใช้ในการตรวจหาเหตุการณ์การละเมิดความปลอดภัยหรือการบุกรุก การรู้จักและเข้าใจเกี่ยวกับ IOCs เป็นสิ่งสำคัญสำหรับทีมตอบสนองเหตุการณ์ฉุกเฉิน ต่อไปนี้เป็นข้อมูลสำคัญเกี่ยวกับ IOCs สำหรับการตอบสนองเหตุการณ์ฉุกเฉิน:

ประเภทของ IOCs:

- Malware IOCs: ซับซ้อนไปยังรูปแบบของไฟล์ที่มีลักษณะเฉพาะของซอฟต์แวร์ที่เป็นอันตราย เช่น ลายเซ็นดิจิตอลของไฟล์มัลแวร์หรือฮาชิด (Hash), ซิกเนเจอร์ (Signature), และแอตทริบิวต์ (Attributes) ของไฟล์
- Network IOCs: ข้อมูลที่เกี่ยวข้องกับการเชื่อมต่อเครือข่ายที่อาจแสดงถึงการทำงานของมัลแวร์หรือการโจมตี เช่น ที่อยู่ IP ของแหล่งที่มาที่ไม่ปกติ, พอร์ตที่ใช้งานที่ไม่สามารถอธิบายได้, และโมดูลการสื่อสารต่างๆ
- Behavioral IOCs: รูปแบบการกระทำที่เกี่ยวข้องกับการเข้าถึงหรือใช้งานที่ไม่เป็นปกติ เช่น การเปลี่ยนแปลงของไฟล์หรือทะเบียนข้อมูล (Exfiltration), การเริ่มต้นกระบวนการหรือบริการที่ไม่คาดคิด, และการเชื่อมต่อไปยังทรัพยากรหรือเครือข่ายที่ไม่เป็นปกติ

แหล่งข้อมูล IOCs:

- Threat Intelligence: ข้อมูลแหล่งการเผยแพร่เกี่ยวกับเหตุการณ์และรูปแบบการโจมตีที่อาจเกิดขึ้น ซึ่งสามารถใช้ในการตรวจหา IOCs เช่น บล็อกลิสต์ IP, ลิงก์ที่เป็นอันตราย, และลายเซ็นดิจิตอลที่เกี่ยวข้องกับมัลแวร์
- Log Data: บันทึกข้อมูลเหตุการณ์และกิจกรรมในระบบที่สามารถใช้เป็นตัวบ่งชี้สำหรับการละเมิดความปลอดภัย เช่น บันทึกเหตุการณ์การเข้าสู่ระบบ, บันทึกการส่งข้อมูลที่ไม่ปกติ, และบันทึกการเข้าถึงไฟล์ที่ผิดปกติ
- Incident Data: ข้อมูลเกี่ยวกับเหตุการณ์และความเสี่ยงที่เกิดขึ้นในอดีต เช่น รายงานการโจมตีที่เกิดขึ้น, สถิติการละเมิดความปลอดภัย, และรายละเอียดของการแก้ไขเหตุการณ์

กรณีละเมิด (Incident) และ ภัยอันตราย (Threat) คืออะไรพร้อมยกตัวอย่าง:

- กรณีละเมิด (Incident) คือเหตุการณ์ที่เกิดขึ้นที่มีความเสี่ยงต่อความปลอดภัยของระบบหรือข้อมูลในองค์กร ซึ่งอาจเป็นผลจากการแทรกแซงหรือการกระทำที่ไม่เหมาะสม ตัวอย่างของกรณีละเมิดอาจเป็นการรั่วไหลข้อมูลสำคัญ, การเข้าถึงไม่ได้รับอนุญาตในระบบ, การโจมตีด้วยมัลแวร์, หรือการแฮ็กเว็บไซต์ขององค์กร
- ภัยอันตราย (Threat) คือสิ่งที่มีความเสี่ยงที่อาจก่อให้เกิดความเสียหายหรือการละเมิดความปลอดภัย ภัยอันตรายอาจเป็นผู้กระทำที่ต้องการเข้าถึงข้อมูลสำคัญ, มัลแวร์ที่อาจทำลายระบบหรือข้อมูล, หรือช่องโหว่ในระบบที่อาจถูกใช้ในการโจมตี ตัวอย่างของภัยอันตรายอาจเป็นผู้บุกรุกแฮ็กเกอร์, ไวรัสคอมพิวเตอร์, หรือเครื่องมือแฮกกิ่ง (hacking tools) ที่ใช้ในการโจมตีระบบ

ตัวอย่างเช่น หากมีการเจาะระบบเครือข่ายขององค์กรโดยมีผู้ไม่ประสงค์ดีพยายามเข้าถึงข้อมูลลับ และเป็นผลให้ข้อมูลลับถูกเข้าถึงโดยไม่ได้รับอนุญาต ในกรณีนี้เราจะพูดถึงภัยอันตราย (Threat) ที่เป็นผู้กระทำ และกรณีละเมิด (Incident) ที่เกิดขึ้นเมื่อข้อมูลลับถูกเข้าถึงโดยไม่ได้รับอนุญาต เป็นตัวอย่างของกรณีละเมิด (Incident) ที่เกิดขึ้นจากภัยอันตราย (Threat) ที่เป็นผู้กระทำ ในกรณีนี้เราอาจพิจารณาว่าภัยอันตรายคือผู้ไม่ประสงค์ดีที่พยายามเข้าถึงข้อมูลลับ โดยอาจใช้เครื่องมือหรือวิธีการต่างๆ เพื่อเจาะระบบหรือรับข้อมูลที่ไม่เป็นสิทธิ์

อีกตัวอย่างหนึ่งคือ การโจมตีด้วยมัลแวร์ (Malware) เป็นภัยอันตรายที่เป็นไปได้มากในการเรียกใช้งานหรือทำลายระบบ โดยมัลแวร์อาจถูกแพร่กระจายผ่านทางอีเมลที่เป็นสแปม (spam email) หรือไฟล์แฝงที่อาจถูกดาวน์โหลดจากเว็บไซต์ที่เป็นอันตราย การเปิดไฟล์นี้อาจทำให้มัลแวร์เข้าสู่ระบบและทำความเสียหายให้กับเครื่องคอมพิวเตอร์

PenTest Report หรือ Penetration Test Report เป็นเอกสารที่จัดทำขึ้นหลังจากการทดสอบการแทรกแซงระบบ (Penetration Testing) เพื่อรายงานผลลัพธ์และความสามารถในการเจาะระบบของผู้ทดสอบหรือทีมงานที่ดำเนินการทดสอบ

- PenTest Report เป็นเอกสารที่มีประโยชน์สำหรับองค์กรหรือลูกค้าที่ได้รับการทดสอบการแทรกแซงระบบ โดยรายงานมีการระบุถึงทรัพยากรหรือระบบที่ทดสอบและแสดงผลลัพธ์ที่ได้รับจากการทดสอบ เช่น ช่องโหว่ที่พบและระดับความรุนแรงของแต่ละช่องโหว่ การบรรลุเป้าหมายที่ถูกกำหนด แนวทางแก้ไขหรือแนะนำที่เกี่ยวข้องกับการเสริมความปลอดภัยของระบบ
- การทำ PenTest Report รวมถึงการรายงานผลและสรุปความสามารถในการเจาะระบบ มีขั้นตอนหลายขั้นตอนเช่นการเก็บข้อมูลก่อนการทดสอบ เช่น ประวัติของระบบและองค์กร การสแกนและทดสอบการแทรกแซงระบบ การวิเคราะห์ผลลัพธ์ และการรวบรวมข้อมูลในรูปแบบของรายงานที่มีความชัดเจนและเป็นระเบียบ
- PenTest Report จะถูกส่งให้กับผู้ที่มีอำนาจในการตัดสินใจ เช่น เจ้าของระบบ ผู้ดูแลระบบ หรือทีมควบคุมความปลอดภัย มีการรายงานผลและแนะนำที่ช่วยให้ผู้รับรู้

สรุปแต่ละหัวข้อสั้นๆ:

PenTest Report เป็นเอกสารที่สรุปผลลัพธ์และความสามารถในการเจาะระบบหลังจากทดสอบการแทรกแซงระบบ (Penetration Testing) รายงานระบุทรัพยากรหรือระบบที่ทดสอบและแสดงผลลัพธ์ที่ได้รับจากการทดสอบ เช่น ช่องโหว่ที่พบและระดับความรุนแรงของแต่ละช่องโหว่

PenTest Report มีขั้นตอนหลายขั้นตอนเช่นการเก็บข้อมูลก่อนการทดสอบ การสแกนและทดสอบการแทรกแซงระบบ การวิเคราะห์ผลลัพธ์ และการรวบรวมข้อมูลในรูปแบบของรายงานที่มีความชัดเจนและเป็นระเบียบ

PenTest Report จะถูกส่งให้กับผู้ที่มีอำนาจในการตัดสินใจ เช่น เจ้าของระบบ ผู้ดูแลระบบ หรือทีมควบคุมความปลอดภัย

PenTest Report เป็นเครื่องมือสำคัญในการปรับปรุงความปลอดภัยของระบบและให้ข้อมูลสำคัญในการตัดสินใจเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยขององค์กร

HACKERRRRRRRRRR

- WiFi Secret-Key Cracking (การถอดรหัสลับของ WiFi): การพยายามคาดเดาหรือการแฮกเข้าสู่ระบบเครือข่าย WiFi โดยการลองทดสอบและค้นหาคีย์เข้ารหัส (encryption key) ของเครือข่าย WiFi เพื่อเข้าถึงการเชื่อมต่อและข้อมูลในเครือข่ายนั้น
- SQL Injection (การฉีดเติมโค้ด SQL): การโจมตีแบบหนึ่งที่ผู้โจมตีแทรกโค้ด SQL เข้าไปในแอปพลิเคชันหรือเว็บไซต์ ซึ่งอาจทำให้ผู้โจมตีสามารถเข้าถึงฐานข้อมูลหรือดำเนินการที่ไม่ได้รับอนุญาตในระบบ
- Offline Password Cracking (การลองถอดรหัสผ่านแบบออฟไลน์): การพยายามทดสอบและค้นหารหัสผ่านที่ถูกเข้ารหัสไว้ในรูปแบบที่ไม่สามารถอ่านได้อย่างเดิม โดยใช้เทคนิคการลองเดาหรือการปรับเปลี่ยนรหัสผ่านเพื่อทำให้สอดคล้องกับการเข้ารหัสที่ถูกใช้งาน
- TCP/UDP Port Scanning (การสแกนพอร์ต TCP/UDP): การสแกนและตรวจสอบพอร์ตเครือข่ายที่เปิดใช้งานบนเครือข่ายเพื่อหาพอร์ตที่เปิดและที่ปิด มีไวรัสหรือเครื่องมือที่ใช้ในการสแกนเพื่อหาจุดบกพร่องหรือจุดที่เปิดใช้งานเพื่อเข้าถึงเครือข่าย
- User Enumeration (การระบุผู้ใช้): การทดสอบและค้นหาข้อมูลเกี่ยวกับผู้ใช้ในระบบโดยการตรวจสอบว่าผู้ใช้งานเป็นที่มีอยู่จริง

Penetration Test

- Penetration Test Vs. Vulnerability Assessment
  - Penetration test คือการทดสอบเพื่อหาช่องทางในการเข้าถึงระบบ
  - Vulnerability Assessment คือ การประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบ
- Penetration tests are valuable for several reasons
  - Determining the feasibility of a particular set of attack vectors
  - Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence
  - Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
  - Assessing the magnitude of potential business and operational impacts of successful attacks
  - Testing the ability of network defenders to successfully detect and respond to the attacks
  - Providing evidence to support increased investments in security personnel and technology
- Black box vs. White box
  - การทำ Penetration Test จากภายนอกระบบเครือข่ายองค์กร หรืออาจเรียกว่าการทำ Black box คือ การใช้เครื่องคอมพิวเตอร์จำลองเป็นนักโจมตีระบบเพื่อหาทางเข้าสู่ระบบเครือข่ายองค์กรที่ให้ทำการประเมินความเสี่ยง
  - การทำ Penetration test ภายในองค์กร หรือจะเรียกว่า White box (ซึ่งการทำงานประเภทนี้ต้องได้รับความร่วมมือกับผู้ดูแลระบบของฝั่งผู้ใช้บริการ ตั้งแต่การให้แผนผังระบบเครือข่าย จำนวน IP Address ตลอดถึงรายละเอียดประเภทอุปกรณ์เครือข่ายที่เกี่ยวข้อง เป็นต้น) คือการทดสอบหาช่องโหว่ที่พบจากการใช้งานไอซีทีในองค์กรเพื่อประเมินช่องโหว่และทำการปิดกั้นช่องโหว่ที่ค้นพบขึ้นเพื่อไม่เกิดปัญหาขึ้นในระยะยาว
- Black box
  - สำรวจ : ตรวจหาเครือข่ายเป้าหมายในการปฏิบัติงาน
  - ตรวจสอบ : เมื่อเราทำการรวบรวมข้อมูลที่ได้มาจากขั้นตอนสำรวจนั้น ก็จะทำการวาดรูปความสัมพันธ์เครือข่ายองค์กรออกมาพร้อมกำหนดจุดที่ทำการตรวจสอบขึ้น การตรวจสอบมักจะใช้ check list ตามมาตรฐาน สิ่งที่ตรวจสอบได้แก่ Information leak, Web Application

checklist, DNS server checklist, E-mail Server checklist, Network Topology checklist, Port services

- วิเคราะห์ : เมื่อทำการตรวจสอบจากการสำรวจและตรวจสอบ ภายนอกเครือข่ายองค์กรแล้วนำข้อมูลเหล่านั้นมาทำการวิเคราะห์เพื่อศึกษาว่าพบช่องโหว่และการเข้าถึงข้อมูล
- ประเมิน : เมื่อทำการวิเคราะห์ถึงช่องโหว่ที่พบแล้ว ถึงขั้นตอนสุดท้ายคือการประเมิน ว่าช่องโหว่ที่พบนั้นมีความเสี่ยงและมีผลกระทบต่อธุรกิจองค์กรอย่างไร ส่วนใหญ่เป็นเอกสารการแนะนำและการปิดช่องโหว่ที่พบ ค่าความเสี่ยง (Risk)ที่พบ จะเกิดจาก ช่องโหว่ที่พบ (Vulnerability) คูณกับค่าภัยคุกคาม (Threat) ลักษณะภัยคุกคามที่พบก็มีความเสี่ยงสูง กลาง และต่ำ ซึ่งส่วนนี้ขึ้นอยู่รูปแบบผู้ทำเอกสารว่าจะจัดทำค่าการประเมินความเสี่ยงจากอุปกรณ์หรือเครื่องมือในตรวจวิเคราะห์ (Tools) มาสรุปความเสี่ยง สูง กลาง และต่ำ ก็ได้
  และจัดทำค่าดัชนีชี้วัดความเสี่ยงที่มีผลกระทบต่อธุรกิจทางด้านเทคนิค ซึ่งเอกสารในผลลัพธ์ของแต่ละบริษัทที่จัดทำอาจจะมีรูปแบบที่แตกต่างกันได้เช่นกัน

- White box
  - สำรวจ : สำรวจผังโครงสร้างงานได้ไอซีทีขององค์กร, แผนผังระบบเครือข่าย, ประเภทอุปกรณ์ประกอบ
  - ตรวจสอบ : ตรวจสอบตามมาตราฐาน Security Checklist
  - วิเคราะห์ : การวิเคราะห์ช่องโหว่ที่พบจากการสำรวจและตรวจสอบ
  - ประเมิน : ขั้นตอนนี้จะเป็นการสรุปผลความเสี่ยงที่พบจากขั้นตอนที่ผ่านมา โดยทำเป็นค่าดัชนีชี้วัดความเสี่ยง และผลการปฏิบัติงาน รวมถึงแนวทางในการปิดกั้นส่วนที่เป็นช่องโหว่ (Hardening) และป้องกันในระยะยาว ซึ่งในส่วนนี้จะเน้นไปทางการทำรายงานผล ในรูปแบบเอกสาร
- สรุป
  - Vulnerability (ช่องโหว่ที่ค้นพบ จาก อุปกรณ์เครือข่ายที่สำคัญ และเครื่องแม่ข่ายที่สำคัญ) จะมีระดับความเสี่ยง สูง กลาง และต่ำ หรืออาจจะมีรายละเอียดมากกว่านั้น
  - Threat (ภัยคุกคาม) ขึ้นกับนโยบายองค์กร และการประเมินค่าจะผู้ปฏิบัติงาน นำมารวมค่ากันแล้วจะได้เป็นดัชนีชี้วัดความเสี่ยงได้ ซึ่งการประเมินส่วนนี้ก็เป็นเทคนิคลับของแต่ละบริษัทที่ใช้ในการประเมินและสามารถวัดผลได้จริงในทางปฏิบัติ
  - การประเมินความเสี่ยงนั้นไม่สามารถที่สิ้นสุดการทำงานได้จากการใช้เครื่องมือ (tools) มาแล้วจะสรุปค่าความเสี่ยงที่เกิดขึ้นจากการใช้งานไอซีทีองค์กรได้จำเป็นต้องอาศัยคนวิเคราะห์ถึงระดับภัยคุกคามและผลลัพธ์รายงานที่มีประโยชน์ต่อบริษัทเพื่อใช้ในการปรับปรุงแก้ไขให้ระบบมีความแข็งแรงและมีความปลอดภัยขึ้น