ประมวลศัพท์เรื่องการจัดการความปลอดภัยของข้อมูล

(Terminology on Information Security Management)

นางสาวกิตติวรรณ ซิมตระการ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาอักษรศาสตรมหาบัณฑิต
สาขาวิชาการแปลและการล่าม หลักสูตรการแปลและการล่าม
คณะอักษรศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

บทคัดย่อ

กิตติวรรณ ซิมตระการ: ประมวลศัพท์เรื่องการจัดการความปลอดภัยของข้อมูล (Terminology on Information Security Management) อาจารย์ที่ปรึกษา: ผู้ช่วยศาสตราจารย์วิโรจน์ อรุณมานะกุล, 181 หน้า

สารนิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อศึกษาระเบียบวิธีการประมวลศัพท์ตามทฤษฎีทางศัพทวิทยา และจัดประมวลศัพท์เรื่องการจัดการความปลอดภัยของข้อมูลซึ่งประกอบไปด้วยชุดคำศัพท์ที่พบบ่อยในนโยบายการจัดการรักษาความปลอดภัยที่องค์กรต่าง ๆ ใช้ ประมวลศัพท์เรื่องการจัดการความปลอดภัยของข้อมูลนี้สามารถนำไปเป็นเอกสารอ้างอิงสำหรับนักแปลและผู้สนใจทั่วไป

ในการประมวลศัพท์ครั้งนี้ ผู้จัดทำได้นำทฤษฎีและแนวทางในการจัดทำประมวลศัพท์ที่นักศัพทวิทยาได้เสนอไว้ โดยแบ่งการดำเนินงานเป็ น 7 ขั้นตอน คือ (1) การกำหนดผู้เชี่ยวชาญ (2) การรวบรวมข้อมูลเพื่อสร้างคลังข้อมูลศัพท์ (3) การสร้างคลังข้อมูลภาษา (4) การวิเคราะห์ข้อมูลและเลือกชุดคำศัพท์ที่จะนำมาสร้างความสัมพันธ์มโนทัศน์ (5) การสร้างมโนทัศน์สัมพันธ์ (6) การบันทึกข้อมูลศัพท์เบื้องต้น (7) การบันทึกข้อมูลศัพท์

ประมวลศัพท์เรื่องการจัดการความปลอดภัยของข้อมูลนี้ประกอบด้วยศัพท์จำนวน 57 คำ และนำเสนอตามกลุ่มมโนทัศน์สัมพันธ์ การนำเสนอศัพท์แต่ละคำประกอบด้วยคำศัพท์ภาษาอังกฤษ ศัพท์เทียบเคียงภาษาไทย ไวยากรณ์ หมวดเรื่อง คำนิยาม บริบท ความสัมพันธ์กับศัพท์อื่น ๆ และรูปอื่น ๆ ทางภาษาศาสตร์

ภาควิชา การแปลและล่าม
สาขาวิชา การแปลและล่าม
ปีการศึกษา 2550

Abstract

KITTIWAN SIMTRAKAN: TERMINOLOGY ON INFORMATION SECURITY MANAGEMENT. SPECIAL RESEARCH ADVISOR: WIROTE AROONMANAKUN, Asst.Prof., Ph.D., 181 pages.

The objective of this special research is to study the methodology of terminology and implement a terminology on Information Security Management. This terminology comprises of terms frequently found in organizations' security policies and is useful for translators as well as people who are interested in the field.

The special research is based on the terminological methods and principles by several terminologists. The methodology of the terminology comprises of 7 steps: (1) Indication of an expert (2) Data compilation (3) Corpus building (4) Corpus Analysis and term extraction (5) Conceptual relationships (6) Extraction recording and (7) Terminology recording.

The terminology on Information Security Management consists of 57 terms presented in conceptual relations, with each term contains information regarding English term(s), Thai term(s), grammatical category, subject, definition, illustration, corss-reference, and linguistic specification

Department: Translation and Intepretation
Field of Study: Translation and Intepretation
Academic year: 2007

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความช่วยเหลือจากบุคคลหลายท่าน โดยเฉพาะอย่างยิ่ง อาจารย์ ผศ. ดร. วิโรจน์ อรุณมานะกุล อาจารย์ที่ปรึกษาผู้ที่กรุณาให้คำปรึกษาและความช่วยเหลือพร้อมทั้งคำแนะนำที่เป็นประโยชน์อย่างยิ่งในการจัดทำสารนิพนธ์ฉบับนี้

ขอขอบพระคุณอาจารย์แห่งศูนย์การแปลและล่ามเฉลิมพระเกียรติผู้ประสิทธิ์ประสาทวิชาการแปลและการล่าม และให้ความรู้ซึ่งนำมาใช้ในการทำสารนิพนธ์

ขอขอบคุณ คุณพงศ์สิทธิ์ จิตตโอวาท ผู้เชี่ยวชาญทางด้านคอมพิวเตอร์โดยเฉพาะอย่างยิ่งในส่วนการจัดการความปลอดภัยของข้อมูลในระบบเครือข่ายคอมพิวเตอร์ที่ให้คำแนะนำในด้านความหมายของศัพท์

และสุดท้ายนี้ขอขอบคุณ บิดา มารดา ของข้าพเจ้าที่เข้าใจและให้ความช่วยเหลือตลอดมา รวมไปถึงเพื่อน ๆ ในศูนย์การแปลและการล่ามเฉลิมพระเกียรติที่คอยให้กำลังใจในการทำสารนิพนธ์เล่มนี้ตลอดมา

สารบัญ

บทที่ 1
บทนำ

1.1. ความเป็นมาและปัญหา

การจัดการความปลอดภัยของข้อมูลได้กลายมาเป็นเรื่องที่หลาย ๆ องค์กรให้ความสนใจศึกษาและหาบุคลากรที่เชี่ยวชาญรวมทั้งเทคโนโลยีเพื่อที่จะนำมาปกป้องทรัพย์สินและข้อมูลที่สำคัญต่อการทำธุรกิจขององค์กรนั้น ๆ ในต่างประเทศได้มีหน่วยงานทั้งภาครัฐบาลและภาคเอกชนก่อตั้งขึ้นมา เพื่อมาดำเนินสร้างนโยบายความปลอดภัยและให้การอบรมแก่บุคคลทั่วไปและผู้ดูแลด้านความปลอดภัย (Information Security Officer) ทั้งนี้ เพื่อนำความรู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูลมาพัฒนาความปลอดภัยของข้อมูลให้องค์กรของตนเองมากขึ้น การจัดการความปลอดภัยของข้อมูลนี้เป็นสาขาย่อยสาขาหนึ่งของเทคโนโลยีสารสนเทศและเป็นสาขาที่ได้รับความสนใจจากองค์กรต่าง ๆ มากที่สุดสาขาหนึ่งจากการที่องค์กรต่าง ๆ พยายามที่จะหาเทคโนโลยีและระบบมาติดตั้งเพื่อเพิ่มความปลอดภัยของทั้งข้อมูลและระบบเครือข่ายของบริษัทตนเอง ทั้งยังได้จัดตั้งนโยบายรักษาความปลอดภัยบังคับใช้กับพนักงานในองค์กรเพื่อเป็นการรักษาความปลอดภัยให้กับข้อมูลในองค์กรอีกด้วย นอกจากนั้นยังมีตำแหน่งที่เกี่ยวข้องกับการจัดการความปลอดภัยของข้อมูลโดยเฉพาะเกิดขึ้นมาในปัจจุบัน เช่น ผู้จัดการด้านความปลอดภัย (Information Security Manager), ผู้จัดการด้านความปลอดภัยหรือ ซี.เอส.โอ (Chief Security Officer), และอื่น ๆ บุคลากรในตำแหน่งเหล่านี้มีหน้าที่ในการตรวจสอบและประเมินว่า พนักงานในองค์กรนั้นได้ปฏิบัติตามกฎที่กำหนดไว้ในนโยบายด้านความปลอดภัยหรือไม่

สำหรับในประเทศไทยเอง ศาสตร์ของการจัดการความปลอดภัยของข้อมูลนี้ได้เริ่มเข้ามามีบทบาทมากขึ้น เนื่องจากว่าได้มีกรณีที่เกิดการลักลอบเข้าใช้งานระบบเครือข่ายขององค์กรที่มีความสำคัญ เช่น หน่วยงานของภาครัฐบาลดั่งที่เคยปรากฏอยู่ในข่าวบ่อยครั้ง ดังนั้น องค์กรที่ตั้งอยู่ในประเทศไทยเหล่านี้จึงต้องพยายามสรรค์สร้างนโยบายออกมาเพื่อที่จะนำมารักษาความปลอดภัยของระบบข้อมูลของตนเอง นอกจากนั้น เมื่อกลางปีที่ผ่านมา กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารหรือกระทรวงไอซีทีนั้นยังได้ออกพระราชบัญญัติว่าด้วยการกระทำผิดที่เกี่ยวกับคอมพิวเตอร์ (Computer Crime Act) ซึ่งเน้นไปที่การจัดเก็บข้อมูลด้านการจราจรในระบบคอมพิวเตอร์และบทลงโทษผู้กระทำผิด โดยเมื่อทำความเข้าใจกับตัวบทพระราชบัญญัตินี้แล้ว จะเห็นได้ว่า ได้มีส่วนหนึ่งที่กล่าวถึงว่า องค์กรต่าง ๆ ควรจะต้องมีการสร้างนโยบายความปลอดภัยและนำมาบังคับใช้กับคนในองค์กรเพื่อเป็นการป้องกันไม่ให้องค์กรโดนโจมตีและเพื่อมีข้อมูลการใช้งานเก็บไว้เป็นหลักฐานที่นำไปยืนยันความไม่มีส่วนเกี่ยวข้องในชั้นศาลได้หากมีความเสียหายเกิดขึ้น เนื่องจากในนโยบายด้านความปลอดภัยจะมีการกำหนดว่า ระบบจะต้องจัดเก็บข้อมูลอะไรบ้างและต้องจัดเก็บด้วยวิธีใด

อย่างไรก็ตาม การทำประมวลศัพท์ทางด้านนี้ ถึงแม้ว่าจะมีมาบ้างแล้ว แต่ก็ยังไม่ครอบคลุมเท่าใดนัก เนื่องจากการจัดการความปลอดภัยของข้อมูลนั้นเป็นสาขาที่มีการเปลี่ยนแปลงและพัฒนาอย่างรวดเร็ว และมีความรู้และศัพท์ที่บัญญัติออกมาใหม่ ๆ อย่างต่อเนื่อง กอปรกับผู้จัดทำเองก็เคยมีประสบการณ์ที่แปลเอกสารที่เกี่ยวข้องกับการจัดการความปลอดภัยของข้อมูลมาบ้าง จึงทำให้เห็นตัวอย่างโดยชัดเจนว่า นโยบายด้านรักษาความปลอดภัยนั้นจะต้องมีส่วนหนึ่ง เช่น ส่วนภาคผนวก ทำเป็นอภิธานศัพท์ (Glossary) เพื่อรวบรวมคำศัพท์เฉพาะที่สำคัญ ๆ ทั้งนี้เพื่อการสื่อสารให้เข้าใจในสิ่งเดียวกันกับคนทั้งองค์กร นอกจากนี้ยังมีการทำอภิธานศัพท์จากหน่วยงานและองค์กรต่าง ๆ ที่ให้ความรู้ทางการจัดการความปลอดภัยของข้อมูล เช่น สถาบันด้านมาตรฐานของทั้งประเทศอังกฤษและสหรัฐอเมริกา หรือ ศูนย์คอมพิวเตอร์และอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติของประเทศไทย ที่ออกมาเพื่อให้ความรู้ที่เกิดขึ้นใหม่ ๆ แก่นักวิชาการหรือบุคคลทั่วไปแต่ประมวลคำศัพท์เหล่านี้ก็มักจะเป็นคำศัพท์และคำอธิบายในภาษานั้น ๆ ภาษาเดียว แต่อภิธานศัพท์หรือชุดคำศัพท์ที่ได้รับการแปลจากภาษาไทยเป็นภาษาอังกฤษ หรือ จากภาษาอังกฤษเป็นภาษาไทยนั้น ยังมีไม่พบให้เห็นมากนัก ที่มีอยู่นั้นก็อาจจะไม่ครอบคลุมความรู้ใหม่ ๆ ที่เกิดขึ้นมา ดังนั้น ผู้จัดทำจึงเล็งเห็นความสำคัญที่ต้องรวบรวมคำศัพท์เฉพาะทางเกี่ยวกับการจัดการความปลอดภัยของข้อมูลขึ้นมาให้เป็นระบบโดยอาศัยหลักวิชาศัพทวิทยา ทั้งนี้เพื่อให้เป็นประโยชน์ต่อผู้ที่ต้องทำงานเกี่ยวด้านความปลอดภัยของข้อมูลขององค์กรและผู้สนใจทั่วไป นอกจากนั้น ประมวลศัพท์ชุดนี้ นักแปลยังสามารถนำไปใช้ในการแปลบทความหรือตัวบทนโยบายด้านความปลอดภัยที่ใช้ในองค์กรต่าง ๆ ได้อีกด้วย ทั้งนี้ เพื่อการสื่อสารที่ถูกต้องกับผู้อ่านที่อยู่ในวงการการจัดการด้านความปลอดภัยข้อมูล

1.2. โครงสร้างของสารนิพนธ์

ในสารนิพนธ์ฉบับนี้ ผู้จัดทำได้นำเสนอในส่วนของทฤษฎีบทที่เกี่ยวข้องกับศัพทวิทยาก่อน ในบทถัด ๆ มา จึงกล่าวถึงขั้นตอนเบื้องต้นในการทำประมวลศัพท์และการสร้างมโนทัศน์สัมพันธ์ ตามลำดับ พร้อมกันนี้ ในส่วนภาคผนวก ผู้จัดทำได้แสดงตารางการบันทึกข้อมูลศัพท์เบื้องต้น และ การบันทึกข้อมูลศัพท์ ที่นำมาประมวลในชุดคำศัพท์การจัดการความปลอดภัยของข้อมูล

บทที่ 2
ศัพทวิทยา

ศัพทวิทยา (Terminology) เป็นศาสตร์ที่เริ่มมีมาช้านานแล้ว ตั้งแต่ศตวรรษที่ 18 โดยในตอนแรกถือว่าเป็นคำที่มีความหมายในเชิงลบ แต่ได้มีการยอมรับเริ่มตั้งแต่ครึ่งหลังของศตวรรษ พบว่ามีการบันทึกคำว่า ศัพทวิทยาที่เป็นภาษาเยอรมัน หรือ คำว่า Terminologie ในบทความที่เขียนโดยอาจารย์ คริสเตียน กอตต์ฟรีด ชู้ทส์ ซึ่งเป็นอาจารย์ประจำมหาวิทยาลัยฮาลเลอ และมหาวิทยาลัยเยนา (Rey, 1995: 15)

ในบทนี้ จะขอกล่าวถึงความเป็นมาของศัพทวิทยา ตามด้วยความหมายและทฤษฎีทั่วไปว่าด้วยเรื่องศัพทวิทยา ศาสตร์ที่เกี่ยวข้องกับศัพทวิทยาและความแตกต่างระหว่างการทำพจนานุกรมและการทำประมวลศัพท์

2.1. ความเป็นมาของศัพทวิทยา

อเลน เรย์ (Rey, 1995: 11 - 22) ได้กล่าวไว้ในเรียงความที่เขาเขียนในเรื่องของความเป็นมาและการพัฒนาของศัพทวิทยาว่า ศัพทวิทยา (Terminology) เป็นศาสตร์ที่มีพื้นฐานเกี่ยวข้องกับชื่อและกระบวนการการตั้งชื่อ เมื่อดูจากหลักฐานทางประวัติศาสตร์ พบว่า ศัพทวิทยาได้ถือกำเนิดขึ้นเมื่อตอนต้นศตวรรษที่ 18 โดยถือกำเนิดมาจากระบบการตั้งชื่อ หรือ Nomenclature เป็นภาษาฝรั่งเศสและอังกฤษซึ่งมีมาตั้งแต่ต้นศตวรรษที่ 16 โดยในตอนนั้น ระบบการตั้งชื่อนี้แทบจะไม่มีความแตกต่างจากอภิธานศัพท์ (Glossary) หรือ พจนานุกรม (Dictionary) เลย แต่ต่อมาในปี ค.ศ. 1615 ได้มีคำภาษาอังกฤษใหม่ นั่นคือ คำว่า Technology เกิดขึ้น และมีความหมายเปลี่ยนไปในช่วงกลางศตวรรษ โดยมีความหมายใหม่ว่า “การทำประมวลศัพท์ที่เป็นคำที่อยู่ในสาขาวิชาหรือหัวข้อที่เฉพาะ” เนื่องจากเหตุนี้นี่เอง ต่อมาในปี ค.ศ. 1690 และในปีค.ศ. 1694 ได้มีการผลิตพจนานุกรมออกมาโดย ผู้รวบรวมคำศัพท์ของพจนานุกรมทั้งสองเล่มนั้นเห็นตรงกันว่า ผู้จัดทำพจนานุกรมควรมีการบัญญัติคำศัพท์ทางด้านเทคโนโลยีและทางด้านวิทยาศาสตร์

จากจุดนี้นี่เองที่ทำให้นักวิทยาศาสตร์หลายท่านเริ่มให้ความสนใจในการทำประมวลศัพท์ในสาขาของตนเพราะนักวิทยาศาสตร์เหล่าต้องการตั้งชื่อให้กับเทคโนโลยีหรือมโนทัศน์ (Concept) ใหม่ ๆ ที่พวกเขาค้นพบขึ้นมาโดยได้รับความสนใจอย่างมากในช่วงต้นศตวรรษที่ 18 นักวิทยาศาสตร์ที่ให้ความสนใจในการทำประมวลศัพท์นั้นส่วนใหญ่จะมาจากแขนงสาขาชีววิทยา เช่น สาขาสัตววิทยา (Zoology) และ สาขาพฤกษศาตร์ (Botany) รวมไปถึงนักเคมีด้วยเช่นกัน (Cabré, 1992: 1-2)

คำว่าศัพทวิทยาที่เป็นภาษาอังกฤษหรือ Terminology ได้อุบัติครั้งแรกในปี ค.ศ. 1801 ซึ่งเป็นปีเดียวกันที่คำภาษาฝรั่งเศสคำว่า Terminologie หรือ ศัพทวิทยาถือกำเนิดเป็นครั้งแรกเช่นกัน แรกเริ่มเดิมทีคำสองคำนี้มีความหมายในเชิงลบ (Rey, 1995: 11 - 22) ในภาษาฝรั่งเศส คำว่า Terminologie นั้นมีความหมายเชิงลบแฝงอยู่โดยมีความหมายในเชิงว่า Terminologie คือ คำที่มีความหมายยากและไร้ประโยชน์ซึ่งมีความหมายในเชิงเดียวกับคำว่า Jargon คำว่า Terminologie คำนี้ยังคงมีความหมายในแง่ลบเรื่อยมาจนถึงปัจจุบัน แต่สำหรับ

ภาษาอังกฤษนั้น คำว่า Terminology นั้นเริ่มมีความหมายในแง่บวกตั้งแต่ปีค.ศ. 1837 และเริ่มมีความหมายในเชิงวิทยาศาสตร์ขึ้นมา ดั่งที่กล่าวไปแล้ว ในช่วงศตวรรษที่ 18 ผู้ที่ให้ความสนใจในเรื่องศัพทวิทยานั้นเป็นกลุ่มของนักวิทยาศาสตร์เป็นหลักโดยเฉพาะนักเคมีและนักชีววิทยา

ต่อมาในศตวรรษที่ 20 กลุ่มนักวิทยาศาสตร์ วิศวกรและกลุ่มผู้ทำงานในด้านเทคโนโลยีเริ่มให้ความสนใจในการจัดทำศัพทวิทยามากขึ้นเนื่องจากได้มีวิทยาการทางด้านเทคโนโลยีและวิทยาศาสตร์แขนงใหม่ ๆ ถือกำเนิดขึ้นรวมไปถึงมโนทัศน์ใหม่ ๆ ที่มีขึ้นตามมา คนกลุ่มนี้ต้องการชื่อที่จะมาเรียกมโนทัศน์ใหม่ ๆ นี้เพื่อการสื่อสารที่ตรงกัน (Cabré, 1992: 2-4)

ถึงแม้ว่าการบัญญัติศัพท์ให้กับมโนทัศน์ที่เกิดขึ้นใหม่ ๆ เพื่อการสื่อสารที่เข้าใจตรงกันในหมู่ผู้ใช้งานจะถือได้ว่าเป็นส่วนหนึ่งของสาขาวิชาภาษาศาสตร์นั้น แต่นักภาษาศาสตร์ก็เพิ่งให้ความใส่ใจในวิชาการศัพทวิทยาในครึ่งหลังของศตวรรษที่ 20 โดยก่อนหน้านั้น นักภาษาศาสตร์แทบจะไม่ให้ความใส่ใจศัพทวิทยาเลย เนื่องจากมีการตีความว่า ศัพทวิทยาอยู่นอกเหนือขอบเขตของวิชาภาษาศาสตร์ (Cabré, 1992: 2-4)

ความสนใจในการจัดทำและรวบรวมคำศัพท์ที่มีความหมายเฉพาะหรือศัพทวิทยานี้ได้มีมาอย่างต่อเนื่องจนมาถึงในศตวรรษที่ 21 นี้โดยเราจะเห็นได้จากที่มีเทคโนโลยีเกิดขึ้นใหม่ ๆ ทุกวัน เช่น เทคโนโลยีทางด้านคอมพิวเตอร์และอินเตอร์เน็ต เทคโนโลยีเหล่านี้มักจะมีมโนทัศน์แปลกใหม่เกิดขึ้นทุกวัน คนทั่วโลกมีการใช้อินเตอร์เน็ตมากขึ้นทุกวันและไม่ได้จำกัดอยู่เฉพาะคนกลุ่มใดกลุ่มหนึ่งอีกต่อไปแล้ว ดังนั้น จึงต้องมีการบัญญัติศัพท์หรือชื่อเพื่อการสื่อสารมโนทัศน์เหล่านี้ให้เข้าใจตรงกัน

2.2. **ความหมายและหน้าที่ของคำ** Terminology

แรกเริ่มเดิมที ความหมายของคำว่า Terminology ที่ปรากฏอยู่ในพจนานุกรมทั่วไปนั้นจำกัดอยู่แค่เป็นการให้คำจำกัดความหรือการตั้งชื่อให้กับกิจกรรมที่เกี่ยวข้องกับทางด้านวิทยาศาสตร์และเทคโนโลยี (Rey, 1995: 127 - 128) ต่อมาความหมายของคำว่า Terminology นั้นขยายวงกว้างครอบคลุมถึงการศึกษาทางด้านศัพทวิทยาอีกด้วยซึ่งเป็นแง่มุมที่ยังไม่มีการกล่าวถึงในพจนานุกรมทั่วไปในปัจจุบัน

ต่อมาได้มีนักภาษาศาสตร์ผู้ที่ให้ความสนใจในการศึกษาศัพทวิทยาบางท่านได้ให้คำจำกัดความของคำว่าศัพทวิทยาไว้ทั้งหมด 3 ความหมายด้วยกัน (Cabré, 1992: 32) กล่าวคือ

1. ศัพทวิทยา หมายถึง หลักการในการศึกษาคำศัพท์เฉพาะทาง
2. การทำประมวลศัพท์ หมายถึง วิธีวิทยา (Methodology) หรือแนวทางในการทำงานด้านศัพทวิยา
3. ประมวลศัพท์ หมายถึง การรวบรวมคำศัพท์เฉพาะทางในหัวข้อใดหัวข้อหนึ่ง

ศัพทวิทยา คือ การศึกษาคำในแง่ของกระบวนการการประกอบขึ้นมาเป็นคำนั้น ๆ (Onomasiological) หรือเป็นการศึกษาในแนวทางจากความหมายของคำย้อนไปที่คำนั้น ๆ ซึ่งสวนทางกับการทำพจนานุกรม (Lexicology) เพราะการทำพจนานุกรมนั้นจะศึกษาจากคำไปที่ความหมายของคำหรือเป็นการศึกษาเชิงวิเคราะห์คำนั่นเอง (Rey, 1995: 127 - 128)

นอกจากนั้น ศัพทวิทยายัง??คือการที่ทำให้คนสามารถสื่อสารมโนทัศน์ที่เกิดขึ้นใหม่กับคนอื่นในกลุ่มที่ต้องใช้มโนทัศน์นี้เช่นกัน เช่น กลุ่มคนในแวดวงวิทยาศาสตร์ เป็นต้น (Rey, 1995: 24)

คาเบร (Cabré) ผู้เชี่ยวชาญด้านการศึกษาศัพทวิทยาของโลกท่านหนึ่งได้ให้คำจำกัดความของ Terminology ไว้ถึง 3 ประการด้วยกัน (Somers, 1996: 16-17) นั่นคือ ประการแรก ศัพทวิทยาคือหลักการสร้างคำศัพท์เฉพาะซึ่งความหมายประการแรกนี้ก่อให้เกิดคำถามมากมายในวงการการศึกษาทางด้านศัพทวิทยา เช่น ศัพทวิทยาคือ หลักการสร้างคำศัพท์เฉพาะจริง ๆ หรือไม่ ถ้าใช่ ถือว่าเป็นศาสตร์ที่เข้าข่ายวิทยาศาสตร์หรือเป็นศาสตร์แบบประยุกต์ ประการที่สอง ศัพทวิทยาคือ การรวบรวมคำศัพท์เฉพาะทาง (Term) ประการที่สาม ศัพทวิทยาคือผลผลิตที่ได้จากการจัดทำประมวลศัพท์นี้เอง

คาเบร ยังมองศัพทวิทยาในแง่มุมของหน่วย (Unit) ต่าง ๆ ด้วยกัน กล่าวคือ ถ้ามองในแง่มุมของนักภาษาศาสตร์ ศัพทวิทยาจะถือเป็นหน่วยที่ใช้แสดงความหมาย (Unit of Meaning) สำหรับนักปรัชญา ศัพทวิทยาจะถือว่าเป็นหน่วยที่แสดงความคิด (Unit of Thought) แต่ถ้าเป็นนักวิทยาศาสตร์หรือนักวิชาการในสาขาวิทยาศาสตร์นั้น จะถือว่าศัพทวิทยาเป็นหน่วยที่ใช้ในการสื่อสาร (Unit of Communication) แต่ละหน่วยจะทำหน้าที่ที่ต่างกันไป (Somers, 1996: 17-18)

สำหรับหน้าที่ของศัพทวิทยานั้น ถ้าแยกเป็นมุมมองของแต่ละหน่วยดังที่กล่าวไปในย่อหน้าถัดมา จะมีหน้าที่ที่แตกต่างกัน กล่าวคือ ในมุมมองของนักภาษาศาสตร์ ศัพทวิทยาจะทำหน้าที่เพื่อให้ความหมายของมโนทัศน์ สำหรับนักปรัชญา ศัพทวิทยาจะทำหน้าที่เพื่อแสดงมโนทัศน์นั้นออกมา และสำหรับนักวิทยาศาสตร์และนักวิชาการนั้น ศัพทวิทยาจะเป็นกระบวนการการตั้งชื่อมโนทัศน์ใหม่ ๆ ที่เกิดขึ้น (Somers, 1996: 18)

นอกจากหน้าที่ที่กล่าวไปแล้วข้างต้น ศัพทวิทยายังทำหน้าที่เป็นเครื่องมือที่ช่วยให้ผู้ทำงานทางด้านภาษา เช่น นักแปล หรือ นักเขียน สามารถทำงานได้อย่างมีประสิทธิภาพในกรณีที่ต้องเขียนหรือแปลบทความที่เป็นสาขาเฉพาะ เพื่อการสื่อสารที่ชัดเจนและถูกต้อง (Cabré, 1992: 9-10)

นอกเหนือไปกว่านั้น นักวิชาการด้านภาษาศาสตร์บางท่านยังกล่าวอีกว่า จุดประสงค์ของศัพทวิทยานั้นมี 3 ประการด้วยกัน คือ ความหมายของคำศัพท์เฉพาะทาง (Description), การเผยแพร่มโนทัศน์ (Transmission), และการสร้างมาตรฐาน (Standardization) (Rey, 1995: 97-98)

1. จุดประสงค์ข้อแรกหรือความหมายของศัพท์เฉพาะทางนั้นมีขึ้นมาเนื่องจากนักภาษาศาสตร์ต้องการให้นิยามความหมายของศัพท์เฉพาะทางซึ่งสามารถหาได้จากกลุ่มของศัพทวิทยาที่รวบรวมได้นี่เอง
2. จุดประสงค์ข้องสองซึ่งก็คือการเผยแพร่มโนทัศน์ใหม่ ๆ นั้นเกิดจากความต้องการที่ผู้ที่คิดค้นมโนทัศน์ใหม่ ๆ ต้องการจะเปิดเผยสิ่งที่เขาคิดค้นได้ซึ่งก็จะทำได้ผ่านทางศัพทวิทยานี่เช่นกัน สำหรับจุดประสงค์ข้อนี้ อาจจะต้องมีการใช้ศัพทวิทยาในหลาย ๆ ภาษา กล่าวคือ คำเรียกมโนทัศน์หนึ่ง ๆ อาจมีได้หลายภาษาเพื่อสื่อสารนักวิชาการในแขนงนั้น ๆ ให้รับรู้ถึงความรู้ใหม่ ๆ
3. จุดประสงค์ข้อสามหรือการสร้างมาตรฐานให้กับภาษามีความจำเป็นเมื่อเราต้องการใช้ภาษาในการถ่ายทอดความรู้ใหม่ ๆ เราจะต้องกำหนดมาตรฐานของภาษาที่ใช้ สำหรับภาษาใดภาษา

หนึ่งแล้ว คำศัพท์ที่อยู่ในกลุ่มศัพทวิทยาสำหรับสาขานั้น ๆ จะต้องมีความสัมพันธ์กันภายในภาษานั้น ๆ เสมอ

ดังนั้น จึงอาจสรุปได้ว่า ศัพทวิทยามีความหมายหลัก ๆ ได้ 3 อย่าง กล่าวคือ ศัพทวิทยา คือ วิชาการที่เกี่ยวข้องกับหลักการการสร้างศัพท์ การทำประมวลศัพท์เฉพาะ และกลุ่มของคำศัพท์เฉพาะที่รวบรวมได้ หน้าที่หลักของศัพทวิทยาคือ การสร้างคำหรือสัญลักษณ์ (Sign) ให้กับมโนทัศน์ที่เกิดขึ้นใหม่เพื่อการสื่อสารให้เกิดความเข้าใจที่ตรงกันในหมู่ผู้ใช้งาน ศัพทวิทยาไม่ได้มีไว้ใช้เพื่องานแปลเพียงอย่างเดียว แต่ยังเป็นการสร้างศัพท์ให้กับมโนทัศน์ใหม่ ๆ ที่เกิดขึ้นมาและสามารถมีได้หลายภาษา

2.3. ทฤษฎีทั่วไปว่าด้วยศัพทวิทยา

ตั้งแต่อดีตจวบจนมาถึงปัจจุบัน ทฤษฎีที่เกี่ยวข้องกับศัพทวิทยานั้นมักจะสัมพันธ์กับการโยงความหมายเข้ากับมโนทัศน์ ความสัมพันธ์ระหว่างมโนทัศน์ต่าง ๆ และความถูกต้องของการตั้งชื่อให้กับมโนทัศน์ กล่าวอีกนัยหนึ่งก็คือ ทฤษฎีที่เกี่ยวข้องกับศัพทวิทยาจะเกี่ยวข้องกับทฤษฎีที่เกี่ยวกับมโนทัศน์เป็นหลัก (Sager: 1990: 9-10)

ทฤษฎีศัพทวิทยานั้นมีการพัฒนาอย่างต่อเนื่องมาตั้งแต่ศตวรรษที่ 18 โดยหัวใจสำคัญที่เกี่ยวข้องกับทฤษฎีนี้นั้นคือ การสร้างศัพท์ขึ้นให้กับมโนทัศน์ที่เกิดขึ้นใหม่ ๆ เพื่อการสื่อสารให้เข้าใจตรงกัน ในช่วงปี ค.ศ. 1930 – 1939 ได้มีนักวิชาการในประเทศออสเตรีย เช็ก และโซเวียตได้ทำการศึกษาทฤษฎีนี้และสามารถแบ่งวิธีการศึกษาออกเป็นสามหัวข้อหลัก ๆ (Cabré, 1992: 7-8)

1. ศัพทวิทยาเป็นศาสตร์ที่สัมพันธ์กับศาสตร์อื่น ๆ และเป็นศาสตร์ที่ศึกษาโดด ๆ ไม่ได้
2. ศัพทวิทยาในแง่ของปรัชญาโดยให้ความสนใจในแง่ของการจัดกลุ่มให้กับคำศัพท์และการจัดระเบียบของความรู้ใหม่ ๆ
3. ศัพทวิทยาในแง่ของภาษาศาสตร์โดยศึกษาในแง่ว่าศัพทวิทยาเป็นส่วนหนึ่งของพจนานุกรม (Lexicon) และภาษาเฉพาะนี้เป็นส่วนหนึ่งของภาษาทั่วไป

ดั่งที่กล่าวไปในตอนต้น ทฤษฎีทั่วไปของศัพทวิทยาจะเกี่ยวข้องกับลักษณะของมโนทัศน์ ความสัมพันธ์ระหว่างมโนทัศน์ และความสัมพันธ์ระหว่างมโนทัศน์กับคำศัพท์ ซึ่งจะสัมพันธ์กับวิธีข้างต้นข้อที่ 1 (Cabré, 1992: 7-8) ทฤษฎีทางศัพทวิทยาถึงจะมีหลักการเป็นของตัวเองและมีการนำไปใช้งาน เช่น การทำอภิธานศัพท์ และการรวบรวมคำศัพท์เฉพาะทาง แต่ทฤษฎีนี้ไม่มีความดั้งเดิมอยู่และไม่มีอะไรที่คิดค้นขึ้นมาเป็นของตัวเอง แต่กลับไปยืมหลักการมาจากศาสตร์ที่เกี่ยวข้องศาสตรอื่น เช่น ภาษาศาสตร์และวิทยาศาสตร์ข้อมูล (Cabré, 1992: 32)

เมื่อมองทฤษฎีในแง่นี้ ศัพทวิทยาจะประกอบไปด้วย 3 ขั้นตอนการทำงานด้วยกัน (Cabré, 1990: 21)

1. การรวบรวมกลุ่มของมโนทัศน์ซึ่งถือว่าเป็นส่วนหนึ่งของความรู้
2. การหาหน่วยของคำที่สัมพันธ์กับมโนทัศน์ในแต่ละกลุ่ม ตามหลักการรับรู้

3. การเชื่อมคำศัพท์เข้ากับมโนทัศน์

งานทั้งสามนั้นถือว่าเป็นส่วนสำคัญในการสร้างคำศัพท์เฉพาะทางอย่างมาก กล่าวคือ ขั้นตอนที่สามหรือการเชื่อมคำศัพท์เข้ากับมโนทัศน์นั้นจะถือเป็นการประกาศความสัมพันธ์ของมโนทัศน์นั้นกับมโนทัศน์อื่น ๆ ในขณะที่ขั้นตอนที่สองหรือการหาหน่วยคำที่เหมาะสมนั้นเกิดขึ้นมาในขณะที่เราต้องการสื่อสารมโนทัศน์ใหม่ ๆ หรือรวบรวมความคิดเพื่อที่จะถ่ายทอดหรืออธิบายมโนทัศน์นั้น ๆ สำหรับขั้นตอนที่หนึ่งหรือการรวบรวมกลุ่มของมโนทัศน์นั้นคือสร้างมโนทัศน์หรือความรู้ขึ้นมาใหม่ ๆ และก่อนที่จะมีการนำออกไปใช้นั้น ก็จะต้องผ่านขั้นตอนการหาคำที่เหมาะสมในขั้นตอนต่อมาเสียก่อน (Cabré, 1990: 21)

2.4. ศาสตร์ที่เกี่ยวข้องกับศัพทวิทยา

ดั่งที่กล่าวไปในหัวข้อที่แล้ว ศัพทวิทยานั้นเป็นศาสตร์ที่มีความสัมพันธ์กับศาสตร์อื่น ๆ และเป็นศาสตร์ที่อยู่โดด ๆ ไม่ได้ ในหัวข้อนี้ จะกล่าวถึงศาสตร์ที่มีส่วนเกี่ยวข้องกับศัพทวิทยา

คาเบรได้อ้างว่ามีสาขาที่เกี่ยวข้องกับศัพทวิทยาทั้งหมด 5 สาขาด้วยกัน (Cabré, 1992: 25-55) นั่นคือ สาขาภาษาศาสตร์ (Linguistics) สาขาวิทยาศาสตร์ปริชาน (Cognitive Science) สาขาการสื่อสาร (Communication) สาขาการบันทึกข้อมูล (Documentation) และสาขาวิทยาการคอมพิวเตอร์และการจัดการความรู้ (Computer Science and Knowledge Engineering)

2.4.1 ภาษาศาสตร์

สาขาแรกที่คนมักจะนึกถึงว่ามีความเกี่ยวข้องกับศัพทวิทยา คือ สาขาภาษาศาสตร์ (Linguistics) เพราะศัพทวิทยานั้นมีขั้นตอนหนึ่งที่เกี่ยวข้องกับการหาคำที่จะมาเชื่อมเข้ากับมโนทัศน์หรือเรียกชื่อความรู้ใหม่ ๆ ภาษาศาสตร์ คือ การศึกษาเกี่ยวกับภาษาในทุก ๆ แง่มุม ตั้งแต่หน่วยของคำ โครงสร้างประโยค หลักภาษาและการนำไปใช้รวมไปถึงการเรียนรู้ภาษานั้น ๆ เริ่มตั้งแต่วัยเด็ก (Cabré, 1992: 26-38)

ภาษาศาสตร์ประยุกต์ (Applied Linguistics) ศึกษาภาษาซึ่งทำหน้าที่ในสังคมหรือทำหน้าที่เป็นเครื่องมือที่ใช้ในการสื่อสาร เพราะการศึกษาภาษานั้นไม่สามารถศึกษาหน่วยคำหรือโครงสร้างประโยคอย่างเดียวแต่ต้องศึกษาการใช้ภาษาเพื่อการสื่อสารอีกด้วย (Cabré, 1992: 26-38)

ภาษาศาสตร์นั้นเน้นการศึกษาไปที่หน่วยของคำเป็นหลัก (Lexicology) โดยจะศึกษาทั้งการออกเสียง หน่วยไวยากรณ์ภาษา รูปประโยค ความหมายของคำ การสร้างคำ การปรับกฎไวยากรณ์ และข้อห้ามทางไวยากรณ์ หรือกล่าวอีกนัยหนึ่งได้ว่า การศึกษาหน่วยของคำ (Lexicology) นั้น คือ การศึกษาหน่วยของคำ หน่วยของไวยากรณ์ การเชื่อมความสัมพันธ์ระหว่างหน่วยคำและหน่วยไวยากรณ์อื่น ๆ เพื่อสร้างเป็นประโยคขึ้นมาซึ่งผู้ที่ใช้ภาษานั้น ๆ จะใช้พูดออกไปเพื่อการสื่อสารกับผู้ใช้งานคนอื่น ๆ นอกจากนี้ผู้ใช้งานภาษานั้น ๆ ยังต้องมีความรู้เรื่องคำของตัวเอง ทั้งนี้เพื่อพวกเขาจะสามารถแต่งประโยคที่ถูกต้องตามหลักไวยากรณ์แบบไหนก็ได้ด้วยตัวเอง นอกเหนือจากการศึกษาของคำแล้ว ภาษาศาสตร์ยังเกี่ยวข้องกับการทำพจนานุกรม (Lexicography) ซึ่งในพจนานุกรมนี้จะรวบรวมคำศัพท์ ความหมายของคำศัพท์ หลักไวยากรณ์

ของคำศัพท์นั้น ข้อมูลการเชื่อมความสัมพันธ์กับหน่วยคำอื่น ๆ รวมไปถึงหน่วยไวยากรณ์เพื่อสร้างเป็นประโยค พจนานุกรมที่มีข้อมูลอื่น ๆ นอกเหนือจากที่กล่าวข้างต้นนี้จะถือว่าเป็นพจนานุกรมของคำศัพท์เฉพาะทาง (Cabré, 1992: 26-38)

ย้อนกลับมาที่ศัพทวิทยาในแง่ที่เกี่ยวกับภาษาศาสตร์ แรกเริ่มเดิมที่ นักภาษาศาสตร์หลายท่านไม่ยอมรับว่า ศัพทวิทยาเป็นส่วนหนึ่งของภาษาศาสตร์เนื่องจาก ศัพท์ที่เข้าเครือข่ายของศัพทวิทยานั้นมีการใช้กับคนเฉพาะกลุ่มเท่านั้นและไม่มีการศึกษาความสัมพันธ์กับหน่วยไวยากรณ์อื่น ๆ ถ้ามองจากมุมนี้จะเห็นว่าศัพทวิทยา (Terminology) จะไม่ถือว่าเป็นส่วนหนึ่งของภาษาศาสตร์ (Cabré, 1992: 26-38)

แต่ต่อมาในภายหลัง นักภาษาศาสตร์บางท่านเริ่มโต้แย้งและกล่าวว่าเนื่องจากการศึกษาทางด้านภาษาศาสตร์นั้นเกี่ยวข้องกับหน้าที่ของการใช้ภาษาซึ่งเป็นส่วนหนึ่งของหน้าที่ในสังคมหรือการสื่อสารจากผู้พูดไปหาผู้ฟังนั่นเอง การศึกษาภาษาศาสตร์ในด้านนี้ถือว่าเป็นส่วนหนึ่งของภาษาศาสตร์ประยุกต์ดั่งที่ได้กล่าวไปในข้างต้น ถ้ามองในแง่นี้จะถือว่า คำศัพท์เฉพาะที่รวบรวมตามหลักของศัพทวิทยาจะเป็นส่วนย่อยของการศึกษาคำในภาษาศาสตร์ ดังนั้น อาจกล่าวได้ว่า ศัพทวิทยา (Terminology) คือส่วนหนึ่งของภาษาศาสตร์ (Sager: 1990: 9-10) นั่นเป็นสาเหตุว่าทำไมนักภาษาศาสตร์เพิ่งจะเริ่มให้ความสนใจศัพทวิทยาในช่วงครึ่งหลังของศตวรรษที่ 19

ถึงแม้ว่าศัพทวิทยาจะถือเป็นส่วนหนึ่งของภาษาศาสตร์ แต่ถึงกระนั้น ศัพทวิทยาก็ยังมีความแตกต่างจากภาษาศาสตร์โดยวูสเตอร์ (Wüster) กล่าวไว้ว่า ศัพทวิทยาแตกต่างจากภาษาศาสตร์ในแง่ของวิธีการศึกษาซึ่งมีความแตกต่าง 2 ประเภทใหญ่ ๆ ด้วยกัน อย่างแรกคือ การสร้างคำศัพท์และคำศัพท์เฉพาะทาง อย่างที่สองคือการรวบรวมคำศัพท์ขึ้นมาในรูปของพจนานุกรมและการประมวลศัพท์ หัวข้อที่สองนั้นจะได้รับการกล่าวถึงในหัวข้อที่ 2.5 แต่ในย่อหน้าถัดมาจะพูดถึงความแตกต่างอย่างแรกก่อน (Cabré, 1992: 26-38)

ความแตกต่างใหญ่อย่างแรกของภาษาศาสตร์และศัพทวิทยาคือการสร้างคำศัพท์ ในทางภาษาศาสตร์ นักวิชาการจะสนใจหน่วยคำในแง่ของคำศัพท์ ตามมาด้วยความหมายและวิธีการใช้ หรือพูดในอีกทางหนึ่งว่า ภาษาศาสตร์จะให้ความสนใจในแง่ของตัวคำก่อนความหมายและไวยากรณ์ แต่ในขณะที่ศัพทวิทยาจะให้ความสนใจทางด้านความหมายก่อนคำ จุดสนใจหลักของศัพทวิทยา คือ ความหมายและจะไม่สนใจหลักไวยากรณ์ที่จะใช้คู่กับคำนั้นหรือการนำไปใช้งาน (Cabré, 1992: 26-38)

จุดแตกต่างอีกอย่างหนึ่งคือการศึกษาทางด้านภาษาศาสตร์นั้นจะศึกษาทั้งการเปลี่ยนแปลงของคำศัพท์ในช่วงเวลาต่างๆ (Diachronic) และการศึกษาคำศัพท์ในช่วงเวลาปัจจุบัน (Synchronic) แต่ในขณะที่ศัพทวิทยาศึกษาเฉพาะในช่วงเวลาปัจจุบัน (Synchronic) เพียงอย่างเดียว (Cabré, 1992: 26-38)

กล่าวโดยสรุป คือ ศัพทวิทยาถือเป็นส่วนหนึ่งของภาษาศาสตร์โดยจะถือเป็นแขนงหนึ่งของภาษาศาสตร์ประยุกต์ และคำศัพท์เฉพาะที่รวบรวมอยู่ในศัพทวิทยาจะถือเป็นหน่วยย่อยของคำที่อยู่ในโดเมนของภาษาศาสตร์ แต่อย่างไรก็ดี ภาษาศาสตร์ก็ยังมีความแตกต่างจากศัพทวิทยาอยู่มากทั้งในเรื่องของวิธีการศึกษา และการรวบรวมคำศัพท์

2.4.2 วิทยาศาสตร์ปริชาน

ศัพทวิทยานั้นคือการศึกษาที่เกี่ยวข้องกับความหมายของคำ นักวิทยาศาสตร์จะใช้คำศัพท์เฉพาะที่อยู่ในโดเมนในศัพทวิทยาในการสื่อสารความคิดของตนและความรู้หรือสิ่งประดิษฐ์ที่ตนคิดค้นได้ให้คนอื่นได้รับรู้ หรืออาจกล่าวได้ว่า ศัพทวิทยาคือหน่วยของความคิด (Cabré, 1992: 39) ดังนั้น สาขาที่เกี่ยวข้องกับศัพทวิทยาก็คือวิทยาศาสตร์ปริชาน (Cognitive Science) หรือศาสตร์ทางด้านจิตวิทยา (Psychology) ซึ่งเป็นสาขาที่ศึกษาการก่อตัวของความคิดจากสมองของมนุษย์และการหาความสัมพันธ์ระหว่างคำและความคิดนั้น ๆ รวมไปถึงความสัมพันธ์ระหว่างความคิดต่าง ๆ

ดั่งที่ได้กล่าวไปแล้วในหัวข้อข้างต้น ศัพทวิทยาสามารถมองได้เป็น 3 หน่วย นั่นคือ หน่วยของความคิด หน่วยของความหมาย หน่วยของการสื่อสาร ในบรรดามุมมองของศัพทวิทยาทั้งสามอย่างนั้น หน่วยของความคิดหรือการมองศัพทวิทยาในแง่ของการรับรู้มโนทัศน์ใหม่ ๆ นั้นถือว่าเป็นสิ่งที่ยากต่อการศึกษามากที่สุด การรับรู้ (Cognitive) นั้นคือผลลัพธ์ที่ได้จากกระบวนการทางความคิดซึ่งนำไปสู่ความรู้ หัวใจสำคัญของการศึกษาศัพทวิทยาคือการศึกษาปัญหาว่าความคิดของมนุษย์สามารถรับรู้สิ่งต่าง ๆ ได้อย่างไรทั้งรูปธรรมและนามธรรม (Cabré, 1992: 41)

การศึกษาศัพทวิทยาในแง่ที่เกี่ยวข้องกับทฤษฎีด้านการรับรู้จะแบ่งออกได้เป็น 3 หัวข้อหลัก ๆ ด้วยกันคือ (Cabré, 1992: 41-42)

1. มนุษย์สามารถรับรู้และเข้าใจความรู้ในโลกแห่งความเป็นจริงและโครงสร้างของมันอย่างไร
2. มโนทัศน์ที่มีอยู่แล้ว มโนทัศน์เกิดขึ้นมาได้อย่างไร ความสัมพันธ์ระหว่างมโนทัศน์ และลำดับของมโนทัศน์แต่ละอันในโครงสร้างของความรู้
3. มโนทัศน์มีความสัมพันธ์กับคำศัพท์เฉพาะทางอย่างไร

ศัพทวิทยาศึกษาการเกิดมโนทัศน์ใหม่ ๆ นักภาษาศาสตร์เชื่อว่า มโนทัศน์คือหน่วยของความคิดประกอบไปด้วยคุณสมบัติซึ่งคุณสมบัติแต่ละประเภทก็คือมโนทัศน์ในตัวของมันเองเช่นกัน มนุษย์จะใช้คุณสมบัติเหล่านี้ในการสร้างประโยคเพื่อสื่อสารความรู้ใหม่ ๆ ออกมา (Cabré, 1992: 41-42)

2.4.3 สาขาการสื่อสาร

ดั่งที่ได้กล่าวไปแล้วว่า มนุษย์จะเริ่มรวบรวมความคิดออกมาเป็นประโยคหลังจากนั้นก็จะสื่อสารออกมา ดังนั้น ศัพทวิทยาจึงเป็นศาสตร์ที่เกี่ยวข้องกับสาขาการสื่อสารโดยตรง เพียงแต่ว่าศัพทวิทยาจะเน้นการสื่อสารเกี่ยวกับสาขาเฉพาะทางและจะอยู่แยกจากการสื่อสารแบบธรรมดาทั่วไป นักวิชาการจะใช้คำศัพท์เฉพาะนี้ในการสื่อสารศาสตร์ของตนในภาษาใดภาษาหนึ่งหรือหลายภาษา (Cabré, 1992: 45)

ในการสื่อสารความรู้เฉพาะทาง (Special communication) นั้นผู้ส่งสารและผู้รับสารมักจะเป็นผู้ที่มีความรู้ในด้านนั้นอยู่แล้วหรืออาจจะเป็นผู้เชี่ยวชาญในสาขานั้น ๆ เช่น แพทย์คุยกับแพทย์ด้วยกันเอง เป็นต้น และสารที่สื่อออกมาก็มักจะเป็นศาสตร์เฉพาะทาง คำศัพท์เฉพาะที่ใช้ในการสื่อสารประเภทนี้มักจะเป็นคำที่มี

ให้ข้อมูลหรืออธิบายศาสตร์ที่ต้องการสื่อสารนั้น ๆ แต่อย่างไรก็ดี ในการสื่อสารแบบนี้ยังต้องมีการใช้ภาษาแบบธรรมดาบ้าง เช่น การออกเสียง การเรียงลำดับประโยคตามไวยากรณ์ (Cabré, 1992: 46-47)

นอกจากนี้ ศัพทวิทยานั้นยังนำไปใช้ในวงการการแปลด้วยเช่นกัน การแปลถือว่าเป็นการสื่อสารชนิดหนึ่งโดยเป็นการสื่อสารจากภาษาหนึ่งไปเป็นอีกภาษาหนึ่ง คำศัพท์เฉพาะทางนั้นอาจมีออกมาได้หลายภาษา นักแปลจะนำคำที่ความเท่าเทียมกันนี้ไปแปลในภาษาปลายทาง หรือถ้ายังที่ไม่มีคำบัญญัติออกมา นักแปลจะต้องหาคำที่ใกล้เคียงโดยอาจจะดูจากความหมายแล้วค่อยเลือกคำที่มีอยู่แล้วมาใช้ประกอบกัน (Cabré, 1992: 48)

ในท้ายที่สุดแล้ว คำศัพท์เฉพาะทางนี้ยังมีส่วนช่วยให้ภาษาหนึ่ง ๆ ยังคงอยู่ต่อไปและไม่สูญไปจากสังคมที่ใช้ภาษานั้น ๆ เนื่องจากคนในสังคมนั้น ๆ ต้องใช้คำศัพท์เฉพาะในการสื่อสารความรู้ที่ต้องถ่ายทอดต่อไปในสังคม สำหรับคำศัพท์เฉพาะทางที่ยืมมาจากภาษาอื่นนั้น ถ้านักภาษาศาสตร์ไม่สามารถหาคำในภาษาของตนที่เหมาะสมพอจะมาแทนคำนั้นได้ เจ้าของภาษาในสังคมนั้นต้องหามาตรการว่าคำส่วนไหนบ้างที่จะกำหนดให้เป็นคำที่ยืมมาจากภาษาต่างประเทศและคำประเภทใดบ้างที่จะใช้ภาษาของตนเองมากำหนดเพื่อเป็นการส่งเสริมให้ภาษานั้น ๆ ยังคงอยู่ต่อไปและไม่ตายในที่สุด (Cabré, 1992: 48-50)

2.4.4 สาขาการบันทึกข้อมูล

ศัพทวิทยานั้นเกี่ยวข้องกับงานเอกสารหรือการบันทึกข้อมูล (Documentation) เช่น การเขียนเอกสารทางเทคโนโลยี การแปลเอกสารทางด้านวิชาการ และการบันทึกศัพท์เฉพาะในกระดาษ ทั้งหมดนี้ล้วนแต่เกี่ยวข้องกับการบันทึกเอกสารทั้งนั้น (Cabré, 1992: 50)

การจัดทำเอกสารนั้นถือเป็นศาสตร์ใหม่ที่เกี่ยวข้องกับการรวบรวม การวิเคราะห์ การจัดประเภทและการจัดเก็บเอกสารเพื่อให้ผู้อื่นเรียกดูได้ การจัดทำเอกสารในปัจจุบันนั้นมีทั้งที่บันทึกในกระดาษ บันทึกลงคอมพิวเตอร์ และการบันทึกในฐานข้อมูลโดยใช้โปรแกรมคอมพิวเตอร์ช่วย (Cabré, 1992: 50-51)

การประมวลศัพท์นั้นมีออกมาทั้งในรูปแบบอภิธานศัพท์ พจนานุกรมศัพท์เฉพาะ และเอกสารอื่น ๆ อีก ดังนั้น ความรู้ทางด้านการประมวลเอกสารและการจัดทำฐานข้อมูลจึงจำเป็นมากสำหรับศัพทวิทยา (Cabré, 1992: 51-52)

2.4.5 สาขาวิทยาการคอมพิวเตอร์

วูสเตอร์ (Wüster) กล่าวไว้ว่า วิทยาการคอมพิวเตอร์เป็นศาสตร์อีกแขนงหนึ่งที่มีส่วนช่วยสร้างรากฐานและพัฒนาศัพทวิทยาโดยเทคโนโลยีคอมพิวเตอร์ช่วยให้การเก็บและสืบค้นข้อมูลคำศัพท์เป็นไปได้อย่างสะดวก รวดเร็วและง่ายขึ้น และในขณะเดียวกันคำศัพท์เฉพาะที่อยู่ในคลังคำศัพท์ของศัพทวิทยานั้นก็จะช่วยในโปรแกรมคอมพิวเตอร์ (Cabré, 1992: 52) เช่น โปรแกรมปัญญาประดิษฐ์ (Artificial Intelligence) ระบบผู้เชี่ยวชาญ (Expert System) และระบบฟัซซี่ (Fuzzy system) โปรแกรมเหล่านี้ใช้ทำโปรแกรมแปลและโปรแกรมหน่วยความจำในการแปล (Translation Memory) นอกจากนั้น ในปัจจุบันยังมีโปรแกรมที่ช่วย

นักแปลในการแปล หรือ Computer-aided translation ซึ่งต้องใช้ศัพทวิทยาในการทำคลังคำศัพท์เฉพาะเช่นกัน

ดังที่ได้กล่าวไปในตอนต้นแล้ว คอมพิวเตอร์มีส่วนช่วยให้การทำงานทางด้านศัพทวิทยาเป็นไปได้อย่างสะดวกและทันสมัยมากขึ้นโดยแรกเริ่มเดิมที คอมพิวเตอร์นำมาใช้ในการเก็บข้อมูลและสร้างรายชื่อหนังสือโดยทำเป็นคลังคำขึ้นมา (Data bank) ภายหลัง ได้มีการนำคอมพิวเตอร์มาเก็บคำศัพท์ในรูปแบบของพจนานุกรมเพื่อนำไปใช้ในการแปล เมื่อคอมพิวเตอร์ได้มีการพัฒนาขึ้น การทำคลังคำและพจนานุกรมแบบอิเลคทรอนิกส์ก็ได้มีการพัฒนาขึ้นเหมือนกันโดยขนาดของฐานข้อมูลมีขนาดเล็กลงและมีความยืดหยุ่นมากขึ้น มีการพัฒนาเป็นอินเตอร์เฟสการใช้งานขึ้นมาทำให้ผู้ใช้งานรู้สึกว่าใช้งานได้ง่ายขึ้น นอกจากนั้น คลังคำศัพท์เหล่านี้ยังสามารถจัดเก็บไว้ในซีดีรอมเพื่อที่นักแปลสามารถนำกลับไปใช้ที่คอมพิวเตอร์ของตนเองได้ ต่อมาเมื่อเทคโนโลยีการค้นหาข้อมูลมีมากขึ้นและขนาดความจุของคอมพิวเตอร์มีมากขึ้น ผู้ใช้งานสามารถหาคำศัพท์ได้อย่างรวดเร็วขึ้นและในคอมพิวเตอร์เครื่องหนึ่ง สามารถบรรจุโปรแกรมเก็บคำศัพท์เฉพาะพจนานุกรมได้มากกว่า 1 เล่ม โปรแกรมพิมพ์เอกสารต่าง ๆ เพื่อใช้จัดเก็บข้อมูล โปรแกรมหาข้อมูลเพื่อหามโนทัศน์ใหม่ ๆ ได้อย่างอัตโนมัติ ศัพทวิทยายังนำไปใช้ในระบบผู้เชี่ยวชาญอีกด้วย ในปัจจุบัน วิทยาการคอมพิวตอร์พัมนาขึ้นมาอย่างมาก ศัพทวิทยายังได้นำไปใช้ในโปรแกรมที่ใช้เพื่อการตัดสินใจ (Decision Making Program) โดยสร้างเป็นส่วนหนึ่งของกฎที่ใช้ในการตัดสินใจ (Decision rule) ในระบบ (Cabré, 1992: 53-55)

ในปัจจุบันนี้ ได้มีโปรแกรมคอมพิวเตอร์สำเร็จรูปที่สร้างขึ้นมาเพื่อช่วยการประมวลศัพท์เฉพาะขององค์กรหรือการทำงานในโครงการต่าง ๆ เพื่อสื่อสารความรู้ให้กับคนทำงานและเพื่อช่วยประหยัดเวลาในการแปลงานที่เคยแปลอีกด้วย นอกจากนี้ ถ้าองค์กรใดต้องการทำรายชื่อศัพท์เฉพาะเพื่อแนบไปกับสินค้าของตน เช่น องค์กรที่ผลิตซอฟต์แวร์ เป็นต้น โปรแกรมเหล่านี้ก็จะช่วยลดเวลาการผลิตลงด้วย (Muegge, 2007: 18)

ดังนั้น จะเห็นว่าวิทยาการคอมพิวเตอร์และศัพทวิทยานั้นเป็นศาสตร์ที่เกี่ยวข้องกันและเอื้อประโยชน์ซึ่งกันและกัน

2.5. ความแตกต่างระหว่างการทำพจนานุกรมและการทำประมวลศัพท์

ถึงแม้ว่า การประมวลศัพท์ในศัพทวิทยานั้นจะถือเป็นส่วนหนึ่งของการทำพจนานุกรม แต่ทว่า การทำพจนานุกรมและการประมวลศัพท์เฉพาะในศัพทวิทยานั้นมีความแตกต่างกันพอสมควร ในหัวข้อนี้จะกล่าวถึงความแตกต่างระหว่างการทำพจนานุกรมและการทำประมวลศัพท์

ความแตกต่างประการแรก คือ พจนานุกรมนั้นมักจะหมายถึงพจนานุกรมที่เกี่ยวกับภาษาทั่วไป (Language Dictionary) กล่าวคือ ในพจนานุกรมทั่วไปนั้นจะมีข้อมูลที่เกี่ยวของทางภาษานั้น ๆ อยู่ เช่น ข้อมูลทางไวยากรณ์ ข้อมูลความถี่ในใช้งานหรือการปรากฏอยู่ในงานเขียน ข้อมูลคำเหมือน ข้อมูลคำตรงข้าม หน้าที่ของคำ ตัวอย่างประโยชน์ แต่พจนานุกรมที่ไม่มีข้อมูลตามที่กล่าวไปนี้จะถือว่าเป็นพจนานุกรมของศัพท์

เฉพาะหรือถือว่าเป็นอภิธานศัพท์ (Glossary) ซึ่งจะรวบรวมแต่คำศัพท์เฉพาะและมักจะมีแต่คำนาม จะไม่มีการแสดงคำกริยาของคำนั้น ๆ และแทบจะไม่มีการแสดงตัวอย่างประโยคทั้งนั้น (Rey, 1995: 114)

ความแตกต่างประการที่สอง คือ การทำพจนานุกรมนั้นจะมองจากในแง่มุมของคำ (Word) ก่อนเป็นหลักแล้วค่อยมุ่งไปสู่ความหมายของคำนั้น กล่าวคือ ในพจนานุกรมจะพูดถึงคำนั้น ๆ ก่อนว่าสะกดอย่างไรมีการเขียนอย่างไร แล้วค่อยอธิบายความหมายของคำนั้นในแง่ต่าง ๆ เช่น ถ้าเป็นคำกริยาจะมีความหมายอย่างไร ถ้าเป็นคำคุณศัพท์จะมีความหมายอย่างไร ในบางภาษา เช่น ภาษาอังกฤษ ความหมายของคำอาจจะเปลี่ยนไปตามลักษณะของคำด้วย เช่น คำว่า Hair ถ้าเป็นนามนับไม่ได้ จะแปลว่า “ผม” และถ้านับได้จะแปลว่า “ขน” เป็นต้น ในพจนานุกรมภาษาทั่วไปนั้น จะมีการอธิบายเหล่านี้ไว้อย่างละเอียด พจนานุกรมบางเล่ม อาจจะมีการทำสถิติความถี่ของคำนั้น ๆ ที่ปรากฏในภาษาพูดและภาษาเขียนด้วยขึ้นอยู่กับความต้องการของผู้ใช้งานที่สำนักพิมพ์สำรวจมาได้ การทำพจนานุกรมจะต้องคำนึงถึงในแง่ของความต้องการของคนในสังคมเพื่อนำไปใช้งานและความต้องการของผู้ใช้งานในเชิงการค้าด้วย แต่สำหรับการทำประมวลศัพท์เฉพาะนั้น ผู้จัดทำจะต้องคำนึงถึงความหมาย (Definition) หรือมโนทัศน์ (Concept) ของคำนั้น ๆ แล้วค่อยหาชื่อมาตั้งให้ความหมายนั้น ๆ ส่วนใหญ่คำศัพท์ (Term) ในศัพทวิทยานั้นจะเป็นคำนามและจะไม่ค่อยมีการบอกรายละเอียดต่าง ๆ อย่างอื่นมากนัก เพราะคำศัพท์ที่อยู่ในศัพทวิทยาจะมองว่าเป็นหน่วยของความรู้ ดังนั้น จึงมักมีแต่คำศัพท์ที่เป็นคำนามและความหมายของคำนั้น ๆ เท่านั้น (Rey, 1995: 114 - 119)

ความแตกต่างประการที่สาม คือ ในการรวบรวมคำศัพท์ในพจนานุกรมนั้น คำศัพท์แต่ละคำจะถือเป็นหนึ่งคำ เช่น คำว่า Economic Bust และ Economic recession แปลว่า เศรษฐกิจขาลง เช่นกัน ถ้าการรวบรวมคำศัพท์ในพจนานุกรมนั้น จะต้องมีการเขียนรายละเอียดแยกกัน และถือว่าเป็นคนละคำกัน เนื่องจากมีรูปคำ (Sign) ที่ต่างกันจึงถือว่าเป็นคนละคำกันเพียงแต่มีความหมายเหมือนกันเท่านั้น แต่ถ้าเป็นการรวบรวมคำศัพท์ในการประมวลศัพท์เฉพาะนั้น ทั้งสองคำจะถือว่าเป็นคำเดียวกัน เพราะการรวบรวมคำศัพท์เฉพาะจะมองจากความหมายของคำเป็นหลัก ถ้าคำไหนที่มีความหมายเหมือนกัน จะถือว่าเป็นคำเดียวกัน นอกจากนั้น คำ ๆ เดียวกันในแต่ละภาษาจะได้รับการบรรจุในพจนานุกรมที่ต่างกันด้วย แต่ถ้าเป็นการประมวลคำศัพท์(Muegge, 2007: 18-19)

ความแตกต่างประการที่สี่ คือ โดเมนของศัพท์ที่บรรจุในการทำพจนานุกรมนั้นจะกว้างมากและครอบคลุมกับคำศัพท์ในภาษานั้น ๆ แต่ถ้าเป็นการประมวลศัพท์ คำศัพท์ที่ได้รับการรวบรวมจะเป็นคำศัพท์ที่อยู่ในโดเมนเฉพาะกลุ่มซึ่งจะถือเป็นส่วนหนึ่งของพจนานุกรมทั่ว ๆ ไป (Cabré, 1992: 35)

ความแตกต่างประการที่ห้า คือ คำศัพท์ (Word) ที่รวบรวมอยู่ในพจนานุกรมทางภาษาทั่วไปนั้นจะเป็นคำที่ได้รับการอธิบายความหมายเดี่ยว ๆ ไม่ได้แต่ต้องอธิบายหน้าที่ทางภาษาด้วย เพราะคำเหล่านี้เป็นหน่วยย่อยของการสื่อสาร เกี่ยวข้องกับผู้ใช้งานทางภาษาในแง่มุมไหนบ้าง และเมื่อนำไปใช้ในสถานการณ์หรือหัวข้อเรื่องการสื่อสารที่ต่างกันนั้น คำเหล่านี้จะมีความหมายอย่างไรบ้าง แต่ศัพท์ (Term) ที่อยู่ในประมวลศัพท์เฉพาะจะบอกแค่ความหมายและชื่อเรียกความหมายนั้น ๆ อย่างเดียวและไม่มีข้อมูลการใช้งานเนื่องจากมีการคาดการณ์ไว้ก่อนหน้านั้นอยู่แล้วว่า ผู้ใช้งานคำศัพท์เฉพาะนั้นเป็นนักวิชาการหรือผู้ที่มีความรู้ในสาขานั้น ๆ อยู่แล้วจึงไม่ต้องคำนึงมากนัก (Cabré, 1992: 35-36)

ความแตกต่างประการที่หก คือ จุดประสงค์ของพจนานุกรมและการประมวลศัพทเฉพาะนั้นมีความแตกต่างกัน กล่าวคือ ข้อมูลในพจนานุกรมมีไว้เพื่อให้ผู้ใช้งานนั้นสามารถนำไปใช้ในภาษาพูดในสถานการณ์ต่าง ๆ ได้ ในขณะที่ศัพท์เฉพาะในการประมวลศัพท์นั้นจะใช้เพื่อนำไปอ้างถึงหน่วยย่อยของความรู้ในโลกของความเป็นจริง การประมวลศัพท์จะไม่นำเสนอการนำไปใช้งานจริงดั่งในพจนานุกรม แต่จะเน้นไปที่กฎการเลือกคำศัพท์ที่จะเหมาะสมในการอธิบายหน่วยความรู้ให้ผู้ใช้งานเข้าใจตรงกันมากที่สุด (Cabré, 1992: 36-37)

ความแตกต่างประการที่เจ็ด คือ วิธีวิทยาที่ใช้ในการรวบรวมคำศัพท์ การรวบรวมคำศัพท์ในพจนานุกรมภาษาทั่วไปจะใช้สมมติฐานในทางทฤษฎีของภาษาและนำเสนอตัวอย่างประโยคที่ผู้พูดใช้ในโอกาสต่าง ๆ เพื่อเป็นการอธิบายคำศัพท์นั้น ๆ ส่วนการประมวลศัพท์นั้น จะไม่มีการคำนึงถึงพฤติกรรมของผู้ใช้งานคำศัพท์นั้น แต่จะนำเสนอคำที่จะมาใช้เรียกมโนทัศน์ที่ค้นพบได้มากกว่า (Cabré, 1992: 37)

2.4.3 สาขาการสื่อสาร

ดั่งที่ได้กล่าวไปแล้วว่า มนุษย์จะเริ่มรวบรวมความคิดออกมาเป็นประโยคหลังจากนั้นก็จะสื่อสารออกมา ดังนั้น ศัพทวิทยาจึงเป็นศาสตร์ที่เกี่ยวข้องกับสาขาการสื่อสารโดยตรง เพียงแต่ว่าศัพทวิทยาจะเน้นการสื่อสารเกี่ยวกับสาขาเฉพาะทางและจะอยู่แยกจากการสื่อสารแบบธรรมดาทั่วไป นักวิชาการจะใช้คำศัพท์เฉพาะนี้ในการสื่อสารศาสตร์ของตนในภาษาใดภาษาหนึ่งหรือหลายภาษา (Cabré, 1992: 45)

ในการสื่อสารความรู้เฉพาะทาง (Special communication) นั้นผู้ส่งสารและผู้รับสารมักจะเป็นผู้ที่มีความรู้ในด้านนั้นอยู่แล้วหรืออาจจะเป็นผู้เชี่ยวชาญในสาขานั้น ๆ เช่น แพทย์คุยกับแพทย์ด้วยกันเอง เป็นต้น และสารที่สื่อออกมาก็มักจะเป็นศาสตร์เฉพาะทาง คำศัพท์เฉพาะที่ใช้ในการสื่อสารประเภทนี้มักจะเป็นคำที่มีให้ข้อมูลหรืออธิบายศาสตร์ที่ต้องการสื่อสารนั้น ๆ แต่อย่างไรก็ดี ในการสื่อสารแบบนี้ยังต้องมีการใช้ภาษาแบบธรรมดาบ้าง เช่น การออกเสียง การเรียงลำดับประโยคตามไวยากรณ์ (Cabré, 1992: 46-47)

นอกจากนี้ ศัพทวิทยานั้นยังนำไปใช้ในวงการการแปลด้วยเช่นกัน การแปลถือว่าเป็นการสื่อสารชนิดหนึ่งโดยเป็นการสื่อสารจากภาษาหนึ่งไปเป็นอีกภาษาหนึ่ง คำศัพท์เฉพาะทางนั้นอาจมีออกมาได้หลายภาษา นักแปลจะนำคำที่ความเท่าเทียมกันนี้ไปแปลในภาษาปลายทาง หรือถ้ายังที่ไม่มีคำบัญญัติออกมา นักแปลจะต้องหาคำที่ใกล้เคียงโดยอาจจะดูจากความหมายแล้วค่อยเลือกคำที่มีอยู่แล้วมาใช้ประกอบกัน (Cabré, 1992: 48)

ในท้ายที่สุดแล้ว คำศัพท์เฉพาะทางนี้ยังมีส่วนช่วยให้ภาษาหนึ่ง ๆ ยังคงอยู่ต่อไปและไม่สูญไปจากสังคมที่ใช้ภาษานั้น ๆ เนื่องจากคนในสังคมนั้น ๆ ต้องใช้คำศัพท์เฉพาะในการสื่อสารความรู้ที่ต้องถ่ายทอดต่อไปในสังคม สำหรับคำศัพท์เฉพาะทางที่ยืมมาจากภาษาอื่นนั้น ถ้านักภาษาศาสตร์ไม่สามารถหาคำในภาษาของตนที่เหมาะสมพอจะมาแทนคำนั้นได้ เจ้าของภาษาในสังคมนั้นต้องหามาตรการว่าคำส่วนไหนบ้างที่จะกำหนดให้เป็นคำที่ยืมมาจากภาษาต่างประเทศและคำประเภทใดบ้างที่จะใช้ภาษาของตนเองมากำหนดเพื่อเป็นการส่งเสริมให้ภาษานั้น ๆ ยังคงอยู่ต่อไปและไม่ตายในที่สุด (Cabré, 1992: 48-50)

2.4.4 สาขาการบันทึกข้อมูล

ศัพทวิทยานั้นเกี่ยวข้องกับงานเอกสารหรือการบันทึกข้อมูล (Documentation) เช่น การเขียนเอกสารทางเทคโนโลยี การแปลเอกสารทางด้านวิชาการ และการบันทึกศัพท์เฉพาะในกระดาษ ทั้งหมดนี้ล้วนแต่เกี่ยวข้องกับการบันทึกเอกสารทั้งนั้น (Cabré, 1992: 50)

การจัดทำเอกสารนั้นถือเป็นศาสตร์ใหม่ที่เกี่ยวข้องกับการรวบรวม การวิเคราะห์ การจัดประเภทและการจัดเก็บเอกสารเพื่อให้ผู้อื่นเรียกดูได้ การจัดทำเอกสารในปัจจุบันนั้นมีทั้งที่บันทึกในกระดาษ บันทึกลงคอมพิวเตอร์ และการบันทึกในฐานข้อมูลโดยใช้โปรแกรมคอมพิวเตอร์ช่วย (Cabré, 1992: 50-51)

การประมวลศัพท์นั้นมีออกมาทั้งในรูปแบบอภิธานศัพท์ พจนานุกรมศัพท์เฉพาะ และเอกสารอื่น ๆ อีก ดังนั้น ความรู้ทางด้านการประมวลเอกสารและการจัดทำฐานข้อมูลจึงจำเป็นมากสำหรับศัพทวิทยา (Cabré, 1992: 52) เช่น โปรแกรมปัญญาประดิษฐ์ (Artificial Intelligence) ระบบผู้เชี่ยวชาญ (Expert System) และระบบฟัซซี่ (Fuzzy system) โปรแกรมเหล่านี้ใช้ทำโปรแกรมแปลและโปรแกรมหน่วยความจำในการแปล (Translation Memory) นอกจากนั้น ในปัจจุบันยังมีโปรแกรมที่ช่วยนักแปลในการแปล หรือ Computer-aided translation ซึ่งต้องใช้ศัพทวิทยาในการทำคลังคำศัพท์เฉพาะเช่นกัน

ดังที่ได้กล่าวไปในตอนต้นแล้ว คอมพิวเตอร์มีส่วนช่วยให้การทำงานทางด้านศัพทวิทยาเป็นไปได้อย่างสะดวกและทันสมัยมากขึ้นโดยแรกเริ่มเดิมที คอมพิวเตอร์นำมาใช้ในการเก็บข้อมูลและสร้างรายชื่อหนังสือโดยทำเป็นคลังคำขึ้นมา (Data bank) ภายหลัง ได้มีการนำคอมพิวเตอร์มาเก็บคำศัพท์ในรูปแบบของพจนานุกรมเพื่อนำไปใช้ในการแปล เมื่อคอมพิวเตอร์ได้มีการพัฒนาขึ้น การทำคลังคำและพจนานุกรมแบบอิเลคทรอนิกส์ก็ได้มีการพัฒนาขึ้นเหมือนกันโดยขนาดของฐานข้อมูลมีขนาดเล็กลงและมีความยืดหยุ่นมากขึ้น มีการพัฒนาเป็นอินเตอร์เฟสการใช้งานขึ้นมาทำให้ผู้ใช้งานรู้สึกว่าใช้งานได้ง่ายขึ้น นอกจากนั้น คลังคำศัพท์เหล่านี้ยังสามารถจัดเก็บไว้ในซีดีรอมเพื่อที่นักแปลสามารถนำกลับไปใช้ที่คอมพิวเตอร์ของตนเองได้ ต่อมาเมื่อเทคโนโลยีการค้นหาข้อมูลมีมากขึ้นและขนาดความจุของคอมพิวเตอร์มีมากขึ้น ผู้ใช้งานสามารถหาคำศัพท์ได้อย่างรวดเร็วขึ้นและในคอมพิวเตอร์เครื่องหนึ่ง สามารถบรรจุโปรแกรมเก็บคำศัพท์เฉพาะพจนานุกรมได้มากกว่า 1 เล่ม โปรแกรมพิมพ์เอกสารต่าง ๆ เพื่อใช้จัดเก็บข้อมูล โปรแกรมหาข้อมูลเพื่อหามโนทัศน์ใหม่ ๆ ได้อย่างอัตโนมัติ ศัพทวิทยายังนำไปใช้ในระบบผู้เชี่ยวชาญอีกด้วย ในปัจจุบัน วิทยาการคอมพิวตอร์พัมนาขึ้นมาอย่างมาก ศัพทวิทยายังได้นำไปใช้ในโปรแกรมที่ใช้เพื่อการตัดสินใจ (Decision Making Program) โดยสร้างเป็นส่วนหนึ่งของกฎที่ใช้ในการตัดสินใจ (Decision rule) ในระบบ (Cabré, 1992: 35)

ความแตกต่างประการที่ห้า คือ คำศัพท์ (Word) ที่รวบรวมอยู่ในพจนานุกรมทางภาษาทั่วไปนั้นจะเป็นคำที่ได้รับการอธิบายความหมายเดี่ยว ๆ ไม่ได้แต่ต้องอธิบายหน้าที่ทางภาษาด้วย เพราะคำเหล่านี้เป็นหน่วยย่อยของการสื่อสาร เกี่ยวข้องกับผู้ใช้งานทางภาษาในแง่มุมไหนบ้าง และเมื่อนำไปใช้ในสถานการณ์หรือหัวข้อเรื่องการสื่อสารที่ต่างกันนั้น คำเหล่านี้จะมีความหมายอย่างไรบ้าง แต่ศัพท์ (Term) ที่อยู่ในประมวลศัพท์เฉพาะจะบอกแค่ความหมายและชื่อเรียกความหมายนั้น ๆ อย่างเดียวและไม่มีข้อมูลการใช้งาน

เนื่องจากมีการคาดการณ์ไว้ก่อนหน้านั้นอยู่แล้วว่า ผู้ใช้งานคำศัพท์เฉพาะนั้นเป็นนักวิชาการหรือผู้ที่มีความรู้ในสาขานั้น ๆ อยู่แล้วจึงไม่ต้องคำนึงมากนัก (Cabré, 1992: 35-36)

ความแตกต่างประการที่หก คือ จุดประสงค์ของพจนานุกรมและการประมวลศัพทเฉพาะนั้นมีความแตกต่างกัน กล่าวคือ ข้อมูลในพจนานุกรมมีไว้เพื่อให้ผู้ใช้งานนั้นสามารถนำไปใช้ในภาษาพูดในสถานการณ์ต่าง ๆ ได้ ในขณะที่ศัพท์เฉพาะในการประมวลศัพท์นั้นจะใช้เพื่อนำไปอ้างถึงหน่วยย่อยของความรู้ในโลกของความเป็นจริง การประมวลศัพท์จะไม่นำเสนอการนำไปใช้งานจริงดั่งในพจนานุกรม แต่จะเน้นไปที่กฎการเลือกคำศัพท์ที่จะเหมาะสมในการอธิบายหน่วยความรู้ให้ผู้ใช้งานเข้าใจตรงกันมากที่สุด (Cabré, 1992: 36-37)

ความแตกต่างประการที่เจ็ด คือ วิธีวิทยาที่ใช้ในการรวบรวมคำศัพท์ การรวบรวมคำศัพท์ในพจนานุกรมภาษาทั่วไปจะใช้สมมติฐานในทางทฤษฎีของภาษาและนำเสนอตัวอย่างประโยคที่ผู้พูดใช้ในโอกาสต่าง ๆ เพื่อเป็นการอธิบายคำศัพท์นั้น ๆ ส่วนการประมวลศัพท์นั้น จะไม่มีการคำนึงถึงพฤติกรรมของผู้ใช้งานคำศัพท์นั้น แต่จะนำเสนอคำที่จะมาใช้เรียกมโนทัศน์ที่ค้นพบได้มากกว่า (Cabré, 1992: 37)

บทที่ 3
ขั้นตอนเบื้องต้นในการทำประมวลศัพท์

ในบทนี้ จะขอกล่าวถึงขั้นตอนในการทำประมวลศัพท์และเอกสารที่มีส่วนใช้ในการค้นหาศัพท์นั้น ๆ โดยคาเบรกล่าวถึงหลักในการทำประมวลศัพท์ว่ามีสองวิธีการหลัก ๆ ด้วยกัน นั่นคือ การค้นหาคำศัพท์แบบเป็นระบบ (Systematic search) และการค้นหาศัพท์แบบเฉพาะหน้า (Ad-hoc search) (Cabré, 1992: 129-159)

3.1. ระเบียบวิธีในการทำประมวลศัพท์

ดั่งที่กล่าวไปแล้วในข้างต้น ระเบียบวิธีการในการทำประมวลศัพท์นั้นมีอยู่ 2 วิธีหลัก ๆ ด้วยกัน วิธีการทั้งสองนี้มีความแตกต่างกัน กล่าวคือ ถ้าเป็นการค้นหาศัพท์แบบเป็นระบบ (Systematic search) นั้นจะรวบรวมและอธิบายคำศัพท์ที่ครอบคลุมสาขาเฉพาะสาขานั้น ๆ หรือส่วนหนึ่งของคำศัพท์กลุ่มที่ว่านี้ ส่วนการค้นหาศัพท์เฉพาะหน้า (Ad-hoc search) นั้นจะมุ่งเน้นไปที่การรวบรวมและอธิบายคำศัพท์คำใดคำหนึ่งหรือกลุ่มเฉพาะเล็ก ๆ ซึ่งส่วนใหญ่จะเป็นวิธีการที่ใช้ในการหาศัพท์ที่มีผู้ถามมาเป็นครั้ง ๆ ไป (Cabré, 1992: 129-159)

การจัดทำประมวลศัพท์ในครั้งนี้ได้ดำเนินการอย่างเป็นระบบโดยใช้หลักการแบบ Systematic Terminology และมีระเบียบวิธีในการจัดทำตามขั้นตอนดังต่อไปนี้

1. กำหนดหัวข้อและขอบเขตของเรื่องที่จะศึกษา รวมถึงจุดประสงค์ของการทำประมวลศัพท์
2. หาข้อมูลที่จะนำมาสร้างเป็นคลังข้อมูลภาษาพร้อมกับหาผู้เชี่ยวชาญทางด้านสาขานี้เพื่อตรวจสอบผลงานในตอนท้าย
3. สร้างคลังข้อมูลภาษา โดยรวบรวมจากตัวบทประเภทต่างๆที่ได้คัดเลือกตามเกณฑ์ที่ได้กำหนดไว้
4. คัดเลือกและดึงศัพท์จากคลังข้อมูลที่สร้างขึ้น หลังจากที่พิจารณาแล้วเห็นว่าคำเหล่านั้นเป็นศัพท์เฉพาะทางของสาขาวิชา หรืออยู่ในขอบเขตของหัวข้อที่ได้กำหนดไว้
5. สร้างมโนทัศน์สัมพันธ์ (Conceptual network) ซึ่งแสดงให้เห็นถึงความสัมพันธ์ของแต่ละมโนทัศน์ที่เชื่อมโยงซึ่งกันและกัน และอยู่ในขอบเขตของหัวข้อในการทำประมวลศัพท์ที่กำหนดไว้
6. จัดทำบันทึกข้อมูลศัพท์เบื้องต้น (Extraction record) โดยบันทึกรายละเอียดต่างๆของศัพท์ที่ดึงมาจากคลังข้อมูลที่จัดทำไว้ ได้แก่ รูปศัพท์, บริบทของคำนั้นๆ ที่มาของเอกสาร และข้อมูลทางไวยากรณ์อื่นๆ

7. จัดทำบันทึกข้อมูลศัพท์ (Terminological record) ซึ่งจะเป็นการบันทึกและแสดงผลรายละเอียดทุกอย่างของศัพท์เฉพาะทางนั้นๆอย่างเป็นระเบียบไม่ว่าจะเป็น คำนิยาม หน้าที่ทางไวยากรณ์ ตัวอย่างการใช้ศัพท์ รายการอ้างอิง หรือคำที่มีความหมายเหมือน เป็นต้น
8. ทบทวนชุดคำศัพท์เพื่อความถูกต้อง
9. ระบุปัญหาที่พบและหาทางแก้ไข

ในหัวข้อถัดไป จะกล่าวถึงรายละเอียดของการทำประมวลศัพท์ด้านการจัดการรักษาความปลอดภัยของข้อมูลแต่ละขั้นตอน โดยจะกล่าวถึงขั้นตอนเบื้องต้นก่อนสำหรับในบทนี้

3.2. ขอบเขตและจุดประสงค์ในการจัดทำประมวลศัพท์

การจัดการความปลอดภัยของข้อมูล (Information Security Management) ถือเป็นสาขาย่อยสาขาหนึ่งของวิทยาการเทคโนโลยีสารสนเทศ (Information Technology) ซึ่งในสาขาการจัดการความปลอดภัยของข้อมูลนี้สามารถแยกได้เป็นหลาย ๆ แขนงย่อยด้วยกัน เช่น ความปลอดภัยของระบบเครือข่ายและนโยบายการรักษาความปลอดภัยของข้อมูล โดยในการทำวิจัยครั้งนี้ ผู้จัดทำได้เลือกทำประมวลศัพท์เจาะลงไปในคำศัพท์ซึ่งใช้ในการร่างนโยบายการจัดการความปลอดภัยของข้อมูล (Information Security Policy) เนื่องจากองค์กรหลาย ๆ องค์กรในเมืองไทยได้ให้ความสนใจในการร่างนโยบายการจัดการความปลอดภัยของข้อมูลอย่างมากขึ้นตามลำดับ และโดยทั่วไปนั้น นโยบายเหล่านี้มักจะมีอภิธานศัพท์แนบท้ายมาเสนอเพื่อเป็นการสร้างความกระจ่างให้กับผู้ใช้งานและผู้อ่านทุกคน

สำหรับคลังข้อมูลที่ใช้ในการทำประมวลศัพท์นั้น ผู้จัดทำได้รวบรวมมาจากตัวมาตรฐานการจัดการความปลอดภัยของข้อมูลที่ออกโดยสถาบันด้านมาตรฐานของประเทศอังกฤษ หรือ British Standard Institute เป็นหลักซึ่งคู่มือเล่มนี้เขียนโดย กระทรวงการค้าและอุตสาหกรรมแห่งประเทศอังกฤษ (Department of Trade and Industry or DTI) และให้ชื่อว่า BS7799 และต่อมาได้นำไปพัฒนาต่อโดย ISO ซึ่งตั้งชื่อมาตรฐานตัวนี้ว่า ISO17799 โดยเนื้อหาหลัก ๆ ใน BS7799 นั้นจะพูดถึงนโยบายการรักษาความปลอดภัย (Security Policy), ระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management System หรือ ISMS) และการจัดการและวิเคราะห์ความเสี่ยง (Risk Analysis and Management) องค์กรที่ต้องการจะผันองค์กรของตนเองให้มีมาตรการรักษาความปลอดภัยของข้อมูลของตนนั้นจะต้องร่างนโยบายการรักษาความปลอดภัยของข้อมูลให้สอดคล้องและได้มาตรฐานกับ BS7799 หรือ ISO17799 โดยทั้งสิ้น

นอกจากนี้ คลังข้อมูลที่ใช้ยังครอบคลุม บทความ (Article), เอกสารปกขาว (White paper) และสิ่งตีพิมพ์อื่น ๆ ที่ออกโดยสถาบันที่ตั้งขึ้นเพื่อให้ความรู้และสร้างมาตรฐานแก่การจัดการความปลอดภัยของข้อมูลโดยเฉพาะ อย่างเช่น สิ่งตีพิมพ์จากหน่วยงานเอส.เอ.เอ็น.เอส ซึ่งเป็นหน่วยงานที่ออกใบประกาศและจัดการอบรมทางด้านการจัดการความปลอดภัยของข้อมูลที่เชื่อถือได้มากที่สุดแห่งหนึ่งในโลก (www.sans.org) และสิ่งตีพิมพ์จากสถาบันด้านมาตรฐานและเทคโนโลยีของรัฐบาลสหรัฐอเมริกา หรือ

National Institute of Standards and Technology (NIST) ซึ่งเป็นหน่วยงานรัฐบาลของประเทศสหรัฐอเมริกาที่มุ่งพัฒนาและส่งเสริมมาตรฐานต่าง ๆ และเทคโนโลยีให้กับประเทศอเมริกาและได้มีสิ่งตีพิมพ์ออกมาเป็นจำนวนมากที่เกี่ยวกับการจัดการความปลอดภัยของข้อมูล และนับเป็นที่เชื่อถือจากองค์กรเอกชนและหน่วยงานรัฐบาลจากประเทศต่าง ๆ ทั่วโลกอีกด้วย

นอกจากบทความและสิ่งตีพิมพ์ที่ออกโดยหน่วยงานต่าง ๆ นี้แล้ว ผู้จัดทำยังได้รวบรวมบทความทางวิชาการที่เกี่ยวข้องกับการจัดการความปลอดภัยของข้อมูลจากฐานข้อมูลทางวิชาการต่าง ๆ ที่ค้นหาได้จากฐานข้อมูลบทความของจุฬาฯ อย่างเช่น ACM Portal และ Applied Science & Technology Full Text ซึ่งเป็นฐานข้อมูลที่รวบรวมบทความทางวิชาการเชิงเทคโนโลยีไว้ บทความที่ปรากฏในฐานข้อมูลเหล่านี้นั้นเขียนโดนนักวิชาการที่มีความรู้ในสาขานั้น ๆ เป็นอย่างดี

ในการจัดทำประมวลศัพท์ในครั้งนี้ ผู้จัดทำได้รวบรวมคำศัพท์ในชุดของการจัดการความปลอดภัยของข้อมูลที่มักพบบ่อยในชุดนโยบายจัดการความปลอดภัยขององค์กรทั่ว ๆ ไปโดยจะถือเป็นส่วนหนึ่งของศัพท์ทางด้านการรักษาความปลอดภัยของข้อมูล แต่ส่วนมากศัพท์ที่ได้รับการบรรจุอยู่ในอภิธานศัพท์ในนโยบายที่ใช้องค์กรนั้นจะมุ่งไปที่การสื่อสารความรู้ทางด้านนี้ให้คนในองค์กรเข้าใจตรงกัน ศัพท์ด้านความปลอดภัยที่ระบุไว้ในอภิธานศัพท์นั้นมักจะเป็นศัพท์การรักษาความปลอดภัยเบื้องต้นที่ไม่เจาะลึกทางด้านเทคนิคมากนักเนื่องจากผู้ที่อ่านนั้นคือคนทุกคนในองค์กรซึ่งอาจจะไม่มีความรู้ทางด้านคอมพิวเตอร์มากนักและมักเป็นคำศัพท์ที่เกี่ยวข้องกับการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ ดังนั้นในชุดของคำศัพท์ที่นำมาทำประมวลศัพท์ด้านการจัดการรักษาความปลอดภัยนั้นจะเกี่ยวข้องกับศัพท์รักษาความปลอดภัยของข้อมูลเบื้องต้นที่ระบุไว้ในนโยบายด้านความปลอดภัย และมีคำศัพท์ที่พบได้บ่อยในอภิธานศัพท์ของนโยบายการจัดการการักษาความปลอดภัยของข้อมูลรวบรวมทั้งหมด 91 คำ

3.3. การเลือกผู้เชี่ยวชาญ

หลังจากที่เราค้นหาข้อมูลที่เกี่ยวข้องกับหัวข้อในการทำประมวลศัพท์แล้วนั้น เราจะต้องหาผู้เชี่ยวชาญในสาขาที่เราทำเพื่อมาเป็นที่ปรึกษาโดยในโครงการการจัดทำประมวลศัพท์นั้นจะต้องประกอบไปด้วยนักภาษาศาสตร์และผู้เชี่ยวชาญในสาขานั้น ๆ เพื่อช่วยกันตรวจสอบความถูกต้องของประมวลศัพท์ (Cabré, 1992: 134)

ในการจัดทำประมวลศัพท์นี้ ผู้จัดทำได้รับความอนุเคราะห์จาก คุณพงศ์สิทธิ์ จิตตโอวาท ซึ่งเป็นผู้ที่มีความเชี่ยวชาญในด้านการจัดการความปลอดภัยของข้อมูลมาเป็นเวลากว่า 5 ปี ตอนนี้คุณพงศ์สิทธิ์ดำรงตำแหน่งเป็น Operation Manager ที่บริษัท Absolute Impact

3.4. การรวบรวมข้อมูลเพื่อสร้างคลังข้อมูลภาษา

คาเบร (1992: 116 – 121) ได้กล่าวไว้ว่า ในการสร้างคลังข้อมูลภาษานั้น ต้องการข้อมูลจากเอกสารทั้งหมด 3 ประเภทด้วยกัน คือ

3.4.1. **เอกสารอ้างอิง** (Reference Documents)

เอกสารอ้างอิง คือ เอกสารที่นักประมวลศัพท์ใช้ในการเรียนรู้ข้อมูลทางด้านทฤษฎี วิธีวิทยา และหนังสือต่าง ๆ ที่เกี่ยวข้องกับหัวข้อที่ใช้ทำประมวลศัพท์ และยังรวมไปถึงเอกสารทางวิชาการหรือทางวิทยาศาสตร์ที่เกี่ยวข้องกับชุดคำศัพท์ที่รวบรวมมาด้วย นอกจากนั้น เอกสารอ้างอิงยังรวมไปถึงทฤษฎีที่เกี่ยวข้องกับศัพทวิทยาและภาษาของชุดประมวลศัพท์ ข้อมูลอ้างอิงนี้สามารถนำไปใช้ในการสร้างมโนทัศน์สัมพันธ์ของศัพท์ในชุดประมวลศัพท์

เอกสารอ้างอิงที่ใช้ในการประมวลศัพท์นโยบายด้านการจัดการความปลอดภัยของข้อมูลมีดังนี้

- ประมวลศัพท์ด้านการจัดการความปลอดภัยของข้อมูลและการป้องกันการกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (www.infosec.gov.hk/docs/english/**glossary**_eng.pdf)
- ประมวลศัพท์ด้านการความปลอดภัยกับการตรวจจับการบุกรุกในระบบเครือข่ายคอมพิวเตอร์ที่จัดทำโดยหน่วยงานเอส.เอ.เอ็น.เอส ซึ่งเป็นหน่วยงานที่ออกใบประกาศและจัดการอบรมทางด้านการจัดการความปลอดภัยของข้อมูลที่เชื่อถือได้มากที่สุดแห่งหนึ่งในโลก (http://www.sans.org/resources/glossary.phpฺX)
- ประมวลศัพท์ด้านความปลอดภัยของข้อมูลที่เป็นคำหลัก ๆ จัดทำขึ้นโดย สถาบันด้านมาตรฐานและเทคโนโลยีของรัฐบาลสหรัฐอเมริกา หรือ National Institute of Standards and Technology (NIST) (http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf)
- ประมวลศัพท์ด้านความปลอดภัยของข้อมูล จัดทำโดยสำนักพิมพ์ Information Security Today ซึ่งตีพิมพ์หนังสือทั้งในรูปแบบซีดีรอมและหนังสือรวมเล่มที่เน้นหนักทางด้านการรักษาความปลอดภัยของข้อมูล (http://www.infosectoday.com/Articles/Glossary.pdf)
- ประมวลศัพท์ด้านความปลอดภัยของข้อมูล รวบรวมโดมหาวิทยาลัยฮาร์เวิร์ด (http://www.security.harvard.edu/glossary.php)
- พจนานุกรมศัพท์เทคโนโลยีสารสนเทศ ฉบับราชบัณฑิตยสถาน ตีพิมพ์ในปีพ.ศ. 2542
- ข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์รวบรวมโดยหน่วยงานเอส.เอ.เอ็น.เอส (SANS) (SAN Institute - Information and Computer Security Resources) (http://www.sans.org/resources/resources.php)
- เอกสารระเบียบการการจัดการความปลอดภัยของข้อมูลจัดทำโดยองค์กร British Standards ซึ่งเป็นองค์กรที่จัดตั้งมาตรฐาน BS7799 ซึ่งเป็นมาตรฐานที่องค์กรต่าง ๆ ถือปฏิบัติตาม

เอกสารนี้มีชื่อว่า Information Technology – Security Techniques – Code of practice for information security management

- เอกสารแนวางการจัดตั้งนโยบายการรักษาความปลอดภัยของข้อมูลเพื่อนำไปใช้งานจัดทำโดยองค์กร British Standards ซึ่งเป็นองค์กรที่จัดตั้งมาตรฐาน BS7799 ซึ่งเป็นมาตรฐานที่องค์กรต่าง ๆ ถือปฏิบัติตาม เอกสารนี้มีชื่อว่า Information Security management systems – specification with guidance for use

3.4.2. **เอกสารเฉพาะทาง** (Specific Documents)

เอกสารเฉพาะทางรวบรวมได้จากบทสนทนาของผู้เชี่ยวชาญในด้านของหัวข้อคำศัพท์ที่อยู่ในชุดประมวลศัพท์และเอกสารทางวิชาการที่ผู้เชี่ยวชาญเหล่านี้เขียนขึ้นมา เพราะนักเชี่ยวชาญเหล่านี้จะต้องใช้คำศัพท์เฉพาะทาง (Term) ในการสื่อสารข้อมูลใหม่ ๆ หรือแก้ไขคำศัพท์ที่มีอยู่แล้วให้สะท้อนถึงหลักความเป็นจริงมากขึ้น คาเบรได้แนะนำไว้ว่า เอกสารเฉพาะทางจะต้องประกอบไปด้วยคุณสมบัติเหล่านี้

- เอกสารเฉพาะทางนี้จะต้องเป็นตัวแทนชุดคำศัพท์เฉพาะนั้น ๆ ได้ โดยจะต้องประกอบไปด้วยคำศัพท์จำนวนมากพอสมควร
- เอกสารเฉพาะทางนี้จะต้องมีความทันสมัยอยู่เสมอ
- เอกสารเฉพาะทางต้องมีความเชื่อถือได้และสามารถนำมาใช้ได้ตลอดไม่ว่าจะมีการใช้งานในช่วงเวลาใดก็ตาม

3.4.3. **เอกสารสนับสนุน** (Support Documents)

เอกสารสนับสนุน คือ บันทึกการทำประมวลศัพท์ซึ่งสำหรับการค้นหาศัพท์แบบเป็นระบบนั้น จะมีการบันทึกอยู่ 3 ประเภทด้วยกัน คือ บันทึกข้อมูลศัพท์เบื้องต้น (Extraction records) บันทึกข้อมูลศัพท์ (Terminological records) และ บันทึกข้อมูลโยงกับศัพท์ภาษาอื่น ๆ (Correspondence records) (Cabré, 1992: 121 – 127) ในประมวลศัพท์การจัดการความปลอดภัยของข้อมูลชุดนี้จะมีการบันทึกศัพท์แบบสองแบบแรกเท่านั้นซึ่งจะกล่าวถึงในบทต่อไป

3.5. **เกณฑ์การเลือกข้อมูลสำหรับคลังข้อมูลภาษา**

ในการคัดเลือกตัวบทที่จะนำมารวบรวมไว้ในคลังข้อมูลนั้น ผู้จัดทำได้พิจารณาลักษณะของเอกสารตามสถานการณ์สื่อสารตามหลักเกณฑ์ของ Pearson (1998) และสามารถจำแนกประเภทของตัวบทที่รวบรวมไว้ในคลังข้อมูลได้ดังนี้

1) เอกสารที่เขียนโดยผู้เชี่ยวชาญเพื่อให้ผู้เชี่ยวชาญที่อยู่ในวงการเดียวกันอ่าน (Expert to expert communication) รวมจำนวนคำทั้งสิ้น 90,551 คำ ประกอบไปด้วยตัวบทแบ่งตามลักษณะที่มาดังต่อไปนี้

- ACM Portal ซึ่งเป็นฐานข้อมูลที่รวบรวมบทความทางวิชาการเชิงเทคโนโลยีไว้ ค้นหาผ่านฐานข้อมูลของจุฬาฯ (http://portal.acm.org/dl.cfm)
- Applied Science & Technology Full Text ซึ่งเป็นฐานข้อมูลที่รวบรวมบทความเชิงเทคโนโลยีอีกฐานหนึ่ง ค้นหาผ่านฐานข้อมูลของจุฬาฯ (http://vnweb.hwwilsonweb.com/hww/)
- หน่วยงาน National Institute of Standards and Technology ซึ่งเป็นหน่วยงานภาครัฐของสหรัฐอเมริกาที่ให้ความรู้และให้บริการการจัดการความปลอดภัยของข้อมูล (http://csrc.nist.gov)
- หน่วยงาน ISMS International User Group ซึ่งก่อตั้งโดยกระทรวงพานิชย์และอุตสาหการของสหรัฐอเมริกาเพื่อช่วยในการแชร์ความรู้และประสบการณ์การใช้งานมาตรฐานการจัดการรักษาความปลอดภัยของข้อมูล ISO/IEC 17799 and BS 7799 Part 2 (http://www.xisec.com/)
- สถาบันตรวจสอบภายในของสหรัฐอเมริกาซึ่งเป็นหน่วยงานที่ตรวจสอบว่าองค์กรต่าง ๆ ในอเมริกาทำตามข้อบังคับทางด้านเทคโนโลยีสารสนเทศหรือไม่ (http://www.theiia.org/)
- กระทรวงพานิชย์และอุตสาหการของประเทศอังกฤษ (http://www.dti.gov.uk/)
- สำนักงานตรวจสอบความไว้วางใจรัฐบาลของสหรัฐอเมริกา หรือ จี.เอ.โอ ซึ่งมีหน้าตรวจสอบการใช้เงินของภาครัฐบาลในสหรัฐอมริกา (www.gao.gov)

2) เอกสารที่เขียนโดยผู้เชี่ยวชาญเพื่อให้ผู้ที่อยู่ในแวดวงเดียวกัน แต่ผู้อ่านไม่เชี่ยวชาญเท่า (Expert to initiates communication) รวมจำนวนคำทั้งสิ้น 18,809 คำ ประกอบด้วยตัวบทแบ่งตามลักษณะที่มาดังต่อไปนี้

- เอส.เอ.เอ็น.เอส ซึ่งเป็นหน่วยงานที่ออกใบประกาศและจัดการอบรมทางด้านการจัดการความปลอดภัยของข้อมูลที่เชื่อถือได้มากที่สุดแห่งหนึ่งในโลก (www.sans.org)
- บริษัทที่จัดจำหน่ายนโยบายการจัดการความปลอดภัยของข้อมูลแบบสำเร็จรูปแบบต่าง ๆ และมีตัวอย่างของนโยบายโหลดให้ทดลองใช้งานชั่วคราวด้วย (http://www.information-security-policies.com/)

3) เอกสารที่เขียนขึ้นเพื่อให้ความรู้ในเรื่องนั้นๆแก่ผู้ที่ไม่เคยมีความรู้มาก่อน (Teacher to pupil communication) รวมจำนวนคำทั้งสิ้น 155,396 คำ ประกอบด้วยตัวบทแบ่งตามลักษณะที่มาดังต่อไปนี้

- บริษัท อาร์คไซต์ ซึ่งเป็นบริษัทที่ได้ให้บริการการจัดการความปลอดภัยของข้อมูลขององค์กรต่าง ๆ โดยให้คำปรึกษาในด้านการจัดการความเสี่ยงของข้อมูลและปกป้องสินทรัพย์ทางข้อมูลขององค์กร (http://www.arcsight.com/)

- เว็บไซต์ที่ให้ความรู้ทางด้านการจัดการความปลอดภัยให้กับไมโครซอฟต์วินโดวส์ ตั้งแต่การตรวจจับการบุกรุก (Intrusion Detection) โปรแกรมต่อต้านไวรัส (Anti-virus) และไฟร์วอลล์ (Firewall) (http://www.windowsecurity.com/)

ผู้จัดทำได้รวบรวมตัวบทสามประเภทข้างต้นไว้ในคลังข้อมูลภาษา เนื่องจากตัวบททั้งประเภท Expert-to-initiates และ Teacher-to-pupil ที่ผู้จัดทำเลือกมานั้นมีบริบทที่ช่วยอธิบายความหมายและให้นิยามของคำศัพท์ (Defining context) และสำหรับตัวบทประเภท Expert-to-expert นั้นมีบริบทที่ช่วยชี้ว่าคำศัพท์นั้นมีใช้อยู่จริง ๆ ในสาขาหรือระบบภาษาชนิดนั้น ๆ (Testimonial Context) ซึ่งทำให้ตัวบททั้งสามประเภทนั้นเอื้อต่อการการทำประมวลศัพท์เป็นอย่างมาก กล่าวคือ ในตัวบทประเภท Expert-to-expert นั้น ผู้ส่งสารและผู้รับสารมีประสบการณ์ร่วมกันในสาขาวิชานั้น ๆ มีการใช้คำศัพท์เฉพาะโดยที่ไม่ได้อธิบายเพิ่มเติม แต่ทำให้เราทราบว่ามีคำศัพท์นั้นใช้อยู่จริงในสาขานั้น ๆ ในตัวบทประเภท expert to initiates นั้น ผู้ส่งสารซึ่งเป็นผู้เชี่ยวชาญจะถือว่าผู้รับสารมีความรู้เบื้องต้นในระดับหนึ่งแต่ไม่ได้มีความเชี่ยวชาญเท่าตน เมื่อมีการใช้ศัพท์เฉพาะทางบางคำที่ยากต่อความเข้าใจของผู้อ่าน ผู้ส่งสารก็จะให้คำอธิบายศัพท์นั้นไว้บ้างเป็นบางครั้ง แต่ถ้าเป็นศัพท์เฉพาะทางเบื้องต้นที่ผู้ส่งสารสันนิษฐานว่าผู้รับสารควรรู้ ก็อาจไม่ให้คำอธิบายใดๆไว้ สำหรับตัวบทประเภท teacher-pupil ผู้ส่งสารกับผู้รับสารจะมีระดับความรู้ในด้านนั้นๆต่างกันมาก โดยผู้ส่งสารเป็นผู้เชี่ยวชาญในขณะที่ผู้รับสารไม่มีความรู้ใดๆในด้านนั้นเลย ผู้ส่งสารจะมีจุดประสงค์ในการสื่อสารเป็นไปในเชิงสอน ดังนั้นเมื่อมีกล่าวถึงศัพท์เฉพาะทางใดๆ ก็มักจะพบคำอธิบายกำกับไว้บ่อยครั้ง

ทั้งนี้ทั้งนั้น การใช้ตัวบททั้งสามประเภทจะช่วยให้เราเข้าใจคำศัพท์เฉพาะทางได้มากขึ้นจากตัวบทที่อยู่ในบริบทที่ให้นิยามคำศัพท์ชัดเจนและจากตัวบทที่มีบริบทแบบ Testimonial context จะช่วยให้เรามั่นใจได้มากขึ้นว่าคำศัพท์ที่เราเลือกมานั้นมีใช้อยู่ในสาขานั้นจริง ๆ

3.6. รายละเอียดคลังข้อมูลภาษา

ข้อมูลที่นำมารวบรวมในคลังข้อมูลภาษานี้เป็นข้อมูลชนิดอิเลคทรอนิกส์ทั้งหมด โดยหาข้อมูลทั้งหมดจากการใช้ Search Engine เช่น เว็บไซต์กูเกิ้ล (www.google.com) และเว็บไซต์ยาฮู (www.yahoo.com) นอกจากนั้นยังมีเอกสารประกอบจำพวกนโยบายการรักษาความปลอดภัยของข้อมูลซึ่งเก็บเป็นข้อมูลชนิดอิเลคทรอนิกส์เช่นกัน เมื่อได้ข้อมูลเหล่านี้มาทั้งหมดแล้ว ก็นำไปทำเป็น Text File เพื่อไปประมวลผลต่อไปในโปรแกรม Win Concordance และ CU Collocation Extract (Version 2.4)

สำหรับความน่าเชื่อถือของข้อมูลนั้น ผู้จัดทำได้พยายามเลือกข้อมูลที่มาจากสถาบันที่น่าเชื่อถือซึ่งมักจะเป็นสถาบันรัฐบาลหรือสถาบันวิจัยในสหรัฐอเมริกาและอังกฤษ เช่น หน่วยงานเอส.เอ.เอ็น.เอส (SANS) (SAN Institute - Information and Computer Security Resources) และสถาบันด้านมาตรฐานและเทคโนโลยีของรัฐบาลสหรัฐอเมริกา หรือ National Institute of Standards and Technology (NIST)

นอกจากนั้น ผู้จัดทำมักจะเลือกข้อมูลที่มีผู้แต่งมีความเชี่ยวชาญในสาขานี้โดยตรงและอาจจะเป็นผู้เขียนที่มีชื่อเสียงเชื่อถือได้ในระดับสูง

เนื่องจากการจัดการความปลอดภัยของข้อมูลนั้นเป็นเรื่องที่หลายฝ่ายให้ความสนใจ ข้อมูลที่มีอยู่ในสาขานี้จึงมักจะเป็นข้อมูลที่ออกมาใหม่เสมอโดยจะตีพิมพ์ทางหน้าเว็บไซต์ประกาศข่าวของเว็บไซต์ในหน่วยงานนั้น ๆ ดังนั้น จึงเป็นสาเหตุว่าผู้จัดทำจึงได้เลือกข้อมูลที่มาจากเว็บไซต์หลัก ๆ เพราะจะได้ข้อมูลที่ใหม่สดมากกว่าจากในตำราเรียนหรือหนังสือทางวิชาการ แต่สำหรับหนังสือเหล่านี้จะใช้เป็นเอกสารอ้างอิงตามที่ได้กล่าวไปในหัวข้อข้างต้น

คลังข้อมูลภาษาที่จัดทำขึ้นเพื่อนำมาใช้ในการทำประมวลศัพท์ในครั้งนี้มีขนาด 338,027 คำ มาจากแหล่งข้อมูลทั้งหมด 140 แหล่ง โดยรายละเอียดข้อมูลคลังภาษามีดังต่อไปนี้

ลำดับที่	001
รหัสอ้างอิง	ISM001.TXT
ที่มาของข้อมูล	http://www.allbusiness.com/technology/computer-software-management/891276-1.html
ชื่อเรื่อง	Enterprise Vulnerability Management and Its Role in Information Security Management
สรุปข้อมูล	เว็บไซต์ที่มีบทความทางด้านการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	All Business Ltd.
ขนาดของข้อมูล	12,230 คำ

ลำดับที่	002
รหัสอ้างอิง	ISM002.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/A_firewall_in_an_IT_system.html
ชื่อเรื่อง	A firewall in an IT system
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	2,829 คำ

ลำดับที่	003
รหัสอ้างอิง	ISM003.TXT

ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Access-Controls-What-is-it-how-undermined.html
ชื่อเรื่อง	Access Control – What was it and how it can be undermined?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,258 คำ

ลำดับที่	004
รหัสอ้างอิง	ISM004.TXT
ที่มาของข้อมูล	http://www.gao.gov/special.pubs/ai9868.pdf
ชื่อเรื่อง	Information Security Management – Learning from leading organizations
สรุปข้อมูล	เว็บไซต์ที่ให้ข้อมูลด้านความปลอดภัยของสำนักงานควบคุมและปกป้องภาษีประชาชนของรัฐบาลสหรัฐอเมริกา
จัดทำโดย	U.S. Government Accountability Office
ขนาดของข้อมูล	16,296 คำ

ลำดับที่	005
รหัสอ้างอิง	ISM005.TXT
ที่มาของข้อมูล	http://www.gao.gov/special.pubs/ai99139.pdf
ชื่อเรื่อง	Information Security Risk Management – Practices of Lead Organizations
สรุปข้อมูล	เว็บไซต์ที่ให้ข้อมูลด้านความปลอดภัยของสำนักงานควบคุมและปกป้องภาษีประชาชนของรัฐบาลสหรัฐอเมริกา
จัดทำโดย	U.S. Government Accountability Office
ขนาดของข้อมูล	13,409 คำ

ลำดับที่	006
รหัสอ้างอิง	ISM006.TXT
ที่มาของข้อมูล	http://www.theiia.org/iia/download.cfm?file=353
ชื่อเรื่อง	Audit security controls that work
สรุปข้อมูล	เว็บไซต์ที่ให้ความรู้กับผู้ตรวจสอบ

จัดทำโดย	The Institute of Internal Auditors
ขนาดของข้อมูล	2,251 คำ

ลำดับที่	007
รหัสอ้างอิง	ISM007.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Auditing-user-accounts.html
ชื่อเรื่อง	Auditing user accounts
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,436 คำ

ลำดับที่	008
รหัสอ้างอิง	ISM008.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/.../Authorization-Manager-Role-Based-Administration-Windows-Server-2003-Part2.html
ชื่อเรื่อง	Network Security Articles for Window Server 2003 Part 2
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	963 คำ

ลำดับที่	009
รหัสอ้างอิง	ISM009.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Being-Big-Brother-Monitoring-employees-network-activity.html
ชื่อเรื่อง	Being Big Brother – Monitoring Employee Network Activity
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,422 คำ

ลำดับที่	010

รหัสอ้างอิง	ISM010.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Biometrics-and-You.html
ชื่อเรื่อง	Biometric and You
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,252 คำ

ลำดับที่	011
รหัสอ้างอิง	ISM011.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Built-in-Groups-Delegation.html
ชื่อเรื่อง	Built-in Groups VS. Delegation
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,541 คำ

ลำดับที่	012
รหัสอ้างอิง	ISM012.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Authentication-Forgotten-Predominant.html
ชื่อเรื่อง	Caveat Lector – Authentication, Forgotten, and Should-be Predominant
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,536 คำ

ลำดับที่	013
รหัสอ้างอิง	ISM013.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Changing-Passwords-Key-User-Accounts.html
ชื่อเรื่อง	Changing Passwords for Key User Accounts
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล

จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,447 คำ

ลำดับที่	014
รหัสอ้างอิง	ISM014.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Code-Signing.html
ชื่อเรื่อง	Code Signing – Is it a security feature?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,444 คำ

ลำดับที่	015
รหัสอ้างอิง	ISM015.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Review-GFI-LANguard-Portable-Storage-Control.html
ชื่อเรื่อง	Controlling Portable Storage Device Usage
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,801 คำ

ลำดับที่	016
รหัสอ้างอิง	ISM016.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Customizing-Windows-Security-Templates.html
ชื่อเรื่อง	Customizing Windows Security Template
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,397 คำ

ลำดับที่	017

รหัสอ้างอิง	ISM017.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Deciphering-Authentication-Events-Domain-Controllers.html
ชื่อเรื่อง	Deciphering Authentication Events on Your Domain Controllers
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,024 คำ

ลำดับที่	018
รหัสอ้างอิง	ISM018.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Digital_Signatures.html
ชื่อเรื่อง	Digital Signatures
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,560 คำ

ลำดับที่	019
รหัสอ้างอิง	ISM019.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Disk-Based-Backup.html
ชื่อเรื่อง	Disk Based Backup – All Hype or the Best Protection for Your Data
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,339 คำ

ลำดับที่	020
รหัสอ้างอิง	ISM020.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Email_Spam.html
ชื่อเรื่อง	E-mail Spam – Is it a Security Issue?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.

ขนาดของข้อมูล	1,750 คำ

ลำดับที่	021
รหัสอ้างอิง	ISM021.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Ethical-Issues-IT-Security-Professionals.html
ชื่อเรื่อง	Ethical Issues for IT Security Professionals
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,464 คำ

ลำดับที่	022
รหัสอ้างอิง	ISM022.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Evaluating-New-Security-Policy.html
ชื่อเรื่อง	Evaluating a New Security Policy
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,461 คำ

ลำดับที่	023
รหัสอ้างอิง	ISM023.TXT
ที่มาของข้อมูล	http://www.infosectoday.com/Articles/gassp.pdf
ชื่อเรื่อง	Generally Accepted System Security Principle
สรุปข้อมูล	เว็บไซต์ที่รวบรวมบทความและจำหน่ายหนังสือด้านการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Auerbach Ltd.
ขนาดของข้อมูล	21,647 คำ

ลำดับที่	024
รหัสอ้างอิง	ISM024.TXT

ที่มาของข้อมูล	http://www.connectingsomerset.co.uk/tips/website%20basics/Information%20Security%20-%20a%20glossary.pdf
ชื่อเรื่อง	Information Security Glossary
สรุปข้อมูล	เว็บไซต์ที่ให้คำปรึกษาด้านเทคโนโลยีสารสนเทศ
จัดทำโดย	Connecting Sommerset Ltd.
ขนาดของข้อมูล	3,784 คำ

ลำดับที่	025
รหัสอ้างอิง	ISM025.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Hackers-Security-Consultants.html
ชื่อเรื่อง	Hiring Hackers as Security Consultants
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,850 คำ

ลำดับที่	026
รหัสอ้างอิง	ISM026.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/How-Do-Compliance-Issues-Affect-your-Network.html
ชื่อเรื่อง	How Do Compliance Issues Affect Your Network?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,371 คำ

ลำดับที่	027
รหัสอ้างอิง	ISM027.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Spyware_Adware_Programs.html
ชื่อเรื่อง	How spyware and adware threaten network security and performance
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	2,391 คำ

ลำดับที่	028
รหัสอ้างอิง	ISM028.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/audit-network-packet-analysis.html
ชื่อเรื่อง	How to audit your network via packet analysis
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,381 คำ

ลำดับที่	029
รหัสอ้างอิง	ISM029.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Plan-Possible-Network-Attack.html
ชื่อเรื่อง	How to plan for a possible network attack
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,190 คำ

ลำดับที่	030
รหัสอ้างอิง	ISM030.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Ideal-to-Realized-Security-Assurance-Cryptographic-Keys-Part1.html
ชื่อเรื่อง	Ideal-to-Realized Security Assurance in Cryptographic Key (Part 1)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,430 คำ

ลำดับที่	031
รหัสอ้างอิง	ISM031.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Ideal-to-Realized-Security-Assurance-Cryptographic-Keys-Part2.html

ชื่อเรื่อง	Ideal-to-Realized Security Assurance in Cryptographic Key (Part 2)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,889 คำ

ลำดับที่	032
รหัสอ้างอิง	ISM032.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Implementing-Troubleshooting-Account-Lockout.html
ชื่อเรื่อง	Implementing and Troubleshooting Account Lockout
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,798 คำ

ลำดับที่	033
รหัสอ้างอิง	ISM033.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Implementing-Principle-Least-Privilege.html
ชื่อเรื่อง	Implementing Principle of Least Privilege
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,610 คำ

ลำดับที่	034
รหัสอ้างอิง	ISM034.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Increasing-Security-Limited-User-Accounts-Restricted-Groups.html
ชื่อเรื่อง	Increasing Security Limited User Accounts and Restricted Groups
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,737 คำ

ลำดับที่	035
รหัสอ้างอิง	ISM035.TXT
ที่มาของข้อมูล	Information Security Governance and Assurance by Charles H. Le Grand, Technology Practices, The Institute of Internal Auditors, Inc.
ชื่อเรื่อง	Information Security Governance and Assurance
สรุปข้อมูล	เว็บไซต์ที่ให้ความรู้กับผู้ตรวจสอบ
จัดทำโดย	The Institute of Internal Auditors
ขนาดของข้อมูล	8,918 คำ

ลำดับที่	036
รหัสอ้างอิง	ISM036.TXT
ที่มาของข้อมูล	http://www.unc.edu/hipaa/policies/Information_Security.pdf
ชื่อเรื่อง	Information Security Policy and Standards, The University of North Carolina at Chapel Hills
สรุปข้อมูล	เว็บไซต์นโยบายความปลอดภัยของมหาวิทยาลัยแห่งรัฐแคโรไลน่า สหรัฐอเมริกา
จัดทำโดย	The University of North Carolina at Chapel Hills
ขนาดของข้อมูล	3,447 คำ

ลำดับที่	037
รหัสอ้างอิง	ISM037.TXT
ที่มาของข้อมูล	Information Security Introduction Factsheet by Department of Trade and Industry, UK
ชื่อเรื่อง	Information Security Introduction Factsheet
สรุปข้อมูล	เว็บไซต์ที่ให้ข้อมูลด้านความปลอดภัยของข้อมูล ของกระทรวงการค้าและอุตสาหกรรมแห่งประเทศอังกฤษ
จัดทำโดย	Department of Trade and Industry, UK
ขนาดของข้อมูล	1,910 คำ

ลำดับที่	038
รหัสอ้างอิง	ISM038.TXT

ที่มาของข้อมูล	http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html
ชื่อเรื่อง	Intrusion Detection System (IDS) Part 2
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	4,715 คำ

ลำดับที่	039
รหัสอ้างอิง	ISM039.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Intrusion_Detection_Systems_IDS_Part__I_network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html
ชื่อเรื่อง	Intrusion Detection System (IDS) Part 1
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	3,547 คำ

ลำดับที่	040
รหัสอ้างอิง	ISM040.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/whitepaper/FAQ_Network_Intrusion_Detection_Systems_.html
ชื่อเรื่อง	Intrusion Detection System (IDS) FAQ
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	3,208 คำ

ลำดับที่	041
รหัสอ้างอิง	ISM041.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Encrypting-Your-E-mail.html
ชื่อเรื่อง	Is it time to start encrypting your e-mail?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล

จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,723 คำ

ลำดับที่	042
รหัสอ้างอิง	ISM042.TXT
ที่มาของข้อมูล	http://www.cncc.edu/institutional_research/cccs_it_security_plan.htm
ชื่อเรื่อง	Information Security Plan, Colorado Community College System
สรุปข้อมูล	เว็บไซต์แสดงแผนงานความปลอดภัยของข้อมูล ของวิทยาลัยโคโรลาโด
จัดทำโดย	Colorado Community College System
ขนาดของข้อมูล	1,706 คำ

ลำดับที่	043
รหัสอ้างอิง	ISM043.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Privacy-Keeping-information-confidential.html
ชื่อเรื่อง	Privacy – Keeping Your Information Confidential
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,659 คำ

ลำดับที่	044
รหัสอ้างอิง	ISM044.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Kerberos-Authentication-Events.html
ชื่อเรื่อง	Kerberos Authentication Events Explained
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,397 คำ

ลำดับที่	045

รหัสอ้างอิง	ISM045.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Internet-Safer-Employees.html
ชื่อเรื่อง	Making the Internet Safer for your Employees
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,612 คำ

ลำดับที่	046
รหัสอ้างอิง	ISM046.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Managed-E-Mail-Security-Services-right-solution-network.html
ชื่อเรื่อง	Managed e-mail security services: Is it the right solution for your network?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,055 คำ

ลำดับที่	047
รหัสอ้างอิง	ISM047.TXT
ที่มาของข้อมูล	http://portal.acm.org/citation.cfm?id=1059538
ชื่อเรื่อง	A novel scenario-based information security management exercise
สรุปข้อมูล	เว็บไซต์ที่รวบรวมบทความด้านวิทยาศาสตร์และเทคโนโลยี
จัดทำโดย	The ACM Portal
ขนาดของข้อมูล	3,688 คำ

ลำดับที่	048
รหัสอ้างอิง	ISM048.TXT
ที่มาของข้อมูล	http://portal.acm.org/citation.cfm?id=792704.792706&coll=GUIDE&dl=GUIDE&CFID=7570047&CFTOKEN=78916351
ชื่อเรื่อง	A policy framework for information security
สรุปข้อมูล	เว็บไซต์ที่รวบรวมบทความด้านวิทยาศาสตร์และเทคโนโลยี

จัดทำโดย	The ACM Portal
ขนาดของข้อมูล	3,271 คำ

ลำดับที่	049
รหัสอ้างอิง	ISM049.TXT
ที่มาของข้อมูล	http://portal.acm.org/ft_gateway.cfm?id=954028&type=pdf&coll=GUIDE&dl=ACM
ชื่อเรื่อง	Information Security Management – A New Paradigm
สรุปข้อมูล	เว็บไซต์ที่รวบรวมบทความด้านวิทยาศาสตร์และเทคโนโลยี
จัดทำโดย	The ACM Portal
ขนาดของข้อมูล	3,362 คำ

ลำดับที่	050
รหัสอ้างอิง	ISM050.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html
ชื่อเรื่อง	Passwords – Common Attacks and Possible Solutions
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	3,340 คำ

ลำดับที่	051
รหัสอ้างอิง	ISM051.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Passwords_Network_Security.html
ชื่อเรื่อง	Passwords – the Weak Link in the Network Security
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	2,017 คำ

ลำดับที่	052

รหัสอ้างอิง	ISM052.TXT
ที่มาของข้อมูล	http://www.gao.gov/archive/1998/ai98068.pdf
ชื่อเรื่อง	Executive Guide – Information Security Management
สรุปข้อมูล	เว็บไซต์ที่ให้ข้อมูลด้านความปลอดภัยของสำนักงานควบคุมและปกป้องภาษีประชาชนของรัฐบาลสหรัฐอเมริกา
จัดทำโดย	U.S. Government Accountability Office
ขนาดของข้อมูล	16,648 คำ

ลำดับที่	053
รหัสอ้างอิง	ISM053.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Personal-Firewalls-Remote-Access.html
ชื่อเรื่อง	Personal Firewalls for Remote Access
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,480 คำ

ลำดับที่	054
รหัสอ้างอิง	ISM054.TXT
ที่มาของข้อมูล	http://www.cio.gov/documents/peruse_model_may_1999.pdf
ชื่อเรื่อง	RECOMMENDED EXECUTIVE BRANCH MODEL POLICY/GUIDANCE ON “LIMITED PERSONAL USE” OF GOVERNMENT OFFICE EQUIPMENT INCLUDING INFORMATION TECHNOLOGY
สรุปข้อมูล	เว็บไซต์รวบรวมบทความด้านความปลอดภัยข้อมูลของสมาคมผู้จัดการใหญ่ด้านข้อมูล
จัดทำโดย	Chief Information Officer Council
ขนาดของข้อมูล	2,241 คำ

ลำดับที่	055
รหัสอ้างอิง	ISM055.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Physical-Security-Primer-Part2.html

ชื่อเรื่อง	Physical Security Primer (Part 2)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,443 คำ

ลำดับที่	056
รหัสอ้างอิง	ISM056.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Preserving-Digital-Evidence.html
ชื่อเรื่อง	Preserving Digital Evidence to bring Hackers and Attackers to Justice
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,374 คำ

ลำดับที่	057
รหัสอ้างอิง	ISM057.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Protect-Weak-Authentication-Protocols-Passwords.html
ชื่อเรื่อง	Protecting Weak Authentication Protocols and Passwords
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	2,349 คำ

ลำดับที่	058
รหัสอ้างอิง	ISM058.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Protect-network-rogue-users.html
ชื่อเรื่อง	Protect your network from rogue users
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,374 คำ

ลำดับที่	059
รหัสอ้างอิง	ISM059.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
ชื่อเรื่อง	Protecting yourself from e-mail virus and malware
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,434 คำ

ลำดับที่	060
รหัสอ้างอิง	ISM060.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Pushing-Out-Security-Settings-Configured-Registry.html
ชื่อเรื่อง	Pushing out the security settings that are configured in the registry
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,535 คำ

ลำดับที่	061
รหัสอ้างอิง	ISM061.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Remote-Authentication-Different-Types-Uses.html
ชื่อเรื่อง	Remote authentication – different types and uses
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,228 คำ

ลำดับที่	062
รหัสอ้างอิง	ISM062.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Microsoft-Security-Risk-Management-Guide.html

ชื่อเรื่อง	Reviews of Microsoft's risk management guides
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,573 คำ

ลำดับที่	063
รหัสอ้างอิง	ISM063.TXT
ที่มาของข้อมูล	www.information-security-policies.com
ชื่อเรื่อง	Information Security Management Policy Glossary by RUSecure
สรุปข้อมูล	เว็บไซต์ที่เสนอขายนโยบายการจัดการความปลอดภัยของข้อมูลแบบสำเร็จรูป
จัดทำโดย	RUsecure Information Security
ขนาดของข้อมูล	10,962 คำ

ลำดับที่	064
รหัสอ้างอิง	ISM064.TXT
ที่มาของข้อมูล	http://www.sans.org/reading_room/whitepapers/iso17799/1454.php
ชื่อเรื่อง	Information Security Management System (7799) for an Internet Gateway
สรุปข้อมูล	เว็บไซต์ที่มีบทความด้านการจัดการความปลอดภัยของข้อมูลซึ่งเป็นมาตรฐาน
จัดทำโดย	หน่วยงานเอส.เอ.เอ็น.เอส ซึ่งเป็นหน่วยงานที่ออกใบประกาศและจัดการอบรมทางด้านการจัดการความปลอดภัยของข้อมูลที่เชื่อถือได้มากที่สุดแห่งหนึ่งในโลก
ขนาดของข้อมูล	7,847 คำ

ลำดับที่	065
รหัสอ้างอิง	ISM065.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Secure_Socket_Layer.html
ชื่อเรื่อง	Secure socket layer
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.

ขนาดของข้อมูล	3,795 คำ

ลำดับที่	066
รหัสอ้างอิง	ISM066.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Securing_Remote_Access_Connections.html
ชื่อเรื่อง	Securing remote access connections
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,644 คำ

ลำดับที่	067
รหัสอ้างอิง	ISM067.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Securing-Network-Within-Part1.html
ชื่อเรื่อง	Securing the network from within (Part 1)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,247 คำ

ลำดับที่	068
รหัสอ้างอิง	ISM068.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part5.html
ชื่อเรื่อง	Security Series: Building Preparation (Part 5 of 6)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,600 คำ

ลำดับที่	069

รหัสอ้างอิง	ISM069.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part4.html
ชื่อเรื่อง	Security Series: Building Preparation (Part 4 of 6)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,663 คำ

ลำดับที่	070
รหัสอ้างอิง	ISM070.TXT
ที่มาของข้อมูล	http://_www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part1.html
ชื่อเรื่อง	Security Series: Building Preparation (Part 1 of 6)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,475 คำ

ลำดับที่	071
รหัสอ้างอิง	ISM071.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part2.html
ชื่อเรื่อง	Security Series: Building Preparation (Part 2 of 6)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,515 คำ

ลำดับที่	072
รหัสอ้างอิง	ISM072.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part6.html
ชื่อเรื่อง	Security Series: Building Preparation (Part 6 of 6)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.

ขนาดของข้อมูล	1,564 คำ

ลำดับที่	073
รหัสอ้างอิง	ISM073.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part3.html
ชื่อเรื่อง	Security Series: Building Preparation (Part 3 of 6)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,679 คำ

ลำดับที่	074
รหัสอ้างอิง	ISM074.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Server-2003-Network-Access-Quarantine-Control-Security.html
ชื่อเรื่อง	Server 2003's network security control
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,186 คำ

ลำดับที่	075
รหัสอ้างอิง	ISM075.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Share-Permissions.html
ชื่อเรื่อง	Share permissions
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,431 คำ

ลำดับที่	076
รหัสอ้างอิง	ISM076.TXT

ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Standardization-security-appliance.html
ชื่อเรื่อง	Standardization and the security appliance
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,232 คำ

ลำดับที่	077
รหัสอ้างอิง	ISM077.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Sys-Admin-Friend-Foe.html
ชื่อเรื่อง	Sys admin: friend or foe?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,104 คำ

ลำดับที่	078
รหัสอ้างอิง	ISM078.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Hacking-Security-Tools.html
ชื่อเรื่อง	The convergence of hacking and security tool
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,344 คำ

ลำดับที่	079
รหัสอ้างอิง	ISM079.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Different-Shades-Hackers.html
ชื่อเรื่อง	The different shades of hackers
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,321 คำ

ลำดับที่	080
รหัสอ้างอิง	ISM080.TXT
ที่มาของข้อมูล	http://www.opsi.gov.uk/SI/si2002/20020318.htm
ชื่อเรื่อง	The Electronic Signatures Regulations 2002
สรุปข้อมูล	เว็บไซต์ที่จัดตั้งข้อกำหนดในการใช้งานข้อมูลด้านภาครัฐของประเทศอังกฤษ และมีบทความทางด้านการจัดการความปลอดภัยของข้อมูลรวบรวมไว้
จัดทำโดย	Office of Public Sector Information, UK
ขนาดของข้อมูล	2,172 คำ

ลำดับที่	081
รหัสอ้างอิง	ISM081.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Security-Risks-Desktop-Searches.html
ชื่อเรื่อง	The security risks of desktop searches
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,540 คำ

ลำดับที่	082
รหัสอ้างอิง	ISM082.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Trojan_Horse_Primer.html
ชื่อเรื่อง	Trojan horse primer
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,207 คำ

ลำดับที่	083
รหัสอ้างอิง	ISM083.TXT

ที่มาของข้อมูล	http://www.windowsecurity.com/faqs/Trojans/
ชื่อเรื่อง	Trojan FAQs
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	8,081 คำ

ลำดับที่	084
รหัสอ้างอิง	ISM084.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Email-Spoofing.html
ชื่อเรื่อง	Understanding e-mail spoofing
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,573 คำ

ลำดับที่	085
รหัสอ้างอิง	ISM085.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Understanding_the_Role_of_the_PKI.html
ชื่อเรื่อง	Understanding the role of PKI
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,593 คำ

ลำดับที่	086
รหัสอ้างอิง	ISM086.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Dual-Accounts-Administrators.html
ชื่อเรื่อง	Using dual accounts for administrators
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,598 คำ

ลำดับที่	087
รหัสอ้างอิง	ISM087.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Passwords_Improve_Windows_Security_Part1.html
ชื่อเรื่อง	Using passwords as a defense mechanism to improve windows security (Part 1)
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,753 คำ

ลำดับที่	088
รหัสอ้างอิง	ISM088.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/VPN_Client_Security_Issues.html
ชื่อเรื่อง	VPN client security issues
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	2,875 คำ

ลำดับที่	089
รหัสอ้างอิง	ISM089.TXT
ที่มาของข้อมูล	http://www.theiia.org/guidance/technology/it-resources/it-security/
ชื่อเรื่อง	IT Security
สรุปข้อมูล	เว็บไซต์ที่ให้ความรู้กับผู้ตรวจสอบ
จัดทำโดย	The Institute of Internal Auditors
ขนาดของข้อมูล	997 คำ

ลำดับที่	090
รหัสอ้างอิง	ISM090.TXT
ที่มาของข้อมูล	http://www.theiia.org/ITAudit/

ชื่อเรื่อง	IT Audits
สรุปข้อมูล	เว็บไซต์ที่ให้ความรู้กับผู้ตรวจสอบ
จัดทำโดย	The Institute of Internal Auditors
ขนาดของข้อมูล	298 คำ

ลำดับที่	091
รหัสอ้างอิง	ISM091.TXT
ที่มาของข้อมูล	http://www.theiia.org/bookstore.cfm?fuseaction=editorial_sum&order_num=482
ชื่อเรื่อง	Editorial Summary: PC Management Best Practices - A Study of the Total Cost of Ownership, Risk, Security, and Audit
สรุปข้อมูล	เว็บไซต์ที่ให้ความรู้กับผู้ตรวจสอบ
จัดทำโดย	The Institute of Internal Auditors
ขนาดของข้อมูล	1,406 คำ

ลำดับที่	092
รหัสอ้างอิง	ISM092.TXT
ที่มาของข้อมูล	http://www.windowsecurity.com/articles/Where_Does_EFS_Fit_into_your_Security_Plan.html
ชื่อเรื่อง	Where does EFS fit into your security plan?
สรุปข้อมูล	เว็บไซต์ที่ให้รู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Tech Genix Ltd.
ขนาดของข้อมูล	1,740 คำ

ลำดับที่	093
รหัสอ้างอิง	ISM093.TXT
ที่มาของข้อมูล	http://www.theiia.org/guidance/technology/it-resources/it-security/
ชื่อเรื่อง	IT Security
สรุปข้อมูล	เว็บไซต์ที่ให้ความรู้กับผู้ตรวจสอบ
จัดทำโดย	The Institute of Internal Auditors
ขนาดของข้อมูล	1,740 คำ

ลำดับที่	094
รหัสอ้างอิง	ISM094.TXT
ที่มาของข้อมูล	http://news.zdnet.com/2100-1009_22-981336.html
ชื่อเรื่อง	Antivirus virus on the loose
สรุปข้อมูล	เว็บไซต์ที่รวบรวมข่าวสารและบทความทันสมัยล่าสุดด้านเทคโนโลยีสารสนเทศ
จัดทำโดย	ZDNet Technology News
ขนาดของข้อมูล	1,089 คำ

ลำดับที่	095
รหัสอ้างอิง	ISM095.TXT
ที่มาของข้อมูล	http://www.oarval.org/avalencia/VirInfen.htm
ชื่อเรื่อง	Antivirus Information
สรุปข้อมูล	เว็บไซต์ที่มีบทความด้านการต่อต้านไวรัส
จัดทำโดย	Avalencia
ขนาดของข้อมูล	3,813 คำ

ลำดับที่	096
รหัสอ้างอิง	ISM096.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Trojan_horse_(computing)
ชื่อเรื่อง	Trojan Horses (Computing)
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	1,250 คำ

ลำดับที่	097
รหัสอ้างอิง	ISM097.TXT

ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Information_security
ชื่อเรื่อง	Information Security
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	6,703 คำ

ลำดับที่	098
รหัสอ้างอิง	ISM098.TXT
ที่มาของข้อมูล	citecclub.org/forum/index.php?showtopic=20944
ชื่อเรื่อง	Info Security 2008 – Threat Analysis
สรุปข้อมูล	ส่วนหนึ่งของหนังสือที่เกี่ยวกับเรื่องภัยคุกคามระบบโดยเฉพาะ และได้รับการตัดเลือกจากคนในวงการคอมพิวเตอร์ให้เป็นหนังสือที่ยอดเยี่ยมที่สุดเล่มหนึ่งด้านภัยคุกคาม
จัดทำโดย	Craig Schiller, Seth Fogie, Colby DeRodeff, and Michael Gregg
ขนาดของข้อมูล	5,200 คำ

ลำดับที่	099
รหัสอ้างอิง	ISM099.TXT
ที่มาของข้อมูล	http://searchwarp.com/swa268042.htm
ชื่อเรื่อง	Confidentiality, Integrity, Availability and What it Means to You
สรุปข้อมูล	บทความที่กล่าวถึงคุณสมบัติของความปลอดภัยข้อมูลต่าง ๆ
จัดทำโดย	Claudio LoCicero
ขนาดของข้อมูล	1,055 คำ

ลำดับที่	100
รหัสอ้างอิง	ISM100.TXT
ที่มาของข้อมูล	http://oit.nd.edu/policies/itpolicies/infosec.shtml
ชื่อเรื่อง	Proposed Information Security Policy
สรุปข้อมูล	รายละเอียดของนโยบายด้านความปลอดภัยข้อมูลที่เสนอพิจารณา

จัดทำโดย	Office of Information Security, University of Notre Dame
ขนาดของข้อมูล	1,076 คำ

ลำดับที่	101
รหัสอ้างอิง	ISM101.TXT
ที่มาของข้อมูล	http://www.certmag.com/articles/templates/cmag_department_sec.asp?articleid=708&zoneid=43
ชื่อเรื่อง	Security policy and procedures
สรุปข้อมูล	บทความที่กล่าวถึงนโยบายด้านความปลอดภัยของข้อมูลรวมไปถึงวิธีการดำเนินงาน
จัดทำโดย	Certification Magazine
ขนาดของข้อมูล	792 คำ

ลำดับที่	102
รหัสอ้างอิง	ISM102.TXT
ที่มาของข้อมูล	www.praxiom.com/iso-27001-definitions.htm
ชื่อเรื่อง	ISO 27001 AND ISO 27002 PLAIN ENGLISH DEFINITIONS
สรุปข้อมูล	อภิธานศัพท์ที่ใช้ในมาตรฐาน ISO 27001 และ ISO 27002 ซึ่งเป็นมาตรฐานที่ใช้ในการจัดการความปลอดภัยของข้อมูล
จัดทำโดย	Praxiom Research Group Limited
ขนาดของข้อมูล	1,726 คำ

ลำดับที่	103
รหัสอ้างอิง	ISM103.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/E-mail_bomb
ชื่อเรื่อง	Email Bomb
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	519 คำ

ลำดับที่	104
รหัสอ้างอิง	ISM104.TXT
ที่มาของข้อมูล	http://www.tech-faq.com/dos-denial-of-service-attack.shtml
ชื่อเรื่อง	What is Denial-of-Service (DOS) Attack?
สรุปข้อมูล	บทความที่กล่าวถึงการโจมตีแบบล่มระบบ
จัดทำโดย	Technology FAQ
ขนาดของข้อมูล	560 คำ

ลำดับที่	105
รหัสอ้างอิง	ISM105.TXT
ที่มาของข้อมูล	http://csrc.nist.gov/publications/nistir/threats/subsection3_4_1.html
ชื่อเรื่อง	Insider Attacks
สรุปข้อมูล	บทความที่กล่าวถึงการโจมตีระบบที่มาจากคนใช้งานในระบบนั้นเอง
จัดทำโดย	Computer Security Resource Center, USA
ขนาดของข้อมูล	172 คำ

ลำดับที่	106
รหัสอ้างอิง	ISM106.TXT
ที่มาของข้อมูล	http://www.securityfocus.com/infocus/1558
ชื่อเรื่อง	Preventing and Detecting Insider Attacks Using IDS
สรุปข้อมูล	บทความที่กล่าวถึงการป้องกันการโจมตีระบบโดยใช้ระบบตรวจจับผู้บุกรุก (IDS)
จัดทำโดย	Security Forcus, The Largest Community of Security Professionals Available Anywhere
ขนาดของข้อมูล	2,472 คำ

ลำดับที่	107
รหัสอ้างอิง	ISM107.TXT
ที่มาของข้อมูล	http://www.bizforum.org/whitepapers/NGC.htm

ชื่อเรื่อง	Insider Attack Detection Using Cyber Sensor Fusion
สรุปข้อมูล	บทความที่กล่าวถึงการตรวจจับการโจมตีจากภายในระบบโดยใช้เครื่องมือทางด้านเทคโนโลยีชิ้นหนึ่ง
จัดทำโดย	The Business Forum
ขนาดของข้อมูล	999 คำ

ลำดับที่	108
รหัสอ้างอิง	ISM108.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Computer_worm
ชื่อเรื่อง	Computer worm
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	687 คำ

ลำดับที่	109
รหัสอ้างอิง	ISM109.TXT
ที่มาของข้อมูล	http://computers-and-technology.rattanapant.com/index.php?id=1889
ชื่อเรื่อง	Security Checklist for Service Providers
สรุปข้อมูล	บทความด้านการจัดการความปลอดภัยข้อมูลที่ผู้ให้บริการทั้งหลายควรรู้
จัดทำโดย	Computer and Technology Website
ขนาดของข้อมูล	788 คำ

ลำดับที่	110
รหัสอ้างอิง	ISM110.TXT
ที่มาของข้อมูล	http://www.microsoft.com/technet/isa/2004/help/FW_AlertAttack.mspx?mfr=true
ชื่อเรื่อง	Attack Detection
สรุปข้อมูล	บทความที่แสดงรายละเอียดการตรวจจับการบุกรุกระบบเครือข่ายในองค์กร
จัดทำโดย	Microsoft Ltd.

ขนาดของข้อมูล	931 คำ

ลำดับที่	111
รหัสอ้างอิง	ISM111.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Malware
ชื่อเรื่อง	Malware
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	3,391 คำ

ลำดับที่	112
รหัสอ้างอิง	ISM112.TXT
ที่มาของข้อมูล	www.infosec.gov.hk/docs/english/glossary_eng.pdf
ชื่อเรื่อง	Glossary for Information Security & Prevention of Computer Related Crime
สรุปข้อมูล	อภิธานศัพท์ของหัวข้อการจัดการความปลอดภัยของข้อมูลและการป้องกันไม่ให้เกิดเหตุร้ายอันเกิดมาจากคอมพิวเตอร์ จัดทำโดยหน่วยงานรัฐบาลฮ่องกง ประเทศจีน
จัดทำโดย	Information Security Website by Hongkong Government
ขนาดของข้อมูล	5,398 คำ

ลำดับที่	113
รหัสอ้างอิง	ISM113.TXT
ที่มาของข้อมูล	www.globalhauri.com/support/service/faq_view.html?uid=3&menu=QTAx
ชื่อเรื่อง	What is a "Virus" and how are they classified?
สรุปข้อมูล	บทความเกี่ยวกับไวรัสคอมพิวเตอร์
จัดทำโดย	Hauri บริษัทที่ช่วยปกป้องข้อมูลลูกค้าจากการโจมตีของไวรัส
ขนาดของข้อมูล	719 คำ

ลำดับที่	114
รหัสอ้างอิง	ISM114.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Logic_bomb
ชื่อเรื่อง	Logic bomb
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	171 คำ

ลำดับที่	115
รหัสอ้างอิง	ISM115.TXT
ที่มาของข้อมูล	http://netsecurity.about.com/cs/hackertools/a/aa121403.htm
ชื่อเรื่อง	Introduction to Packet Sniffing
สรุปข้อมูล	บทความอธิบายรายละเอียดเบื้องต้นของภัยคุกคามชนิดหนึ่ง
จัดทำโดย	About.com Internet/Network Security
ขนาดของข้อมูล	536 คำ

ลำดับที่	116
รหัสอ้างอิง	ISM116.TXT
ที่มาของข้อมูล	http://safari.oreilly.com/1587051354/ch05lev1sec2
ชื่อเรื่อง	Costs of Network Security Breaches
สรุปข้อมูล	บทความเกี่ยวกับการละเมิดกฎความปลอดภัยของระบบเครือข่าย
จัดทำโดย	Safari Books Online
ขนาดของข้อมูล	399 คำ

ลำดับที่	117
รหัสอ้างอิง	ISM117.TXT
ที่มาของข้อมูล	http://www.policies.uchc.edu/policies/2005%20-%20HIPAA%20Glossary.pdf
ชื่อเรื่อง	GLOSSARY For the purposes of UCHC HIPAA Security Policies

สรุปข้อมูล	อภิธานศัพท์นโยบายรักษาความปลอดภัยข้อมูลของสถานพยาบาล มหาวิทยาลัยคอนเนคติกัต
จัดทำโดย	สถานพยาบาล มหาวิทยาลัยคอนเนคติกัต
ขนาดของข้อมูล	1,980 คำ

ลำดับที่	118
รหัสอ้างอิง	ISM118.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Information_technology_controls
ชื่อเรื่อง	Information Technology Controls
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	363 คำ

ลำดับที่	119
รหัสอ้างอิง	ISM119.TXT
ที่มาของข้อมูล	http://www.informit.com/articles/article.aspx?p=31339&seqNum=3
ชื่อเรื่อง	Network Security Controls
สรุปข้อมูล	บทตัดตอนมาจากหนังสือมาตรการควบคุมความปลอดภัยของระบบเครือข่าย
จัดทำโดย	Charles P. Pfleeger, Shari Lawrence Pfleeger
ขนาดของข้อมูล	10,345 คำ

ลำดับที่	120
รหัสอ้างอิง	ISM120.TXT
ที่มาของข้อมูล	www-935.ibm.com/services/us/index.wss/offering/gbs/a1002379
ชื่อเรื่อง	Network Security Assessment
สรุปข้อมูล	บทความเกี่ยวกับการประเมินความปลอดภัยของระบบเครือข่าย
จัดทำโดย	IBM
ขนาดของข้อมูล	382 คำ

ลำดับที่	121
รหัสอ้างอิง	ISM121.TXT
ที่มาของข้อมูล	www.skyboxsecurity.com/products/assure.html
ชื่อเรื่อง	Managing the risks that matter
สรุปข้อมูล	บทความที่กล่าวถึงความเสี่ยง
จัดทำโดย	Skybox Security
ขนาดของข้อมูล	224 คำ

ลำดับที่	122
รหัสอ้างอิง	ISM122.TXT
ที่มาของข้อมูล	www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf
ชื่อเรื่อง	Security Standards: Technical Safeguards
สรุปข้อมูล	บทความที่ให้ความรู้ด้านสิ่งป้องกันที่ใช้ในการรักษาความปลอดภัยของข้อมูล เป็นส่วนหนึ่งของบทความให้ความรู้ซึ่งเป็นส่วนหนึ่งของนโยบายความปลอดภัยของสถานพยาบาลมหาวิทยาลัยคอนเนคติกัต
จัดทำโดย	สถานพยาบาล มหาวิทยาลัยคอนเนคติกัต
ขนาดของข้อมูล	3,541 คำ

ลำดับที่	123
รหัสอ้างอิง	ISM123.TXT
ที่มาของข้อมูล	www.informit.com/articles/article.aspx?p=26952
ชื่อเรื่อง	Information Security Must Balance Business Objectives
สรุปข้อมูล	บทตัดตอนมาจากหนังสือความปลอดภัยของข้อมูล ชื่อเรื่องตามข้างต้น
จัดทำโดย	F. Christian Byrnes, Paul E. Proctor
ขนาดของข้อมูล	1,703 คำ

ลำดับที่	124

รหัสอ้างอิง	ISM124.TXT
ที่มาของข้อมูล	Information Technology – Security techniques – Code of practice for Information security management (BS 7799)
ชื่อเรื่อง	Glossary for Information Technology – Security techniques – Code of practice for Information security management (BS 7799)
สรุปข้อมูล	อภิธานศัพท์ที่ใช้ในแนวทางการดำเนินงานการจัดการความปลอดภัยของข้อมูล จัดทำโดยมาตรฐาน BS 7799 ซึ่งเป็นมาตรฐานที่ใช้ในการจัดตั้งระบบจัดการความปลอดภัยของข้อมูล
จัดทำโดย	BS 7799
ขนาดของข้อมูล	310 คำ

ลำดับที่	125
รหัสอ้างอิง	ISM125.TXT
ที่มาของข้อมูล	www.activsupport.com/network-disaster-recovery-**plan**-san-francisco-bay-area.html
ชื่อเรื่อง	Network Disaster Recovery Plan in San Francisco Bay Area
สรุปข้อมูล	แผนการป้องกันภัยพิบัติที่ใช้ในซานฟรานซิสโก
จัดทำโดย	รัฐซานฟรานซิสโก
ขนาดของข้อมูล	771 คำ

ลำดับที่	126
รหัสอ้างอิง	ISM126.TXT
ที่มาของข้อมูล	http://ahds.ac.uk/creating/information-papers/risk-management/index.htm
ชื่อเรื่อง	Risk Management and Contingency Planning
สรุปข้อมูล	บทความเกี่ยวกับการจัดการความเสี่ยง
จัดทำโดย	Arts and Humanity Data Service, UK
ขนาดของข้อมูล	3,093 คำ

ลำดับที่	127
รหัสอ้างอิง	ISM127.TXT
ที่มาของข้อมูล	http://www.astoninfosec.co.uk/risk_assessment.html
ชื่อเรื่อง	Risk Assessment and Management
สรุปข้อมูล	บทความเกี่ยวกับการประเมินและจัดการความเสี่ยง
จัดทำโดย	Aston Information Security

ขนาดของข้อมูล	589 คำ

ลำดับที่	128
รหัสอ้างอิง	ISM128.TXT
ที่มาของข้อมูล	http://chppm-www.apgea.army.mil/risk/whatis.aspx
ชื่อเรื่อง	What is risk communication?
สรุปข้อมูล	บทความเกี่ยวกับการสื่อสารความเสี่ยง
จัดทำโดย	US Army Center for Health Promotion and Preventive Medicine
ขนาดของข้อมูล	329 คำ

ลำดับที่	129
รหัสอ้างอิง	ISM129.TXT
ที่มาของข้อมูล	www.noweco.com/risk/riske13.htm
ชื่อเรื่อง	Risk Management Software and ISO 17799 / ISO 27000
สรุปข้อมูล	บทความเกี่ยวกับการจัดการความเสี่ยง
จัดทำโดย	Northwest Controlling Cooperation Ltd.
ขนาดของข้อมูล	150 คำ

ลำดับที่	130
รหัสอ้างอิง	ISM130.TXT
ที่มาของข้อมูล	www.training-hipaa.net/compliance/Security_Risk_Assessment.htm
ชื่อเรื่อง	HIPAA Risk assessment and risk analysis management
สรุปข้อมูล	บทความเกี่ยวกับการจัดการความเสี่ยง
จัดทำโดย	Supremus Group LLC
ขนาดของข้อมูล	362 คำ

ลำดับที่	131
รหัสอ้างอิง	ISM131.TXT

ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Public-key_cryptography
ชื่อเรื่อง	Public Key Cryptography
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	485 คำ

ลำดับที่	132
รหัสอ้างอิง	ISM132.TXT
ที่มาของข้อมูล	http://www.sun.com/bigadmin/features/articles/intrusion_detection.html
ชื่อเรื่อง	Introduction to Intrusion Detection With Snort
สรุปข้อมูล	บทความเกี่ยวกับการตรวจจับการบุกรุก
จัดทำโดย	Sun Microsystem
ขนาดของข้อมูล	680 คำ

ลำดับที่	133
รหัสอ้างอิง	ISM133.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Intrusion-detection_system
ชื่อเรื่อง	Intrusion Detection System
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	374 คำ

ลำดับที่	134
รหัสอ้างอิง	ISM134.TXT
ที่มาของข้อมูล	http://en.wikipedia.org/wiki/Cryptography
ชื่อเรื่อง	Cryptography
สรุปข้อมูล	เว็บไซต์สารนุกรมสาธารณะที่รวบรวมข้อมูลด้านต่าง ๆ ไว้ รวมถึงหัวข้อด้านการจัดการความ

	ปลอดภัยของข้อมูล และภัยคุกคามระบบต่าง ๆ
จัดทำโดย	Wikipedia
ขนาดของข้อมูล	1,426 คำ

ลำดับที่	135
รหัสอ้างอิง	ISM135.TXT
ที่มาของข้อมูล	http://www.proprofs.com/forums/index.php?showtopic=14014
ชื่อเรื่อง	Public-key/asymmetric cryptography, digital signatures, etc
สรุปข้อมูล	บทความเกี่ยวกับการเข้ารหัสข้อมูลแบบสมมาตรและอสมมาตรรวมไปถึงลายมือชื่อดิจิทัล
จัดทำโดย	Educational Freeway by Professional and Professors
ขนาดของข้อมูล	149 คำ

ลำดับที่	136
รหัสอ้างอิง	ISM136.TXT
ที่มาของข้อมูล	http://www.firstmonday.org/issues/issue5_8/mccullagh/
ชื่อเรื่อง	Non-repudiation in the digital environment
สรุปข้อมูล	บทความเกี่ยวกับการปฏิเสธไม่ได้ของข้อมูล
จัดทำโดย	Peer Review Journals on the Internet
ขนาดของข้อมูล	806 คำ

ลำดับที่	137
รหัสอ้างอิง	ISM137.TXT
ที่มาของข้อมูล	http://users.tkk.fi/~lhuovine/study/hacker98/dos.html
ชื่อเรื่อง	Denial of Service Attacks: Teardrop and Land
สรุปข้อมูล	บทความเกี่ยวกับการล่มระบบ
จัดทำโดย	Department of Computer Science, Helsinki University of Technology
ขนาดของข้อมูล	2,959 คำ

ลำดับที่	138
รหัสอ้างอิง	ISM138.TXT
ที่มาของข้อมูล	http://www.us-cert.gov/reading_room/JIB-Trojan122105.pdf
ชื่อเรื่อง	Look Before You Click: Trojan Horses And Other Attempts To Compromise Networks
สรุปข้อมูล	บทความเกี่ยวกับภัยคุกคามต่าง ๆ
จัดทำโดย	United States Department of Homeland Security
ขนาดของข้อมูล	1,985 คำ

ลำดับที่	139
รหัสอ้างอิง	ISM139.TXT
ที่มาของข้อมูล	istprojects.syr.edu/~sise/flexwiki/default.aspx/MyWiki/cracker.html
ชื่อเรื่อง	Cracker
สรุปข้อมูล	บทความเกี่ยวกับผู้บุกรุกระบบ
จัดทำโดย	Syracuse University
ขนาดของข้อมูล	265 คำ

ลำดับที่	140
รหัสอ้างอิง	ISM140.TXT
ที่มาของข้อมูล	http://www.risk-analysis-guide.com/information-security-controls.html
ชื่อเรื่อง	Risk Analysis – Information Security Controls
สรุปข้อมูล	บทความเกี่ยวกับมาตรการควบคุมความปลอดภัยข้อมูล
จัดทำโดย	Risk Analysis Website
ขนาดของข้อมูล	484 คำ

3.7. การดึงศัพท์จากคลังข้อมูล

การดึงศัพท์จากคลังข้อมูลภาษาที่จัดทำไว้นั้นมีหลักเกณฑ์เบื้องต้นในการพิจารณาว่าคำคำนั้นเป็นศัพท์เฉพาะทางในสาขาที่ต้องทำประมวลศัพท์หรือไม่อยู่ 2 ข้อ อันได้แก่

1) ใช้ความถี่ของการพบศัพท์ โดยศัพท์ที่พบมากครั้งน่าจะมีโอกาสเป็นศัพท์เฉพาะทางได้

2) ใช้ความรู้ในสาขานั้นๆ ของผู้จัดทำ หรือค้นคว้าคำอธิบายจากแหล่งอ้างอิงต่าง ๆ เช่ สารานุกรม แต่อย่างไรก็ดีเกณฑ์เบื้องต้นดังกล่าวอาจไม่เพียงพอในการตัดสินว่ากลุ่มคำที่เลือกมานั้นคำใดเป็นศัพท์เฉพาะในสาขาที่ต้องการทำประมวลศัพท์จริงๆ ดังนั้นจึงควรพิจารณาจากเกณฑ์อื่นๆด้วย ดังจะได้กล่าวต่อไป

สำหรับการทำประมวลศัพท์ครั้งนี้ ผู้จัดทำได้ใช้โปรแกรม Concordancer for Windows (Wconcord) 2.0 และ Collocation Extract 3.04 มาช่วยในการดึงศัพท์จากคลังข้อมูล โดยมีขั้นตอนดังนี้

1) สร้าง Word Frequency List เพื่อรวมรวบคำทั้งหมดที่พบในคลังข้อมูล เมื่อรวบรวมเสร็จจึงพิจารณาจากรายการที่ได้ โดยเน้นไปที่คำนามซึ่งเป็น Content word ซึ่งคำส่วนมากที่พบใน Frequency list จะเป็นประเภทคำเดี่ยว

2) คำบางครั้งตามหลังคำว่า ‘known as’, ‘called’ หรือ ‘defined as’ เพราะบ่งบอกว่าคำที่ตามหลังมาเป็นคำศัพท์เฉพาะ เช่น Public key encryption, also called asymmetric encryption, is popular because it is more secure than secret key (symmetric) encryption

3) ไม่สามารถแทรกคำทางไวยากรณ์ได้ เช่น คำว่า Chief Security Officer ไม่สามารถเขียนเป็นคำว่า Chief of the Security Officer ได้

4) คำนี้ไม่สามารถนำคำขยายมาขยายเฉพาะคำใดคำหนึ่งได้ เช่น คำว่า ‘symmetric encryption’ ไม่สามารถเป็น ‘symmetric pattern encryption’ ได้ หรือ คำว่า ‘private key’ ไม่สามารถเป็น ‘private secret key’ ได้

5) พบศัพท์ที่มีความหมายตรงกันข้ามกัน ซึ่งก็คือ คำว่า ‘public key’ ตรงข้ามกับคำว่า ‘private key’

6) มีคำหลักเหมือนกันคือคำว่า ‘key’ ซึ่งเป็นคำ Generic Language และมีคำอื่นที่ทำให้คำหลักนั้นมีความหมายต่างกันออกไปปรากฏอยู่ควบคู่กัน เช่น คำว่า ‘public key’ และ ‘private key’ ซึ่งก็คือ ‘public’ และ ‘private’ และเมื่อสร้างคำประสมจากศัพท์สามคำนี้ก็จะได้ความหมายเดียวและมักจะพบใน Domain เดียว

7) มักใช้กับคำกริยาและคำคุณศัพท์เพียงกลุ่มหนึ่งเท่านั้น เช่น ‘public key’ และ ‘private key’ มักจะใช้ร่วมกับคำกริยา ‘generate’ และคำว่า ‘compromise’ มักจะใช้กับคำคุณศัพท์ว่า ‘Corresponding’ ส่วนคำว่า ‘symmetric encryption’ และ ‘asymmetric encryption’ มักจะพบกับคำนามคำว่า ‘algorithm’

8) มักจะพบศัพท์ทั้งสี่ในรูปประโยคลักษณะเดียวกันในที่อื่นๆ ของตัวบทที่เกี่ยวกับเรื่องการจัดการความปลอดภัยของข้อมูลและมักจะใช้ภายใน Domain นี้เท่านั้น และแทบจะไม่พบการใช้คำทั้งสี่คำใน Domain อื่น

9) ไม่สามารถเดาความหมายของศัพท์เฉพาะทางทั้งสี่ซึ่งเป็นกลุ่มคำ โดยการแยกดูความหมายของแต่ละคำที่นำมาประกอบเข้าด้วยกันได้ เช่น คำว่า ‘public key’ ไม่ได้มีความหมายว่า public = สาธารณะ + key = กุญแจ คำเหล่านี้จะมีความหมายที่แท้จริงมากกว่ารูปศัพท์ที่ปรากฏ

10) บางครั้งมีคำเหมือน (Synonym) เช่น ‘asymmetric encryption’ บางครั้งสามารถเรียกได้ว่า ‘Public key encryption’ และ ‘symmetric encryption’ บางครั้งสามารถเรียกได้ว่า ‘Secret key encryption’

เมื่อทำตามขั้นตอนข้างต้น จะได้ศัพท์ในการประมวลศัพท์ด้านการจัดการความปลอดภัยของข้อมูล ได้ทั้งหมด 57 คำ

บทที่ 4
การประมวลศัพท์และการสร้างมโนทัศน์สัมพันธ์

ในบทนี้ จะขอกล่าวถึงความหมายของมโนทัศน์ มโนทัศน์สัมพันธ์ในแบบต่าง ๆ การบันทึกศัพท์เบื้องต้น และการบันทึกศัพท์

4.1. **มโนทัศน์** (Concept)

ในการจัดทำประมวลศัพท์นั้น ต้องมี 2 ส่วนหลัก ๆ ด้วยกัน นั่นคือ คำศัพท์ (Term) ซึ่งใช้เป็นสัญลักษณ์แทนมโนทัศน์ที่เกิดขึ้นใหม่ ๆ โดยมโนทัศน์จะต้องปรากฏขึ้นก่อนคำศัพท์เสมอ (Sager, 1990: 22)

แรกเริ่มเดิมทีนั้น ความหมายของคำว่า มโนทัศน์ ไม่มีความตรง ๆ แต่จากการรวบรวมความหมายของมโนทัศน์ที่กำหนดโดยคณะกรรมการหลายกลุ่มซึ่งมีดังต่อไปนี้

- มโนทัศน์ คือ หน่วยของความคิดที่มนุษย์สร้างขึ้นเพื่อแทนสิ่งของที่อยู่ในโลกและนอกเหนือจากโลก
- มโนทัศน์ ใช้เป็นสิ่งที่แสดงขององค์ประกอบต่าง ๆ ของความรู้และกิจกรรมของมนุษย์ เช่น สิ่งของ คุณสมบัติ และปรากฏการณ์ต่าง ๆ
- มโนทัศน์ คือ หน่วยของความคิดที่ใช้จัดกลุ่มสิ่งของที่มีคุณลักษณะคล้ายคลึงกัน

ความหมายที่นำมากล่าวข้างต้นเป็นเพียงตัวอย่างความหมายที่หลากหลายของมโนทัศน์ แต่เราอาจกล่าวได้ว่า มโนทัศน์คือหน่วยความคิดที่ใช้อธิบายความรู้ใหม่ ๆ ที่เกิดขึ้นมาทั้งในโลกและนอกโลก

4.2. **มโนทัศน์สัมพันธ์**

ในความรู้ทั่ว ๆ ไปที่เกิดขึ้นในโลกนี้นั้น สามารถแบ่งออกเป็นสาขาวิชาเฉพาะได้มากมาย ในแต่ละสาขานั้นจะประกอบไปด้วยมโนทัศน์ต่าง ๆ มากมาย มโนทัศน์แต่ละมโนทัศน์นั้นอาจจะมีความสัมพันธ์ซึ่งกันและกันเอง และอาจจะมีความสัมพันธ์กับมโนทัศน์ที่อยู่ในสาขาวิชาอื่นด้วย ๆ มโนทัศน์สัมพันธ์มีได้มากมายและหลากหลาย (Sager, 1990: 29)

ตามที่ Sager (1990) กล่าวไว้ มโนทัศน์สัมพันธ์มีได้ 4 ประเภทด้วยกัน ซึ่งจะขออธิบายดังต่อไปนี้

1. ความสัมพันธ์ทั่วไป (Generic Relationships) เป็นความสัมพันธ์แบบลำดับขั้น (Hierarchy Relations) ที่มีมโนทัศน์ที่อยู่เหนือกว่าหรือมีความหมายกว้างกว่า (Superordinate concept) ภายใต้มโน

ทัศน์ที่มีความหมายกว้างกว่าเหล่านี้จะประกอบไปด้วยมโนทัศน์ซึ่งอยู่ต่ำกว่าหรือมีความหมายแคบลงมา (Subordinate concept) โดยทั่วไปแล้ว ความสัมพันธ์แบบทั่วไปนี้จะมีสูตรดังต่อไปนี้

- ก. เป็นประเภทหนึ่งของ ง.
- ก. ข. และ ค. เป็นประเภทหนึ่ง ๆ ของ ง.
- ง. มีมโนทัศน์เป็น ก. ข. และ ค.
- ง. มีประเภทย่อยเป็น ก.

ความสัมพันธ์แบบนี้จะเป็นไปในทางกลับกันไม่ได้ กล่าวคือ ถ้าเราพูดว่า ก. เป็นคุณลักษณะของ ง. เราจะไม่สามารถกล่าวได้ว่า ง. เป็นคุณลักษณะของ ก. ตัวอย่างเช่น ถ้าเรากล่าวถึงกลุ่มคำศัพท์ของ “เครื่องนุ่งห่ม” ในกลุ่มเครื่องนุ่งห่มจะประกอบไปด้วย “เสื้อ” “กางเกง” และ “กระโปรง” แต่ในทางกลับกันคำว่า “กระโปรง” ไม่ได้เป็นเครื่องนุ่งห่มชนิดเดียวที่มนุษย์ใส่ ดังนั้น “เครื่องนุ่งห่ม” เป็นคำศัพท์ที่มีความหมายกว้างกว่า (Superordinate concept) และ“เสื้อ” “กางเกง” และ “กระโปรง” เป็นคำศัพท์ที่มีความหมายแคบกว่า (Subordinate concept) ในมโนทัศน์สัมพันธ์แบบทั่วไปนี้

นอกจากนั้น กลุ่มคำศัพท์ที่มีความหมายแคบกว่าในมโนทัศน์สัมพันธ์แบบทั่วไปนี้ จะมีคุณสมบัติที่เหมือนกันอย่างเดียว คือ คุณสมบัติที่เป็นคำศัพท์ที่มีความหมายกว้างกว่า แต่จะมีคุณลักษณ์ส่วนอื่นที่ต่างกัน เช่น จากตัวอย่างข้างต้น “เสื้อ” “กางเกง” และ “กระโปรง” มีคุณสมัติเป็นเครื่องนุ่งห่มเหมือนกันหมด แต่คุณสมบัติอื่น ๆ ของ “เสื้อ” “กางเกง” และ “กระโปรง” นั้นมีความแตกต่างกันไป

กลุ่มคำศัพท์บางกลุ่มอาจเชื่อมด้วยมโนทัศน์สัมพันธ์แบบทั่วไปอย่างเดียวไม่ได้ แต่ต้องอธิบายด้วยมโนทัศน์สัมพันธ์แบบอื่นด้วย กลุ่มคำศัพท์บางคำนั้นอาจจะเชื่อมกันด้วยมโนทัศน์ได้ไม่สมบูรณ์นักซึ่งมักจะเกิดขึ้นในกรณีที่ศัทพ์นั้น ๆ สามารถอยู่ในหมวดหมู่ได้มากกว่า 1 ประเภทขึ้นไปแล้วแต่มุมมองของผู้ทำประมวลศัพท์ เช่น พืชบางชนิดอาจจะอยู่ในดิวิชั่นพืชได้สองประเภทขึ้นอยู่กับมุมมอง เราจะเรียกมโนทัศน์ประเภทนี้ว่า มโนทัศน์สัมพันธ์ค่อนไปทางทั่วไป (Quasi-generic relationship)

2. ความสัมพันธ์ประเภทนี้เป็นแบบส่วนประกอบ (Partitive Relationships) หรือ “WP” (Whole-part relationship) ซึ่งเป็นความสัมพันธ์แบบลำดับขั้น (Hierarchy Relations) ซึ่งในความสัมพันธ์ประเภทนี้มโนทัศน์หนึ่งเป็นสิ่งของชิ้นหนึ่งหรือคำจำกัดความหนึ่ง (Whole) ที่มีส่วนประกอบของอีกมโนทัศน์หนึ่ง (Part) ความสัมพันธ์แบบส่วนประกอบนี้จะมีสูตรดังต่อไปนี้

- ก. เป็นส่วนประกอบหนึ่งของ ง.
- ก. ข. และ ค. เป็นส่วนประกอบหนึ่ง ๆ ของ ง.
- ง. ประกอบไปด้วย ก.

- ง. ประกอบไปด้วย ก. ข. และ ค.

ส่วนประกอบย่อย ๆ นี้สามารถเป็นได้หลายประเภทซึ่งอาจจะแบ่งได้ตามนี้

1) ส่วนประกอบที่ย่อยที่สุดของกลุ่มนั้น ๆ เช่น ตัวอักษรภาษาไทยแต่ละตัว

2) จำนวนสิ่งของ เช่น ไพ่ 52 ใบในหนึ่งสำรับ

3) ส่วนประกอบต่าง ๆ ของสิ่งของ เช่น ชิ้นส่วนรถยนต์ รวมไปถึงส่วนประกอบเสริมของสิ่งนั้น ๆ ด้วย

4) ส่วนประกอบที่บางครั้งเป็นอุปกรณ์นั้นทั้งชิ้น

ตัวอย่างความสัมพันธ์แบบส่วนประกอบนั้นเช่น รถยนต์และส่วนประกอบต่าง ๆ ของรถยนต์ เป็นต้น

3. มโนทัศน์แบบหลายขั้ว (Polyvalent relationship) นั้นใช้สำหรับสิ่งของที่มีความสัมพันธ์กับลำดับขั้นมากกว่า 1 ลำดับขึ้นไป เช่น ผักประกอบไปด้วย ผักพื้นบ้าน ผักสวนครัว ฯลฯ ส่วนมะเขือเทศเป็นได้ทั้งผักพื้นบ้านและผักสวนครัว

4. มโนทัศน์แบบซับซ้อน (Complex relationship) นั้นเป็นความสัมพันธ์ของมโนทัศน์ต่าง ๆ ที่ไม่สามารถเชื่อมกันด้วยมโนทัศน์แบบทั่วไปและแบบส่วนประกอบได้ มโนทัศน์แบบซับซ้อนนี้เป็นความสัมพันธ์แบบเชื่อมโยงกัน (Associative Relations) ซึ่งเป็นความสัมพันธ์ที่ไม่เป็นลำดับขั้นและไม่มีมโนทัศน์ใดอยู่เหนือกว่ามโนทัศน์ใด แต่มโนทัศน์เหล่านั้นจะมีความเกี่ยวข้องกันในรูปแบบใดรูปแบบหนึ่ง เช่น ความสัมพันธ์ระหว่างมโนทัศน์ที่มโนทัศน์หนึ่งเป็นวิธีการและอีกมโนทัศน์หนึ่งเป็นเครื่องมือหนึ่งที่ใช้ในกระบวนการนั้น โดยกำหนดชื่อเรียกความสัมพันธ์ประเภทนี้ว่า “PI” (Process - Instrument) และความสัมพันธ์ระหว่างมโนทัศน์ที่มโนทัศ์หนึ่งเป็นสิ่งของที่ก่อให้เกิดผลอย่างหนึ่งและอีกมโนทัศน์หนึ่งก่อให้เกิดผลตรงข้ามกัน โดยกำหนดชื่อเรียกความสัมพันธ์ประเทนี้ว่า “OC” (Object - Counteragent)

ในการประมวลศัพท์การจัดการความปลอดภัยของข้อมูลครั้งนี้จะมีรูปแบบความสัมพันธ์แบบซับซ้อนทั้งหมด 18 ประเภท และมีรายละเอียดตามตารางดังต่อไปนี้

รหัสเรียก	รูปแบบความสัมพันธ์	คำอธิบาย
AO	Action – Object	แสดงการกระทำของมโนทัศน์หนึ่งที่เกิดขึ้นกับอีกมโนทัศน์หนึ่ง เช่น การละเมิดความปลอดภัยของข้อมูล
CE	Cause – Effect	แสดงว่ามโนทัศน์หนึ่งเป็นสาเหตุที่ทำให้เกิดมโนทัศน์

		หนึ่ง เช่น ไวรัส (Virus) สามารถก่อให้เกิดภัยคุกคาม (Threat) ต่อระบบสารสนเทศขององค์กรได้
CO	Counter – Object	แสดงความสัมพันธ์ว่ามโนทัศน์เป็นตัวป้องกันมโนทัศน์หนึ่ง เช่น โปรแกรมต่อต้านไวรัสนั้นปกป้องระบบจากไวรัส
CrO	Creator – Object	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเกิดจากการออกโดยอีกมโนทัศน์หนึ่ง เช่น ผู้ประกอบการรับรอง (Certification authority) เป็นผู้ออกใบรับรองดิจิทัล (Digital Certificate)
CS	Condition – Selection	แสดงว่ามโทนัศน์หนึ่งได้รับการรับเลือกโดยอ้างอิงเงื่อนไขการเลือกของอีกมโนทัศน์หนึ่ง เช่น การเลือกวิธีหรือประเภทของมาตราการควบคุมความปลอดภัยนั้นจะอ้างอิงจากเนื้อหาในนโยบายการรักษาความปลอดภัยขององค์กร
GS	Generic – Specific	แสดงว่ามโนทัศน์หนึ่งเป็นประเภทย่อยของอีกมโนทัศน์หนึ่ง เช่น ภัยคุกคามของระบบสามารถแยกย่อยได้เป็นภัยที่เกิดจากไวรัสคอมพิวเตอร์ การโจมตีจากบุคคลภายในองค์กร และการล่อลวงข้อมูลจากผู้ใช้งาน เป็นต้น
MB	Method – Branch	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเป็นสาขาของอีกมโนทัศน์หนึ่ง เช่น ลายมือชื่อดิจิทัล (Digital Signature) เป็นสาขาย่อยของการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption)
MP	Method – Process	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเป็นกระบวนการภายใต้มโนทัศน์อีกอันหนึ่ง เช่น การเข้ารหัสลับ (Encryption) เป็นกระบวนการซ่อนเนื้อหาข้อมูลในวิธีการการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption)
OC	Object – Counter-Object	แสดงความสัมพันธ์ของมโนทัศน์หนึ่งว่าเป็นคู่ตรงข้ามของอีกมโนทัศน์หนึ่ง เช่น กุญแจสาธารณะ (Public Key) นั้นตรงข้ามกับกุญแจส่วนตัว (Private Key)
PC	Process - Consequence	แสดงความสัมพันธ์ว่ามโนทัศน์เกิดจากกระบวนการ

		ตัดสินใจของอีกมโนทัศน์หนึ่ง เช่น หลังจากทำการลดความเสี่ยงแล้ว ผู้จัดทำอาจจะต้องยอมรับความเสี่ยงนั้น ๆ
PI	Process – Instrument	แสดงความสัมพันธ์ของมโนทัศน์กับอีกมโนทัศน์หนึ่งในเชิงกระบวนการและเครื่องมือที่ใช้ เช่น การอนุญาตให้เข้าใช้ระบบ (Authorization) ใช้ชื่อระบุผู้ใช้งานระบบ (Unique User Identifier) ในการตรวจสอบและระบุชื่อผู้เข้าใช้งานในระบบ
PM	Process – Method	แสดงความสัมพันธ์ของมโนทัศน์กับอีกมโนทัศน์หนึ่งในเชิงกระบวนการและวิธีการ เช่น การอนุญาตให้เข้าใช้ระบบ (Authorization)เป็นกระบวนการที่ประกอบไปด้วยวิธีการพิสูน์ตัวจริง (Authentication)
PO	Process – Outcome	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเป็นผลของกระบวนการมโนทัศน์หนึ่ง เช่น กระบวนการการพิสูจน์ตัวจริง (Authentication) ก่อให้เกิดหรือรักษาไว้ซึ่งบูรณภาพของข้อมูล (Integrity)
PP	Process – Principle	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเป็นหลักการของกระบวนการที่เป็นมโนทัศน์อีกอันหนึ่ง เช่น การจัดการความปลอดภัยของข้อมูลเป็นกระบวนการจัดการเพื่อปกป้องความปลอดภัยของข้อมูล
PS	Process – Solution	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเป็นผลลัพธ์ของอีกมโนทัศน์หนึ่ง เช่น แผนแก้ไขปัญหาจากภัยพิบัติเป็นวิธีการตอบสนองต่อการจัดการความเสี่ยงต่าง ๆ
PT	Process – Target	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งเป็นเป้าหมายของกระบวนการที่เป็นมโนทัศน์อีกอันหนึ่ง เช่น การระบุภัยคุกคามเป็นผลลัพธ์ของการจัดการความเสี่ยง
UM	User – Method	แสดงความสัมพันธ์ว่ามโนทัศน์หนึ่งใช้วิธีการแบบมโนทัศน์หนึ่งในการทำงาน เช่น ในการทำลายระบบด้วยการใช้โปรแกรมม้าโทรจันนั้น ผู้มุ่งร้ายมักใช้วิธีการล่อลวงผู้ใช้งานหรือติดตั้งโปรแกรมทำงานหลังระบบเพื่อให้ผู้มุ่งร้ายบุกรุกเข้าระบบไปได้
WP	Whole – Part	แสดงว่ามโนทัศน์เป็นส่วนประกอบของอีกมโนทัศน์หนึ่ง เช่น เช่น กระบวนการประเมินความเสี่ยง

		ประกอบไปด้วยกระบวนการวิเคราะห์ความเสี่ยงกับกระบวนการประเมินความรุนแรงของความเสี่ยง

4.3. **การบันทึกข้อมูลศัพท์เบื้องต้น** (Extraction Record)

เมื่อดึงศัพท์จากคลังข้อมูลภาษาตามหลักการที่ได้กล่าวไว้ในข้อ 3.7 แล้ว ก็นำศัพท์เหล่านี้มาบันทึกข้อมูลคำศัพท์เบื้องต้นซึ่งในการบันทึกรายละเอียดคำศัพท์คำหนึ่ง จะต้องบันทึกรายละเอียดตามที่แสดงในตารางด้านล่างดังต่อไปนี้

CNXXX	Concept:
Eng:	Grammatical Category:
Thai:	
Feature:	
Conceptual Relation:	
Extraction:	

1. CNXXX แสดงลำดับที่ของมโนทัศน์
2. Concept แสดงชื่อของมโนทัศน์ที่ต้องการอธิบาย
3. Eng คือ คำศัพท์ภาษาอังกฤษในขอบข่ายมโนทัศน์นั้น ๆ ซึ่งในมโนทัศน์หนึ่ง ๆ อาจมีคำศัพท์ได้มากกว่า 1 คำขึ้นไป
4. Grammatical Category แสดงชนิดของคำศัพท์ เช่น คำนาม เป็นต้น
5. Feature แสดงความหมายของศัพท์โดยสรุปโดยวิเคราะห์และอ้า งอิงบริบทที่พบในคลังข้อมูลภาษา
6. Conceptual Relation แสดงมโนทัศน์สัมพันธ์
7. Extraction แสดงรูปประโยคสมบูรณ์ของคำศัพท์นั้นที่ดึงมาจากคลังข้อมูลภาษาโดยระบุบริบทของประโยคนั้นด้วยโดย Cabré(1999) ได้กล่าวไว้ว่า บริบทนั้นมี 3 ประเภทด้วยกัน คือ
   ก. Testimonial context เป็นบริบทที่แสดงให้เห็นการใช้ศัพท์แต่ไม่ได้ให้ข้อมูลอื่น ๆ ของศัพท์นั้น เช่น To use e-mail encryption, both sender and recipient need to have compatible encryption software.
   ข. Defining Context เป็นบริบทที่แสดงความหมายของคำศัพท์ เช่น User A is depicted above and has two keys a public key, this key is available to the public for download, and a private key, this key is not available to the public

ค. **Metalinguistic Context** เป็นบริบทที่ให้ข้อมูลของศัพท์ในฐานะที่เป็ นหน่วยทางภาษา เช่น Public key encryption, also called asymmetric encryption, is popular because it is more secure than secret key (symmetric) encryption

คาเบรกล่าวว่า บริบทที่ดีที่สุดในการประมวลศัพท์นั้น คือ Defining Context และการบันทึกนั้นควรจะมีข้อมูลบันทึกอย่างน้อย 2 ข้อมูลก็จะเพียงพอกับการบันทึกศัพท์คำนั้นแล้ว (Cabré: 1999: 137)

4.4. **การบันทึกข้อมูลศัพท์** (Terminological Record)

คาเบร กล่าวว่า การบันทึกข้อมูลศัพท์ (Terminological Record) นั้นเป็นการรวบรวมข้อมูลที่จำเป็นและเกี่ยวข้องของศัพท์นั้น ๆ โดยอาจจะรวบรวมจากข้อมูลที่ได้จากการบันทึกข้อมูลศัพท์เบื้องต้น (Extraction Record) และเอกสารอ้างอิง (Reference Document) (Cabré, 1990: 143-145) ซึ่งจะประกอบไปด้วยข้อมูลพื้นฐานดังต่อไปนี้

1. **Source information** แสดงแหล่งที่มาของคำศัพท์นั้นว่ามาจากแหล่งข้อมูลดิบที่ใด ความหมายและบริบทที่ดึงคำศัพท์นั้นรวมไปถึงข้อมูลอื่น ๆ ที่เกี่ยวข้องด้วย
2. **Entry term** แสดงคำศัพท์ที่แท้จริงหรือแค่มโนทัศน์หรืออาจจะเป็นทั้งสองอย่างก็ได้
3. **Semantic and conceptual specification** แสดงความหมายของคำศัพท์ ประเภทของคำศัพท์และความสัมพันธ์กับมโนทัศน์อื่น ๆ
4. **Linguistic specification** แสดงข้อมูลทางภาษาศาสตร์ในรูปแบบต่าง ๆ ซึ่งจะเอื้ออำนวยต่อการแปลเป็นภาษาอื่น ๆ เช่น รูปแบบของคำและไวยากรณ์ของคำศัพท์นั้น ๆ
5. **Pragmatic specification** แสดงข้อมูลบริบทที่พบคำศัพท์นั้น
6. **Administrative information** แสดงข้อมูลปลีกย่อยที่ช่วยให้การประมวลศัพท์นั้นมีประสิทธิภาพมากขึ้น เช่น หมายเลขอ้างอิงคำศัพท์ วันที่ที่จัดทำ ชื่อของผู้จัดทำ จำนวนครั้งที่มีการแก้ไขการบันทึก
7. **Equivalent foreign language** คำศัพท์ภาษาอื่นที่มีความหมายตรงกันหรือใกล้เคียงกันซึ่งจะเอื้อประโยชน์ต่อการแปลบทความในสาขานั้น ๆ

ในการจัดทำประมวลศัพท์ในครั้งนี้ ผู้จัดทำได้เลือกบันทึกศัพท์ในส่วนที่จำเป็นต่อการใช้งานของผู้จัดทำเองซึ่งสามารถสรุปเป็นตารางได้ดังต่อไปนี้

TXXX	English term:	Grammatical Category:
Thai:		

Subject Field:
Definition:
Illustration:
Note:
Linguistic specification:
Cross-reference:

1. TXXX แสดงลำดับที่ของมโนทัศน์
2. English term คือ คำศัพท์ภาษาอังกฤษในขอบข่ายมโนทัศน์นั้น ๆ
3. Grammatical Category แสดงชนิดของคำศัพท์ เช่น คำนาม เป็นต้น
4. Thai คือ ความหมายภาษาไทยของมโนทัศน์นั้น ๆ อาจจะเป็นคำที่มีการบัญญัติโดยราชบัณฑิตยสถาน หรือมาจากการแนะนำของผู้เชี่ยวชาญในสาขานี้
5. Subject Field คือ หัวข้อซึ่งพบศัพท์นั้น เช่น Confidentiality มาจากหมวด Information Security
6. Definition แสดงความหมายของศัพท์นั้น
7. Illustration แสดงตัวอย่างประโยคการนำไปใช้ของศัพท์นั้น
8. Note แสดงรายละเอียดอื่น ๆ นอกเหนือจากความหมายและองค์ประกอบอื่น ๆ
9. Linguistic specification แสดงรายละเอียดทางด้านภาษาศาสตร์ เช่น คำย่อ (Abbreviation) คำที่มีความหมายเหมือน (Synonym) และคำที่มีความหมายตรงข้าม (Antonym)
10. Cross-reference แสดงศัพท์ที่มีความหมายเกี่ยวข้องกับศัพท์นั้น ๆ

บทที่ 5
บทสรุป

ปัญหาที่พบและแนวทางการแก้ไขปัญหา

ในการจัดทำประมวลศัพท์เรื่องการจัดการความปลอดภัยของข้อมูล ได้พบปัญหาในการทำงานดังนี้

1. ตัวบทที่เลือกมาสำหรับการทำประมวลศัพท์ในครั้งนี้มักจะอยู่ในบริบทที่เป็น Expert-to-initiate และ Teacher-to-pupil มากกว่าแบบ Expert-to-expert ซึ่งอาจจะทำให้การดึงศัพท์เพื่อนำมาทำประมวลศัพท์นั้นไม่มีประสิทธิภาพเท่าที่ควร ถ้าต้องการจะขยายการจัดทำประมวลศัพท์ครั้งนี้ แต่ทั้งนี้ทั้งนั้น ก็ต้องยอมรับว่า สาขาการจัดการความปลอดภัยของข้อมูลนี้ ได้มีทั้งผลงานทางวิชาการ บทความโดยบุคคลทั่วไป ออกมามากมาย เพราะเป็นสาขาที่กำลังมีการตื่นตัวสูง กอปรกับได้มีการทำอภิธานศัพท์ออกมามากมายจากสถาบันให้ความรู้ต่าง ๆ จึงไม่น่าที่จะพบปัญหาในการเลือกตัวบทหรือดึงคำศัพท์มากนัก ผู้จัดทำคงต้องไปหาตามฐานข้อมูลที่เก็บวารสารทางวิชาการที่เกี่ยวกับเทคโนโลยีมากขึ้นกว่านี้

2. คำศัพท์ทางด้านเทคโนโลยีนั้น ส่วนหนึ่งได้รับการบัญญัติศัพท์เป็นภาษาไทยแล้ว แต่ยังคงมีคำศัพท์บางกลุ่มที่ไม่ได้รับการบัญญัติ เช่น Denial-of-Service ผู้จัดทำจึงต้องไปสอบถามผู้เชี่ยวชาญว่า ต้องใช้คำไหนจึงจะเหมาะสม หรือมีคำไหนที่ใช้กันเป็นที่กว้างขวางอยู่แล้ว

บรรณานุกรม

ภาษาไทย

ชนะ โศภารักษ์. ศัพท์ไมโครคอมพิวเตอร์. กรุงเทพฯ :
ศูนย์หนังสือจุฬาลงกรณ์มหาวิทยาลัย, 2540

ศ.ดร. วิทย์ เที่ยงบูรณธรรม. Se-ed's Modern English-Thai Dictionary. กรุงเทพมหานคร :
ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2541.

ราชบัณฑิตยสถาน. ศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ. กรุงเทพมหานคร :
ราชบัณฑิตยสถาน, 2549.

จิรายุส ภาสวัต. พจนานุกรมคอมพิวเตอร์. กรุงเทพมหานคร :
The Knowledge Center, 2546.

ภาษาอังกฤษ

Longman Dictionary of Contemporary English. 3rd ed. Essex :
Longman, 2000.

Rey, Alain. Essay on Terminology. North Carolina:
John Benjamins Publishing Company, 1995.

Cabré, M. Teresa. Terminology Theory, methods and applications. Amsterdam:
John Benjamins Publishing Company, 1992.

Somers, Harolds. Terminology, LSP and Translation – Studies in Language Engineering in Honour of Juan C. Sager. Amsterdam:
John Benjamins Publishing Company, 1996.

Sager, Juan C. A Practical Course in Terminology Processing. Amsterdam:
John Benjamins Publishing Company, 1990.

Muegge, Uwe. Disciplining Word. Germany
TC World Magazine, May 2007.

ภาคผนวก ก
รายละเอียดคลังข้อมูลภาษา

รายละเอียดของคลังข้อมูลภาษา

รหัสอ้างอิง	ที่มาของเอกสาร	จำนวนคำ
ISM001	http://www.allbusiness.com/technology/computer-software-management/891276-1.html	12,230
ISM002	http://www.windowsecurity.com/articles/A_firewall_in_an_IT_system.html	2,829
ISM003	http://www.windowsecurity.com/articles/Access-Controls-What-is-it-how-undermined.html	1,258
ISM004	http://www.gao.gov/special.pubs/ai9868.pdf	16,296
ISM005	http://www.gao.gov/special.pubs/ai99139.pdf	13,409
ISM006	http://www.theiia.org/iia/download.cfm?file=353	2,251
ISM007	http://www.windowsecurity.com/articles/Auditing-user-accounts.html	1,436
ISM008	http://www.windowsecurity.com/.../Authorization-Manager-Role-Based-Administration-Windows-Server-2003-Part2.html	963
ISM009	http://www.windowsecurity.com/articles/Being-Big-Brother-Monitoring-employees-network-activity.html	1,422
ISM010	http://www.windowsecurity.com/articles/Biometrics-and-You.html	1,252
ISM011	http://www.windowsecurity.com/articles/Built-in-Groups-Delegation.html	1,541
ISM012	http://www.windowsecurity.com/articles/Authentication-Forgotten-Predominant.html	1,536
ISM013	http://www.windowsecurity.com/articles/Changing-Passwords-Key-User-Accounts.html	1,447
ISM014	http://www.windowsecurity.com/articles/Code-Signing.html	1,444
ISM015	http://www.windowsecurity.com/articles/Review-GFI-LANguard-Portable-Storage-Control.html	1,801
ISM016	http://www.windowsecurity.com/articles/Customizing-Windows-Security-Templates.html	1,397
ISM017	http://www.windowsecurity.com/articles/Deciphering-Authentication-Events-Domain-Controllers.html	1,024
ISM018	http://www.windowsecurity.com/articles/Digital_Signatures.html	1,560
ISM019	http://www.windowsecurity.com/articles/Disk-Based-Backup.html	1,339
ISM020	http://www.windowsecurity.com/articles/Email_Spam.html	1,750
ISM021	http://www.windowsecurity.com/articles/Ethical-Issues-IT-Security-Professionals.html	1,464
ISM022	http://www.windowsecurity.com/articles/Evaluating-New-Security-Policy.html	1,461
ISM023	http://www.infosectoday.com/Articles/gassp.pdf	21,647
ISM024	http://www.connectingsomerset.co.uk/tips/website%20basics/Information%20Security%20-%20a%20glossary.pdf	3,784
ISM025	http://www.windowsecurity.com/articles/Hackers-Security-Consultants.html	1,850
ISM026	http://www.windowsecurity.com/articles/How-Do-Compliance-Issues-Affect-your-Network.html	1,371
ISM027	http://www.windowsecurity.com/articles/Spyware_Adware_Programs.html	2,391

ISM028	http://www.windowsecurity.com/articles/audit-network-packet-analysis.html	1,381
ISM029	http://www.windowsecurity.com/articles/Plan-Possible-Network-Attack.html	1,190
ISM030	http://www.windowsecurity.com/articles/Ideal-to-Realized-Security-Assurance-Cryptographic-Keys-Part1.html	1,430
ISM031	http://www.windowsecurity.com/articles/Ideal-to-Realized-Security-Assurance-Cryptographic-Keys-Part2.html	1,889
ISM032	http://www.windowsecurity.com/articles/Implementing-Troubleshooting-Account-Lockout.html	1,798
ISM033	http://www.windowsecurity.com/articles/Implementing-Principle-Least-Privilege.html	1,610
ISM034	http://www.windowsecurity.com/articles/Increasing-Security-Limited-User-Accounts-Restricted-Groups.html	1,737
ISM035	Information Security Governance and Assurance by Charles H. Le Grand, Technology Practices, The Institute of Internal Auditors, Inc.	8,918
ISM036	http://www.unc.edu/hipaa/policies/Information_Security.pdf	3,447
ISM037	Information Security Introduction Factsheet by Department of Trade and Industry, UK	1,910
ISM038	http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html	4,715
ISM039	http://www.windowsecurity.com/articles/Intrusion_Detection_Systems_IDS_Part__I _network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html	3,547
ISM040	http://www.windowsecurity.com/whitepaper/FAQ_Network_Intrusion _Detection_Systems_.html	3,208
ISM041	http://www.windowsecurity.com/articles/Encrypting-Your-E-mail.html	1,723
ISM042	http://www.cncc.edu/institutional_research/cccs_it_security_plan.htm	1,706
ISM043	http://www.windowsecurity.com/articles/Privacy-Keeping-information-confidential.html	1,659
ISM044	http://www.windowsecurity.com/articles/Kerberos-Authentication-Events.html	1,397
ISM045	http://www.windowsecurity.com/articles/Internet-Safer-Employees.html	1,612
ISM046	http://www.windowsecurity.com/articles/Managed-E-Mail-Security-Services-right-solution-network.html	1,055
ISM047	http://portal.acm.org/citation.cfm?id=1059538	3,688
ISM048	http://portal.acm.org/citation.cfm? id=792704.792706&coll=GUIDE&dl=GUIDE&CFID=7570047&CFTOKEN=78916351	3,271
ISM049	http://portal.acm.org/ft_gateway.cfm?id=954028&type=pdf&coll=GUIDE&dl=ACM	3,362
ISM050	http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html	3,340
ISM051	http://www.windowsecurity.com/articles/Passwords_Network_Security.html	2,017
ISM052	http://www.gao.gov/archive/1998/ai98068.pdf	16,648
ISM053	http://www.windowsecurity.com/articles/Personal-Firewalls-Remote-Access.html	1,480
ISM054	http://www.cio.gov/documents/peruse_model_may_1999.pdf	2,241
ISM055	http://www.windowsecurity.com/articles/Physical-Security-Primer-Part2.html	1,443

ISM056	http://www.windowsecurity.com/articles/Preserving-Digital-Evidence.html	1,347
ISM057	http://www.windowsecurity.com/articles/Protect-Weak-Authentication-Protocols-Passwords.html	2,349
ISM058	http://www.windowsecurity.com/articles/Protect-network-rogue-users.html	1,374
ISM059	http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html	1,434
ISM060	http://www.windowsecurity.com/articles/Pushing-Out-Security-Settings-Configured-Registry.html	1,535
ISM061	http://www.windowsecurity.com/articles/Remote-Authentication-Different-Types-Uses.html	1,228
ISM062	http://www.windowsecurity.com/articles/Microsoft-Security-Risk-Management-Guide.html	1,573
ISM063	www.information-security-policies.com	10,962
ISM064	http://www.sans.org/reading_room/whitepapers/iso17799/1454.php	7,847
ISM065	http://www.windowsecurity.com/articles/Secure_Socket_Layer.html	3,795
ISM066	http://www.windowsecurity.com/articles/Securing_Remote_Access_Connections.html	1,644
ISM067	http://www.windowsecurity.com/articles/Securing-Network-Within-Part1.html	1,247
ISM068	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part5.html	1,600
ISM069	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part4.html	1,663
ISM070	http://_www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part1.html	1,475
ISM071	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part2.html	1,515
ISM072	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part6.html	1,564
ISM073	http://www.windowsecurity.com/articles/Disaster-Recovery-Tactics-Part3.html	1,679
ISM074	http://www.windowsecurity.com/articles/Server-2003-Network-Access-Quarantine-Control-Security.html	1,186
ISM075	http://www.windowsecurity.com/articles/Share-Permissions.html	1,431
ISM076	http://www.windowsecurity.com/articles/Standardization-security-appliance.html	1,232
ISM077	http://www.windowsecurity.com/articles/Sys-Admin-Friend-Foe.html	1,104
ISM078	http://www.windowsecurity.com/articles/Hacking-Security-Tools.html	1,344
ISM079	http://www.windowsecurity.com/articles/Different-Shades-Hackers.html	1,321
ISM080	http://www.opsi.gov.uk/SI/si2002/20020318.htm	2,172
ISM081	http://www.windowsecurity.com/articles/Security-Risks-Desktop-Searches.html	1,540
ISM082	http://www.windowsecurity.com/articles/Trojan_Horse_Primer.html	1,207
ISM083	http://www.windowsecurity.com/faqs/Trojans/	8,081
ISM084	http://www.windowsecurity.com/articles/Email-Spoofing.html	1,573
ISM085	http://www.windowsecurity.com/articles/Understanding_the_Role_of_the_PKI.html	1,593
ISM086	http://www.windowsecurity.com/articles/Dual-Accounts-Administrators.html	1,598

ISM087	http://www.windowsecurity.com/articles/Passwords_Improve_Windows_Security_Part1.html	1,753
ISM088	http://www.windowsecurity.com/articles/VPN_Client_Security_Issues.html	2,875
ISM089	http://www.theiia.org/guidance/technology/it-resources/it-security/	997
ISM090	http://www.theiia.org/ITAudit/	298
ISM091	http://www.theiia.org/bookstore.cfm?fuseaction=editorial_sum&order_num=482	1,406
ISM092	http://www.windowsecurity.com/articles/Where_Does_EFS_Fit_into_your_Security_Plan.html	1,740
ISM093	http://www.theiia.org/guidance/technology/it-resources/it-security/	997
ISM094	http://news.zdnet.com/2100-1009_22-981336.html	1,089
ISM095	http://www.oarval.org/avalencia/VirInfen.htm	3,813
ISM096	http://en.wikipedia.org/wiki/Trojan_horse_(computing)	1,250
ISM097	http://en.wikipedia.org/wiki/Information_security	6,703
ISM098	Info Security 2008 – Threat Analysis	5,200
ISM099	http://searchwarp.com/swa268042.htm	1,055
ISM100	http://oit.nd.edu/policies/itpolicies/infosec.shtml	1,076
ISM101	http://www.certmag.com/articles/templates/cmag_department_sec.asp?articleid=708&zoneid=43	792
ISM102	www.praxiom.com/iso-27001-definitions.htm	1,726
ISM103	http://en.wikipedia.org/wiki/E-mail_bomb	519
ISM104	http://www.tech-faq.com/dos-denial-of-service-attack.shtml	560
ISM105	http://csrc.nist.gov/publications/nistir/threats/subsection3_4_1.html	172
ISM106	http://www.securityfocus.com/infocus/1558	2,472
ISM107	http://www.bizforum.org/whitepapers/NGC.htm	999
ISM108	http://en.wikipedia.org/wiki/Computer_worm	687
ISM109	http://computers-and-technology.rattanapant.com/index.php?id=1889	788
ISM110	http://www.microsoft.com/technet/isa/2004/help/FW_AlertAttack.mspx?mfr=true	931
ISM111	http://en.wikipedia.org/wiki/Malware	3,391
ISM112	www.infosec.gov.hk/docs/english/glossary_eng.pdf	5,398
ISM113	www.globalhauri.com/support/service/faq_view.html?uid=3&menu=QTAx	719
ISM114	http://en.wikipedia.org/wiki/Logic_bomb	171
ISM115	http://netsecurity.about.com/cs/hackertools/a/aa121403.htm	536
ISM116	http://safari.oreilly.com/1587051354/ch05lev1sec2	399
ISM117	http://www.policies.uchc.edu/policies/2005%20-%20HIPAA%20Glossary.pdf	1,980

ISM118	http://en.wikipedia.org/wiki/Information_technology_controls	363
ISM119	http://www.informit.com/articles/article.aspx?p=31339&seqNum=3	10,345
ISM120	www-935.ibm.com/services/us/index.wss/offering/gbs/a1002379	382
ISM121	www.skyboxsecurity.com/products/assure.html	224
ISM122	www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf	3,541
ISM123	www.informit.com/articles/article.aspx?p=26952	1,703
ISM124	Glossary for Information Technology – Security techniques – Code of practice for Information security management (BS 7799)	310
ISM125	www.activsupport.com/network-disaster-recovery-plan-san-francisco-bay-area.html	771
ISM126	http://ahds.ac.uk/creating/information-papers/risk-management/index.htm	3,093
ISM127	http://www.astoninfosec.co.uk/risk_assessment.html	589
ISM128	http://chppm-www.apgea.army.mil/risk/whatis.aspx	329
ISM129	www.noweco.com/risk/riske13.htm	150
ISM130	www.training-hipaa.net/compliance/Security_Risk_Assessment.htm	362
ISM131	http://en.wikipedia.org/wiki/Public-key_cryptography	485
ISM132	http://www.sun.com/bigadmin/features/articles/intrusion_detection.html	680
ISM133	http://en.wikipedia.org/wiki/Intrusion-detection_system	374
ISM134	http://en.wikipedia.org/wiki/Cryptography	1,426
ISM135	http://www.proprofs.com/forums/index.php?showtopic=14014	149
ISM136	http://www.firstmonday.org/issues/issue5_8/mccullagh/	806
ISM137	http://users.tkk.fi/~lhuovine/study/hacker98/dos.html	2,959
ISM138	http://www.us-cert.gov/reading_room/JIB-Trojan122105.pdf	1,985
ISM139	istprojects.syr.edu/~sise/flexwiki/default.aspx/MyWiki/cracker.html	265
ISM140	http://www.risk-analysis-guide.com/information-security-controls.html	484

ภาคผนวก ข
รายการคำศัพท์ในชุดประมวลศัพท์

- A -

Access Control

Administrative control

Anti-virus Software

Asymmetric Encryption

Authentication

Authorization

Availability

- B -

Biometrics

- C -

Certificate Authority

Ciphertext

Compromise

Contingency Plan

Confidentiality

Controls

Cracker

Cryptography

- D -

Decryption

Denial of Service

Digital Certificate

Digital Signature

- E -

Encryption

- F -

Firewall

- H -

Hacker

- I -

Identification

Information Security

Information Security Management

Insider Attack

Integrity

Intrusion Detection

- L -

Logical Controls

- M -

Malware

- N -

Non-repudiation

Network security control

- P -

Password

Physical Control

Private Key

Public Key

Public Key Cryptography

- R -

Risk Acceptance

Risk Analysis

Risk Assessment

Risk Communication

Risk Evaluation

Risk Management

Risk Treatment

- S -

Safeguards

Secret Key Cryptography

Security Policy

Social Engineering

Symmetric Cryptography

- T -

Threat

Token

Trojan Horse

- U -

Unique User Identifier

- V -

Virus

Vulnerability

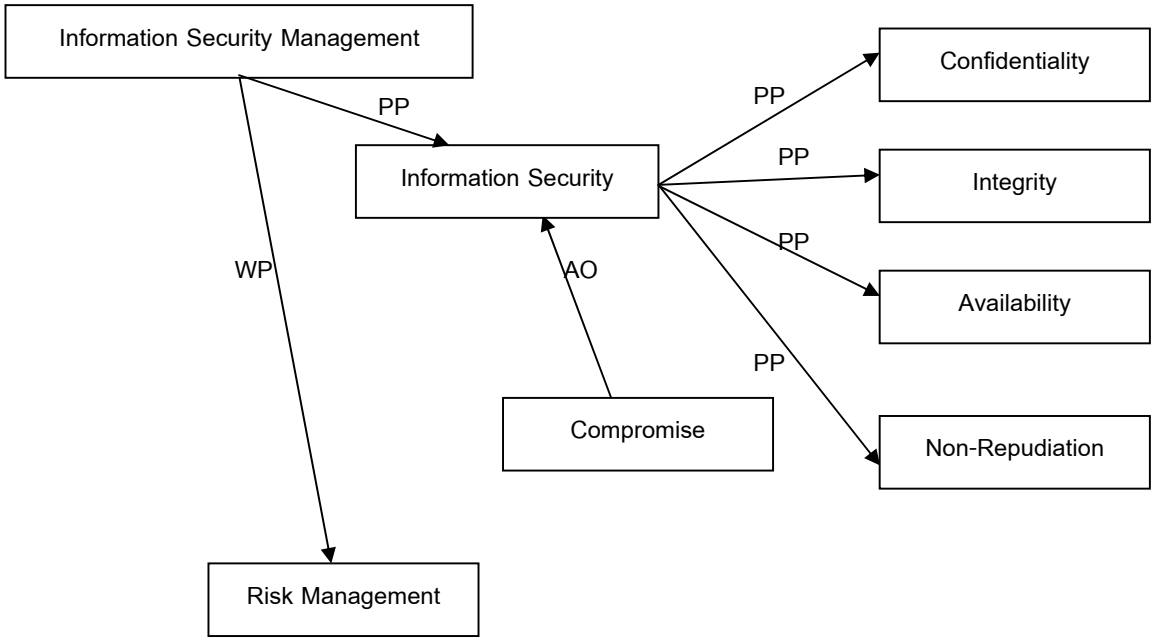
- W -

Website Intrusion

Worm

ภาคผนวก ค
การบันทึกข้อมูลศัพท์เบื้องต้น

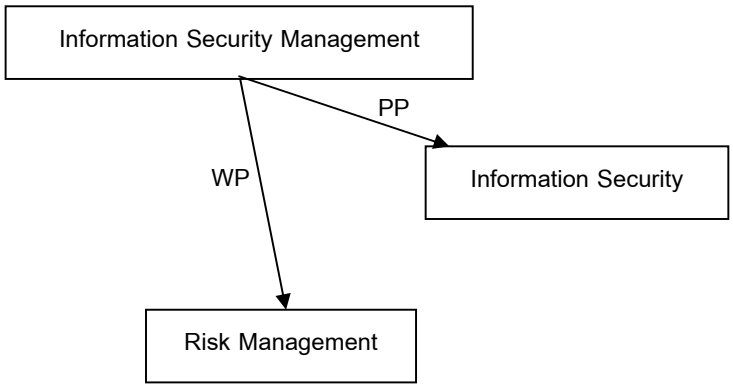
แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
หลักการเบื้องต้นของการจัดการความปลอดภัยของข้อมูล



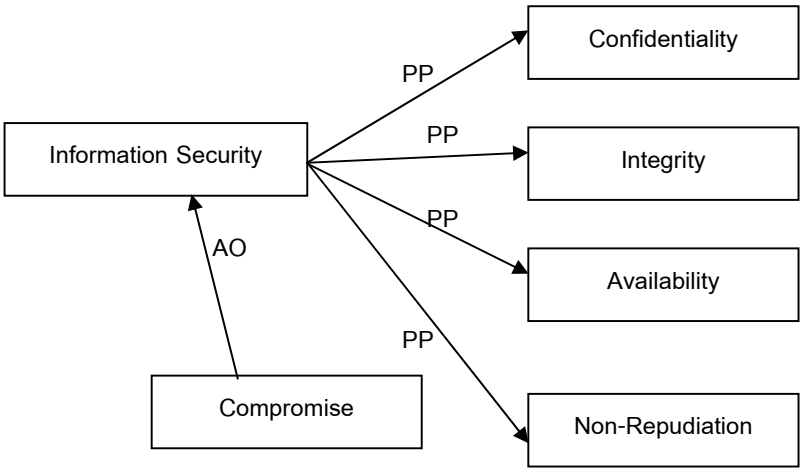
AO **แทน** Action – Object

PP **แทน** Process - Principle

WP **แทน** Whole – Part

CN001	**Concept:** Information Security Management
Eng: Information Security Management	**Grammatical Category:** Noun
Thai: การจัดการความปลอดภัยของข้อมูล [ราชบัณฑิตยสถาน]	
Feature: การจัดการความปลอดภัยของข้อมูล หมายถึง การปกป้องข้อมูลและป้องกันระบบสารสนเทศจากการเข้าถึง การใช้งาน การเปิดเผย และการปรับเปลี่ยนเนื้อหาโดยไม่ได้รับอนุญาต นอกจากนั้น การจัดการความปลอดภัยของข้อมูลยังเกี่ยวข้องกับการประเมินความเสี่ยง การปกป้องระบบข้อมูลจากความเสี่ยงที่อาจเกิดขึ้นและการหามาตรการควบคุมต่าง ๆ เพื่อปกป้องระบบข้อมูลนั้น ๆ	
Conceptual Relation:  **PP แทน** Process - Principle **WP แทน** Whole – Part	
Extraction: 1. The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment; security policy, organization of information security, asset management, human resources security, physical and environmental security, communications [ISM097.TXT] 2. Information security management is a process for establishing and maintaining information security. [ISM035.TXT] 3. Information Security Management is the protection of the confidentiality, integrity, and availability of University information. [ISM100.TXT] 4. It is clear that hands on experience with the valuation of assets, assessment of security risk, and the evaluation of tradeoffs (i.e. risk management), the key elements of the information security management function, are best learned by doing. [ISM047.TXT] 5. ISO 27001 / ISO 17799 / ISO 27005 require risk management as part of an Information Security	

Management. [ISM001.TXT]

CN002	**Concept:** Information Security
Eng: Information Security	**Grammatical Category:** Noun
Thai: ความปลอดภัยของข้อมูล [ราชบัณฑิตยสถาน]	
Feature: คุณสมบัติของความปลอดภัยของข้อมูลนั้นประกอบไปด้วยหลักสำคัญ ๆ 4 ประการด้วยกัน คือ ความลับของข้อมูล ความสมบูรณ์ถูกต้อง ความคงอยู่ การปฏิเสธไม่ได้ว่าเป็นข้อมูลของตนเอง การกระทำที่เป็นภัยต่อคุณสมบัติอย่างใดอย่างหนึ่งของความปลอดภัยของข้อมูลไป เช่น สูญเสียความลับของข้อมูลนั้น จะนำมาซึ่งปัญหาที่เกี่ยวข้องกับความปลอดภัยของข้อมูลได้	
Conceptual Relation:  **AO แทน** Action – Object **PP แทน** Process - Principle **WP แทน** Whole – Part	
Extraction: 1. Information security management is a process for establishing and maintaining information security. [ISM035.TXT] 2. Information security has four objectives: confidentiality, integrity, availability, and non-repudiation (NR). Securing information is equivalent to ensuring that computers keep your secrets, hold valid information, are ready to work when you are, and keep records of your transactions. [ISM123.TXT] 3. Information Security issues to be considered when implementing your policy include the following: • Legacy data from old systems can still remain accessible and thus compromise the confidentiality of	

information. [ISM063.TXT]

4. Information security incident - An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of your information and weaken or impair your business operations. [ISM012.TXT]

CN003	**Concept:** Confidentiality
Eng: Confidentiality	**Grammatical Category:** Noun
Thai: ความลับ [ราชบัณฑิตยสถาน]	
Feature: คุณสมบัติอย่างหนึ่งของการรักษาความปลอดภัยของข้อมูล คือ การรักษาไว้ซึ่งความลับของข้อมูล กล่าวคือ ระบบสารสนเทศนั้นจะต้องมีมาตรการความปลอดภัยที่เพียงพอ เพื่อไม่ให้ข้อมูลลับของลูกค้ารั่วไหลไปตกอยู่ในมือของคนที่ไม่ควรจะรับทราบข้อมูลนี้ ข้อมูลที่เก็บที่อยู่ในระบบสารสนเทศนี้ควรจะให้รับทราบเฉพาะผู้ที่มีสิทธ์เท่านั้น	
Conceptual Relation: ดูภาพใน CN002	
Extraction: 1. Security of information is achieved through the preservation of appropriate confidentiality, integrity, and availability. [ISM023.TXT] 2. Where confidentiality is the act of preventing Eve from reading our conversation, integrity ensures that Eve won't be able to alter our conversation, which is much more important to us. [ISM012.TXT] 3. Confidentiality is the systems deserve reassurance regarding characteristic of data and information their rights and obligations, including being disclosed only to authorized per- responsibility for system failures. [ISM023.TXT]	

CN004	**Concept:** Integrity
Eng: Integrity	**Grammatical Category:** Noun
Thai: บูรณภาพ [ราชบัณฑิตยสถาน]	
Feature: คุณสมบัติประการที่สองของการรักษาความปลอดภัยของข้อมูล คือ การรักษาไว้ซึ่งบูรณภาพของข้อมูล กล่าวคือ ระบบสารสนเทศนั้นจะต้องมีมาตรการความปลอดภัยที่เพียงพอ เพื่อให้ข้อมูลที่เก็บไว้ในนั้นมีความสมบูรณ์ถูกต้องตลอดเวลา และไม่มีการปรับเปลี่ยนเนื้อหาโดยไม่ได้รับอนุญาต	
Conceptual Relation: ดูภาพใน CN002	

Extraction:
1. Integrity is the characteristic of information being accurate and complete and the information systems' preservation of accuracy and completeness. [ISM023.TXT]
2. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. [ISM097.TXT]
3. Information Technology (IT) security includes all aspects related to defining, achieving and maintaining the five security services of identification & authentication, authorisation, confidentiality, integrity and non-repudiation as specified by the ISO 7498-2 standard. [ISM049.TXT]

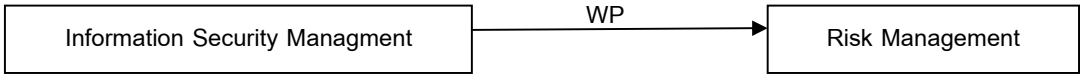
CN005	**Concept:** Availability
Eng: Availability	**Grammatical Category:** Noun
Thai: สภาพพร้อมใช้งาน [ราชบัณฑิตยสถาน]	
Feature: คุณสมบัติประการที่สามของการรักษาความปลอดภัยของข้อมูล คือ สภาพพร้อมใช้งานของข้อมูล กล่าวคือ ระบบสารสนเทศนั้นจะต้องมีมาตรการความปลอดภัยที่เพียงพอ เพื่อให้ข้อมูลที่เก็บไว้ในนั้นคงอยู่ในระบบตลอดเวลาเมื่อมีผู้ใช้งานต้องการเรียกใช้ และไม่มีการสูญหายไปโดยที่เจ้าหน้าที่ไม่รับทราบ	
Conceptual Relation: ดูภาพใน CN002	
Extraction:	
1. Availability is the characteristic of information and supporting information systems being accessible and usable on a timely basis in the required manner. [ISM023.TXT]	
2. When the disaster strikes it is important to maintain the security of the organization maintaining application and data availability, integrity and confidentiality ensures organizational security at an IT/IS level. [ISM071.TXT]	
3. For over twenty years information security has held that confidentiality, integrity and availability (known as the CIA Triad) are the core principles of information security. [ISM097.TXT]	

CN006	**Concept:** Non-Repudiation
Eng: Non-Repudiation	**Grammatical Category:** Noun
Thai: การปฏิเสธไม่ได้ [ราชบัณฑิตยสถาน]	
Feature: คุณสมบัติประการที่สี่ของการรักษาความปลอดภัยของข้อมูล คือ การปฏิเสธไม่ได้ เมื่อมีข้อมูลส่งมา ผู้ส่งจะไม่	

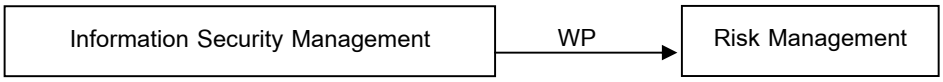
สามารถปฏิเสธได้ว่า เขาไม่ได้ส่งข้อมูลมา ดังนั้น ระบบสารสนเทศจะต้องมีมาตรการที่ตรวจสอบได้ว่า ข้อมูลนั้นส่งมาจากผู้ส่งจริง ๆ มาตรการที่นำมาใช้ เช่น การใช้ลายเซ็นอิเลคทรอนิกส์ (Digital signature)
Conceptual Relation: ดูภาพใน CN002
Extraction: 1. Information Technology (IT) security includes all aspects related to defining, achieving and maintaining the five security services of identification & authentication, authorisation, confidentiality, integrity and non-repudiation as specified by the ISO 7498-2 standard. [ISM049.TXT] 2. Non- repudiation provides proof of the origin such that the sender cannot deny sending the message, and the recipient cannot deny the receipt of the message. [ISM112.TXT] 3. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non- repudiation. [ISM097.TXT]

CN007	**Concept:** Compromise	
Eng: Compromise		**Grammatical Category:** Verb
Thai: เป็นอันตราย [วิทย์ เที่ยงบูรณธรรม]		
Feature: การกระทำที่ทำให้ระบบคอมพิวเตอร์นั้นสูญเสียความปลอดภัยของระบบ เช่น ไม่สามารถรักษาความลับของข้อมูลที่เก็บในนั้นได้ ตัวอย่างการกระทำที่ว่านั้น เช่น การขโมยเครื่องคอมพิวเตอร์ เป็นต้น		
Conceptual Relation: ดูภาพใน CN002		
Extraction: 1. Where a laptop is used by persons with differing access control privilege, residual data and / or other information could compromise the confidentiality of your information. [ISM063.TXT] 2. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. [ISM039.TXT] 3. Information Security issues to be considered when implementing your policy include the following: • Theft of equipment is most likely to result in additional cost to the organisation and could compromise data security. [ISM063.TXT]		

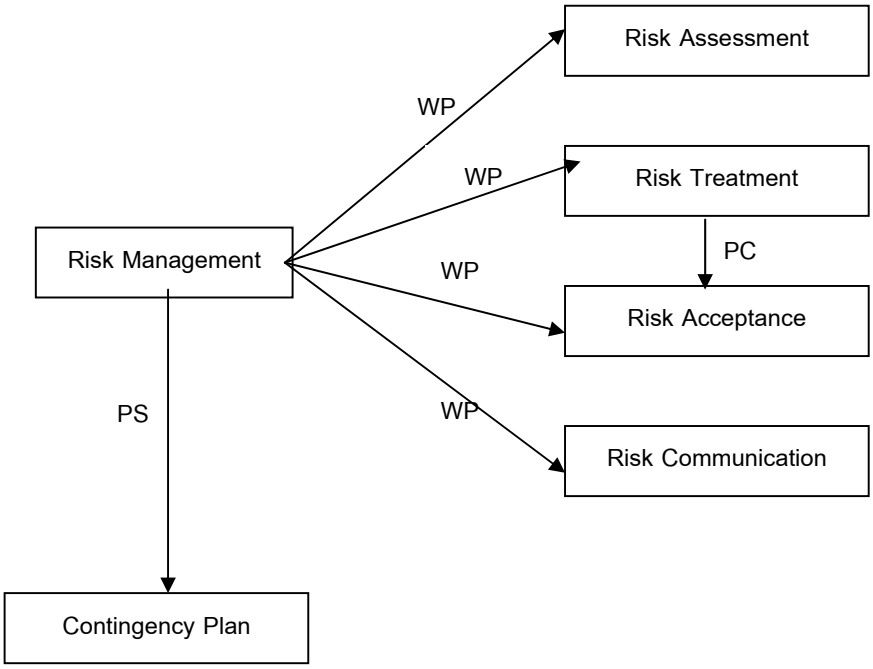
แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ขั้นตอนการทำงานในการจัดการความปลอดภัยของข้อมูล



WP **แทน** Whole – Part

CN008	**Concept:** Risk Management
Eng: Risk Management	**Grammatical Category:** Noun
Thai: การจัดการความเสี่ยง [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: ขั้นตอนหนึ่งในการจัดการความปลอดภัยของข้อมูล คือ การจัดการความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กร การจัดการความเสี่ยงนั้นจะประกอบไปด้วยขั้นตอนย่อยต่าง ๆ เพื่อระบุอันตรายที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กรรวมไปถึงมาตรการที่จะมาลดความเสี่ยงนั้น	
Conceptual Relation:  **WP แทน** Whole – Part	
Extraction: 1. ISO 27001 / ISO 17799 / ISO 27005 require risk management as part of an Information Security Management. [ISM001.TXT] 2. Risk management is a set of principles and practices like any other management discipline, and involves evaluating the value of your assets, possible threats to them, and determining appropriate measures to take to secure them. [ISM062.TXT] 3. Risk management is a process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. [ISM102.TXT]	

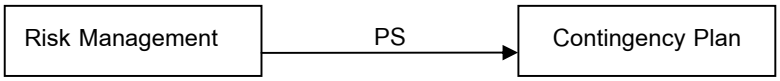
แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ขั้นตอนการทำงานในการจัดการความเสี่ยง

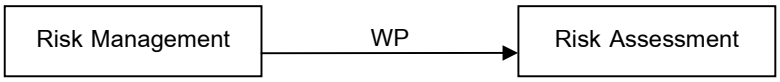


PC **แทน** Process – Consequence

PS **แทน** Problem – Solution

WP **แทน** Whole – Part

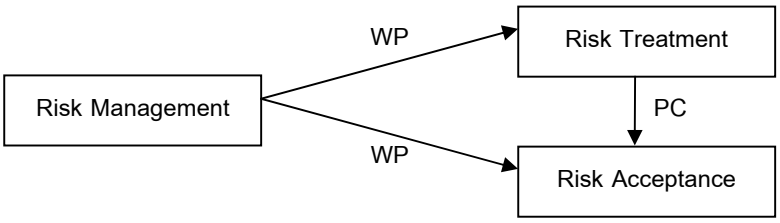
CN009	**Concept:** Contingency Plan
Eng: Contingency Plan, Business Continuity Plan	**Grammatical Category:** Noun
Thai: แผนแก้ไขปัญหาจากภัยพิบัติ [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: แผนแก้ไขปัญหาจากภัยพิบัติ คือ รายละเอียดแผนการที่ผู้ใช้งานปฏิบัติตามเมื่อมีเหตุการณ์ฉุกเฉินที่เกี่ยวข้องกับการละเมิดความปลอดภัยของข้อมูลสารสนเทศเกิดขึ้น ตัวอย่างเหตุการณ์ที่ว่านี้ เช่น ไฟไหม้ การขโมยข้อมูล และภัยธรรมชาติต่าง ๆ ในการจัดการความเสี่ยงนั้น ถ้าความเสี่ยงใดที่เป็นที่ยอมรับได้ ก็จะต้องสร้างแผนแก้ไขปัญหาจากภัยพิบัติขึ้นมา นอกจากนั้น ยังต้องมีการทดสอบแผนการเป็นระยะ ๆ เพื่อดูว่าแผนการนี้เหมาะสมหรือไม่และมีภัยอื่น ๆ เกิดขึ้นมาหรือไม่ ถ้ามี จะต้องอัพเดทแผนแก้ไขปัญหาจากภัยพิบัตินี้เพื่อให้รองรับภัยที่ค้นพบใหม่อยู่เสมอ	
Conceptual Relation:  **PS แทน Problem – Solution**	
Extraction: 1. Risk management is an essential component of managing a digitisation project and should involve the original assessment of risks associated with the project, the implementation of changes to the plans of the project if the risks involved are too high, and the transference and mitigation of high risk areas. For those areas of risk that are acceptable it means the development of appropriate contingency plans. [ISM126.TXT] 2. Every organization must plan to respond to an emergency or other occurrence (fire, vandalism, system failure or natural disaster) that damages systems. This activity will result in the development of a contingency plan. The objective of the contingency plan is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain vital enterprise information. [ISM101.TXT] 3. Testing and revision procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary. [ISM036.TXT] 4. Business Continuity Plan – Also known as contingency plan. [ISM117.TXT]	

CN010	**Concept:** Risk Assessment
Eng: Risk Assessment	**Grammatical Category:** Noun
Thai: การประเมินความเสี่ยง [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: การประเมินความเสี่ยงเป็นการระบุและการจัดลำดับความสำคัญของความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กรโดยเทียบดูว่าถ้าความเสี่ยงนั้นเกิดขึ้นกับองค์กร จะส่งผลกระทบมากน้อยเท่าใดและองค์กรสามารถยอมรับความเสี่ยงนี้ได้หรือไม่	
Conceptual Relation:  **WP แทน** Whole – Part	
Extraction: 1. The Risk Assessment is a process to identify the risks and assess the damage it could cause. The end result of a risk assessment is justification of any control or safeguards that need to be implemented to mitigate the risk to an acceptable level. [ISM064.TXT] 2. In the absence of effective risk management, the auditor will conduct a risk assessment of the organization to determine the areas of greatest risk to audit resources can be most efficiently applied. [ISM035.TXT] 3. Finally, a formal risk assessment program provided an efficient means for communicating assessment findings and recommended actions to business unit managers as well as to senior corporate officials. [ISM005.TXT] 4. Risk assessments are designed to identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. [ISM127.TXT] 5. Risk management is a process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. [ISM102.TXT]	

CN011	**Concept:** Risk Treatment
Eng: Risk Treatment	**Grammatical Category:** Noun
Thai: การลดความเสี่ยง [ผู้เชี่ยวชาญ]	
Feature: เมื่อประเมินความเสี่ยงเป็นที่เรียบร้อยแล้ว สำหรับความเสี่ยงแต่ละชนิด ผู้จัดทำจะต้องประเมินว่าจะจัดการกับ	

ความเสี่ยงนั้นอย่างไรโดยจัดการได้ 4 ประการ คือ ยอมรับความเสี่ยงนั้น ๆ หลีกเลี่ยงความเสี่ยง ถ่ายโอนความเสี่ยง หรือลดความเสี่ยงนั้น ๆ ลง หลังจากนั้น ผู้จัดทำต้องหามาตรการมาแก้ไขความเสี่ยงนั้น ๆ ตามประเภทที่จัดไว้ อนึ่ง การลดความเสี่ยงเป็นขั้นตอนหนึ่งของการจัดการความเสี่ยง (Risk Management)

Conceptual Relation:



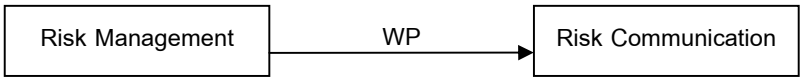
PC แทน Process – Consequence

WP แทน Whole – Part

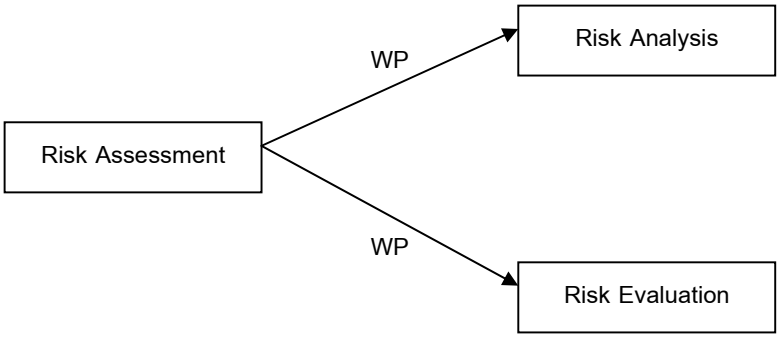
Extraction:

1. For each risk, risk treatment involves choosing amongst at least four options: accept the risk, avoid the risk, transfer the risk, or reduce the risk. [ISM102.TXT]
2. Risk treatment process of selection and implementation of measures to modify risk. [ISM124.TXT]
3. Risk management is a process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. [ISM102.TXT]
4. Risk acceptance is part of the risk treatment decision making process. [ISM102.TXT] ถ้าเช่นนั้นไม่ใช่ WP หรือ หนูแก้รูปแล้วค่ะ อาจารย์ หนูลืมโยง WP ไปที่ Risk Acceptance ค่ะ

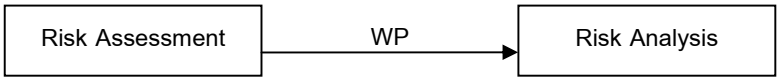
CN012	**Concept:** Risk Acceptance
Eng: Risk Acceptance, Acceptance of Risk	**Grammatical Category:** Noun
Thai: การยอมรับความเสี่ยง [ผู้เชี่ยวชาญ]	
Feature: ในขั้นตอนการลดความเสี่ยงนั้น จะมีขั้นตอนการตัดสินใจว่าจะจัดการความเสี่ยงนั้นอย่างไร โดยทางเลือกในการตัดสินใจนั้นคือการยอมรับความเสี่ยงนั้นหรือสามารถทนความเสี่ยงนั้นได้	
Conceptual Relation: ดูภาพใน CN011	
Extraction: 1. Risk acceptance is part of the risk treatment decision making process. [ISM102.TXT] 2. Risk acceptance means that you've decided that you can live with a particular risk. [ISM102.TXT] 3. Risk management is a process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. [ISM102.TXT]	

CN013	**Concept:** Risk Communication
Eng: Risk Communication	**Grammatical Category:** Noun
Thai: การสื่อสารความเสี่ยง [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: การสื่อสารความเสี่ยงนั้นเป็นการโต้ตอบและการบอกข่าวสารให้กับผู้ที่เกี่ยวข้องถึงลักษณะของความเสี่ยงและวิธีการที่จะตอบสนองกับความเสี่ยงนั้น ๆ จุดประสงค์ของการสื่อสารความเสี่ยงนั้นจะช่วยให้ผู้ที่เกี่ยวข้องเข้าใจถึงกระบวนการประเมินความเสี่ยงและการจัดการความเสี่ยง นอกจากนั้นยังช่วยตัดสินใจด้วยว่าจะตอบสนองกับความเสี่ยงอย่างไร อนึ่ง การสื่อสารความเสี่ยงเป็นส่วนหนึ่งของการจัดการความเสี่ยง	
Conceptual Relation:  	
Extraction: 1. Risk management is a process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. [ISM112.TXT] 2. The purpose of risk communication is to help those affected by the issue; understand risk assessment and risk management and participate in making decisions about how risk should be managed. [ISM128.TXT] 3. Risk Communication is an interactive process of exchange of information and opinion among individuals, groups, and institutions; often involves multiple messages about the nature of risk or expressing concerns, opinion, or reactions to risk messages. [ISM128.TXT]	

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ขั้นตอนการทำงานในการประเมินความเสี่ยง

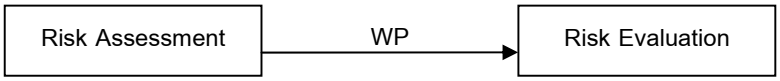


WP **แทน** Whole – Part

CN014	**Concept:** Risk Analysis
Eng: Risk Analysis	**Grammatical Category:** Noun
Thai: การวิเคราะห์ความเสี่ยง [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: ขั้นตอนหนึ่งในการประเมินความเสี่ยง คือ การวิเคราะห์ความเสี่ยงโดยผู้รับผิดชอบจะต้องประเมินปริมาณความเสี่ยงที่อาจเกิดขึ้นและหาทางดำเนินการแก้ไข อาจกล่าวได้ว่า การวิเคราะห์ความเสี่ยงคือการประเมินความเสี่ยงและจุดอ่อนที่อาจส่งผลทำให้ระบบสารสนเทศสูญเสียความลับ (Confidentiality) บูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูล	
Conceptual Relation:  **WP แทน Whole – Part**	
Extraction: 1. A risk assessment combines two techniques: a risk analysis and a risk evaluation. [ISM102.TXT] 2. Risk Analysis is a formal process of determining risks and developing a plan to deal with them. [ISM037.TXT] 3. Risk Analysis – An assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of IT resources. [ISM117.TXT]	

CN015	**Concept:** Risk Evaluation
Eng: Risk Evaluation	**Grammatical Category:** Noun
Thai: การประเมินความรุนแรงของความเสี่ยง [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: ขั้นตอนอีกขั้นตอนหนึ่งในการประเมินความเสี่ยง คือ การประเมินความรุนแรงความเสี่ยงซึ่งจะตัดสินจากเงื่อนไขความเสี่ยง นอกจากนั้นเงื่อนไขในการประเมินความรุนแรงของความเสี่ยงจะนำไปเป็นเงื่อนไขในการเลือกหนทางที่จะนำมาลดความเสี่ยงนั้น ๆ ด้วย	

Conceptual Relation:

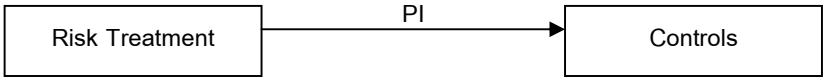


WP **แทน** Whole – Part

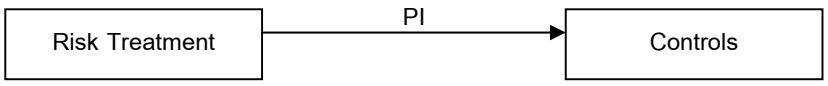
Extraction:

1. A risk assessment combines two techniques: a risk analysis and a risk evaluation. [ISM102.TXT]
2. The risk evaluation criteria are used as a guide to enable decisions to be made on risk treatment options. [ISM064.TXT]
3. A risk evaluation compares the estimated risk with a set of risk criteria. This is done in order to determine how significant the risk really is. [ISM102.TXT]

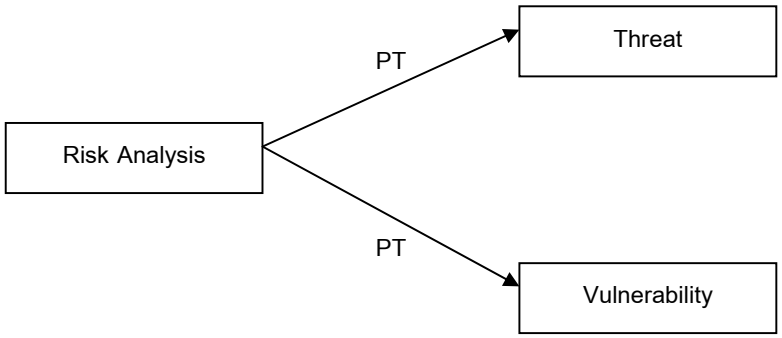
แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
การหามาตรการมาลดความเสี่ยง



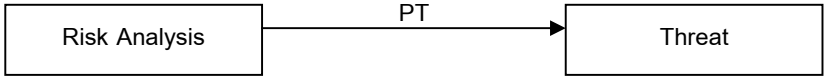
PI แทน Process - Instrument

CN016	**Concept:** Controls
Eng: Controls	**Grammatical Category:** Noun
Thai: มาตราการควบคุมความปลอดภัย [ศัพท์บัญญัติราชบัณฑิตยสถาน]	
Feature: ขั้นตอนหนึ่งของการลดความเสี่ยงที่อาจเกิดขึ้นในระบบสารสนเทศ คือ การหามาตรการความปลอดภัยมาใช้เพื่อลดความเสี่ยง ตัวอย่างของมาตรการควบคุมความปลอดภัย คือ การดำเนินการ การจัดตั้งนโยบาย วิธีการปฏิบัติงาน และการนำเทคโนโลยีมาใช้	
Conceptual Relation:  **PI แทน** Process - Instrument	
Extraction: 1. The risk treatment plan coordinates the treatments to reduce risks and implement controls required to protect information. [ISM064.TXT] 2. Specific controls are put in place that would reduce the level of risk. [ISM001.TXT] 3. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures. [ISM102.TXT]	

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
การระบุความเสี่ยง

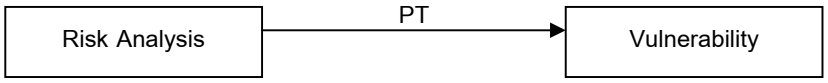


PT **แทน** Process – Target

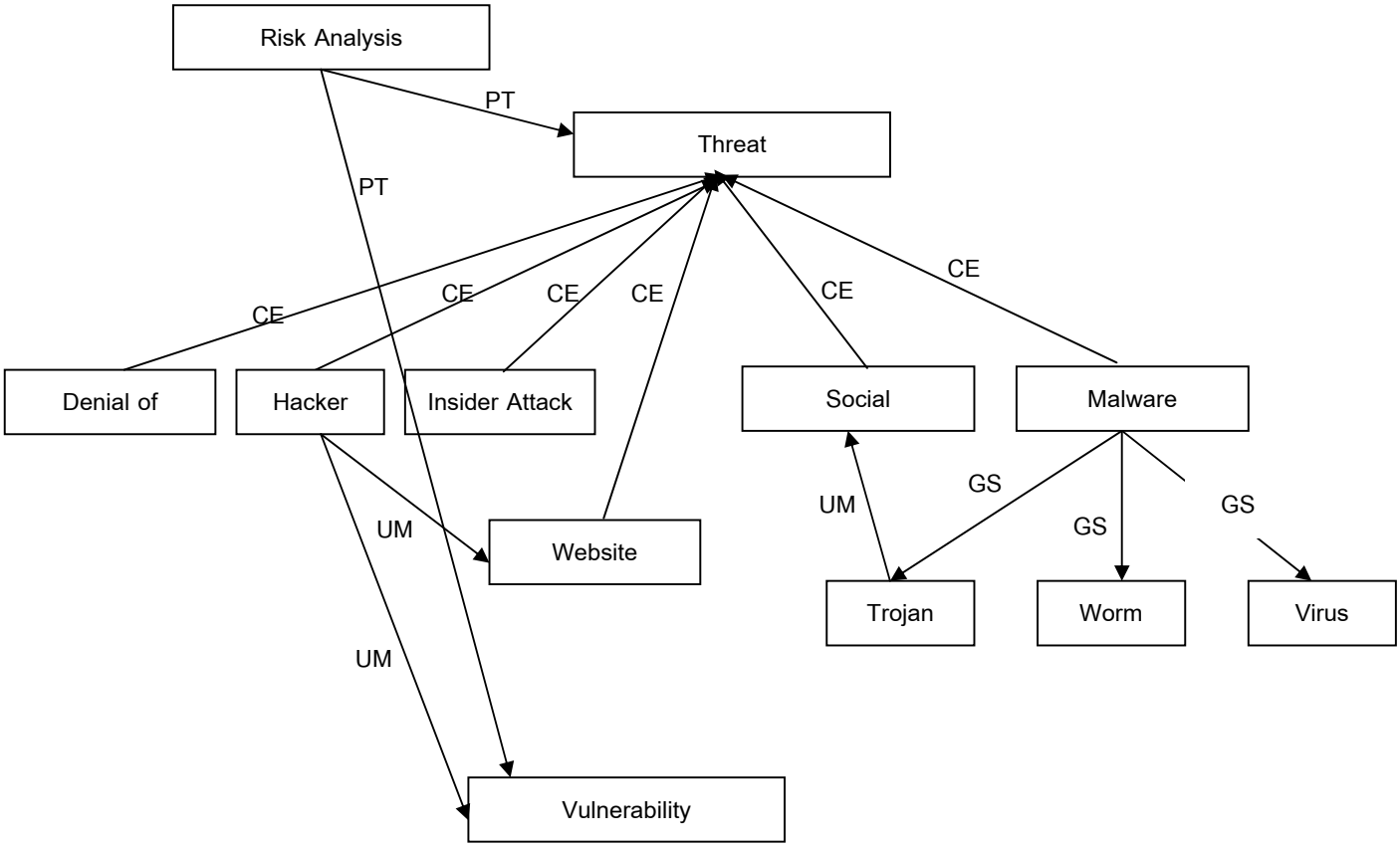
CN017	**Concept:** Threat
Eng: Threat	**Grammatical Category:** Noun
Thai: ภัยคุกคาม [วิทย์ เที่ยงบูรณธรรม]	
Feature: ในขั้นตอนการวิเคราะห์ความเสี่ยง ผู้จัดทำต้องวิเคราะห์ภัยคุกคามที่อาจจะเกิดขึ้นในระบบได้ โดยภัยคุกคามนั้นอาจจะเกิดจากฝีมือมนุษย์หรืออาจเกิดมาจากภัยธรรมชาติ ภัยคุกคามก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์	
Conceptual Relation:  PT **แทน** Process – Target	
Extraction: 1. Risk analysis requires understanding the core business functions of the enterprise and then analyzing	

potential threats and vulnerabilities to assets and information. [ISM130.TXT]

2. A threat is anything (man made or act of nature) that has the potential to cause harm. [ISM097.TXT]
3. Threat -An action or event that posses a possible danger to a computer system. [ISM117.TXT]
4. Threat a potential cause of an unwanted incident, which may result in harm to a system or organization. [ISM124.TXT]

CN018	**Concept:** Vulnerability
Eng: Vulnerability	**Grammatical Category:** Noun
Thai: ความอ่อนแอของระบบ [ราชบัณฑิตยสถาน]	
Feature: ในขั้นตอนการวิเคราะห์ความเสี่ยง นอกจากผู้รับผิดชอบจะต้องระบุภัยคุกคามที่อาจจะก่อให้ผลเสียหายต่อระบบสารสนเทศแล้ว ผู้รับผิดชอบยังต้องระบุความอ่อนแอของระบบที่อาจเป็นช่องโหว่ให้ผู้คุกคามใช้โจมตีระบบสารสนเทศได้ โดยความอ่อนแอของระบบก่อให้เกิดความเสียหายต่อระบบข้อมูลขององค์กร	
Conceptual Relation:  **PT แทน** Process – Target	
Extraction: 1. Risk analysis requires understanding the core business functions of the enterprise and then analyzing potential threats and vulnerabilities to assets and information. [ISM130.TXT] 2. Vulnerability is a weakness in an asset or group of assets. [ISM102.TXT] 3. Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. [ISM097.TXT]	

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ประเภทของภัยคุกคาม



CE **แทน** Cause – Effect

GS **แทน** Generic – Specific

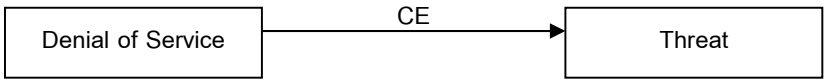
PT **แทน** Process – Target

UM **แทน** User – Method

CN019	**Concept:** Denial of Service
Eng: Denial of Service, DoS Attack	**Grammatical Category:** Noun
Thai: การล่มระบบ [ราชบัณฑิตยสถาน]	
Feature: การโจมตีประเภทหนึ่ง คือ การล่มบริการระบบโดยเกิดจากการที่ส่งข้อความหรือการร้องขอเข้ามามากอย่างท่วม	

ท้นจนระบบไม่สามารถรองรับการรับข้อความหรือการร้องขอรับบริการนั้นได้ซึ่งอาจก่อให้เกิดความเสียหายต่อธุรกิจได้ นอกจากนั้น เมื่อมีข้อความส่งเข้ามามาก ๆ อาจกันไม่ให้ผู้ใช้งานคนอื่นสามารถใช้ระบบเครือข่ายได้

Conceptual Relation:



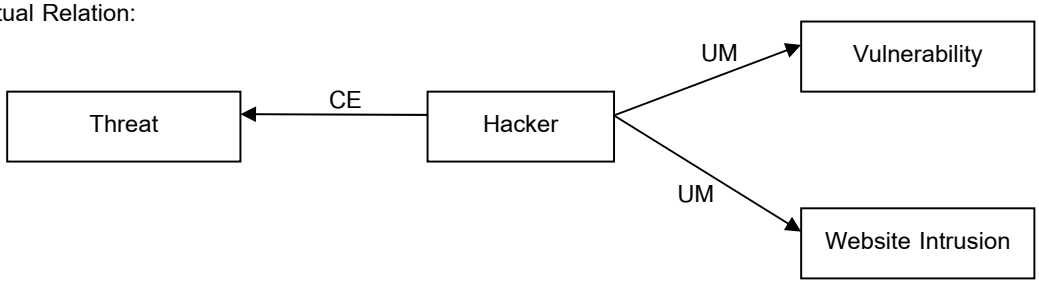
CE แทน Cause – Effect

Extraction:

1. A denial of service can occur when a service is overwhelmed by requests, causing legitimate business requests not to be processed. [ISM001.TXT]
2. Denial-of-service (DoS attacks): An attempt to break the system and make it inaccessible to other users. [ISM040.TXT]
3. A Denial of Service (DoS) attack is an attack which attempts to prevent the victim from being able to use all or part of their network connection. [ISM104.TXT]
4. Denial of Service is a security threat that has recently gained much public attention. Typically the attacks use bugs found in common operating systems and cause the machines to slow down their operation or crash. This paper has described two attack types, Land and Teardrop that use vulnerabilities on IP packet reassembly and the opening of a TCP connection. [ISM137.TXT]

CN020	**Concept:** Hacker
Eng: Hacker	**Grammatical Category:** Noun
Thai: ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ [วิทย์ เที่ยงบูรณธรรม]	
Feature: ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ที่เจาะระบบเข้ามาเพื่อขโมยข้อมูลหรือมีเจตนาที่จะทำลายระบบเพื่อให้ระบบสารสนเทศขององค์กรใช้งานไม่ได้ โดยใช้จุดอ่อนแอของระบบสารสนเทศ เว็บไซต์หรือระบบอินเตอร์เน็ตขององค์กรในการบุกรุกเข้าไป ผู้เจาะระบบเครือข่ายคอมพิวเตอร์นี้ จะหมายถึง ผู้ที่ใช้ความรู้ความสามารถของตนในการบุกรุกเข้าไปในระบบเครือข่ายของผู้อื่นโดยที่ไม่ได้รับอนุญาต โดยเจตนาการบุกรุกนั้นคือเพื่อต้องการทดสอบฝีมือของตนและเข้ามาขโมยข้อมูลหรือสร้างความเสียหายให้แก่ระบบสารสนเทศนั้น เดิมที ผู้เจาะระบบเครือข่ายคอมพิวเตอร์มีเจตนาแค่ต้องการศึกษาระบบคอมพิวเตอร์เท่านั้น เพื่อช่วยบริษัทต่าง ๆ ค้นหาจุดอ่อนระบบของตน	

Conceptual Relation:



CE แทน Cause – Effect

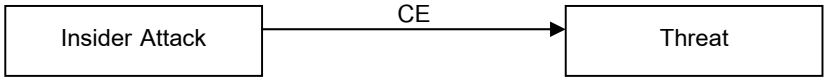
UM แทน User – Method

Extraction:

1. A hacker is basically someone who hacks a system - he could do this because he finds it interesting or because he wants to access your system. [ISM040.TXT]
2. A user operating with elevated privileges can do all manner of damage and presents a vulnerability that a hacker can exploit. [ISM058.TXT]
3. As long as an organization has an Internet presence, the hacker threat will remain. [ISM001.TXT]
4. The New Zealand Herald's website fell victim to a page spoofing stunt earlier today, by hackers wanting to publicise their upcoming Kiwicon security conference in November. [ISM025.TXT]
5. The word cracker is often confused with hacker, when in reality most hackers act ethically and it is the black hat hackers (crackers) that act unethically. It is because of this that traditional hackers have obtained their negative reputation from Crackers who exploit weaknesses and compromise the security of a system without permission. [ISM139.TXT]
6. On the other hand, traditional hackers are interested in gaining knowledge about computer systems, most often to help companies identify weaknesses in their system's security. [ISM139.TXT]

CN021	**Concept:** Insider Attack
Eng: Insider Attack	**Grammatical Category:** Noun
Thai: การโจมตีจากภายในองค์กร [วิทย์ เที่ยงบูรณธรรม]	
Feature: ภัยที่เกิดจากการโจมตีที่เกิดขึ้นในระบบเครือข่ายภายในองค์กรเองและอาจจะเกิดจากคนในองค์กรนั้นเองหรือคนที่สามารถเข้าไปในระบบภายในได้ ผู้เชี่ยวชาญบางคนถึงกับกล่าวว่า การโจมตีจากภายในองค์กรนั้นถือเป็นภัยคุกคามที่ร้ายแรงที่สุด	

Conceptual Relation:



CE **แทน** Cause – Effect

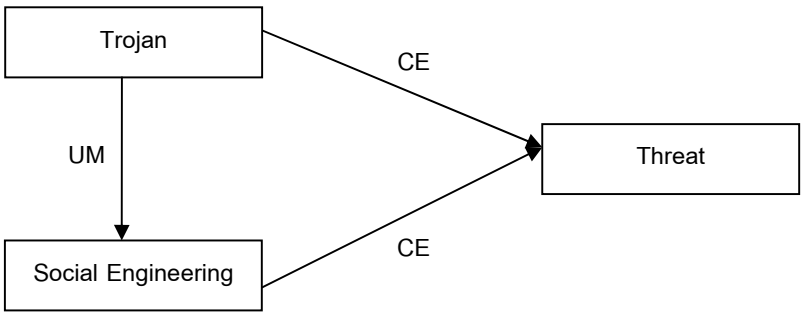
Extraction:

1. Insider Attacks is the primary threat to computer systems has traditionally been the insider attack. [ISM105.TXT]
2. Insider Attacks are an unusual type of threat. Unlike external attacks, the intruder is someone who has been entrusted with authorized access to the network. [ISM106.TXT]
3. By any way you want to measure it, the number one threat for any information system is the insider attack. Cited across the board, from government to military to businesses to warfare attacks for any system, military or otherwise, is the insider attack. [ISM107.TXT]

CN022	**Concept:** Social Engineering
Eng: Social Engineering	**Grammatical Category:** Noun
Thai: กลลวงทางสังคม [ผู้เชี่ยวชาญ]	

Feature: ภัยที่เกิดจากการการหลอกลวงหรือการพูดจาหลอกล่อเพื่อให้ผู้ใช้งานระบบสารสนเทศบอกข้อมูลที่เป็นความลับมา เช่น รายชื่อของผู้ใช้งานในระบบและรหัสผ่านเข้าระบบ เพื่อเข้าไปในบริษัทเพื่อขโมยข้อมูลออกมา ตัวอย่างภัยคุกคามประเภทนี้ ผู้ใช้งานที่โดนหลอกโดยใช้ทางกลลวงทางสังคมนี้มักจะให้ความร่วมมือกับผู้โจมตีเป็นอย่างดีโดยที่ไม่สะดุดใจแต่อย่างใด ผู้บุกรุกอาจจะหลอกถามผู้ใช้งานทางทางตรงและทางอ้อมเพื่อให้ได้ข้อมูลที่สำคัญมา

Conceptual Relation:

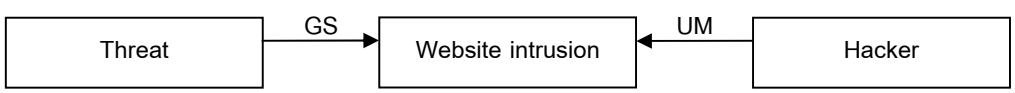


CE **แทน** Cause – Effect

UM **แทน** User – Method

Extraction:

1. Users disclosing sensitive information or passwords in response to seemingly innocent requests from strangers either over the phone or in person can provide intruders easy access to an organization's information and systems. Such techniques often referred to as "social engineering," exploit users' tendencies to be cooperative and helpful, instead of guarded, careful, and suspicious, when information is requested. [ISM004.TXT]
2. Use another employee's account and password (which he cracked technologically or discovered through social engineering techniques) to get access to files or programs he can't access with his own account. [ISM058.TXT]
3. One of the most critical and easy to conduct ways of obtaining sensitive data is simply to ask for it, both in a direct or an indirect way, which is what social engineering is all about. [ISM050.TXT]
4. In the UK, the National Infrastructure Security Coordination Center (NISCC), part of MI5, noted that 300 companies have been targeted by Trojan programs delivered by hackers as email attachments, CDs, or links to phony websites. The NISCC warned that the emails used social engineering techniques to entice opening the Trojan Horseinfected documents. [ISM138.TXT]

CN023	**Concept:** Website intrusion
Eng: Website intrusion	**Grammatical Category:** Noun
Thai: การบุกรุกทางเว็บไซต์ [ราชบัณฑิตยสถาน]	
Feature: การบุกรุกทางเว็บไซต์ก่อให้เกิดภัยคุกคามอย่างหนึ่งในระบบสารสนเทศขององค์กรซึ่งมีช่องโหว่ทำให้บุคคลภายนอกหรือแม้แต่กระทั่งบุคคลภายในองค์กรเองบุกรุกเข้ามาในเว็บไซต์ขององค์กรหรือเข้ามาในส่วนที่ไม่ได้รับอนุญาตซึ่งเป็นส่วนที่มีข้อมูลความลับขององค์กรเก็บอยู่ การบุกรุกทางเว็บไซต์นี้เป็นวิธีการอย่างหนึ่งที่ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ (Hacker) ใช้และเป็นภัยคุกคามอันดับต้น ๆ ขององค์กรขนาดเล็กไปจนถึงขนาดกลาง	
Conceptual Relation:  CE **แทน** Cause – Effect UM **แทน** User – Method	

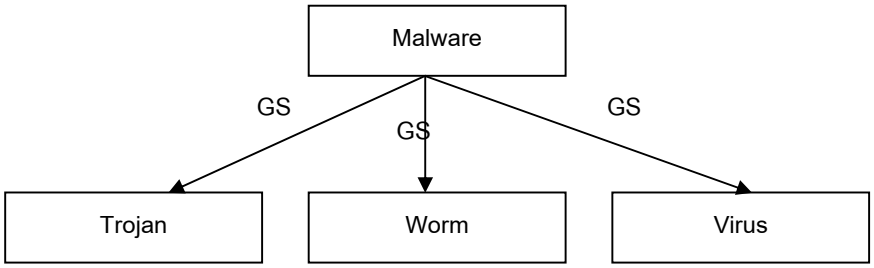
Extraction:

1. Website Intrusion is attacks that invade a website. These intrusions can be attacks from outside the organization and misuse from within the organization. [ISM112.TXT]
2. The security threats that most often and most seriously contribute to small-medium business days lost include virus incidents and website intrusion (by hacking). [ISM116.TXT]

CN024	**Concept:** Malware
Eng: Malware	**Grammatical Category:** Noun
Thai: โปรแกรมมุ่งร้าย [ราชบัณฑิตยสถาน]	

Feature: โปรแกรมมุ่งร้ายนั้นเป็นโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์และเครือข่าย โดยโปรแกรมมุ่งร้ายจะทำงานในลักษณะที่เป็นไวรัส ทั้งประเภทหนอนอินเตอร์เน็ต ม้าโทรจัน แอบดักข้อมูล ตลอดจนโปรแกรมขโมยข้อมูล แต่ผู้ใช้งานบางคนก็ยังไม่คุ้นเคยในการใช้คำว่า โปรแกรมมุ่งร้ายและมักจะใช้คำว่าไวรัส แทน แต่โปรแกรมมุ่งร้ายนั้นไม่ได้หมายถึงไวรัสคอมพิวเตอร์อย่างเดียว ผู้ใช้งานมักจะประมวลผลโปรแกรมมุ่งร้ายโดยไม่รู้ตัวเพราะบางครั้งโปรแกรมมุ่งร้ายนี้จะหน้าตาเหมือนโปรแกรมปกติทั่ว ๆ ไป

Conceptual Relation:

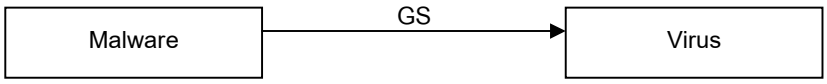


GS แทน Generic – Specific

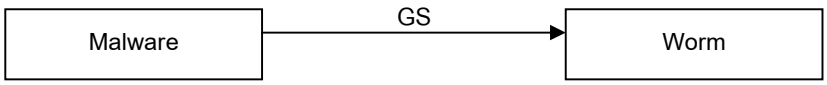
Extraction:

1. Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. [ISM111.TXT]
2. Malware are programs that do harm to your system or leave you vulnerable to attack such as Virus, Worms, and Trojans. [ISM111.TXT]
3. The attacker leaves a malware-infected floppy disc, CD ROM or USB flash drive in a location sure to be

found or that is commonly visited, gives it a legitimate looking label and then waits in the hopes that someone will eventually use it. [ISM096.TXT]

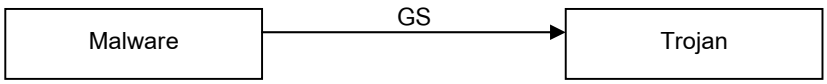
CN025	**Concept:** Virus
Eng: Virus	**Grammatical Category:** Noun
Thai: ไวรัสคอมพิวเตอร์ [ราชบัณฑิตยสถาน]	
Feature: ภัยคุกคามประเภทที่เกิดจากไวรัสคอมพิวเตอร์หรือโปรแกรมร้ายแรงที่จ้องทำลายระบบสารสนเทศขององค์กรหรือคอมพิวเตอร์ของผู้ใช้งาน ไวรัสคอมพิวเตอร์นี้ คือ โปรแกรมที่สามารถประมวลผลได้และสามารถแตกตัวเองต่อไปเรื่อย ๆ อาจจะไปติดกับโปรแกรมอื่น ๆ เช่น โปรแกรมพิมพ์งาน หรือไปติดกับแผ่นดิสก์ที่เสียบมาในคอมพิวเตอร์ เมื่อใดก็ตามที่มีการประมวลผลไฟล์ ๆ นั้น ไวรัสนั้นก็จะโดนประมวลผลไปด้วย คอมพิวเตอร์ที่มีไวรัสอาจมีการทำงานที่แปรปรวนไปโดยที่ผู้ใช้งานไม่ได้ปรับเปลี่ยนอะไรทั้งสิ้น อนึ่ง ไวรัสอาจจะทำให้ระบบคอมพิวเตอร์สูญเสียบูรณภาพ (Integrity)ได้	
Conceptual Relation:  **GS แทน** Generic – Specific	
Extraction: 1. A computer virus is a program designed to replicate and spread on its own, preferably without you knowing it exists. Computer viruses spread by attaching themselves to another program (such as your word processing or spreadsheet programs) or to the boot sector of a diskette. When an infected file is executed, or the computer is started from an infected disk, the virus itself is executed. [ISM095.TXT] 2. A virus is a piece of software designed and written to adversely affect your computer by altering the way it works without your knowledge or permission. [ISM096.TXT] 3. A loss of integrity can occur if a computer virus is released onto the computer. [ISM097.TXT]	

CN026	**Concept:** Worm
Eng: Worm	**Grammatical Category:** Noun

Thai: หนอนคอมพิวเตอร์ [ราชบัณฑิตยสถาน]
Feature: ภัยคุกคามที่เกิดจากหนอนคอมพิวเตอร์ที่สามารถแพร่ตัวเองได้โดยไม่ต้องพึ่งผู้ใช้งาน หนอนคอมพิวเตอร์จะเหมือนกับไวรัสคอมพิวเตอร์ตรงที่เป็นโปรแกรมที่ประมวลผลตัวเองได้ แต่สิ่งที่เป็นความแตกต่างระหว่างไวรัสกับหนอนคือหนอนคอมพิวเตอร์ไม่จำเป็นต้องพึ่งโปรแกรมอื่นที่จะช่วยแพร่ตนเองไปได้แต่ในขณะที่ไวรัสต้องมีโปรแกรมแม่ที่จะสร้างไวรัสตัวลูกไปเรื่อย ๆ
Conceptual Relation:    **GS แทน** Generic – Specific
Extraction: 1. Worm is programs that spread themselves from computer to computer over a network without user intervention. [ISM095.TXT] 2. A worm is a program that self replicates itself and sends itself from computer to computer, a worm is not considered a virus because it is the whole program that is self replicating rather than infecting files with the virus code. [ISM094.TXT] 3. A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. [ISM108.TXT]

CN027	**Concept:** Trojan	
Eng: Trojan, Trojan Horse		**Grammatical Category:** Noun
Thai: ม้าโทรจัน [ราชบัณฑิตยสถาน]		
Feature: ภัยคุกคามที่เกิดจากม้าโทรจันซึ่งเป็นโปรแกรมที่ดูเหมือนเป็นโปรแกรมที่ทำงานแบบปกติทั่ว ๆ ไปแต่แท้จริงแล้วมีโปรแกรมร้ายซ่อนอยู่ไว้ข้างหลังและทำร้ายระบบเครือข่าย เมื่อผู้ใช้งานประมวลผลโปรแกรมนี้โดยไม่รู้ตัว โปรแกรมม้าโทรจันก็จะก่อความเสียหายแก่คอมพิวเตอร์ที่ติดม้าโทรจัน เช่น มีการลบข้อมูลบางอย่างทิ้ง โดยปกติแล้ว คำว่าม้าโทรจันนี้ เรามักจะได้ยินจากในตำนานสงครามโทรจันที่มีการส่งม้าโทรจันให้เป็นของขวัญแต่ปรากฏว่ามีทหารทรอยซ่อนอยู่ในนั้นซึ่งพอมาถึงที่ ทหารโทรจันก็เปิดประตูออกมาและโจมตีฝ่ายตรงข้าม ในปัจจุบัน ม้าโทรจันนั้นนำมาใช้ในการติดตั้งโปรแกรมที่ก่อให้เกิดรูรั่วซึ่งผู้โจมตีจะผ่านเข้าไปเพื่อขโมยข้อมูลโดยม้าโทรจันอาจจะมาในรูปของหนอนคอมพิวเตอร์และไวรัสคอมพิวเตอร์ก็ได้		

Conceptual Relation:

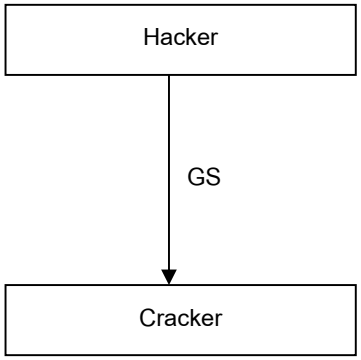


GS แทน Generic – Specific

Extraction:

1. Trojan Horse is a programme that causes unexpected and usually undesirable effects when installed or run by an unsuspecting user. [ISM024.TXT]
2. A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and do its chosen form of damage, such as erasing the data on your hard drive. [ISM082.TXT]
3. Simply put, a Trojan horse is not a computer virus in most cases. Unlike such badware, it does not propagate by self-replication but relies heavily on the exploitation of an end-user (see Social engineering). It is instead a categorical attribute which can encompass many different forms of codes. Therefore, a computer worm or virus may be a Trojan horse. The term is derived from the classical myth of the Trojan Horse. In the field of computer architecture, 'Trojan Horse' can also refer to security loopholes that allow kernel code to access anything for which it is not authorized. [ISM096.TXT]

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ประเภทของการโจมตีจากผู้เจาะระบบเครือข่ายคอมพิวเตอร์

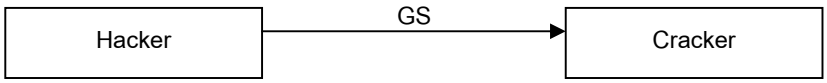


GS **แทน** Generic – Specific

CN028	**Concept:** Cracker
Eng: Cracker, Black hat hacker	**Grammatical Category:** Noun
Thai: ผู้บุกรุกระบบ [ราชบัณฑิตยสถาน]	

Feature: ผู้บุกรุกระบบนั้นจะพยายามบุกรุกเข้าไปในระบบเครือข่ายสารสนเทศขององค์กรโดยที่ไม่ได้รับอนุญาตโดยที่ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ (Hacker) กับผู้บุกรุกระบบนั้นมีส่วนแตกต่างที่ว่า ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ จะใช้วิธีการที่ชาญฉลาดและมีการวางแผนมาอย่างดีเพื่อเจาะเข้าระบบ ในขณะที่ผู้บุกรุกระบบนั้นจะพยายามบุกรุกเข้าระบบคอมพิวเตอร์ผ่านทางเครือข่าย เช่น ข้ามระบบรหัสผ่านไป แต่วิธีการที่จะบุกรุกเข้าไปนั้นอาจจะไม่ชาญฉลาดเท่ากับที่ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ใช้ ในปัจจุบัน ผู้บุกรุกระบบมักจะเรียกตนเองว่า ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ และข่าวในปัจจุบันมักจะใช้ศัพท์สองคำนี้จนแทบจะมีความหมายอย่างเดียวกันไปแล้ว แต่แท้จริงแล้วนั้นความหมายของคำว่า ผู้บุกรุกระบบไม่เหมือนกับผู้เจาะระบบเสียทีเดียวโดยผู้บุกรุกระบบจะใช้วิธีการที่ไม่รุนแรงหรือฉลาดเท่ากับที่ผู้เจาะระบบใช้ และผู้เจาะระบบมักจะมีเจตนาที่มีคุณธรรมกว่า ในขณะที่ผู้บุกรุกระบบนั้นมักจ้องจะทำลายระบบคอมพิวเตอร์เป็นหลัก

Conceptual Relation:



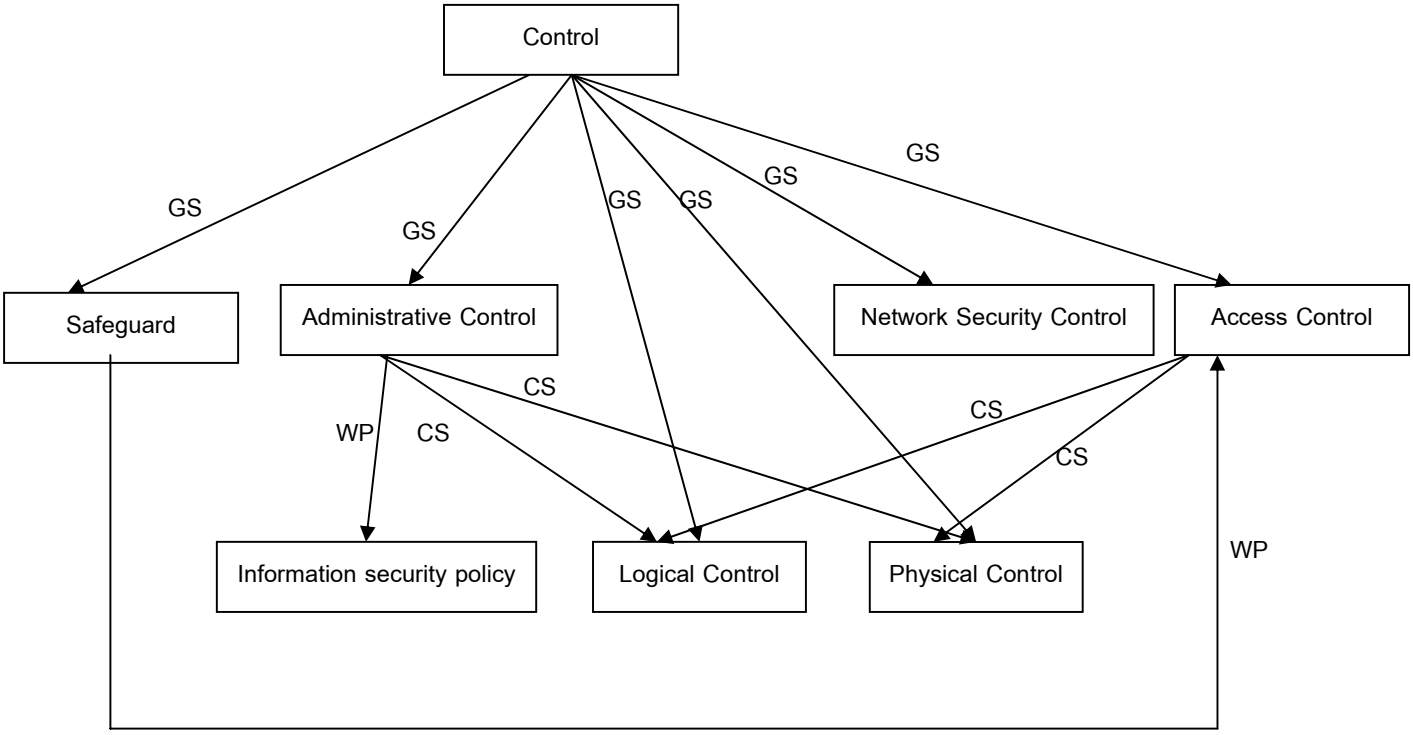
GS แทน Generic – Specific

Extraction:

1. Cracker - An individual who attempts to gain unauthorised access to a computer system. These individuals are often malicious and have many means at their disposal for breaking into a system. Crackers often like to describe themselves as hackers. Cracking does not usually involve some mysterious leap of hackerly brilliance but rather persistence and repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. [ISM112.TXT]
2. A cracker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. The term "cracker" is not to be confused with "hacker". Hackers generally deplore cracking. [ISM050.TXT]
3. A computer cracker is a person who breaks into a computer system without authorization, whose purpose is to do damage (destroy files, steal credit card numbers, plant viruses, etc.). Because a cracker uses low-level hacker skills to do cracking, the terms "cracker" and "hacker" have become synonymous with the latter becoming the most widely used term. [ISM095.TXT]
4. A Cracker is a type of hacker that breaks into computer systems for monetary gain or to maliciously cause damage. The word cracker is often confused with hacker, when in reality most hackers act ethically and it is the black hat hackers (crackers) that act unethically. It is because of this that traditional hackers have obtained their negative reputation from Crackers who exploit weaknesses and compromise the security of

a system without permission. Hackers originally came up with the name “Cracker” in the 1980's to disconnect themselves from the actions of these individuals, whose only purpose was to gain unauthorized access to network systems. On the other hand, traditional hackers are interested in gaining knowledge about computer systems, most often to help companies identify weaknesses in their system’s security. [ISM139.TXT]

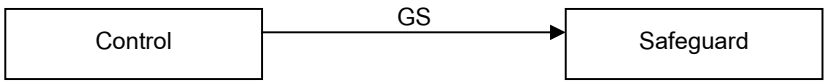
แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ประเภทของมาตราการควบคุมความปลอดภัย



CS **แทน** Condition – Selection

GS **แทน** Generic – Specific

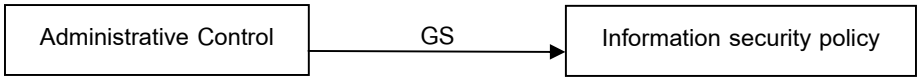
WP **แทน** Whole – Part

CN029	**Concept:** Safeguard
Eng: Safeguard, Security Control	**Grammatical Category:** Noun
Thai: สิ่งป้องกัน [วิทย์ เที่ยงบูรณธรรม]	
Feature: สิ่งป้องกันนั้นจะปกป้องระบบคอมพิวเตอร์ให้คงความปลอดภัยของระบบไว้โดยสิ่งป้องกันนั้นเป็นได้ตั้งแต่ฮาร์ดแวร์และซอฟต์แวร์ที่ทำมาเพื่อรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ วิธีการในการทำงาน มาตรการควบคุมการเข้าถึงและการแจกจ่ายข้อมูล เครื่องมือทางกายภาพ สิ่งป้องกันที่มีประสิทธิภาพมากที่สุดอย่างหนึ่ง คือ การที่ให้จอคอมพิวเตอร์ไม่มีข้อมูลค้างไว้ในขณะที่ผู้ใช้งานไม่อยู่ที่โต๊ะ อนึ่ง ถ้าสิ่งป้องกันที่เลือกใช้ไม่มีประสิทธิภาพเพียงพออาจจะก่อให้เกิดเหตุการณ์ทางด้านความปลอดภัยขึ้น	
Conceptual Relation:  **GS แทน** Generic – Specific	
Extraction: 1. Safeguards- (also called security controls). The protective measure and controls that are prescribed to meet the security requirements specified for systems. Safeguards may include, but are not limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints, ;personnel security; and physical structures, areas, and devices. [ISM117.TXT] 2. Information can be read from your screen, especially when your workstation is logged on and you are away from your desk. A Clear Screen Policy is an effective safeguard. [ISM063.TXT] 3. An information security event indicates that an information security policy may have been violated or a safeguard may have failed. [ISM102.TXT]	

CN030	**Concept:** Information security policy
Eng: Information security policy	**Grammatical Category:** Noun
Thai: นโยบายรักษาความปลอดภัยของข้อมูล [ราชบัณฑิตยสถาน]	
Feature: มาตราการควบคุมความปลอดภัยประเภทแรกที่องค์กรมักนำมาใช้ในการวางแผนงานรูปแบบใหม่ วิธีการบริการ	

องค์กรแบบใหม่เพื่อให้พนักงานในองค์กรปฏิบัติตามทุกคน นโยบายรักษาความปลอดภัยของข้อมูลจะบอกรายละเอียดถึงแนวทางการปฏิบัติ มาตรฐานการรักษาความปลอดภัย ให้พนักงานในองค์กรทราบเพื่อปฏิบัติตามอย่างถูกต้อง นอกจากนี้นโยบายรักษาความปลอดภัยของข้อมูลจะเป็นตัวกำหนดว่า องค์กรหนึ่ง ๆ ต้องใช้มาตราการควบคุมความปลอดภัยทางวัตถุ เช่น การเปลี่ยนล็อกกุญแจ และมาตราการควบคุมความปลอดภัยแบบตรรก เช่น การเลือกซอฟต์แวร์มาใช้การรักษาความปลอดภัย ซึ่งมาตราการควบคุมความปลอดภัยแบบทางวัตถุและแบบตรรกนั้นก็ถือเป็นส่วนหนึ่งของสิ่งป้องกันด้วย

Conceptual Relation:



GS แทน Generic – Specific

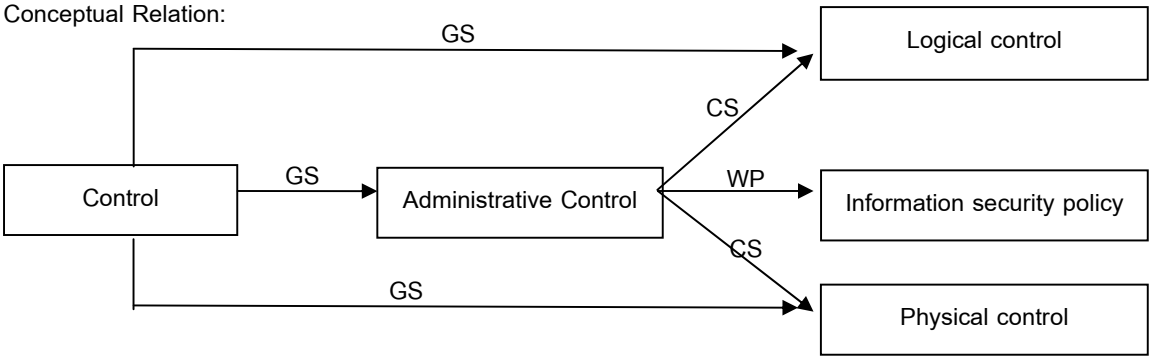
Extraction:

1. Information Security Policies are the cornerstone of Information Security effectiveness. Without a policy upon which to base standards and procedures, decisions are likely to be inconsistent and security holes will be present - ready to be exploited by both internal and external persons alike. [ISM063.TXT
2. The objective of developing security policies should include the development of information security and other security policy documents, documentation of security procedures, determination of contingency planning requirements and development of physical security plans. [ISM101.TXT]
3. After the quality review is completed, the analysis group inputs the information about the current controls, as derived from the questionnaire's answers, into a software program. The software program compares these controls to control requirements documented in the company's information security policies. [ISM005.TXT]
4. Other examples of administrative controls include the corporate security policy. [ISM097.TXT]

CN031	**Concept:** Administrative Control
Eng: Administrative Control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมทางด้านบริหาร [ราชบัณฑิตยสถาน]	
Feature: มาตรการควบคุมทางด้านบริหาร เป็นโครงสร้างการบริหารคนและงานต่าง ๆ และเป็นสิ่งที่บอกว่า ในแต่ละวันนั้นใครต้องทำอะไร และงานต่าง ๆ มีกระบวรการอย่างไรบ้าง มาตรการควบคุมทางด้านบริหารนั้นเป็นตัวกำหนดว่าจะต้องใช้มาตรการควบคุมด้านตรรกะ (Logical Control) และ มาตรการควบคุมแบบกายภาพ (Physical Control) ตัวอย่างของ	

มาตรการควบคุมทางด้านบริหาร เช่น นโยบายรักษาความปลอดภัย (Security policy)

Conceptual Relation:



CS แทน Condition – Selection

GS แทน Generic – Specific

WP แทน Whole – Part

Extraction:

1. Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. [ISM097.TXT]
2. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. [ISM097.TXT]
3. Other examples of administrative controls include the corporate security policy. [ISM097.TXT]

CN031	**Concept:** Logical control
Eng: Logical control, technical control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมแบบตรรกะ [ราชบัณฑิตยสถาน]	
Feature: มาตรการควบคุมแบบตรรกะใช้ซอฟต์แวร์และข้อมูลในการควบคุมการเรียกดูข้อมูลและการเข้าถึงระบบคอมพิวเตอร์ภายในองค์กร ตัวอย่างมาตรการควบคุมแบบนี้ เช่น รหัสผ่าน ระบบไฟร์วอลล์ ระบบตรวจเจอการบุกรุกเข้าสู่ระบบเครือข่าย รายชื่อผู้ใช้งานที่มีสิทธิ์เข้าสู่ระบบเครือข่ายได้ และการเข้ารหัสข้อมูล การเลือกมาตรการควบคุมแบบตรรกะนั้นขึ้นอยู่กับเนื้อหาในนโยบายรักษาความปลอดภัยที่องค์กรนั้น ๆ ใช้	
Conceptual Relation: ดูภาพใน CN030	
Extraction: 1. Logical controls (also called technical controls) use software and data to monitor and control access to	

information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls. [ISM097.TXT] 2. Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. [ISM097.TXT] 3. Technological refers to logical controls such as passwords, encryption, protocols, anti-virus software, firewall, etc. [ISM112.TXT]

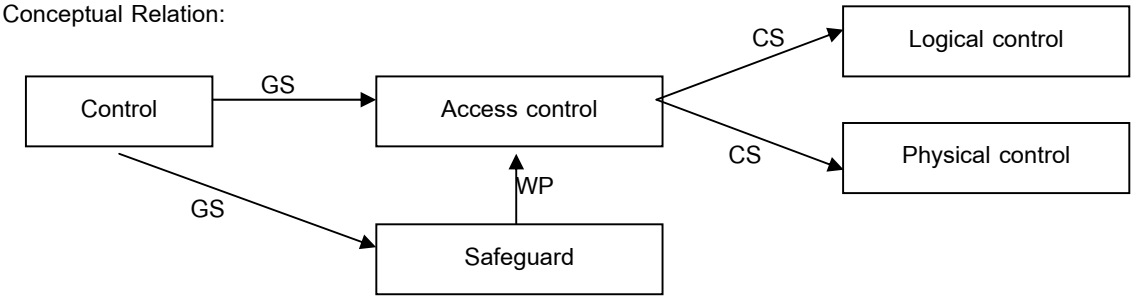
CN032	**Concept:** Physical control
Eng: Physical control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมทางกายภาพ [ราชบัณฑิตยสถาน]	
Feature: มาตรการควบคุมทางวัตถุนั้นใช้เฝ้าดูและควบคุมสถานที่การทำงานและห้องเครื่องคอมพิวเตอร์รวมไปถึงผู้ที่เข้าไปใช้งานสถานที่นั้น ๆ ด้วย ตัวอย่างมาตรการควบคุมทางวัตถุ เช่น ล็อกกุญแจ ระบบเตือนควัน และกล้องวงจรปิด การเลือกมาตรการควบคุมทางวัตถุนั้นขึ้นอยู่กับเนื้อหาในนโยบายรักษาความปลอดภัยที่องค์กรนั้น ๆ ใช้	
Conceptual Relation: ดูภาพใน CN030	
Extraction: 1. Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls. [ISM097.TXT] 2. Administrative controls consist of approved written policies, procedures, standards and guidelines. Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. [ISM097.TXT] 3. These actions can include implementing new organizational policies and procedures as well as technical or physical controls. [ISM005.TXT]	

CN033	**Concept:** Access control
Eng: Access control	**Grammatical Category:** Noun

Thai: การควบคุมการเข้าถึงข้อมูล [วิทย์ เที่ยงบูรณธรรม]

Feature: การควบคุมการเข้าถึงข้อมูลนั้นจะใช้ตรวจสอบว่าใครสามารถและไม่สามารถเข้ามาในระบบได้บ้าง โดยการติดตั้งมาตรการควบคุมทางตรรกและทางกายภาพหรือมีการนำเทคโนโลยีต่าง ๆ มาใช้ในการควบคุม การเลือกวิธีการควบคุมการเข้าถึงข้อมูลนั้นขึ้นอยู่กับระดับความสำคัญของข้อมูลนั้น ๆ กล่าวคือ ถ้าข้อมูลนั้นมีความสำคัญมาก ระบบควบคุมการเข้าถึงข้อมูลที่เลือกมาก็ต้องมีความเข้มแข็งพอเพื่อที่จะปกป้องข้อมูลนั้นได้มากตามกัน

Conceptual Relation:



CS แทน Condition – Selection

GS แทน Generic – Specific

WP แทน Whole – Part

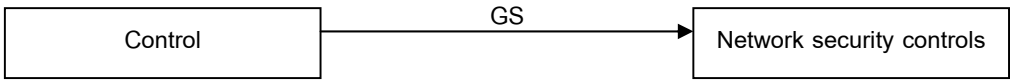
Extraction:

1. Access control -- Only authorized authenticated users and remote applications may have access. [ISM005.TXT]
2. Access Control is the process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use. [ISM117.TXT]
3. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. [ISM097.TXT]
4. Safeguards- (also called security controls). The protective measure and controls that are prescribed to meet the security requirements specified for systems. Safeguards may include, but are not limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints, ;personnel security; and physical structures, areas, and devices. [ISM117.TXT]

CN034	**Concept:** Network security control
Eng: Network security control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมความปลอดภัยของระบบเครือข่าย [วิทย์ เที่ยงบูรณธรรม]	

Feature: มาตรการควบคุมความปลอดภัยของระบบเครือข่ายนั้นมุ่งเน้นไปที่การรักษาความปลอดภัยของระบบเครือข่ายอันเกิดมาจากการมุ่งร้ายที่เจาะเข้ามาในระบบเพื่อป้องกันไม่ให้องค์กรเปิดเผยข้อมูลที่มีค่าต่อสารธารณะโดยไม่จำเป็น มาตรการควบคุมความปลอดภัยนั้นเป็นได้ทั้งกระบวนการการจัดการระบบและเทคโนโลยีที่นำมาช่วยรักษาความปลอดภัย นอกจากนั้น มาตรการนชนิดนี้ยังนำไปวิเคราะห์เพื่อที่ผู้ดูแลระบบจะได้เข้าใจการเชื่อมต่อของระบบเครือข่ายและหนทางที่จะติดต่อเข้ามา ตัวอย่างของมาตรการควบคุมความปลอดภัยของระบบเครือข่ายที่สำคัญตัวอย่างหนึ่ง คือ ระบบไฟร์วอลล์

Conceptual Relation:

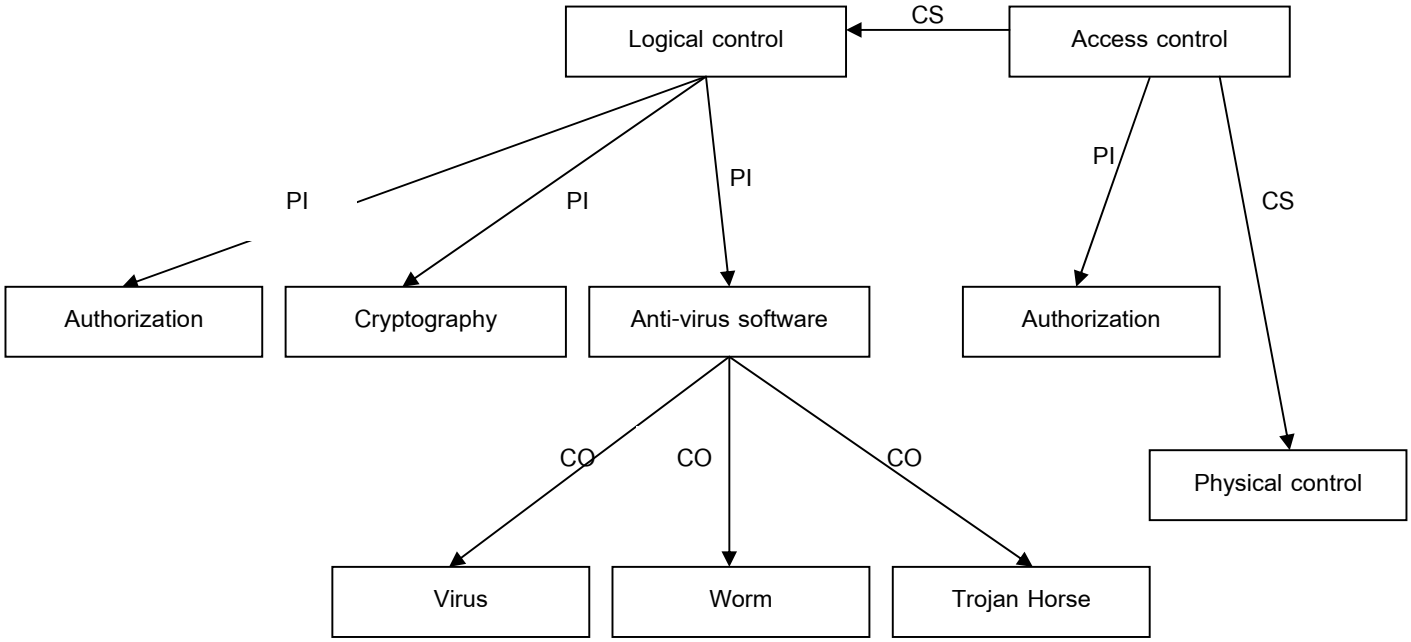


GS แทน Generic – Specific

Extraction:

1. Properly implemented network security controls, both management processes and technology, are needed to thwart intentional attacks, to minimize unintentional mistakes from trusted insiders and to prevent exposure of your valuable information assets unnecessarily. [ISM120.TXT]
2. Network security controls are continuously and automatically analyzed to understand network connectivity and access paths. [ISM121.TXT]
3. Because they are an extremely important network security control, we study firewalls in an entire section later in this chapter. [ISM119.TXT]
4. Network security controls - Network security controls are one of the main parts of information systems security and control that most business houses have preferred using. This ensures that no outsiders get access to the network that is used by the company for internal purposes. Thus any infiltration into the operating network of these companies may prove to be very harmful in the future. [ISM140.TXT]

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
ประเภทของมาตรการควบคุมแบบตรรก



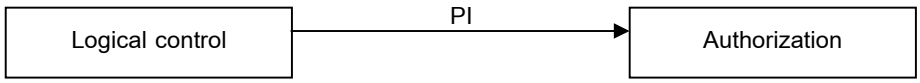
CS **แทน** Condition – Selection

GS **แทน** Generic – Specific

CO **แทน** Counter-Object

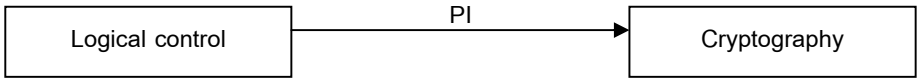
PI **แทน** Process - Instrument

PM **แทน** Process – Method

CN035	**Concept:** Authorization
Eng: Authorization	**Grammatical Category:** Noun
Thai: การอนุญาต [ราชบัญฑิตยสถาน]	
Feature: การได้รับสิทธ์อนุญาตนั้นเป็นกลไกอย่างหนึ่งที่กันให้บุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าใช้งานในระบบได้ โดยผู้ใช้งานในระบบนั้นจะได้รับสิทธิ์อนุญาตที่ต่างกันขึ้นอยู่กับหน้าที่งานของตนและจะได้รับเท่าที่จำเป็นเท่านั้นเพื่อเป็นการทำให้มั่นใจว่า ข้อมูลแต่ละชิ้น คนที่นำไปใช้คือคนที่ต้องใช้จริง ๆ นอกจากนั้น สิทธิ์อนุญาตยังนำไปใช้กำหนดสิทธิ์ของผู้ใช้งานว่าสามารถกระทำการใดได้บ้าง กล่าวคือ สามารถประมวลผล เรียกดู สร้าง ลบ หรือแก้ไขข้อมูลได้หรือไม่	
Conceptual Relation:  **PI แทน** Process - Instrument	
Extraction: 1. Authorization is controls that ensure only approved business users have access to the application system. [ISM118.TXT] 2. After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization. [ISM097.TXT] 3. Authorization: Access will be granted on a “need to know” or “Minimum Necessary” basis and must be authorized by the immediate information owner or user management with the assistance of the Information Security Officer. [ISM036.TXT]	

CN036	**Concept:** Cryptography
Eng: Cryptography	**Grammatical Category:** Noun
Thai: วิทยาการรหัสลับ [วิทย์ เที่ยงบูรณธรรม]	
Feature: วิทยาการรหัสลับเป็นการเข้ารหัสข้อมูลเพื่อที่จะให้ข้อมูลนั้นอ่านไม่ออกและจะถอดรหัสกลับเพื่ออ่านข้อมูลยาก วิทยาการรหัสลับนี้ใช้เพื่อป้องกันการเปิดเผยข้อมูลในระหว่างการส่งหรือในขณะที่ข้อมูลนั้นเก็บไว้ที่ใดที่หนึ่ง การป้องกันนี้จะทำให้ข้อมูลนั้นยังคงไว้ซึ่งความลับ บูรณภาพ การคงอยู่ และการปฏิเสธไม่ได้ซึ่งเป็นคุณสมบัติของความปลอดภัยของข้อมูล	

Conceptual Relation:



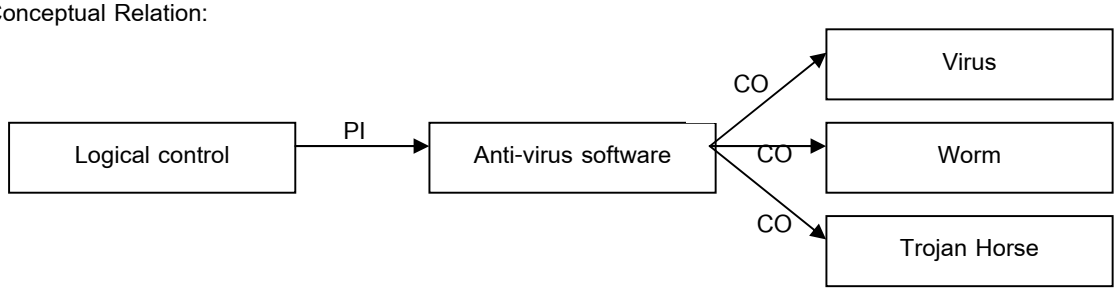
PI แทน Process - Instrument

Extraction:

1. Cryptography is the study and practice of scrambling information in a manner that makes it difficult to unscramble, and makes scrambled information intelligible. [ISM024.TXT]
2. Cryptography is used in information security to protect information from unauthorized or accidental discloser while the information is in transit (either electronically or physically) and while information is in storage. [ISM097.TXT]
3. Controls, such as cryptography, over information transmitted and stored to ensure confidentiality, authenticity, integrity, and non-repudiation. [ISM091.TXT]

CN037	**Concept:** Anti-virus software
Eng: Anti-virus software	**Grammatical Category:** Noun
Thai: โปรแกรมป้องกันไวรัสในคอมพิวเตอร์ [จิรายุส ภาสวัต]	
Feature: ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ คือ โปรแกรมคอมพิวเตอร์ที่ได้รับการออกแบบมาเพื่อกำจัดไวรัส ดักจับไวรัส เพื่อไม่ให้ออกมาทำลายคอมพิวเตอร์รวมไปถึงการกู้ข้อมูลที่ถูกทำลายไปแล้วโดยไวรัสตัวนั้นด้วยโดยในปัจจุบันองค์กรหลาย ๆ องค์กรต้องมีมาตรการนำซอฟต์แวร์ต่อต้านไวรัสมาลงเพื่อป้องกันโปรแกรมมุ่งร้ายต่าง ๆ เช่น ไวรัส ม้าโทรจัน หนอนคอมพิวเตอร์ และระเบิดตรรกะ	

Conceptual Relation:



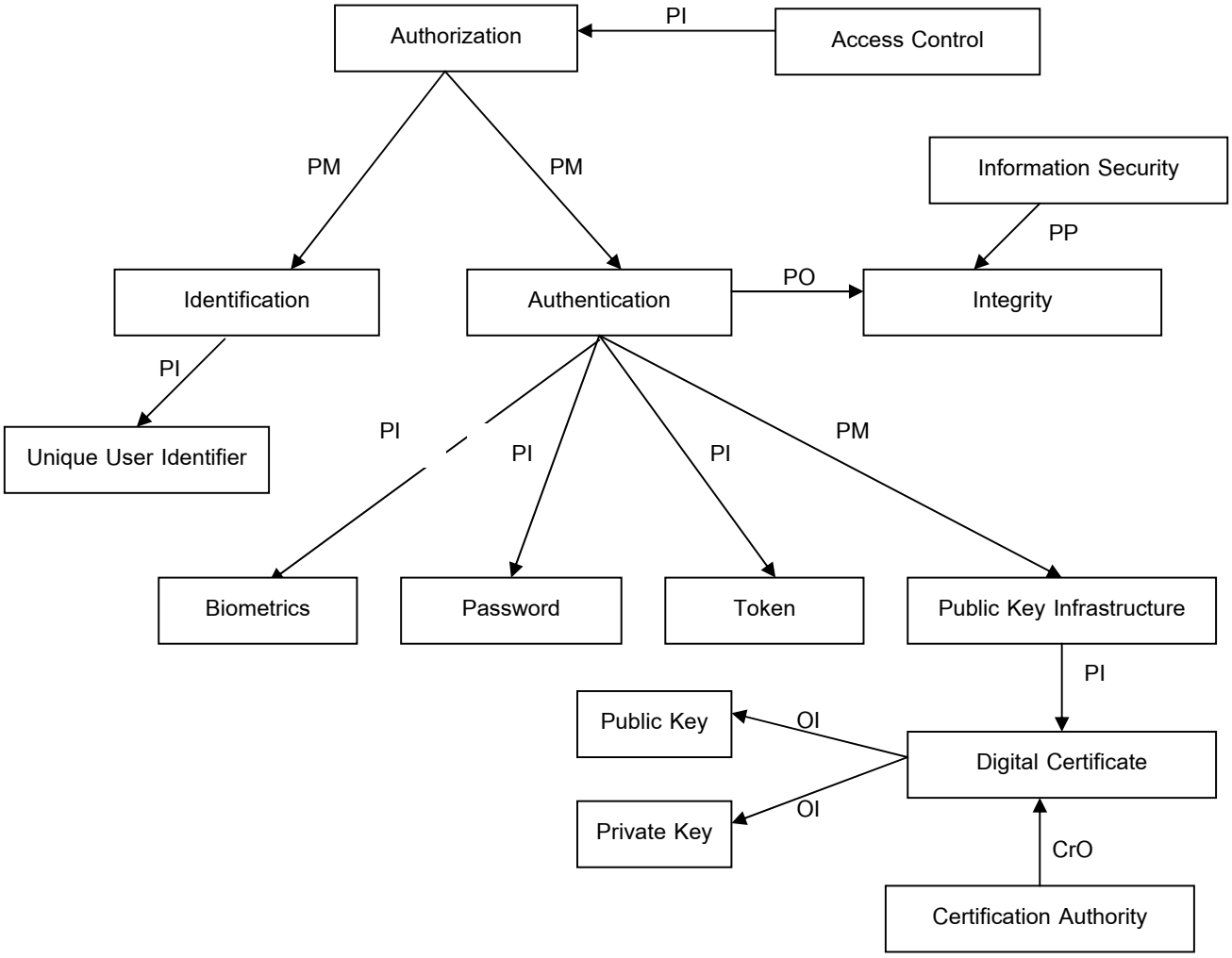
CO แทน Counter-Object

PI แทน Process - Instrument

Extraction:

1. Anti-virus software is software tools for detecting, blocking and/or removing viruses from files, emails or network communications. [ISM024.TXT]
2. Anti-virus Software is software that is designed to stop viruses, eliminate viruses, and/or recover data affected by viruses. [ISM112.TXT]
3. Anti-virus software is designed to detect malicious software such as viruses, Trojan horses, worms, bacteria, logic bombs. [ISM039.TXT]

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
การอนุญาตให้เข้าใช้งานในระบบ



OI **แทน** Object – Identification

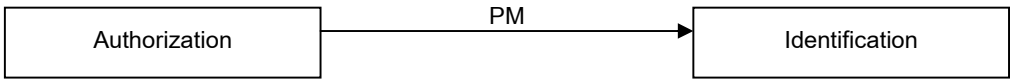
CrO **แทน** Creator – Object

PM **แทน** Process – Method

PI **แทน** Process – Instrument

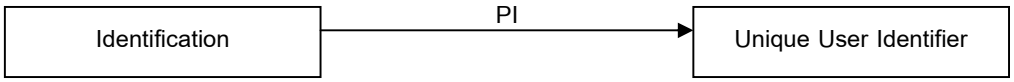
PO **แทน** Process – Outcome

PP **แทน** Process - Principle

CN038	**Concept:** Identification
Eng: Identification	**Grammatical Category:** Noun
Thai: การระบุผู้ใช้งาน [ผู้เชี่ยวชาญ]	
Feature: การระบุผู้ใช้งานเป็นการอ้างว่า คน ๆ นั้นที่จะเข้าใช้งานในระบบคือใคร แต่อย่างไรก็ดี การอ้างนั้นอาจจะไม่เป็นจริงก็ได้ กล่าวคือ ชื่อที่บุคคลนั้นกล่าวอ้างอาจจะไม่ใช่คน ๆ นั้นอย่างแท้จริง ดังนั้น จึงต้องมีการพิสูจน์ตัวตนที่แท้จริง (Authentication) เสียก่อนเพื่อเป็นการตรวจสอบว่า บุคคลนั้นเป็นคนตามที่กล่าวอ้างหรือไม่ ตัวอย่างการพิสูจน์ตัวตน เช่น รหัสผ่าน (Password) และโทเก็น (Token)	
Conceptual Relation:  **PM แทน Process – Method**	
Extraction: 1. Identification and authentication controls to establish accountability and to prevent unauthorized persons from gaining access to the systems through, for example, passwords or smart tokens. [ISM91.TXT] 2. Identification is an assertion of who someone is or what something is. If a person makes the statement *"Hello, my name is John Doe."* they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. [ISM097.TXT]	

CN039	**Concept:** Unique User Identifier
Eng: Unique User Identifier	**Grammatical Category:** Noun
Thai: ชื่อระบุผู้ใช้งาน [ผู้เชี่ยวชาญ]	
Feature: ชื่อระบุผู้ใช้งานนั้นจะเป็นชื่อที่ให้ไว้กับผู้ใช้งานในระบบเพื่อไว้คอยตรวจสอบการใช้งานและเป็นตัวที่ใช้ระบุชื่อและตัวตนของผู้เข้าใช้งานในระบบด้วยโดยชื่อระบุผู้ใช้งานนี้จะมีความแตกต่างกันในแต่ละบุคคล กล่าวคือ ผู้ใช้งานแต่ละคนในระบบนั้นจะได้รับชื่อระบุผู้ใช้งานที่แตกต่างกันทุกคน	

Conceptual Relation:



PI **แทน** Process – Instrument

Extraction:

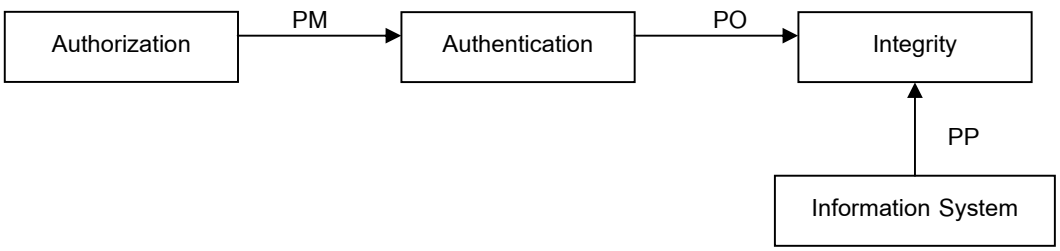
1. Unique User Identifier – A unique set of characters assigned to an individual for the purpose of identifying and tracking user identity. [ISM117.TXT]
2. A unique user identifier allows an entity to track specific user activity when that user is logged into an information system. [ISM122.TXT]

CN040	**Concept:** Authentication
Eng: Authentication	**Grammatical Category:** Noun

Thai: การพิสูจน์ตัวตนที่แท้จริง [ราชบัณฑิตยสถาน]

Feature: การพิสูจน์ตัวตนที่แท้จริง คือ วิธีการที่ใช้พิสูจน์ว่าคนที่เข้าระบบมาโดยใช้ชื่อระบุนั้น ๆ เป็นคน ๆ นั้นจริง ๆ โดยวิธีการนี้จะนำมาใช้เพื่อปกป้องการหลอกลวงในการเข้าระบบและหลอกว่าเป็นบุคคลนั้น ๆ วิธีการพิสูจน์ตัวตนที่แท้จริงนี้ใช้ในการรักษาไว้ซึ่งบูรณภาพ (Integrity) ของระบบสารสนเทศขององค์กร โดยทั่วไปแล้ว การพิสูจน์ตัวตนที่แท้จริงนั้นตรวจสอบได้ 3 อย่างหลัก ๆ คือ ตรวจสอบจากสิ่งที่ผู้ใช้งานมี เช่น โทเค็น (Token) ตรวจสอบจากสิ่งที่ผู้ใช้งานรู้ เช่น รหัสผ่าน (Password) และตรวจสอบจากสิ่งที่ผู้ใช้งานเป็น เช่น ชีวมาตร (Biometrics)

Conceptual Relation:



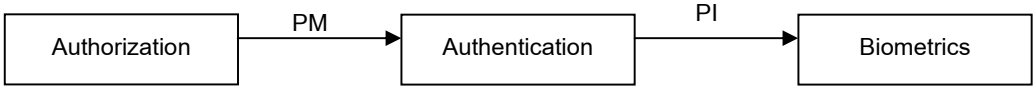
PP **แทน** Process - Principle

PM **แทน** Process – Method

PO **แทน** Process – Outcome

Extraction:

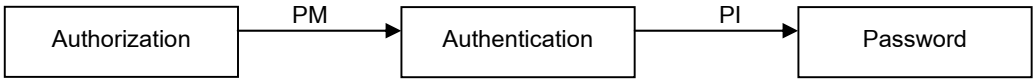
1. Authentication is the process of accepting a user's claimed identity (their username) and verifying they are actually that user. [SIM024.TXT]
2. Authentication – The corroboration that a person is the one claimed. Authentication is the act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It also can refer to the verification of the correctness of a piece of data. [ISM117.TXT]
3. Proper encryption ensures confidentiality, but what about integrity? Authentication is the appropriately crucial manner of addressing this. [ISM012.TXT]
4. Authentication is the process of validating a user, ensuring that you are who you say you are. Solutions range from traditional username/password regimens to the use of complex devices such as tokens and biometric scanners. A system can authenticate you by examining three things: what you know, what you have, and what you are. Not all solutions use all three, though. Tokens (what you have) must be paired with passwords (what you know) or biometric technology (what you are) to produce a stronger solution. This helps prevent the use of stolen tokens. [ISM051.TXT]
5. Passwords, tokens, public key infrastructure and biometrics are all examples of authentication technologies that can help verify identity and control access to resources. [ISM050.TXT]

CN041	**Concept:** Biometrics
Eng: Biometrics, Biometry	**Grammatical Category:** Noun
Thai: ชีวมาตร [ราชบัณฑิตยสถาน]	
Feature: ชีวมาตร คือ วิธีการพิสูจน์ตัวตนที่แท้จริงวิธีหนึ่ง โดยชีวมาตร คือ การพิสูจน์ตัวตนจากสิ่งที่ผู้ใช้งานคนนั้นเป็นซึ่งไม่สามารถขโมยไปได้และให้ผลการพิสูจน์แม่นยำมากที่สุดได้ถึง 99% ตัวอย่างของการตรวจสอบชีวมาตร คือ การตรวจสอบลายนิ้วมือ การตรวจสอบเสียง การสแกนรูม่านตา การตรวจสอบลายนิ้วมือ และการตรวจสอบลายมือเขียนหนังสือ คนแต่ละคนจะมีรายละเอียดเหล่านี้ที่แตกต่างกันไป ดังนั้น ข้อมูลจึงไม่สามารถซ้ำกันได้ จึงทำให้ชีวมาตรเป็นวิธีการพิสูจน์ตัวตนที่มีประสิทธิภาพมากกว่ารหัสผ่านหรือบัตรผ่านเข้าออก และถือเป็นนิมิตรหมายใหม่ของการพิสูจน์ตัวตน	
Conceptual Relation:  **PM แทน** Process – Method	

PI **แทน** Process – Instrument
Extraction: 1. Biometrics is the next generation of authentication methods. Although it's still in its early implementation period due to the associated costs, and sometimes the number of false results, biometrics will change the way we authenticate ourselves, hopefully with 99% accuracy. Simply, biometrics cannot be stolen, cannot be forgotten, neither can they be given to another person. Biometrics systems may include fingerprint systems, voice recognition systems, Eye/Retina scanner systems, hand geometry systems and handwriting systems. [ISM050.TXT] 2. Biometric information is difficult to duplicate and when used in conjunction other access methods such as passwords and badges creates a very good defense against unauthorized access to organizational resources. [ISM099.TXT] 3. Authentication is the process of validating a user, ensuring that you are who you say you are. Solutions range from traditional username/password regimens to the use of complex devices such as tokens and biometric scanners. A system can authenticate you by examining three things: what you know, what you have, and what you are. Not all solutions use all three, though. Tokens (what you have) must be paired with passwords (what you know) or biometric technology (what you are) to produce a stronger solution. This helps prevent the use of stolen tokens. [ISM051.TXT] 4. Passwords, tokens, public key infrastructure and biometrics are all examples of authentication technologies that can help verify identity and control access to resources. [ISM050.TXT]

CN042	**Concept:** Password
Eng: Password	**Grammatical Category:** Noun
Thai: รหัสผ่าน [ราชบัณฑิตยสถาน]	
Feature: รหัสผ่าน คือ วิธีการพิสูจน์ตัวตนที่แท้จริงวิธีหนึ่ง โดยรหัสผ่าน คือ การพิสูจน์ตัวตนจากสิ่งที่ผู้ใช้งานคนนั้นรู้ รหัสผ่าน คือ ชุดอักษรผสมที่ผู้ใช้งานต้องเก็บไว้เป็นความลับส่วนตัว เมื่อจะเข้าใช้ระบบ ผู้ใช้งานต้องใส่ชุดอักษรเหล่านี้เพื่อสามารถเข้าไปในระบบได้ การที่รหัสผ่านจะสร้างความปลอดภัยให้กับระบบมากน้อยเพียงใดนั้นขึ้นอยู่กับความยาวของชุดอักษรนั้น ตามหลักแล้ว รหัสผ่านที่ดีควรจะมีจำนวนอักษรในชุดอักษรนั้นอย่างน้อย 8 ตัวอักษรขึ้นไปและมีส่วนผสมของทั้งตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และตัวอักษรพิเศษด้วย ถ้ารหัสผ่านสั้น จะทำให้ผู้บุกรุกสามารถเดาได้ง่ายขึ้น ส่งผลต่อความปลอดภัยของระบบ	

Conceptual Relation:



PM **แทน** Process – Method

PI **แทน** Process – Instrument

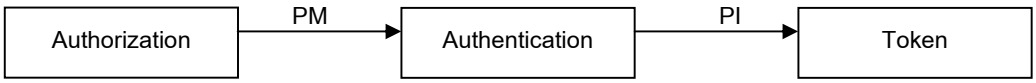
Extraction:

1. Password - A secret string which is known only to the user and the system which the user can enter. It is used for identification and authentication purposes. The strength of a password (and thus the level of security it provides) is directly related to its length and how easy it would be for an attacker to guess it. [ISM024.TXT]
2. Password - A private and unique series of numbers or letters which enable a user to gain access to a system or service. [ISM112.TXT]
3. Choosing secure passwords consists of knowing what their insecurities are, how passwords are cracked and what's behind the "at least 8 characters long, consisting of lower and capital letters, special characters and a number" requirement. Basically, the shorter the password, the more opportunities for observing, guessing and cracking it. A password cracker would try to guess all the possible combinations of letters, numbers and characters until he/she finds the right one. [ISM050.TXT]
4. Authentication is the process of validating a user, ensuring that you are who you say you are. Solutions range from traditional username/password regimens to the use of complex devices such as tokens and biometric scanners. A system can authenticate you by examining three things: what you know, what you have, and what you are. Not all solutions use all three, though. Tokens (what you have) must be paired with passwords (what you know) or biometric technology (what you are) to produce a stronger solution. This helps prevent the use of stolen tokens. [ISM051.TXT]
5. Passwords, tokens, public key infrastructure and biometrics are all examples of authentication technologies that can help verify identity and control access to resources. [ISM050.TXT]

CN043	**Concept:** Token
Eng: Token	**Grammatical Category:** Noun
Thai: โทเก็น [ราชบัณฑิตยสถาน]	

Feature: โทเก็น คือ วิธีการพิสูจน์ตัวตนที่แท้จริงวิธีหนึ่งโดยโทเก็น คือ การพิสูจน์ตัวตนจากสิ่งที่ผู้ใช้งานคนนั้นมีหรือครอบครองไว้ โทเก็น คือ เครื่องมือพกพาที่ใช้เทคนิคการโต้ตอบหรือเทคนิคอื่น ๆ มาใช้เพื่อพิสูจน์ตัวตนของผู้ใช้งานนี้ ตัวอย่างของโทเก็น คือ เครื่องมืออิเลคทรอนิกที่สามารถเสียบไปที่ประตูหรือระบบคอมพิวเตอร์ได้เพื่อตรวจสอบข้อมูลของผู้เข้าใช้งาน

Conceptual Relation:



PM แทน Process – Method

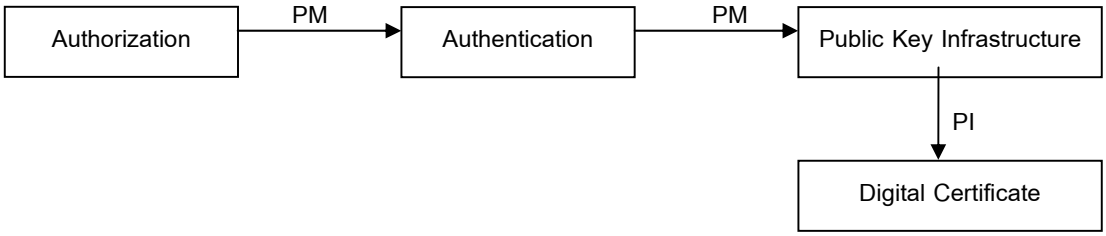
PI แทน Process – Instrument

Extraction:

1. Authentication Token - A portable device operates by using challenge/response, time sequence, or other techniques in order to authenticate a user. [ISM112.TXT]
2. Token - A physical item that is used to provide identity. Typically, an electronic device that can be inserted in a door or a computer system to gain access. [ISM117.TXT]
3. Authentication is the process of validating a user, ensuring that you are who you say you are. Solutions range from traditional username/password regimens to the use of complex devices such as tokens and biometric scanners. A system can authenticate you by examining three things: what you know, what you have, and what you are. Not all solutions use all three, though. Tokens (what you have) must be paired with passwords (what you know) or biometric technology (what you are) to produce a stronger solution. This helps prevent the use of stolen tokens. [ISM051.TXT]
4. Passwords, tokens, public key infrastructure and biometrics are all examples of authentication technologies that can help verify identity and control access to resources. [ISM050.TXT]

CN044	**Concept:** Public Key Infrastructure
Eng: Public Key Infrastructure, PKI	**Grammatical Category:** Noun
Thai: โครงสร้างพื้นฐานกุญแจสาธารณะ [ผู้เชี่ยวชาญ]	
Feature: โครงสร้างพื้นฐานกุญแจสาธารณะ คือ วิธีการพิสูจน์ตัวตนที่แท้จริงวิธีหนึ่งโดยโครงสร้างพื้นฐานกุญแจสาธารณะนี้จะเอื้อให้ผู้ใช้งานและเซิร์ฟเวอร์สื่อสารระหว่างกัน เซ็นชื่อและยืนยันระหว่างกันว่า เป็นบุคคลหรือเครื่องที่ว่าอย่างแท้จริง โดยจะต้องมีใบรับรองดิจิทัลซึ่งมีกุญแจสาธารณะและกุญแจส่วนตัวติดอยู่ด้วย โครงสร้างพื้นฐานกุญแจสาธารณะสามารถนำไปใช้ในการรักษาความปลอดภัยของข้อมูลในสมาร์ทการ์ดได้ด้วย	

Conceptual Relation:



PM **แทน** Process – Method

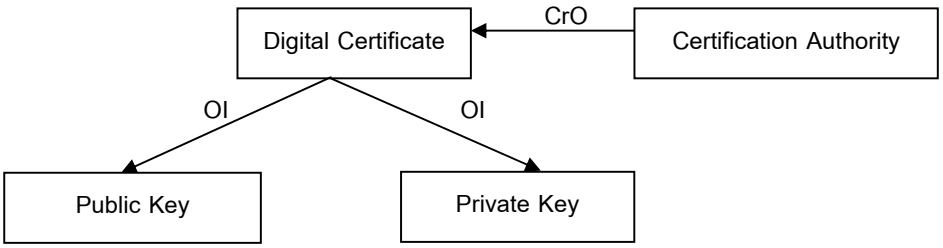
PI **แทน** Process – Instrument

Extraction:

1. Public Key Infrastructure(PKI) functions give entities, namely employees or servers the ability to communicate, authenticate, sign and verify identities by creating digital certificates, each of which containing private and public keys. [ISM050.TXT]
2. The Public Key Infrastructure is a framework for using digital certificates and their associated keys to verify the identity of users and computers to other users, computers and applications. [ISM085.TXT]
3. A smart card is a credit card sized plastic card with an embedded chip that can hold a digital certificate so user authentication is accomplished through a public key infrastructure. [ISM051.TXT]
4. Passwords, tokens, public key infrastructure and biometrics are all examples of authentication technologies that can help verify identity and control access to resources. [ISM050.TXT]

CN045	**Concept:** Digital Certificate
Eng: Digital Certificate	**Grammatical Category:** Noun
Thai: ใบรับรองดิจิทัล [ราชบัณฑิตยสถาน]	
Feature: ใบรับรองดิจิทัล คือ ใบรับรองที่ออกให้กับผู้ใช้งานคนนั้นเพื่อรับประกันว่า ผู้ใช้งานคนนั้น คือ คน ๆ นั้นจริง ๆ โดยในใบรับรองดิจิทัลประกอบไปด้วยข้อมูลของผู้ใช้งาน กุญแจสาธารณะที่เป็นของผู้ใช้งานคนนั้น วันหมดอายุ และลายมือชื่อดิจิทัลของผู้ประกอบการรับรองซึ่งเป็นผู้ที่ออกใบรับรองนั้น ใบรับรองดิจิทัลยังเป็นส่วนหนึ่งของโครงสร้างพื้นฐานกุญแจสาธารณะซึ่งถือเป็นวิธีการหนึ่งที่ใช้ในการพิสูจน์ตัวตนที่แท้จริงอีกด้วย	

Conceptual Relation:



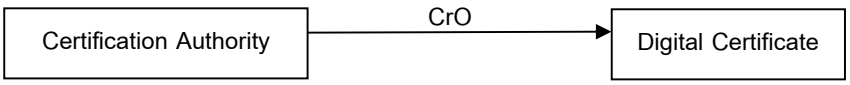
OI แทน Object – Identification

CrO แทน Creator – Object

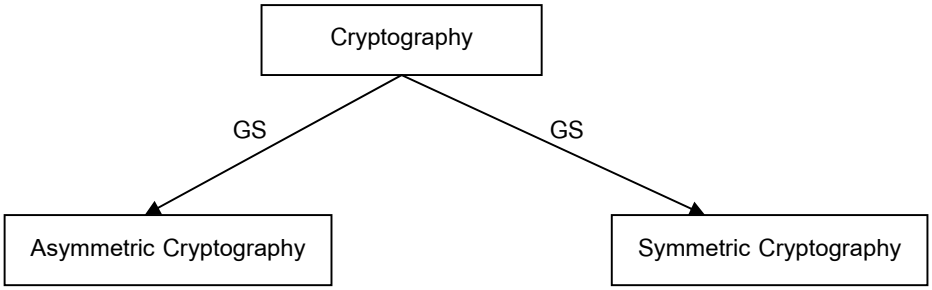
Extraction:

1. It [Digital Security] insures by means of verification and validation that the user is whom he/she claims to be. This is done by combine the users credential to the digital certificate and in turn this method uses one point of authentication. [ISM018.TXT]
2. Digital certificates also provide a means for users to exchange encrypted information using a combination of a private key (owned by the sender) and public key (freely shared with recipients) to encrypt and decrypt message text. [ISM050.TXT]
3. Digital certificates contain information about the holder, the holder's public key, an expiration date, and the digital signature of the issuer (the certification authority). [ISM085.TXT]
4. Public Key Infrastructure(PKI) functions give entities, namely employees or servers the ability to communicate, authenticate, sign and verify identities by creating digital certificates, each of which containing private and public keys. [ISM050.TXT]

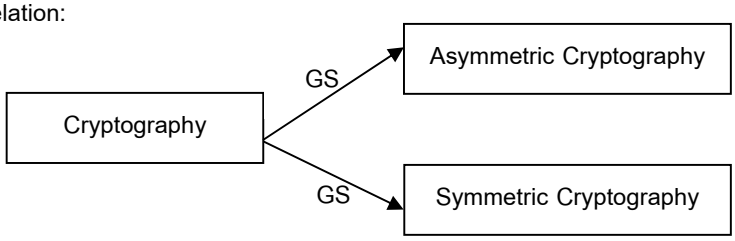
CN046	**Concept:** Certification Authority
Eng: Certification Authority, Certificate Authority, CA	**Grammatical Category:** Noun
Thai: ผู้ประกอบการรับรอง [ราชบัณฑิตยสถาน]	
Feature: ผู้ประกอบการรับรองนั้นมีหน้าที่ออกใบรับรองดิจิทัล (Digital Certificate) และเซ็นรับรองว่า ผู้ที่ถือใบรับรองนั้นเป็นคน ๆ นั้นจริง ๆ โดยใช้กุญแจส่วนตัวของตนในการเซ็นรับรอง ผู้ประกอบการรับรองจะเป็นบุคคลอีกกลุ่มหนึ่งที่ไม่เกี่ยวข้องกับผู้ใช้งานที่ได้ใบรับรองดิจิทัลและเสมือนเป็นบุคคลอ้างอิงที่รองรับว่า ผู้ใช้งานคือ บุคคลคนนั้นจริง ๆ ผู้ประกอบการรับรองและใบรับรองดิจิทัลนี้ ถือเป็นส่วนหนึ่งในโครงสร้างพื้นฐานกุญแจสาธารณะซึ่งเป็นวิธีการหนึ่งที่ใช้ใน	

การพิสูจน์ตัวตนที่แท้จริงอีกด้วย
Conceptual Relation:    **CrO แทน Creator – Object**
Extraction: 1. Either way, the PKI consists of the following components: At least one certification authority (CA) to issue certificates. Policies that govern the operation of the PKI. The digital certificates themselves. Applications that are written to use the PKI. [ISM085.TXT] 2. Digital certificates contain information about the holder, the holder's public key, an expiration date, and the digital signature of the issuer (the certification authority). [ISM085.TXT] 3. A certificate is issued and digitally signed by a trusted third party or Certification Authority. [ISM112.TXT] 4. Digital certificates often are issued by an independent certificate authority that then acts as a third-party reference regarding the owner's identity. [ISM050.TXT]

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
วิทยาการรหัสลับ

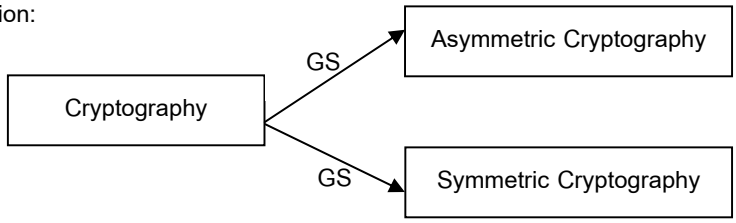


GS **แทน** Generic – Specific

CN047	**Concept:** Asymmetric Cryptography
Eng: Asymmetric Cryptography, Public-Key Cryptography	**Grammatical Category:** Noun
Thai: การเข้ารหัสแบบอสมมาตร [ราชบัณฑิตยสถาน]	
Feature: การเข้ารหัสแบบอสมมาตรนั้นเป็นวิธีการเข้ารหัสรูปแบบหนึ่งซึ่งใช้กุญแจสองชนิด คือ กุญแจสาธารณะและกุญแจส่วนตัวโดยจะใช้กุญแจสาธารณะในการเข้ารหัสและกุญแจส่วนตัวในการถอดรหัส	
Conceptual Relation:  **GS แทน Generic – Specific**	
Extraction: 1. Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys—a public key and a private key. [ISM131.TXT] 2. Public Key Cryptography - A technique that uses a pair of keys for encryption and decryption. [ISM112.TXT] 3. Public key cryptography can solve both of these problems. It can be used to digitally sign your messages so recipients can be confident that they're really from you (or so you can be confident of the identity of those from whom you receive mail). It can also be used to encrypt the message data itself, to protect it from prying eyes. [ISM041.TXT]	

CN048	**Concept:** Symmetric Cryptography
Eng: Symmetric Cryptography, Secret-Key Cryptography	**Grammatical Category:** Noun
Thai: การเข้ารหัสแบบสมมาตร [ราชบัณฑิตยสถาน]	
Feature: การเข้ารหัสแบบสมมาตรนั้นเป็นวิธีการเข้ารหัสรูปแบบหนึ่งซึ่งใช้กุญแจเพียงชนิดเดียว คือ กุญแจส่วนตัวโดยจะในการเข้ารหัสข้อมูล โดยทั่วไปแล้ว การเข้ารหัสแบบอสมมาตร (Asymmetric Cryptography) จะมีความปลอดภัยมากกว่าการเข้ารหัสแบบสมมาตร	

Conceptual Relation:

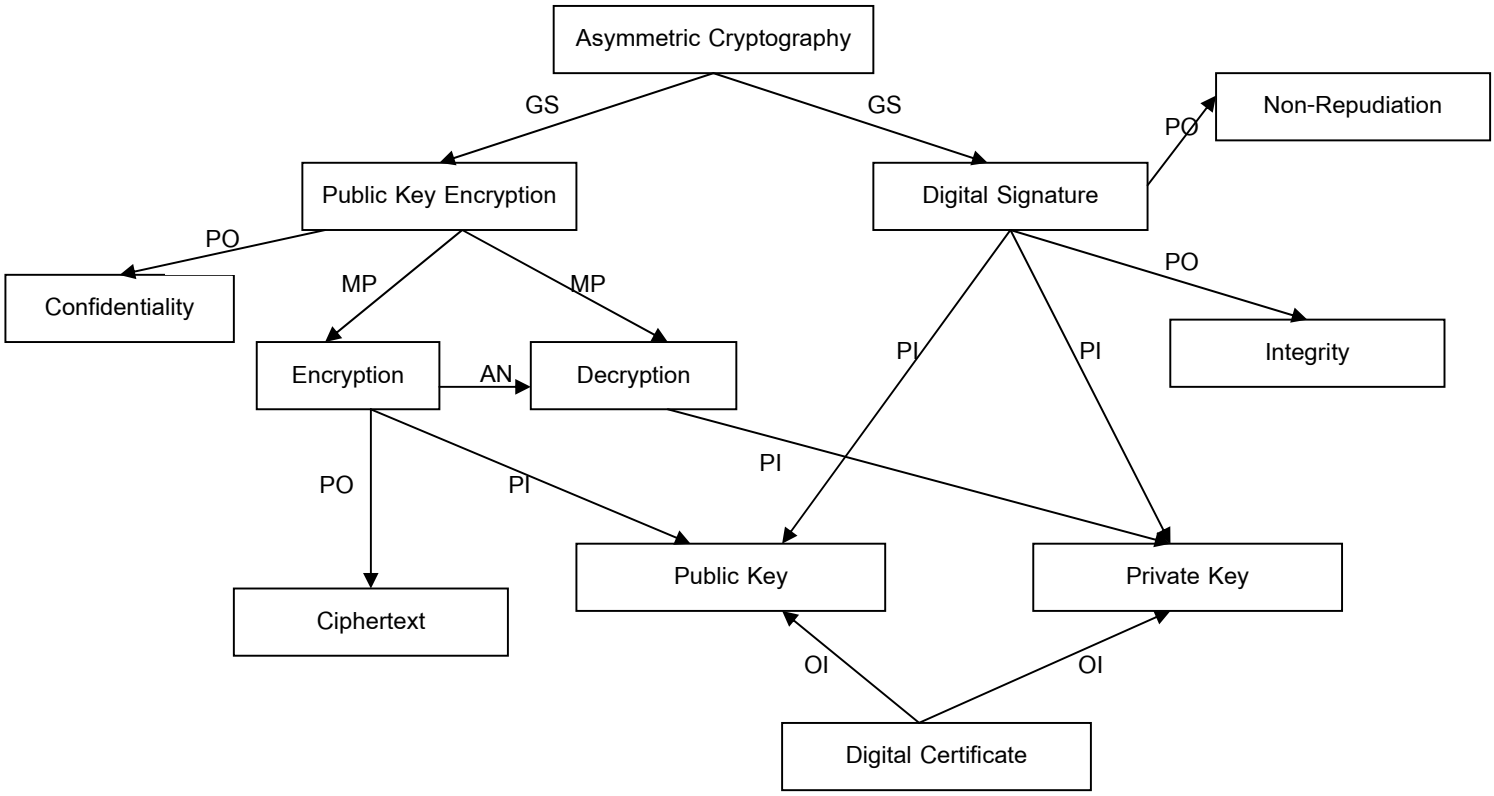


GS แทน Generic – Specific

Extraction:

1. Conversely, secret key cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption. [ISM131.TXT]
2. Symmetric cryptography uses a single private key to both encrypt and decrypt data. Any party that has the key can use it to encrypt and decrypt data. [ISM092.TXT]
3. Symmetric, or secret key, cryptography has been in use for thousands of years and includes any form where the same key is used both to encrypt and to decrypt the text involved. [ISM097.TXT]

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
การเข้ารหัสแบบอสมมาตร



GS **แทน** Generic – Specific

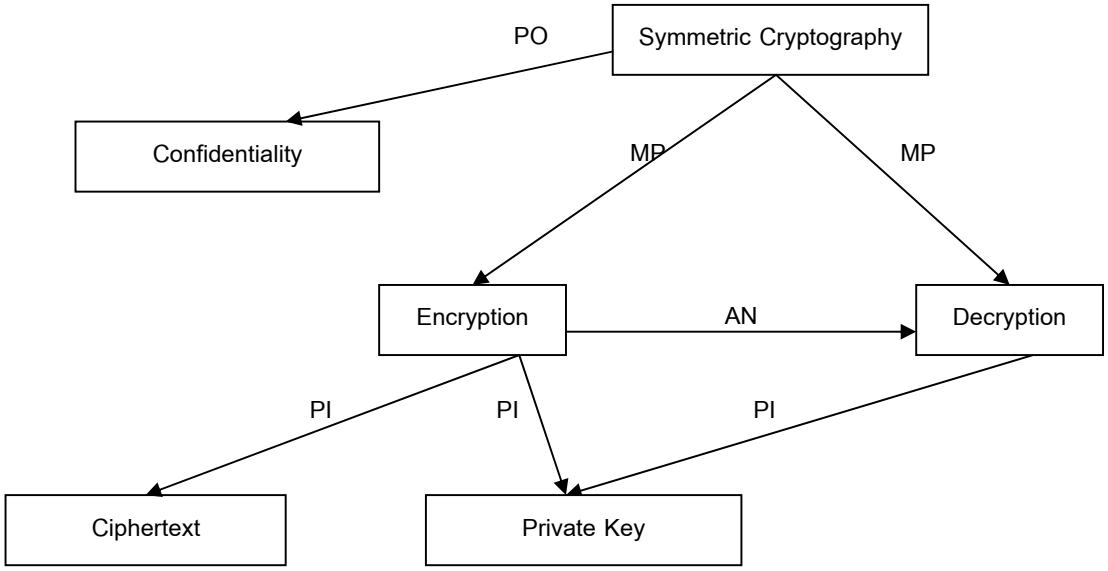
AN **แทน** Antonym

PI **แทน** Process – Instrument

MP **แทน** Method – Process

PO **แทน** Process – Outcome

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
การเข้ารหัสแบบสมมาตร



AN **แทน** Antonym

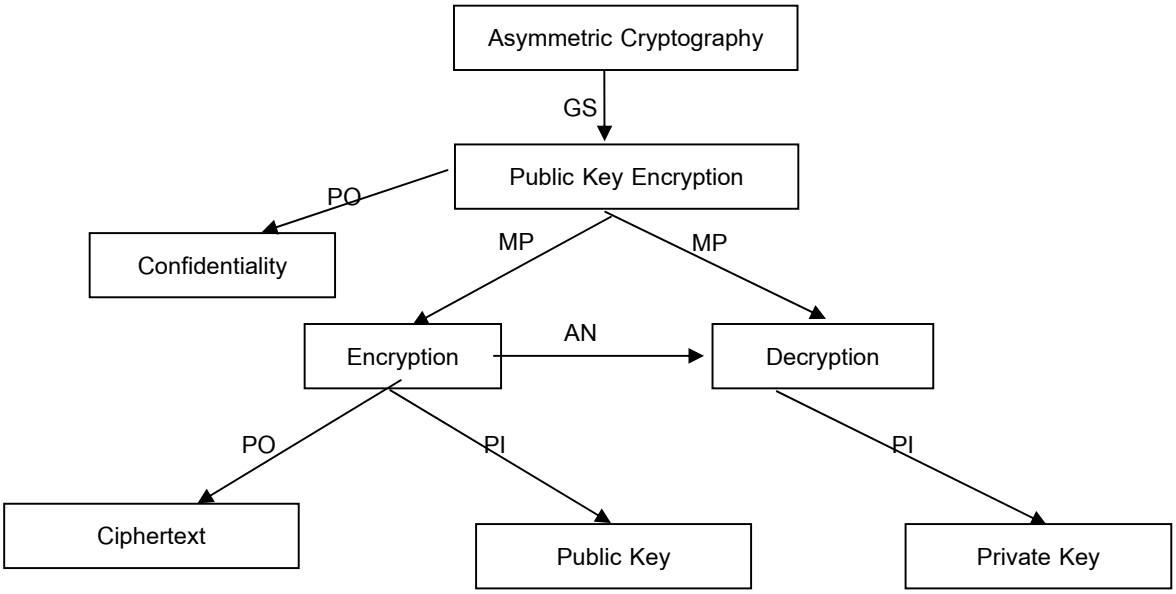
PI **แทน** Process – Instrument

PO **แทน** Process – Outcome

MP **แทน** Method – Process

CN049	**Concept:** Public-Key Encryption
Eng: Public-Key Encryption, Asymmetric Encryption	**Grammatical Category:** Noun
Thai: การเข้ารหัสกุญแจสาธารณะ [ราชบัณฑิตยสถาน]	
Feature: การเข้ารหัสกุญแจสาธารณะนั้น จะใช้กุญแจสาธารณะ (Public Key) ในการเข้ารหัสข้อมูลและกุญแจส่วนตัว (Private Key) ที่เป็นคู่กันนั้นในการถอดรหัสข้อมูล การเข้ารหัสข้อมูลด้วยวิธีนี้จะช่วยรักษาความลับของข้อมูล (Confidentiality)	

Conceptual Relation:



GS แทน Generic – Specific
AN แทน Antonym
PI แทน Process – Instrument
MP แทน Method – Process
PO แทน Process – Outcome

Extraction:

1. Public-Key Encryption, also known as Asymmetric Encryption, uses a public key to encrypt and a private key to decrypt. The encryption is done using an asymmetric algorithm. [ISM135.TXT]
2. Public key encryption — a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality. [ISM131.TXT]
3. Asymmetric Encryption - Two different keys are used with one for encryption and the other for decryption. [ISM112.TXT]

CN050	**Concept:** Encryption
Eng: Encryption	**Grammatical Category:** Noun
Thai: การเข้ารหัสลับ [ราชบัณฑิตยสถาน]	
Feature: การเข้ารหัสลับ คือ กระบวนการที่แปลงข้อความปกติไปเป็นข้อความที่เป็นรหัสลับเพื่อป้องกันไม่ให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตและเป็นการป้องกันข้อมูลในระหว่างส่งไปที่คอมพิวเตอร์เครื่องอื่น	
Conceptual Relation: ดูภาพใน CN049	
Extraction: 1. Encryption is any process that converts readable (plaintext) data into secret code (ciphertext) to prevent unauthorized disclosure of the information. [ISM099.TXT] 2. Encryption - A process to encode the contents of message so as to hide it from outsiders. [ISM112.TXT] 3. Encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts. [ISM119.TXT] 4. Decryption - The reverse process of encryption i.e. to turn scrambled data back into its original form. [ISM024.TXT]	

CN051	**Concept:** Ciphertext
Eng: Ciphertext	**Grammatical Category:** Noun
Thai: ข้อความเข้ารหัส [ผู้เชี่ยวชาญ]	
Feature: เมื่อข้อความธรรมดาได้รับการเข้ารหัสเป็นที่เรียบร้อยแล้วก็จะกลายเป็นข้อความเข้ารหัส ข้อความเข้ารหัสนี้เป็นข้อความที่ประกอบไปด้วยรหัสลับและไม่สามารถอ่านออกได้นอกจากจะได้รับการถอดรหัสออกเสียก่อน	
Conceptual Relation: ดูภาพใน CN049	
Extraction: 1. Encryption is any process that converts readable (plaintext) data into secret code (ciphertext) to prevent unauthorized disclosure of the information. [ISM099.TXT] 2. Ciphertext - A scrambled, unreadable contents of an encrypted, secretive message or data which is	

converted from plaintext using an encryption algorithm. [ISM112.TXT]

3. A cryptographic checksum (sometimes called a message digest) is a cryptographic function that produces a checksum. The cryptography prevents the attacker from changing the data block (the plaintext) and also changing the checksum value (the ciphertext) to match. [ISM119.TXT]

CN052	**Concept:** Decryption
Eng: Decryption	**Grammatical Category:** Noun
Thai: การถอดรหัสลับ [ราชบัณฑิตยสถาน]	
Feature: การถอดรหัสลับ คือ กระบวนการย้อนกลับของการเข้ารหัสลับ (Encryption) โดยการถอดรหัสลับนี้จะแปลงข้อความเข้ารหัส (Ciphertext) กลับไปเป็นข้อความที่อ่านออกได้อีกครั้งหนึ่งโดยผู้ที่ได้รับข้อความจะต้องมีกุญแจเพื่อถอดรหัสนี้ออกมา	
Conceptual Relation: **ดูภาพใน** CN049	
Extraction: 1. Decryption - The reverse process of encryption in which encoded messages or ciphertext is decoded from its protected, scrambled form into original plaintext so that they can be easily readable. [ISM112.TXT] 2. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. [ISM097.TXT] 3. The public key is used for encryption and the private key is used for decryption. [ISM092.TXT]	

CN053	**Concept:** Public Key
Eng: Public Key	**Grammatical Category:** Noun
Thai: กุญแจสาธารณะ [ราชบัณฑิตยสถาน]	
Feature: สำหรับการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptography) จะต้องใช้กุญแจสาธารณะในการเข้ารหัสข้อมูล เช่น ถ้าผู้ส่งต้องการเข้ารหัสข้อความในอีเมล์ของตน ผู้ส่งจะต้องเข้ารหัสโดยใช้กุญแจสาธารณะของตนและแจกจ่ายกุญแจนี้ให้กับผู้ที่จะเปิดอ่านข้อความในอีเมล์นั้น กุญแจคู่หนึ่งจะประกอบไปด้วยกุญแจสาธารณะที่สามารถแจกจ่ายให้ใครก็ได้	

และกุญแจส่วนตัว (Private Key) ที่เจ้าของนั้นจะต้องเก็บไว้เอง นอกจากนั้น กุญแจสาธารณะยังนำไปใช้เป็นข้อมูลหนึ่งใบรับรองดิจิทัล (Digital Certificate) โดยในใบนั้นจะมีข้อมูลของผู้ถือ กุญแจสาธารณะของผู้ถือ วันหมดอายุ และลายเซ็นของผู้ประกอบการรับรอง (Certificate Authority) นอกเหนือไปกว่านั้น กุญแจสาธารณะยังสามารถนำไปใช้ตรวจสอบลายมือชื่อดิจิทัล (Digital Signature) ว่าเป็นลายเซ็นของคน ๆ นั้นจริงหรือไม่ด้วย
Conceptual Relation: **ดูภาพใน** CN049
Extraction: 1. Encryption can be either: Symmetric (where the same key is used to encrypt and decrypt) Asymmetric (where two mathematically related keys are used, one (the public key) to encrypt, and the other (the private key) to decrypt). [ISM024.TXT] 2. The key pair consists of a public key that is distributed openly to others and a private key that is available only to the user. To encrypt the contents of your e-mail, you need to have the recipient's public key. [ISM041.TXT] 3. The public key is available to anyone wanting to exchange data with the entity and the private key is the only way for the entity to decrypt, or identify itself properly. [ISM050.TXT] 4. Digital certificates contain information about the holder, the holder's public key, an expiration date, and the digital signature of the issuer (the certification authority). [ISM085.TXT] 5. Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. [ISM131.TXT]

CN054	**Concept:** Private Key
Eng: Private Key	**Grammatical Category:** Noun
Thai: กุญแจส่วนตัว [ราชบัณฑิตยสถาน]	
Feature: สำหรับการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptography) จะต้องใช้กุญแจส่วนตัวในการถอดรหัสข้อมูล เช่น ถ้าผู้ส่งต้องการถอดรหัสข้อความในอีเมล์ของตน ผู้รับจะต้องนำกุญแจส่วนตัวของตนในการถอดรหัสข้อมูลนั้น กุญแจคู่หนึ่งจะประกอบไปด้วยกุญแจสาธารณะที่สามารถแจกจ่ายให้ใครก็ได้ และกุญแจส่วนตัว (Private Key) ที่เจ้าของนั้นจะต้องเก็บไว้เอง นอกจากนั้น กุญแจส่วนตัวยังสามารถนำไปใช้เป็นลายมือชื่อดิจิทัล (Digital Signature) หรือใช้กุญแจส่วนตัวเซ็นรับรองข้อมูลว่า ข้อมูลนั้นส่งมาจากคน ๆ นั้นจริง ผู้รับสามารถใช้กุญแจสาธารณะ (Public Key) ที่ผู้ส่งนั้นให้มาก่อนในการตรวจสอบได้	
Conceptual Relation: **ดูภาพใน** CN049	

Extraction:

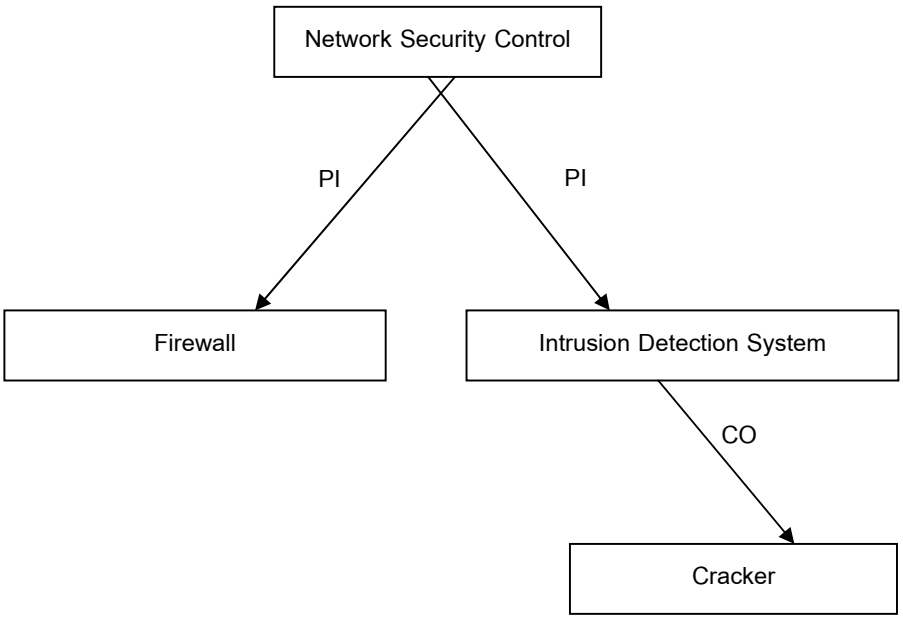
1. Digital certificates also provide a means for users to exchange encrypted information using a combination of a private key (owned by the sender) and public key (freely shared with recipients) to encrypt and decrypt message text. [ISM050.TXT]
2. Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. [ISM131.TXT]
3. The public key is used for encryption and the private key is used for decryption. [ISM112.TXT]
4. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key. [ISM131.TXT]

CN055	**Concept:** Digital Signature
Eng: Digital Signature	**Grammatical Category:** Noun
Thai: ลายมือชื่อดิจิทัล [ราชบัณฑิตยสถาน]	
Feature: ลายมือชื่อดิจิทัล คือ ข้อความที่มีการเซ็นด้วยกุญแจส่วนตัว (Private Key) ของผู้ส่งเพื่อเป็นยืนยันว่า ผู้ที่ส่งนั้นเป็นผู้นั้นอย่างแท้จริงและเนื้อหาไม่โดนเปลี่ยนแปลงในระหว่างทางที่ส่ง โดยในการสร้างลายมือชื่อดิจิทัลนั้น ผู้ส่งจะต้องใช้กุญแจส่วนตัว (Private Key) ของตนในการเข้ารหัสข้อมูล เมื่อข้อความถึงปลายทางแล้ว ผู้รับสามารถใช้กุญแจสาธารณะ (Public Key) ที่ผู้ส่งได้ให้ไว้ในการตรวจสอบ อนึ่ง ลายมือชื่อดิจิทัลจะช่วยให้ข้อมูลมีบูรณภาพ (Integrity) และการปฏิเสธไม่ได้ (Non-Repudiation)	
Conceptual Relation: **ดูภาพใน** CN049	
Extraction: 1. The two main branches of public key cryptography are: Public key encryption — a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality. Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity. [ISM131.TXT] 2. To create a digital signature, the software uses the private key and the message contents (in its binary	

form) to generate a number that is then hashed (run through an algorithm that creates a numerical summary). Any changes made to the message will invalidate the signature, because the message content is used to create the digital signature. [ISM041.TXT]

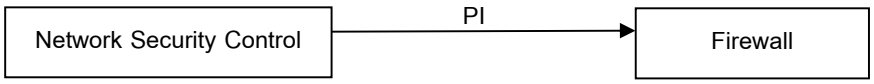
3. Digital signature is usually used to verify whether a message really comes from the claimed originator, and simultaneously guarantees the integrity of the message. [ISM112.TXT]
4. A further claimed advantage of digital signature technology concerns the issue of "non-repudiation" claimed by the relying party against the alleged signer of an electronic document. [ISM136.TXT]

แผนภูมิมโนทัศน์สัมพันธ์แสดงเรื่อง
มาตรการความปลอดภัยของระบบเครือข่าย



CO **แทน** Counter – Object

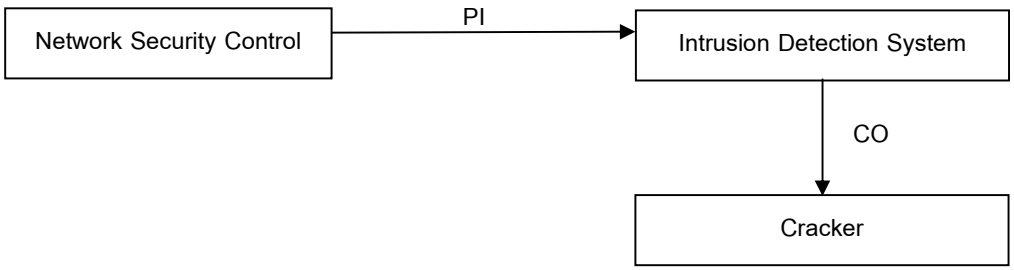
PI **แทน** Process – Instrument

CN056	**Concept:** Firewall
Eng: Firewall	**Grammatical Category:** Noun
Thai: ไฟร์วอลล์, ด่านกันบุกรุก [ราชบัณฑิตยสถาน]	
Feature: ไฟร์วอลล์หรือด่านกันการบุกรุก คือ เครื่องมือและซอฟต์แวร์ที่ทำหน้าที่เป็นด่านหรือประตูเข้าออกระหว่างระบบเครือข่าย 2 ระบบหรือระหว่างส่วนย่อย ๆ ของระบบเครือข่าย 2 ส่วนได้ ไฟร์วอลล์เป็นระบบที่ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้ามาในระบบได้ ไฟร์วอลล์ถือเป็นมาตรการควบคุมระบบเครือข่าย (Network security control) ที่สำคัญมากที่สุดระบบหนึ่ง	
Conceptual Relation:  **PI แทน Process – Instrument**	
Extraction: 1. A Firewall is a device or software package that provides a secure gateway between two networks. [SIM024.TXT] 2. A firewall is a system or combination of systems that helps to prevent outsiders from obtaining unauthorised access to internal information resources. [ISM112.TXT] 3. A firewall is an access control device that sits between two networks or two network segments. [ISM119.TXT] 4. Because they are an extremely important network security control, we study firewalls in an entire section later in this chapter. [ISM119.TXT]	

CN057	**Concept:** Intrusion Detection System
Eng: Intrusion Detection System, IDS	**Grammatical Category:** Noun
Thai: ระบบตรวจจับการบุกรุก [ผู้เชี่ยวชาญ]	
Feature: ระบบตรวจจับการบุกรุก หรือ ระบบไอดีเอส คือ ระบบป้องกันที่คอยตรวจสอบกิจกรรมผิดปกติที่อาจก่อให้เกิดผลร้ายต่อความปลอดภัยในระบบเครือข่ายและเมื่อตรวจเจอ ระบบก็จะส่งคำเตือนไปยังผู้บริหารระบบเครือข่าย ถึงแม้ว่า ผู้เจาะระบบเครือข่าย (Hacker) สามารถบุกรุกเข้ามาในระบบได้ แต่ระบบตรวจจับการบุกรุกก็ยังสามารถกันการโจมตีได้ตั้งแต่เนิ่น ๆ ได้โดยการตรวจสอบกิจกรรมที่ผิดปรกติในระบบเครือข่าย ระบบตรวจจับการบุกรุกต่างจากไฟร์วอลล์ตรงที่ว่าไฟร์วอลล์จะกันไม่ให้ผู้บุกรุกเข้ามาในระบบเครือข่ายได้ในขณะที่ระบบตรวจจับการบุกรุกจะกันไม่ให้เกิดเหตุการณ์ร้าย ๆ	

ชิ้นในระบบเครือข่าย

Conceptual Relation:

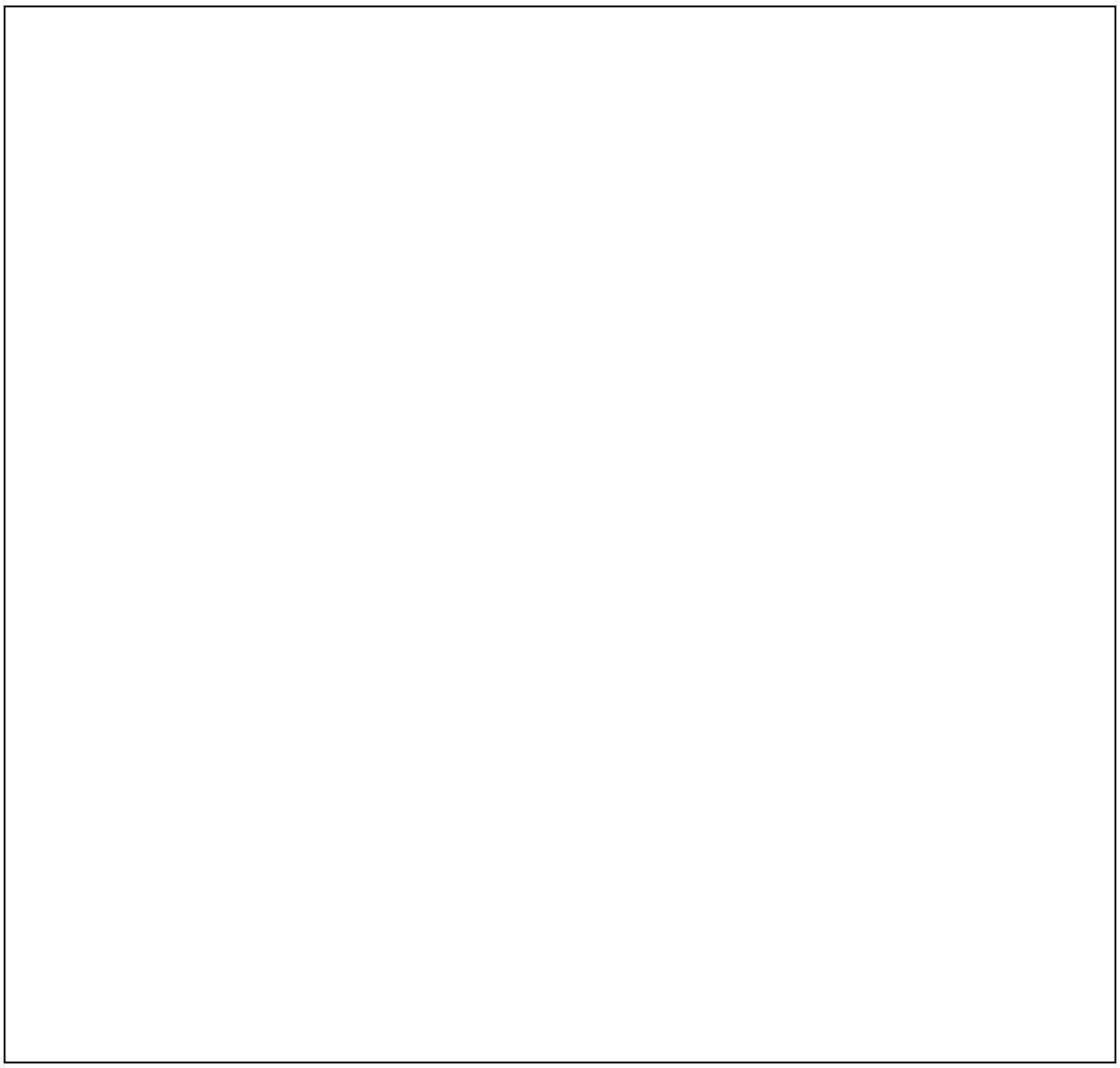


CO **แทน** Counter – Object

PI **แทน** Process – Instrument

Extraction:

1. An Intrusion Detection System (abbreviated as IDS) is a defense system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. [ISM039.TXT]
2. An intrusion detection system is a device that is placed inside a protected network to monitor what occurs within the network. If an attacker is able to pass through the router and pass through the firewall, an intrusion detection system offers the opportunity to detect the attack at the beginning, in progress, or after it has occurred. Intrusion detection systems activate an alarm, which can take defensive action. [ISM119.TXT]
3. As soon as someone discovers a new computer security vulnerability, hordes of crackers start knocking at the doors of computers worldwide to see if they can penetrate their defenses. Many sites employ a combination of border router firewalls and host-based packet filters and wrappers to protect themselves, but what if the vulnerability is in the very mechanism that's used to secure a service? How can systems administrators know that their machines are under attack and/or have been compromised? The best way to catch the crackers in the act is to use an intrusion detection system (IDS). [ISM132.TXT]
4. Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. [ISM133.TXT]



ภาคผนวก ง
การบันทึกข้อมูลศัพท์

รหัสอ้างอิงที่ใช้ในการประมวลศัพท์

ในการบันทึกข้อมูลศัพท์เรื่อง การจัดการความปลอดภัยของข้อมูล ได้กำหนดรหัสผ้างอิงดังต่อไปนี้

TXXX	หมายถึง	เลขที่ศัพท์ เช่น T001
ISMXXX.TXT	หมายถึง	เลขที่แฟ้มข้อมูลจากคลังข้อมูล เช่น ISM001.TXT
SYN	หมายถึง	คำเหมือน
ANT	หมายถึง	คำตรงข้าม
ABRV	หมายถึง	คำย่อ

T001	**English term:** Information Security Management	**Grammatical Category:** Noun
Thai: การจัดการความปลอดภัยของข้อมูล [ราชบัณฑิตยสถาน]		
Subject Field: Information Security Management		
Definition: การจัดการความปลอดภัยของข้อมูล หมายถึง การจัดการที่ช่วยรักษาคุณสมบัติของข้อมูลในระบบคอมพิวเตอร์ครบ 4 ประการ คือ ความลับ บูรณภาพ สภาพพร้อมใช้งาน และการปฏิเสธไม่ได้ การจัดการที่ว่านี้รวมไปถึงการจัดการความเสี่ยงที่มาจากภัยคุกคามทั้งภายในและภายนอกองค์กร เมื่อระบุความเสี่ยงได้แล้ว ก็จะต้องหามาตรการควบคุมความปลอดภัยนั้นเพื่อมาช่วยลดหรือกำจัดความเสี่ยงด้วย		
Illustration: It is clear that hands on experience with the valuation of assets, assessment of security risk, and the evaluation of tradeoffs (i.e. risk management), the key elements of the information security management function, are best learned by doing. [ISM037.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Confidentiality (T003), Integrity (T004), Availability (T005), Non-Repudiation (T006), Risk Management (T008)		

T002	**English term:** Information Security	**Grammatical Category:** Noun
Thai: ความปลอดภัยของข้อมูล [ราชบัณฑิตยสถาน]		
Subject Field: Information Security		
Definition: ความปลอดภัยของข้อมูล คือ การที่ข้อมูลนั้น ๆ จะต้องรักษาไว้ซึ่งคุณสมบัติ 4 ประการด้วยกัน คือ ความลับ บูรณภาพ สภาพพร้อมใช้งาน และการปฏิเสธไม่ได้		
Illustration: Poor security procedures during equipment testing can compromise the confidentiality of your data. [ISM063.TXT]		

Note: -
Linguistic specification: -
Cross-reference: Information Security System (T001)

T003	**English term:** Confidentiality	**Grammatical Category:** Noun
Thai: ความลับ [ราชบัณฑิตยสถาน]		
Subject Field: Confidentiality		
Definition: ความลับ คือ คุณสมบัติประการหนึ่งของความปลอดภัยของข้อมูล ความลับของข้อมูลนั้นหมายถึง ข้อมูลนั้น ๆ จะเปิดได้แต่เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น		
Illustration: Poor security procedures during equipment testing can compromise the confidentiality of your data. [ISM063.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Information Security (T002)		

T004	**English term:** Integrity	**Grammatical Category:** Noun
Thai: บูรณภาพ [ราชบัณฑิตยสถาน]		
Subject Field: Integrity		
Definition: บูรณภาพ คือ คุณสมบัติประการหนึ่งของความปลอดภัยของข้อมูล บูรณภาพของข้อมูลนั้นหมายถึง ข้อมูลนั้น ๆ ไม่มีการเปลี่ยนแปลงเนื้อหาโดยที่ไม่ได้รับอนุญาตเกิดขึ้น		
Illustration: Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information. [ISM042.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Information Security (T002)		

T005	**English term:** Availability	**Grammatical Category:** Noun
Thai: สภาพพร้อมใช้งาน [ราชบัณฑิตยสถาน]		
Subject Field: Availability		
Definition: สภาพพร้อมใช้งาน คือ คุณสมบัติประการหนึ่งของความปลอดภัยของข้อมูล สภาพพร้อมใช้งานของข้อมูลนั้น หมายถึงว่า ข้อมูลนั้น ๆ จะต้องคงอยู่ในระบบตลอดเวลาเมื่อมีผู้ใช้งานต้องการเรียกใช้ ไม่มีการสูญหายไปโดยที่เจ้าหน้าที่ไม่รับทราบ		
Illustration: In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. [ISM005.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Information Security (T002)		

T006	**English term:** Non-Repudiation	**Grammatical Category:** Noun
Thai: การปฏิเสธไม่ได้ [ราชบัณฑิตยสถาน]		
Subject Field: Non-Repudiation		
Definition: การปฏิเสธไม่ได้นั้น คือ คุณสมบัติประการหนึ่งของความปลอดภัยของข้อมูล การปฏิเสธไม่ได้ของข้อมูลนั้น คือ ผู้ส่งข้อมูลไม่สามารถปฏิเสธได้ว่า ไม่ได้ข้อมูลนั้น ๆ มา		
Illustration: Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non -repudiation, and encrypted network communications. [ISM097.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Information Security (T002)		

T007	**English term:** Compromise	**Grammatical Category:** Noun
Thai: เป็นอันตราย [ผู้เชี่ยวชาญ]		
Subject Field: Compromise		
Definition: การกระทำที่ทำให้ระบบคอมพิวเตอร์นั้นสูญเสียความปลอดภัยของระบบ		

Illustration: Information Security issues to be considered when implementing your policy include the following: • Theft of equipment is most likely to result in additional cost to the organisation and could compromise data security. [ISM063.TXT]
Note: -
Linguistic specification: -
Cross-reference: Information Security (T002)

T008	**English term:** Risk Management	**Grammatical Category:** Noun
Thai: การจัดการความเสี่ยง [ราชบัณฑิตยสถาน]		
Subject Field: Risk Management		
Definition: การจัดการความเสี่ยงเป็นขั้นตอนหนึ่งในการจัดการความปลอดภัยของข้อมูล ประกอบไปด้วยขั้นตอนย่อยต่าง ๆ เพื่อระบุอันตรายที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กรรวมไปถึงมาตรการที่จะมาลดความเสี่ยงนั้น		
Illustration: Considering that information security management is a risk reduction program, we present vulnerability management as a component of risk management where decisions as to whether to fix a given vulnerability are based on the potential loss and the associated cost of mitigating the risk. [ISM001.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Information Security System (T001)		

T009	**English term:** Contingency Plan	**Grammatical Category:** Noun
Thai: แผนแก้ไขปัญหาจากภัยพิบัติ [ราชบัณฑิตยสถาน]		
Subject Field: Contingency Plan		
Definition รายละเอียดแผนการที่ผู้ใช้งานปฏิบัติตามเมื่อมีเหตุการณ์ร้ายที่เกี่ยวข้องกับการละเมิดความปลอดภัยของข้อมูลสารสนเทศเกิดขึ้น เหตุการณ์ที่ว่านี้ครอบคลุมเหตุการณ์ที่เกิดจากน้ำมือของมนุษย์ไปจนถึงเหตุการณ์ร้ายที่เกิดจากภัยธรรมชาติ		
Illustration: For residual risks that may occur contingency plans should be developed in case they do. Contingency plans should be appropriate and commensurate to the impact of the original risk. [ISM026.TXT]		
Note: -		
Linguistic specification: (SYN) Business Continuity Plan [ISM117.TXT]		

Cross-reference: Risk Management (T008)

T010	**English term:** Risk Assessment	**Grammatical Category:** Noun
Thai: การประเมินความเสี่ยง [ราชบัณฑิตยสถาน]		
Subject Field: Risk Assessment		
Definition: การประเมินความเสี่ยงเป็นขั้นตอนหนึ่งของการจัดการความเสี่ยง เป็นการระบุและการจัดลำดับความสำคัญของความเสี่ยงของภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กร		
Illustration: These organizations establish a central management focal point, promote awareness, link policies to business risks, and develop practical risk assessment procedures that link security to business needs. [ISM052.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Management (T008)		

T011	**English term:** Risk Treatment	**Grammatical Category:** Noun
Thai: การลดความเสี่ยง [ผู้เชี่ยวชาญ]		
Subject Field: Risk Treatment		
Definition: การลดความเสี่ยงเป็นขั้นตอนหนึ่งของการจัดการความเสี่ยง เป็นการประเมินว่าจะจัดการกับความเสี่ยงนั้นอย่างไรโดยจัดการได้ 4 ประการ คือ ยอมรับความเสี่ยงนั้น ๆ หลีกเลี่ยงความเสี่ยง ถ่ายโอนความเสี่ยง หรือลดความเสี่ยงนั้น ๆ ลง		
Illustration: The cost of risk treatment plans should depend on the risk (i.e., it should be based on potential impact). [ISM001.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Management (T007)		

T012	**English term:** Risk Acceptance	**Grammatical Category:** Noun
Thai: การยอมรับความเสี่ยง [ผู้เชี่ยวชาญ]		
Subject Field: Risk Acceptance		
Definition: ในขั้นตอนการลดความเสี่ยงนั้น จะมีขั้นตอนการตัดสินใจว่าจะจัดการความเสี่ยงนั้นอย่างไร โดยทางเลือกในการตัดสินใจนั้นคือการยอมรับความเสี่ยงนั้นหรือสามารถทนความเสี่ยงนั้นได้		
Illustration: Areas that are low risk and common vulnerabilities that are generally known to exist typically do not require a risk acceptance statement. [ISM005.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Management (T008)		

T013	**English term:** Risk Communication	**Grammatical Category:** Noun
Thai: การสื่อสารความเสี่ยง [ราชบัณฑิตยสถาน]		
Subject Field: Risk Communication		
Definition: การสื่อสารความเสี่ยงเป็นขั้นตอนหนึ่งของการจัดการความเสี่ยง เป็นการโต้ตอบและการบอกข่าวสารให้กับผู้ที่เกี่ยวข้องถึงลักษณะของความเสี่ยงและวิธีการที่จะตอบสนองกับความเสี่ยงนั้น ๆ		
Illustration: In order to engage in effective risk communication planning, it is important to understand how to apply the principles of risk communication, as well as the variety of tools and resources available. [ISM028.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Management (T008)		

T014	**English term:** Risk Analysis	**Grammatical Category:** Noun
Thai: การวิเคราะห์ความเสี่ยง [ราชบัณฑิตยสถาน]		
Subject Field: Risk Analysis		
Definition: การวิเคราะห์ความเสี่ยงเป็นขั้นตอนหนึ่งของการประเมินความเสี่ยง โดยผู้รับผิดชอบจะต้องประเมินปริมาณความเสี่ยงที่อาจเกิดขึ้นและหาทางดำเนินการแก้ไข		

Illustration: Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to Confidential Health Information. [ISM036.TXT]
Note: -
Linguistic specification: -
Cross-reference: Risk Management (T008)

T015	**English term:** Risk Evaluation	**Grammatical Category:** Noun
Thai: การประเมินความรุนแรงของความเสี่ยง [ราชบัณฑิตยสถาน]		
Subject Field: Risk Evaluation		
Definition: การประเมินความรุนแรงความเสี่ยงเป็นขั้นตอนหนึ่งของการประเมินความเสี่ยง โดยตัดสินจากเงื่อนไขความเสี่ยง และนำไปเลือกหนทางที่จะนำมาลดความเสี่ยงนั้น ๆ ด้วย		
Illustration: The risk evaluation criteria are used as a guide to enable decisions to be made on risk treatment options. [ISM064.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Management (T008)		

T016	**English term:** Controls	**Grammatical Category:** Noun
Thai: มาตราการควบคุมความปลอดภัย [ราชบัณฑิตยสถาน]		
Subject Field: Controls		
Definition: มาตรการความปลอดภัยใช้เพื่อลดความเสี่ยงที่อาจเกิดขึ้นในองค์กร มาตรการความปลอดภัยนั้นสามารถเป็นได้ทั้งเทคโนโลยี เครื่องมือเสริมต่าง ๆ รวมไปถึงกฎระเบียบต่าง ๆ ด้วย		
Illustration: Security managers told us that identifying and assessing information security risks in terms of the impact on business operations was an essential step in determining what controls were needed and what level of resources could be expended on controls. [ISM004.TXT]		
Note: -		
Linguistic specification: -		

Cross-reference: Risk Treatment (T011)

T017	**English term**: Threat	**Grammatical Category**: Noun
Thai: ภัยคุกคาม [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Threat		
Definition: เหตุการณ์ที่อาจจะเกิดขึ้นและอาจก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ขององค์กรได้ ภัยคุกคามเป็นสิ่งที่ต้องวิเคราะห์ในขั้นตอนการวิเคราะห์ความเสี่ยง		
Illustration: Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected. [ISM005.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Analysis (T014)		

T018	**English term**: Vulnerability	**Grammatical Category**: Noun
Thai: ความอ่อนแอของระบบ [ราชบัณฑิตยสถาน]		
Subject Field: Vulnerability		
Definition: จุดอ่อนของระบบที่ผู้บุกรุกสามารถใช้เป็นเครื่องมือในการโจมตีระบบคอมพิวเตอร์ขององค์กรได้ ส่งผลให้ระบบนั้นเกิดความเสียหาย ความอ่อนแอของระบบเป็นสิ่งที่ต้องวิเคราะห์ในขั้นตอนการวิเคราะห์ความเสี่ยง		
Illustration: However, your email system is a point of vulnerability that can be exploited to invade your system and network. [ISM059.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Risk Analysis (T014)		

T019	**English term**: Denial of Service	**Grammatical Category**: Noun

Thai: การล่มระบบ [ราชบัณฑิตยสถาน]
Subject Field: Denial of Service
Definition: การล่มบริการระบบโดยเกิดจากการที่ส่งข้อความหรือการร้องขอเข้ามามากอย่างท่วมท้นจนระบบไม่สามารถรองรับการรับข้อความหรือการร้องขอรับบริการนั้นได้ซึ่งอาจก่อให้เกิดความเสียหายต่อธุรกิจได้
Illustration: Denial of service attacks are much easier to accomplish than remotely gaining administrative access to a target system. Because of this, denials of service attacks have become very common on the Internet. [ISM104.TXT]
Note: -
Linguistic specification: (SYN) DoS Attack [ISM040.TXT]
Cross-reference: Threat (T017)

T020	**English term:** Hacker	**Grammatical Category:** Noun
Thai: ผู้เจาะระบบเครือข่ายคอมพิวเตอร์ [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Hacker		
Definition: ผู้เจาะระบบเครือข่ายคอมพิวเตอร์นี้ จะหมายถึง ผู้ที่ใช้ความรู้ความสามารถของตนในการบุกรุกเข้าไปในระบบเครือข่ายของผู้อื่นโดยใช้จุดอ่อนของระบบ เจตนาการบุกรุกนั้นคือเพื่อต้องการทดสอบฝีมือของตน หรือเข้ามาตรวจสอบจุดอ่อนของระบบคอมพิวเตอร์ นอกจากนั้นอาจยังเข้ามาขโมยข้อมูลหรือสร้างความเสียหายให้แก่ระบบสารสนเทศนั้น		
Illustration: The content of your e-mail correspondence, personal projects, documents and photos, could be exposed to a malicious hacker or someone targeting especially you as an individual. [ISM050.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Threat (T017), Cracker (T027)		

T021	**English term:** Insider Attack	**Grammatical Category:** Noun
Thai: การโจมตีจากภายในองค์กร [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Insider Attack		
Definition: การโจมตีที่เกิดขึ้นในระบบเครือข่ายภายในองค์กรเองและอาจจะเกิดจากคนในองค์กรนั้นเองหรือคนที่สามารถเข้าไปในระบบภายในได้		

Illustration: At Northrop Grumman IT, we believe that there are other available measurements that exist that when viewed in their entirety can potentially declare an insider attack and can perform that analysis in real time. [ISM107.TXT]
Note: -
Linguistic specification: -
Cross-reference: Threat (T017)

T022	**English term:** Social Engineering	**Grammatical Category:** Noun
Thai: กลลวงทางสังคม [ผู้เชี่ยวชาญ]		
Subject Field: Social Engineering		
Definition: การหลอกลวงหรือการพูดจาหลอกล่อเพื่อให้ผู้ใช้งานระบบสารสนเทศบอกข้อมูลที่เป็นความลับมา เช่น รายชื่อของผู้ใช้งานในระบบและรหัสผ่านเข้าระบบ เพื่อเข้าไปในบริษัทเพื่อขโมยข้อมูลอื่น ๆ ออกมา ผู้ใช้งานที่โดนหลอกโดยใช้ทางกลลวงทางสังคมนี้มักจะให้ความร่วมมือกับผู้โจมตีเป็นอย่างดีโดยที่ไม่สะดุดใจแต่อย่างใด		
Illustration: Use another employee's account and password (which he cracked technologically or discovered through social engineering techniques) to get access to files or programs he can't access with his own account. [ISM058.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Threat (T017)		

T023	**English term:** Website Intrusion	**Grammatical Category:** Noun
Thai: การบุกรุกทางเว็บไซต์ [ราชบัณฑิตยสถาน]		
Subject Field: Website Intrusion		
Definition: การบุกรุกทางเว็บไซต์เป็นการอาศัยช่องโหว่ในเว็บไซต์ขององค์กรที่บุคคลภายนอกหรือแม้แต่กระทั่งบุคคลภายในองค์กรเองใช้บุกรุกเข้ามาในส่วนที่ไม่ได้รับอนุญาตซึ่งเป็นส่วนที่มีข้อมูลความลับขององค์กรเก็บอยู่		
Illustration: The security threats that most often and most seriously contribute to small-medium business days lost include virus incidents and |website| intrusion (by hacking) [ISM116.TXT]		
Note: -		

Linguistic specification: -
Cross-reference: Threat (T017)

T024	**English term**: Malware	**Grammatical Category**: Noun
Thai: โปรแกรมมุ่งร้าย [ราชบัณฑิตยสถาน]		
Subject Field: Malware		
Definition: โปรแกรมมุ่งร้ายนั้นเป็นโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์และเครือข่าย โดยโปรแกรมมุ่งร้ายจะทำงานในลักษณะที่เป็นไวรัส ทั้งประเภทหนอนอินเตอร์เน็ต ม้าโทรจัน แอบดักข้อมูล ตลอดจนโปรแกรมขโมยข้อมูล		
Illustration: Visiting unsafe Web sites may introduce viruses and other malware to the company network. [ISM009.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Threat (T017)		

T025	**English term**: Virus	**Grammatical Category**: Noun
Thai: ไวรัสคอมพิวเตอร์ [ราชบัณฑิตยสถาน]		
Subject Field: Virus		
Definition: โปรแกรมมุ่งร้ายที่สามารถประมวลผลได้และสามารถแตกตัวเองต่อไปเรื่อย ๆ อาจจะไปติดกับโปรแกรมอื่น ๆ หรือไปติดกับแผ่นดิสก์ที่เสียบมาในคอมพิวเตอร์ เมื่อใดก็ตามที่มีการประมวลผลไฟล์ ๆ นั้น ไวรัสนั้นก็จะโดนประมวลผลไปด้วย คอมพิวเตอร์ที่มีไวรัสอาจมีการทำงานที่แปรปรวนไปโดยที่ผู้ใช้งานไม่ได้ปรับเปลี่ยนอะไรทั้งสิ้น		
Illustration: Virus writers, who used to spread their virtual “diseases” via infected floppies and network shares, have seized the opportunity posed by email programs that support attached files, HTML messages, and embedded scripts to send viruses and other malicious software (called “malware”) to hundreds or thousands of people with just a few keystrokes. [ISM059.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Malware (T024)		

T026	**English term:** Worm	**Grammatical Category:** Noun
Thai: หนอนคอมพิวเตอร์ [ราชบัณฑิตยสถาน]		
Subject Field: Worm		
Definition: หนอนคอมพิวเตอร์ คือ โปรแกรมมุ่งร้ายที่สามารถแพร่ตัวเองได้โดยไม่ต้องพึ่งผู้ใช้งานและโปรแกรมอื่น ๆ		
Illustration: Love Bug affected systems running Microsoft Windows. It was a program that spread through various means, including e-mail, Windows file sharing, USENET news, and possibly web pages. The people who received copies of the worm via e-mail most likely would have recognized the sender, and the subject line read, ILOVEYOU. [ISM116.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Malware (T024)		

T027	**English term:** Trojan	**Grammatical Category:** Noun
Thai: ม้าโทรจัน [ราชบัณฑิตยสถาน]		
Subject Field: Trojan		
Definition: โปรแกรมมุ่งร้ายที่ทำงานแบบปกติทั่ว ๆ ไปแต่แท้จริงแล้วมีโปรแกรมร้ายซ่อนอยู่ไว้ข้างหลังและทำร้ายระบบเครือข่าย เมื่อผู้ใช้งานประมวลผลโปรแกรมนี้โดยไม่รู้ตัว จะก่อความเสียหายแก่คอมพิวเตอร์ โดยปกติแล้ว คำว่าม้าโทรจันนี้มาจากตำนานสงครามโทรจันที่มีการส่งม้าโทรจันให้เป็นของขวัญแต่ปรากฏว่ามีทหารทรอยซ่อนอยู่ในนั้นซึ่งพอมาถึงที่ทหารโทรจันก็เปิดประตูออกมาและโจมตีฝ่ายตรงข้าม		
Illustration: W32.DlDer.Trojan was one such Trojan and it was found to be bundled with a very popular entertainment application. Once it was found that this Trojan was distributed the company was confronted. [ISM027.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Malware (T024)		

T028	**English term:** Cracker	**Grammatical Category:** Noun
Thai: ผู้บุกรุกระบบ [ราชบัณฑิตยสถาน]		
Subject Field: Cracker		
Definition: ผู้ที่พยายามบุกรุกเข้าไปในระบบเครือข่ายสารสนเทศขององค์กรโดยที่ไม่ได้รับอนุญาตเพื่อก่อความเสียหายให้แก่ระบบ ผู้บุกรุกจะพยายามหลายครั้งจนกว่าจะเข้าระบบได้		
Illustration: A password cracker would try to guess all the possible combinations of letters, numbers and characters until he/she finds the right one. [ISM050.TXT]		
Note: -		
Linguistic specification: Black hat hacker [ISM139.TXT]		
Cross-reference: Hacker (T020)		

T029	**English term:** Safeguard	**Grammatical Category:** Noun
Thai: สิ่งป้องกัน [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Safeguard		
Definition: สิ่งป้องกันนั้นจะปกป้องระบบคอมพิวเตอร์ให้คงความปลอดภัยของระบบไว้โดยสิ่งป้องกันนั้นเป็นได้ตั้งแต่ฮาร์ดแวร์และซอฟต์แวร์ที่ทำมาเพื่อรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ วิธีการในการทำงาน มาตรการควบคุมการเข้าถึงและการแจกจ่ายข้อมูล เครื่องมือทางกายภาพ		
Illustration: Each department responsible for maintaining covered data and information should coordinate with the Office of Legal Services on an annual basis for the coordination and review of additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard covered data and information security. [ISM042.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Controls (T016)		

T030	**English term:** Information security policy	**Grammatical Category:** Noun
Thai: นโยบายรักษาความปลอดภัยของข้อมูล [ราชบัณฑิตยสถาน]		

Subject Field: Security policy
Definition: นโยบายรักษาความปลอดภัยของข้อมูลจะบอกรายละเอียดถึงแนวทางการปฏิบัติ มาตรฐานการรักษาความปลอดภัย ให้พนักงานในองค์กรทราบเพื่อปฏิบัติตามอย่างถูกต้อง นอกจากนี้ นโยบายรักษาความปลอดภัยของข้อมูลนั้นจะเป็นตัวกำหนดว่า องค์กรหนึ่ง ๆ ต้องใช้มาตราการควบคุมความปลอดภัยทางวัตถุและมาตราการควบคุมความปลอดภัยแบบตรรก
Illustration: A security policy would specify the necessary course of action based on the above risk assessment table. [ISM001.TXT]
Note: -
Linguistic specification: -
Cross-reference: Controls (T016)

T031	**English term:** Administrative Control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมทางด้านบริหาร [ราชบัณฑิตยสถาน]		
Subject Field: Administrative Control		
Definition: มาตรการควบคุมทางด้านบริหาร เป็นโครงสร้างการบริหารคนและงานต่าง ๆ รวมไปถึงรายละเอียดการปฏิบัติงานรายวัน มาตรการควบคุมทางด้านบริหารนั้นเป็นตัวกำหนดว่าจะต้องใช้มาตรการควบคุมด้านตรรกะและมาตรการควบคุมแบบกายภาพ		
Illustration: Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the bases upon which to build a defence-in depth-strategy. With this approach, defence in depth can be conceptualised as three distinct layers or planes laid one on top of the other. [ISM097.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Controls (T016), Logical control (T032), Physical control (T033)		

T031	**English term:** Logical Control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมแบบตรรกะ [ราชบัณฑิตยสถาน]		

Subject Field: Logical Control
Definition: มาตรการควบคุมแบบตรรกะใช้ซอฟต์แวร์และข้อมูลในการควบคุมการเรียกดูข้อมูลและการเข้าถึงระบบคอมพิวเตอร์ภายในองค์กร ตัวอย่างมาตรการควบคุมแบบนี้ เช่น รหัสผ่าน ระบบไฟร์วอลล์ และการเข้ารหัสข้อมูล การเลือกมาตรการควบคุมแบบตรรกะนั้นขึ้นอยู่กับเนื้อหาในนโยบายรักษาความปลอดภัยที่องค์กรนั้น ๆ ใช้
Illustration: Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the bases upon which to build a defence-in depth-strategy. [ISM097.TXT]
Note: -
Linguistic specification: (SYN) Technical Control [ISM097.TXT]
Cross-reference: Controls (T016)

T032	**English term:** Physical Control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมทางกายภาพ [ราชบัณฑิตยสถาน]		
Subject Field: Physical Control		
Definition: มาตรการควบคุมทางกายภาพนั้นใช้เฝ้าดูและควบคุมสถานที่การทำงานและห้องเครื่องคอมพิวเตอร์รวมไปถึงผู้ที่เข้าไปใช้งานสถานที่นั้น ๆ ด้วย การเลือกมาตรการควบคุมทางกายภาพนั้นขึ้นอยู่กับเนื้อหาในนโยบายรักษาความปลอดภัยที่องค์กรนั้น ๆ ใช้		
Illustration: Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls. [ISM005.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Controls (T016)		

T033	**English term:** Access Control	**Grammatical Category:** Noun
Thai: การควบคุมการเข้าถึงข้อมูล [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Access Control		

Definition: การควบคุมการเข้าถึงข้อมูลนั้นจะคอยตรวจสอบว่าใครสามารถและไม่สามารถเข้ามาในระบบได้บ้างโดยการติดตั้งมาตรการควบคุมทางตรรกและทางกายภาพหรือมีการนำเทคโนโลยีต่าง ๆ มาใช้ในการควบคุม การเลือกวิธีการควบคุมการเข้าถึงข้อมูลนั้นขึ้นอยู่กับระดับความสำคัญของข้อมูลนั้น ๆ
Illustration: A great deal of functionality exists in such enterprise class firewalls. It will act as a very powerful access control mechanism if properly configured. [ISM005.TXT]
Note: -
Linguistic specification: -
Cross-reference: Controls (T016)

T034	**English term:** Network security control	**Grammatical Category:** Noun
Thai: มาตรการควบคุมความปลอดภัยของระบบเครือข่าย [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Network security control		
Definition: มาตรการควบคุมความปลอดภัยของระบบเครือข่ายนั้นมุ่งเน้นไปที่การรักษาความปลอดภัยของระบบเครือข่ายอันเกิดมาจากการมุ่งร้ายที่เจาะเข้ามาในระบบเพื่อป้องกันไม่ให้องค์กรเปิดเผยข้อมูลที่มีค่าต่อสารธารณะโดยไม่จำเป็น		
Illustration: Because they are an extremely important network security control, we study firewalls in an entire section later in this chapter. [ISM119.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Logical Control (T031)		

T035	**English term:** Authorization	**Grammatical Category:** Noun
Thai: การอนุญาต [ราชบัญฑิตยสถาน]		
Subject Field: Authorization		
Definition: กลไกอย่างหนึ่งที่กันให้บุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบได้ โดยผู้ใช้งานในระบบนั้นจะได้รับสิทธิ์อนุญาตที่ต่างกันขึ้นอยู่กับหน้าที่ของงานและจะได้รับเท่าที่จำเป็นเท่านั้นเพื่อเป็นการทำให้มั่นใจว่า ข้อมูลแต่ละชิ้น คนที่นำไปใช้คือคนที่ต้องใช้จริง ๆ นอกจากนั้น สิทธ์อนุญาตยังนำไปใช้กำหนดสิทธิ์ของผู้ใช้งานว่าสามารถกระทำการใดได้บ้าง		
Illustration: To automate the process of determining whether particular roles or tasks are allowed, you can use		

scripts within role and task definitions. These scripts can be written in VBScript or JScript, and are called authorization rules. This gives you tremendous control to define the conditions that must be met for authorization to occur. You can limit authorization to a specific time of day, for example, or base it on whether an expense limit has been met or the amount in a specified account balance. [ISM008.TXT]
Note: -
Linguistic specification: -
Cross-reference: Logical Control (T031), Access Control (T033)

T036	**English term**: Cryptography	**Grammatical Category**: Noun
Thai: วิทยาการรหัสลับ [วิทย์ เที่ยงบูรณธรรม]		
Subject Field: Cryptography		
Definition: วิทยาการรหัสลับเป็นการเข้ารหัสข้อมูลเพื่อที่จะให้ข้อมูลนั้นอ่านไม่ออกและจะถอดรหัสกลับเพื่ออ่านข้อมูลยาก วิทยาการรหัสลับนี้ใช้เพื่อป้องกันการเปิดเผยข้อมูลในระหว่างการส่งหรือในขณะที่ข้อมูลนั้นเก็บไว้ที่ใดที่หนึ่ง		
Illustration: Cryptography can introduce security problems when it is not implemented correctly. [ISM097.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Logical Control (T031)		

T037	**English term**: Anti-virus Software	**Grammatical Category**: Noun
Thai: โปรแกรมป้องกันไวรัสในคอมพิวเตอร์ [จิรายุส ภาสวัต]		
Subject Field: Anti-virus Software		
Definition: โปรแกรมคอมพิวเตอร์ที่ได้รับการออกแบบมาเพื่อกำจัดไวรัส ดักจับไวรัสเพื่อไม่ให้ออกมาทำลายคอมพิวเตอร์ รวมไปถึงการกู้ข้อมูลที่ถูกทำลายไปแล้วโดยไวรัสตัวนั้นด้วย		
Illustration: The security risks of e-mail borne viruses and worms and liability implications of e-mail containing pornography or other undesirable content. It's getting harder and harder for network administrators to keep it all under control. And if you're in a regulated industry, you may have no choice: communications containing clients' personal information, medical records, financial data and so forth must, by law, be secured. One solution is to work harder, invest more money in anti-spam software, anti-virus software and more sophisticated		

firewalls. [ISM097.TXT]
Note: -
Linguistic specification: -
Cross-reference: Logical Control (T031), Virus (T025), Worm (T026), Trojan (T027)

T038	**English term**: Identification	**Grammatical Category**: Noun
Thai: การระบุผู้ใช้งาน [ผู้เชี่ยวชาญ]		
Subject Field: Identification		
Definition: การอ้างว่า คน ๆ นั้นที่จะเข้าใช้งานในระบบคือใคร การระบุผู้ใช้งานนี้เป็นเครื่องมือหนึ่งที่ใช้ตัดสินใจว่า ระบบจะอนุญาตให้บุคคลนั้น ๆ เข้าระบบหรือไม่		
Illustration: Issues to consider include: specification of ownership of data and information; identification of users and others who access the system in a unique manner; recording of activities through the provision of management audit trails; assignment of responsibility for maintenance of data and information. [ISM089.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Authorization (T035)		

T039	**English term**: Unique User Identifier	**Grammatical Category**: Noun
Thai: ชื่อระบุผู้ใช้งาน [ผู้เชี่ยวชาญ]		
Subject Field: Unique User Identifier		
Definition: ชื่อระบุผู้ใช้งานนั้นจะเป็นชื่อที่ให้ไว้กับผู้ใช้งานในระบบ เพื่อไว้คอยตรวจสอบการใช้งานและเป็นตัวที่ใช้ระบุชื่อและตัวตนของผู้เข้าใช้งานในระบบด้วยซึ่งจะมีความแตกต่างกันในแต่ละบุคคล		
Illustration: Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role. c) User-based access: A security mechanism used to grant users of a system access based upon the identity of the user. 2. Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential Information. Users will be held accountable for all actions performed on the system with their user identification.		

[ISM036.TXT]
Note: -
Linguistic specification: -
Cross-reference: Identification (T038)

T040	**English term**: Authentication	**Grammatical Category**: Noun
Thai: การพิสูจน์ตัวตนที่แท้จริง [ราชบัณฑิตยสถาน]		
Subject Field: Authentication		
Definition: วิธีการที่ใช้พิสูจน์ว่าคนที่เข้าระบบมาโดยใช้ชื่อระบุนั้น ๆ เป็นคน ๆ นั้นจริง ๆ โดยวิธีการนี้จะนำมาใช้เพื่อปกป้องการหลอกลวงในการเข้าระบบและหลอกว่าเป็นบุคคลนั้น ๆ การพิสูจน์ตัวตนที่แท้จริงนี้จะใช้ร่วมกับวิธีการระบุผู้ใช้งาน เพื่อใช้ตัดสินใจว่า ระบบจะอนุญาตให้บุคคลนั้น ๆ เข้าระบบหรือไม่		
Illustration: Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role. c) User-based access: A security mechanism used to grant users of a system access based upon the identity of the user. 2. Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential Information. Users will be held accountable for all actions performed on the system with their user identification. [ISM036.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Authorization (T035)		

T041	**English term**: Biometrics	**Grammatical Category**: Noun
Thai: ชีวมาตร [ราชบัณฑิตยสถาน]		
Subject Field: Biometrics		
Definition: การพิสูจน์ตัวตนจากสิ่งที่ผู้ใช้งานคนนั้นเป็น หรือใช้ส่วนใดส่วนหนึ่งในร่างกายของผู้ใช้งานมาเป็นบททดสอบ เช่น การตรวจสอบลายนิ้วมือ เป็นต้น ชีวมาตรเป็นเครื่องมือที่ใช้ในการพิสูจน์ตัวตนชนิดหนึ่ง		
Illustration: There is far more to biometrics though then a facial scan. Other biometrics exist such as the now more common thumbprint scanner on some laptops. These two methods of biometric identification are not the		

only ones though. You can also see or may have heard of retina scans, iris scans, and voice recognition, amongst others. [ISM010.TXT]
Note: -
Linguistic specification: -
Cross-reference: Authentication (T040)

T042	**English term**: Password	**Grammatical Category**: Noun
Thai: รหัสผ่าน [ราชบัณฑิตยสถาน]		
Subject Field: Password		
Definition: รหัสผ่าน คือ ชุดอักษรผสมที่ผู้ใช้งานต้องเก็บไว้เป็นความลับส่วนตัว เป็นการพิสูจน์ตัวตนจากสิ่งที่ผู้ใช้งานคนนั้นรู้ เมื่อจะเข้าใช้ระบบ ผู้ใช้งานต้องใส่ชุดอักษรเหล่านี้เพื่อสามารถเข้าไปในระบบได้ รหัส่ผ่านเป็นเครื่องมือที่ใช้ในการพิสูจน์ตัวตนชนิดหนึ่ง		
Illustration: If a user has not changed the password within the time frame dictated by the password policy for maximum time that the password is valid, then this might be an indication that the user account is no longer being used. [ISM007.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Authentication (T040)		

T043	**English term**: Token	**Grammatical Category**: Noun
Thai: โทเก็น [ราชบัณฑิตยสถาน]		
Subject Field: Token		
Definition: เครื่องมือพกพาที่ใช้เทคนิคการโต้ตอบหรือเทคนิคอื่น ๆ มาใช้เพื่อพิสูจน์ตัวตนของผู้ใช้งานนี้ เป็นการพิสูจน์ตัวตนจากสิ่งที่ผู้ใช้งานคนนั้นมีหรือครอบครองไว้ โทเก็นเป็นเครื่องมือที่ใช้ในการพิสูจน์ตัวตนชนิดหนึ่ง		
Illustration: When Employee A starts the accounts payable application, the security token is created from the original security token created at logon, plus the additional information provided by the new policy. [ISM033.TXT]		
Note: -		

Linguistic specification: -
Cross-reference: Authentication (T040)

T044	**English term**: Public Key Infrastructure	**Grammatical Category**: Noun
Thai: โครงสร้างพื้นฐานกุญแจสาธารณะ [ผู้เชี่ยวชาญ]		
Subject Field: Public Key Infrastructure		
Definition: โครงสร้างพื้นฐานกุญแจสาธารณะนี้จะผูกกุญแจสาธารณะเข้าไว้กับตัวตนของผู้ใช้งาน และระบุรายละเอียดนั้นไว้ในใบรับรองดิจิทัลซึ่งจะต้องมีการเซ็นรับรองเอกสารจากผู้ประกอบการรับรองด้วย โครงสร้างพื้นฐานกุญแจสาธารณะเป็นวิธีการที่ใช้ในการพิสูจน์ตัวตนชนิดหนึ่ง		
Illustration: A smart card is a credit card sized plastic card with an embedded chip that can hold a digital certificate so user authentication is accomplished through a public key infrastructure. [ISM051.TXT]		
Note: -		
Linguistic specification: (ABRV) PKI [ISM050.TXT]		
Cross-reference: Authentication (T040)		

T045	**English term**: Digital Certificate	**Grammatical Category**: Noun
Thai: ใบรับรองดิจิทัล [ราชบัณฑิตยสถาน]		
Subject Field: Digital Certificate		
Definition: ใบรับรองที่ออกให้กับผู้ใช้งานคนนั้นเพื่อรับประกันว่า ผู้ใช้งานคนนั้น คือ คน ๆ นั้นจริง ๆ โดยในใบรับรองดิจิทัลประกอบไปด้วยข้อมูลของผู้ใช้งาน กุญแจสาธารณะที่เป็นของผู้ใช้งานคนนั้น วันหมดอายุ และลายมือชื่อดิจิทัลของผู้ประกอบการรับรองซึ่งเป็นผู้ที่ออกใบรับรองนั้น		
Illustration: Some banking institutions require that a user verifies his/her identity by validating identification credentials using a digital certificate. [ISM018.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Public Key Infrastructure (T044)		

T046	**English term:** Certification Authority	**Grammatical Category:** Noun
Thai: ผู้ประกอบการรับรอง [ราชบัณฑิตยสถาน]		
Subject Field: Certification Authority		
Definition: ผู้ประกอบการรับรองนั้นมีหน้าที่ออกใบรับรองดิจิทัล (Digital Certificate) และเซ็นรับรองว่า ผู้ที่ถือใบรับรองนั้นเป็นคน ๆ นั้นจริง ๆ		
Illustration: Signing Works Code signing is based on the use of a digital signature, which is in turn is based on a digital certificate issued by a trusted third party (a certification authority) that has verified the identity of the software or content publisher. [ISM014.TXT]		
Note: -		
Linguistic specification: (ABRV) CA [ISM085.TXT]		
Cross-reference: Public Key Infrastructure (T044)		

T047	**English term:** Asymmetric Cryptography	**Grammatical Category:** Noun
Thai: การเข้ารหัสแบบอสมมาตร [ราชบัณฑิตยสถาน]		
Subject Field: Asymmetric Cryptography		
Definition: วิธีการเข้ารหัสรูปแบบหนึ่งซึ่งใช้กุญแจสองชนิด คือ กุญแจสาธารณะและกุญแจส่วนตัวโดยจะใช้กุญแจสาธารณะในการเข้ารหัสและกุญแจส่วนตัวในการถอดรหัส		
Illustration: Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys—a public key and a private key. [ISM131.TXT]		
Note: -		
Linguistic specification: (SYN) Public-Key Cryptography [ISM041.TXT]		
Cross-reference: Cryptography (T036)		

T048	**English term:** Symmetric Cryptography	**Grammatical Category:** Noun
Thai: การเข้ารหัสแบบสมมาตร [ราชบัณฑิตยสถาน]		
Subject Field: Symmetric Cryptography		

Definition: การเข้ารหัสแบบสมมาตรนั้นเป็นวิธีการเข้ารหัสรูปแบบหนึ่งซึ่งใช้กุญแจเพียงชนิดเดียว คือ กุญแจส่วนตัวในการเข้ารหัสข้อมูลและถอดรหัสข้อมูล
Illustration: Conversely, secret key cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption. [ISM131.TXT]
Note: -
Linguistic specification: (SYN) Secret-Key Cryptography [ISM131.TXT]
Cross-reference: Cryptography (T036)

T049	**English term:** Public-Key Encryption	**Grammatical Category:** Noun
Thai: การเข้ารหัสกุญแจสาธารณะ [ราชบัณฑิตยสถาน]		
Subject Field: Public-Key Encryption		
Definition: การเข้ารหัสกุญแจสาธารณะนั้น จะใช้กุญแจสาธารณะในการเข้ารหัสข้อมูลและกุญแจส่วนตัว (Private Key) ที่เป็นคู่กันนั้นในการถอดรหัสข้อมูล การเข้ารหัสข้อมูลด้วยวิธีนี้จะช่วยรักษาความลับของข้อมูล		
Illustration: The main objectives for SSL are: Authenticating the client and server to each other: the SSL protocol supports the use of standard key cryptographic techniques (public key encryption) to authenticate the communicating parties to each other. [ISM065.TXT]		
Note: -		
Linguistic specification: (SYN) Asymmetric Encryption [ISM135.TXT]		
Cross-reference: Asymmetric Cryptography (T047)		

T050	**English term:** Encryption	**Grammatical Category:** Noun
Thai: การเข้ารหัสลับ [ราชบัณฑิตยสถาน]		
Subject Field: Encryption		
Definition: การเข้ารหัสลับ คือ กระบวนการที่แปลงข้อความปกติไปเป็นข้อความที่เป็นรหัสลับเพื่อป้องกันไม่ให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตและเป็นการป้องกันข้อมูลในระหว่างส่งไปที่คอมพิวเตอร์เครื่องอื่น		
Illustration: Encryption will be the next big thing for the majority of small and middle size companies as well as the adoption of various biometrics methods. [ISM050.TXT]		
Note: -		

Linguistic specification: -
Cross-reference: Asymmetric Cryptography (T047), Symmetric Cryptography (T048), Decryption (T052)

T051	**English term**: Ciphertext	**Grammatical Category**: Noun
Thai: ข้อความเข้ารหัส [ผู้เชี่ยวชาญ]		
Subject Field: Ciphertext		
Definition: ข้อความได้รับการเข้ารหัสเป็นที่เรียบร้อยแล้ว เป็นผลผลิตของกระบวนการเข้ารหัสลับ		
Illustration: The cryptography prevents the attacker from changing the data block (the plaintext) and also changing the checksum value (the ciphertext) to match. [ISM019.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Encryption (T050)		

T052	**English term**: Decryption	**Grammatical Category**: Noun
Thai: การถอดรหัสลับ [ราชบัณฑิตยสถาน]		
Subject Field: Decryption		
Definition: การถอดรหัสลับ คือ กระบวนการย้อนกลับของการเข้ารหัสลับ โดยการถอดรหัสลับนี้จะแปลงข้อความเข้ารหัสกลับไปเป็นข้อความที่อ่านออกได้อีกครั้งหนึ่งโดยผู้ที่ได้รับข้อความจะต้องมีกุญแจเพื่อถอดรหัสนี้ออกมา		
Illustration: Documents need to be encrypted and the decryption information needs to be documented and kept separate and offsite. [ISM069.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Asymmetric Cryptography (T047), Symmetric Cryptography (T048), Encryption (T050)		

T053	**English term**: Public Key	**Grammatical Category**: Noun
Thai: กุญแจสาธารณะ [ราชบัณฑิตยสถาน]		

Subject Field: Public Key
Definition: กุญแจที่ใช้เข้ารหัสข้อมูล สำหรับการเข้ารหัสแบบอสมมาตร โดยเจ้าของกุญแจจะต้องแจกจ่ายกุญแจสาธารณะนี้ไปยังคนที่ต้องการติดต่อ บุคคลเหล่านั้นก็จะใช้กุญแจนี้เข้ารหัสข้อมูลได้เพื่อส่งข้อมูลมายังเจ้าของได้ กุญแจคู่หนึ่งจะประกอบไปด้วยกุญแจสาธารณะที่สามารถแจกจ่ายให้ใครก็ได้ และกุญแจส่วนตัวที่เจ้าของนั้นจะต้องเก็บไว้เอง นอกจากนั้น กุญแจสาธารณะยังนำไปใช้ใส่เป็นรายละเอียดใบรับรองดิจิทัลโดยเพื่อยืนยันความน่าเชื่อถือ นอกเหนือไปกว่านั้น กุญแจสาธารณะยังสามารถนำไปใช้ตรวจสอบลายมือชื่อดิจิทัล (Digital Signature) ว่าเป็นลายเซ็นของคน ๆ ที่ส่งมาจริงหรือไม่
Illustration: The problem with public key encryption is the difficulty of knowing whether a public key is really owned by the person it is claimed to belong to. [ISM085.TXT]
Note: -
Linguistic specification: -
Cross-reference: Encryption (T050), Decryption (T052)

T054	**English term:** Private Key	**Grammatical Category:** Noun
Thai: กุญแจส่วนตัว [ราชบัณฑิตยสถาน]		
Subject Field: Private Key		
Definition: กุญแจที่ใช้ในการถอดรหัสข้อมูล สำหรับการเข้ารหัสแบบอสมมาตร ถ้าผู้ส่งต้องการถอดรหัสอีเมล์ของตน ผู้รับจะต้องนำกุญแจส่วนตัวของตนในการถอดรหัสข้อมูลนั้น กุญแจคู่หนึ่งจะประกอบไปด้วยกุญแจสาธารณะที่สามารถแจกจ่ายให้ใครก็ได้ และกุญแจส่วนตัวที่เจ้าของนั้นจะต้องเก็บไว้เอง นอกจากนั้น กุญแจส่วนตัวยังสามารถนำไปใช้เป็นลายมือชื่อดิจิทัล (Digital Signature) หรือใช้กุญแจส่วนตัวเซ็นรับรองข้อมูลว่า ข้อมูลนั้นส่งมาจากตนจริง ๆ		
Illustration: If the two digests match, you know that the public key is the one that matches the private key used to sign the code, and you know that the code hasn't been changed since it was signed. [ISM014.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Encryption (T050), Decryption (T052)		

T055	**English term:** Digital Signature	**Grammatical Category:** Noun
Thai: ลายมือชื่อดิจิทัล [ราชบัณฑิตยสถาน]		
Subject Field: Digital Signature		

Definition: ข้อความที่มีการเข็นด้วยกุญแจส่วนตัวของผู้ส่งเพื่อเป็นยืนยันว่า ผู้ที่ส่งนั้นเป็นผู้นั้นอย่างแท้จริงและเนื้อหาไม่โดนเปลี่ยนแปลงในระหว่างทางที่ส่ง โดยในการสร้างลายมือชื่อดิจิทัลนั้น ผู้ส่งจะต้องใช้กุญแจส่วนตัวของตนในการเข้ารหัสข้อมูล เมื่อข้อความถึงปลายทางแล้ว ผู้รับสามารถใช้กุญแจสาธารณะที่ผู้ส่งได้ให้ไว้ในการตรวจสอบ
Illustration: When a digital signature is compromised the user that suspects that the certificate is compromised should report the incident to the certificate authority. [ISM018.TXT]
Note: -
Linguistic specification: -
Cross-reference: Asymmetric Cryptography (T047)

T056	**English term:** Firewall	**Grammatical Category:** Noun
Thai: ไฟร์วอลล์, ด่านกันบุกรุก [ราชบัณฑิตยสถาน]		
Subject Field: Firewall		
Definition: เครื่องมือและซอฟต์แวร์ที่ทำหน้าที่เป็นด่านระหว่างระบบเครือข่าย 2 ระบบหรือระหว่างส่วนย่อยของระบบเครือข่าย 2 ส่วนด้วยกัน เป็นระบบที่ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้ามาในระบบได้		
Illustration: The big advantage of doing some of the spam filtering at the firewall is that it takes some of the processing load off the mail server. [ISM020.TXT]		
Note: -		
Linguistic specification: -		
Cross-reference: Network Security Control (T034)		

T057	**English term:** Intrusion Detection System	**Grammatical Category:** Noun
Thai: ระบบตรวจจับการบุกรุก [ผู้เชี่ยวชาญ]		
Subject Field: Intrusion Detection System		
Definition: ระบบป้องกันที่คอยตรวจสอบกิจกรรมผิดปกติที่อาจก่อให้เกิดผลร้ายต่อความปลอดภัยในระบบเครือข่ายและเมื่อตรวจเจอ ระบบก็จะส่งคำเตือนไปยังผู้บริหารระบบเครือข่าย ระบบจะตรวจสอบกิจกรรมที่ผิดปรกติในระบบเครือข่าย ทำให้ถึงแม้ว่าผู้บุกรุกระบบเจาะเข้ามาสำเร็จแล้ว ก็จะยังไม่สามารถกระทำการใดได้มาก เพราะระบบนี้ตรวจจับได้เสียก่อน		
Illustration: In the figure, there is a device indicated as an IDS (that stands for Intrusion Detection System), which under certain circumstances may operate in a standalone manner and re-configure a firewall with which		

it operates in conjunction. [ISM002.TXT]
Note: -
Linguistic specification: (ABRV) IDS [ISM039.TXT]
Cross-reference: Network Security Control (T034)