บทที่ 3
สถานภาพด้านความมั่นคงปลอดภัย ICT กรณีศึกษา

ด้านความมั่นคงปลอดภัยการป้องกันความมั่นคงปลอดภัยระบบสารสนเทศที่เป็นระบบและได้มาตรฐาน สถานภาพทิศทางการเปลี่ยนแปลงและสถานภาพด้านความมั่นคงปลอดภัย การใช้เทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย ที่ได้จากการรวบรวมผลสำรวจพบว่าในวันนี้องค์กรจำนวนมากภายในประเทศไทยต้องเผชิญกับภัยคุกคามต่อความมั่นคงปลอดภัยข้อมูลสารสนเทศ อาทิเช่น การโจมตีผ่านระบบอินเตอร์เน็ต (Internet Threat) โดย ไวรัส (Virus) สปายแวร์ (Spy Ware) โทรจัน (Trojan) เป็นต้น การวิเคราะห์สถานภาพด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของประเทศไทยจะออกเป็น 3 ส่วน ดังนี้

1. กระบวนการ (Process)
2. บุคคลและองค์กร (People)
3. เทคโนโลยี (Technology)

ผลการสำรวจสถานภาพด้านความมั่นคงปลอดภัยของประเทศไทยที่ประกอบด้วย การสำรวจสัมภาษณ์และจัดทำแบบสอบถามกลุ่มหน่วยงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรและด้านสถานภาพนโยบายความมั่นคงปลอดภัยของเครือข่ายสำหรับประเทศไทยในการรักษาความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต

ส่วนการวิเคราะห์สถานภาพด้านความมั่นคงปลอดภัยการใช้เทคโนโลยีสารสนเทศและการสื่อสารของต่างประเทศประกอบด้วย ประเทศสหรัฐอเมริกา ประเทศออสเตรเลีย ประเทศสิงคโปร์ การศึกษาสถานภาพของแต่ละประเทศจะประกอบด้วยหัวข้อ ดังนี้

1. ด้านนโยบายและการบริหารจัดการ (Process)
2. ด้านการควบคุมและการปฏิบัติงานตามนโยบาย (People)
3. ด้านเทคโนโลยี (Technology)

3.1 สถานภาพด้านความมั่นคงปลอดภัย การใช้เทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย

3.1.1 กระบวนการ (Process)

กระบวนการที่เกี่ยวข้องกับมาตรการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร เช่น ด้านกฎหมาย แผนแม่บท โครงการและนโยบายที่เกี่ยวกับ ICT Security ประกอบด้วย

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

1. ด้านกฎหมาย

มีการออกกฎข้อบังคับและกฎหมายทางด้าน ICT Security ที่ถูกนำมาใช้ปฏิบัติ (Regulatory Compliance) กฎหมายของประเทศไทยที่เกี่ยวข้องกับมาตรการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งที่ออกบังคับใช้แล้ว และที่กำลังดำเนินการ รวมทั้งแสดงรายละเอียดความจำเป็นทางด้านสถานภาพด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศและการทำธุรกรรมอิเล็กทรอนิกส์ที่ทำให้ต้องมี IT Control Laws มารองรับ

ลำดับ	ชื่อกฎหมาย	สาระสำคัญ/ความจำเป็น
1	พระราชกฤษฎีกากำหนดธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549 ประกาศราชกิจจานุเบกษาเมื่อวันที่ 20 มีนาคม 2549	เพื่อกำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาบังคับใช้ ปัจจุบันแม้ว่าพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้บัญญัติรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ให้เท่าเทียมกับธุรกรรมที่ทำลงบนกระดาษและการลงลายมือชื่อด้วยมือไว้แล้วก็ตาม แต่เนื่องจากการทำธุรกรรมบางประเภท ยังไม่สมควรให้กระทำได้ด้วยวิธีการทางอิเล็กทรอนิกส์กล่าวคือมิให้นำนิติกรรมใดๆ เกี่ยวกับสิทธิในครอบครัว เช่น การให้ความยินยอมการสมรส หรือ การทำสัญญาระหว่างสมรสกับนิติกรรมใด เกี่ยวกับมรดก เช่นการทำสัญญาประนีประนอม ยอมความสละมรดกหรือการทำพินัยกรรมแบบธรรมดา มาใช้รูปแบบทางอิเล็กทรอนิกส์ซึ่งทั้งสองเรื่องมีความละเอียดอ่อนและเกี่ยวข้องกับความสงบเรียบร้อยของประชาชน นอกจากนั้นยังอาจมีปัญหาทางความเชื่อมั่น ในการรับรองสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์อีกด้วย

DRAFT

ลำดับ	ชื่อกฎหมาย	สาระสำคัญ/ความจำเป็น
2	ร่างพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.	เพื่อกำหนดมาตรการทางอาญาในการลงโทษผู้กระทำผิดต่อระบบการทำงานทางคอมพิวเตอร์ ระบบข้อมูลและระบบเครือข่ายซึ่งในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายฉบับใดกำหนดว่าเป็นความผิด
3	ร่างพระราชบัญญัติว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์	การโอนเงินทางอิเล็กทรอนิกส์เป็นวิธีการโอนเงินที่สะดวก รวดเร็ว ปลอดภัยและประหยัด เป็นผลให้การโอนเงินด้วยวิธีนี้มีความแพร่หลายในปัจจุบัน โดยเฉพาะในภาคธุรกิจ เพื่อเพิ่มประสิทธิภาพในการดำเนินกิจการ อย่างไรก็ตามประเทศไทยยังไม่มีกฎหมายที่เกี่ยวกับเรื่องนี้โดยตรง ทำให้ขาดความชัดเจนแน่นอนในเรื่องของสิทธิ หน้าที่และความรับผิดระหว่างบุคคลที่เกี่ยวข้องกับการโอนเงินดังกล่าว ดังนั้น เพื่อเป็นการรองรับความต้องการที่เพิ่มมากขึ้นและเป็นการรองรับความก้าวหน้าทางเทคโนโลยีสารสนเทศเพื่อให้ความสัมพันธ์ของคู่กรณีในการโอนเงินทางอิเล็กทรอนิกส์มีความชัดเจนแน่นอน อันจะเป็นการสร้างความเชื่อมั่นในการดำเนินการธุรกิจและส่งเสริมเศรษฐกิจของประเทศ และเพื่อคุ้มครองคู่กรณีที่เป็นผู้บริโภคซึ่งโดยทั่วไปมีความอ่อนด้อยในการรักษาสิทธิของตนในความสัมพันธ์ดังกล่าว จึงจำเป็นต้องมีการตรากฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ขึ้นใช้บังคับ เพื่อใช้เป็นกฎเกณฑ์ในการวางระเบียบให้เป็นมาตรฐานเดียวกัน

DRAFT

ลำดับ	ชื่อกฎหมาย	สาระสำคัญ/ความจำเป็น
4	ร่างพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ	โดยที่ประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ เป็นเหตุให้มีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น ทั้งในการดำเนินงาน กิจกรรมภายในหน่วยงาน ทั้งกับหน่วยงานภายนอกหรือกับประชาชนในรูปแบบต่างๆ ในขณะที่หน่วยงานภาครัฐเอง ยังไม่พร้อมทางด้านบุคคลากร ด้านเทคโนโลยี ด้านระเบียบ และด้านความมั่นคงปลอดภัย อันอาจเป็นปัญหาอุปสรรคสำคัญที่ส่งผลกระทบต่อความเชื่อมั่นในการดำเนินกิจกรรมใดๆของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ดังนั้นเพื่อให้หน่วยงานของรัฐดำเนินการกิจกรรมใดด้วยวิธีการทางอิเล็กทรอนิกส์ภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน
5	ร่างกฎหมายประกอบร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์	โดยเหตุที่มีความจำเป็นต้องแก้ไขกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ให้สอดคล้องกับการปรับปรุงโครงสร้างระบบราชการตามพระราชบัญญัติปรับปรุง กระทรวง ทบวง กรม พ.ศ. 2545 ที่กำหนดให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานที่มีอำนาจหน้าที่เกี่ยวกับการวางแผน ส่งเสริม พัฒนา และดำเนินกิจการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร
6	ร่างพระราชกฤษฎีกาว่าด้วยการกำกับดูแลให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority หรือ CA)	เพื่อตรวจสอบความเปลี่ยนแปลงหรือการแก้ไขข้อมูลอิเล็กทรอนิกส์โดยมิชอบนั้นได้ด้วย และโดยที่สามารถประยุกต์ใช้ใบรับรองอิเล็กทรอนิกส์ได้ค่อนข้างหลากหลาย อันรวมถึงการทำธุรกรรมทางการเงินด้วย ประกอบกับการให้บริการนั้นผู้ให้บริการจำเป็นต้องปฏิบัติ

DRAFT

ลำดับ	ชื่อกฎหมาย	สาระสำคัญ/ความจำเป็น
		ตามแนวนโยบาย หรือปรับใช้มาตรฐานสากลจำนวนมากในการให้บริการ
7	ร่างพระราชบัญญัติว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศ	เพื่อทำหน้าที่ในการวางแผนส่งเสริมและพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ รวมถึงภารกิจในการพัฒนากฎหมายที่เกี่ยวข้อง ประกอบกับมาตรา 57 แห่งพระราชบัญญัติฉบับเดียวกันได้กำหนดให้มีการจัดตั้งสำนักงานส่งเสริมเทคโนโลยีสารสนเทศและการสื่อสาร ขึ้นภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารภายใน 1 ปี นับจากพระราชบัญญัติมีผลบังคับใช้ โดยภารกิจของทั้งสองสำนักงานนั้นเป็นไปในทำนองเดียวกันกับสำนักโครงสร้างพื้นฐานสารสนเทศแห่งชาติตามความร่างพระราชบัญญัติที่กล่าวข้างต้น

DRAFT

2. แผนแม่บทเทคโนโลยีสารสนเทศแห่งชาติ IT2010

การจัดทำกรอบนโยบายเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็นการให้ความสำคัญกับบทบาทของเทคโนโลยีสารสนเทศ โดย IT2010 นั้นจะเน้นการพัฒนาด้านเทคโนโลยีสารสนเทศใน 5 สาขา มีดังนี้

1. การพัฒนาเทคโนโลยีสารสนเทศในภาครัฐ (e-Government)
2. การพัฒนาเทคโนโลยีสารสนเทศในภาคพาณิชย์ (e-Commerce)
3. การพัฒนาเทคโนโลยีสารสนเทศในอุตสาหกรรม (e-Industry)
4. การพัฒนาเทคโนโลยีสารสนเทศในภาคการศึกษา (e-Education)
5. การพัฒนาเทคโนโลยีสารสนเทศในภาคสังคม (e-Society)

โดยมีเป้าหมายกลยุทธ์การพัฒนาทั้ง 5 สาขา สรุปในแต่ละสาขา มีดังนี้

1. การพัฒนาเทคโนโลยีสารสนเทศในภาครัฐ (e-Government)

เป็นการพัฒนาเทคโนโลยีสารสนเทศในภาครัฐทั้งการบริหารราชการ ที่ประกอบด้วยส่วนกลาง ส่วนภูมิภาค และส่วนท้องถิ่น เพื่อนำไปสู่การบริหารประเทศและสังคม โดยมีการพัฒนาระบบงาน 2 ระบบ คือ

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

- พัฒนาระบบบริหาร (Back Office) ประกอบด้วยงานสารบรรณ งานพัสดุ งานบุคคล งานการเงินและบัญชี และงานงบประมาณโดยใช้เทคโนโลยีสารสนเทศอย่างครบวงจรใน พ.ศ. 2547
- พัฒนาระบบบริการ (Front Office) ที่ครอบคลุมตามลักษณะงานของหน่วยต่างๆ โดยใช้ระบบอิเล็กทรอนิกส์ได้ร้อยละ 70 ใน พ.ศ. 2548 และครบทุกขั้นตอนใน พ.ศ. 2553

2. การพัฒนาเทคโนโลยีสารสนเทศในภาคพาณิชย์ (e-Commerce)

เป็นการเสริมสร้างขีดความสามารถในการแข่งขันของผู้ประกอบการไทยโดยใช้พาณิชย์อิเล็กทรอนิกส์เป็นเครื่องมือสำคัญเพื่อประกอบธุรกิจ และเป็นยุทธศาสตร์ที่สำคัญในการพัฒนาการให้บริการผ่านสื่ออิเล็กทรอนิกส์ของการพัฒนาระบบ เพื่อรองรับธุรกรรมอิเล็กทรอนิกส์ การจัดทำฐานข้อมูลเพื่อการบริการ

3. การพัฒนาเทคโนโลยีสารสนเทศในอุตสาหกรรม (e-Industry)

การส่งเสริมและพัฒนาการใช้และการผลิตเทคโนโลยีสารสนเทศในภาคเอกชนภายใน พ.ศ. 2553 โดยมียุทธศาสตร์หลัก คือ การสร้างตลาดกลางสินค้าอุตสาหกรรมผ่านศูนย์ธุรกรรมการซื้อขายผ่านอินเตอร์เน็ตในรูปแบบของ B2B (Business to Business) แบบออนไลน์ การจัดตั้งศูนย์ข้อมูลการตลาดเพื่อบริการข้อมูลอุปสงค์และอุปทานสินค้าและบริการ สนับสนุนการใช้เทคโนโลยีสารสนเทศเพื่อพัฒนาอุตสาหกรรมขนาดกลาง ขนาดย่อม และการพัฒนาภาคการเกษตรและอุตสาหกรรมการเกษตร

4. การพัฒนาเทคโนโลยีสารสนเทศในภาคการศึกษา (e-Education)

เป็นการพัฒนาและเตรียมพร้อมด้านทรัพยากรมนุษย์ โดยสร้างระบบบริหารจัดการร่วมกัน การพัฒนาโครงสร้างพื้นฐานเพื่อการศึกษา การพัฒนาสื่อการเรียนการสอน

5. การพัฒนาเทคโนโลยีสารสนเทศในภาคสังคม (e-Society)

เป็นการลดความเหลื่อมล้ำในการเข้าถึงสารสนเทศและความรู้ของสังคม โดยพัฒนาโครงสร้างพื้นฐานให้ทั่วถึง พัฒนาความรู้และทักษะด้านเทคโนโลยีสารสนเทศ

3.1.2 บุคคลและองค์กร (People)

โครงสร้างพื้นฐานสำคัญ และโครงสร้างพื้นฐานด้านอื่นๆ องค์กรต่างๆ ที่มีการจัดทำโครงสร้างพื้นฐานที่มีความสำคัญกับการปรับโครงสร้างด้าน ICT ของประเทศไทย มีดังนี้

- แผนแม่บทเทคโนโลยีสารสนเทศแห่งชาติ IT2010 แผนแม่บทเทคโนโลยีสารสนเทศแห่งชาติ ฉบับที่ 1 IT2005

DRAFT

- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติที่กล่าวถึงการส่งเสริมการประยุกต์ใช้ ICT หรือโครงการ SchoolNet
- โครงการจัดตั้งศูนย์พัฒนาพาณิชย์อิเล็กทรอนิกส์
- โครงการจัดตั้งสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ
- โครงการจัดตั้งศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย
- โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ

การมีหน่วยงานกลางที่ทำหน้าที่ในการควบคุมองค์กรที่อยู่ในความรับผิดชอบ เช่น ธนาคารแห่งประเทศไทยควบคุมธนาคารพาณิชย์ หรือ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ควบคุม บริษัทหลักทรัพย์ เป็นต้น ซึ่งองค์กรที่อยู่ภายใต้การควบคุมมีความจำเป็นต้อง “ผ่าน” มาตรฐานและกฎเกณฑ์ต่างๆ ตามที่กำหนด

จากกระบวนการด้านกฎหมาย แผนแม่บทและโครงการต่างๆ ที่เกิดขึ้นต่อไปนี้จำเป็นต้องมีหน่วยงานหลักที่เกี่ยวกับสถานภาพเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัย มีดังนี้

1. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร งานส่งเสริมเทคโนโลยีสารสนเทศและการสื่อสาร งานวิจัยและพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร
2. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจะมีการแก้ไขเพิ่มเติมกฎหมายที่เกี่ยวข้องเพื่อให้มีการจัดตั้งสำนักงานคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เลขาธิการสำนักงานและเพิ่มอำนาจหน้าที่คณะกรรมการเกี่ยวกับการบริหารสำนักงาน
3. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค)
4. ธนาคารแห่งประเทศไทยจะมีส่วนร่วมที่สำคัญที่จะต้องกำกับดูแลเกี่ยวกับบริการชำระเงินทางอิเล็กทรอนิกส์ ทั้งในภาคสถาบันการเงินและในภาคเอกชน รวมทั้งนิติบุคคล
5. สำนักงานสภาความมั่นคงแห่งชาติ ซึ่งต้องมีหน้าที่ดูแลเรื่องความมั่นคงปลอดภัยด้านทรัพยากร วิกฤติของประเทศ (Critical Infrastructure) และภาวะฉุกเฉินต่างๆ
6. สำนักงานตำรวจแห่งชาติ
7. สำนักงานป้องกันและปราบปรามการฟอกเงิน
8. สำนักงานอัยการสูงสุด

3.1.3 เทคโนโลยี (Technology)

(เป็นการสรุปจาก มาตรฐาน ISO/IEC 17799:2000 Version 1 , ISO/IEC 17799:2005Version 2 ของประเทศไทย)

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

1. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (มาตรฐานISO/IEC17799:2000 เวอร์ชั่น 1)โดยคณะอนุกรรมการด้านความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 คณะอนุกรรมการด้านความมั่งคง มีหน้าที่หลัก 5 ประการคือ

1. เสนอแนะนโยบายและมาตรการด้านความมั่นคงให้เกิดความเชื่อมั่นและปลอดภัยในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของประเทศในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
2. ติดตามวิเคราะห์กลั่นกรองและเผยแพร่ข้อมูลที่เกี่ยวกับความมั่นคงของธุรกรรมทางอิเล็กทรอนิกส์ให้แก่หน่วยงานภาครัฐ ภาคธุรกิจและประชาชน
3. สร้างความตื่นตัวเพื่อให้ภาคเอกชนหรือประชาชนตระหนักถึงความสำคัญของความมั่นคงในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
4. ดำเนินการหรือประสานงานกับหน่วยงานอื่นๆ ในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรในด้านดังกล่าว
5. ร่วมมือหรือประสานงานในการดำเนินการตามข้อ 1 ถึงข้อ 4 กับต่างประเทศ หรือองค์การระหว่างประเทศปฏิบัติการอื่นใดตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมาย

มาตรฐานนี้จึงเป็นหนึ่งในภารกิจที่คณะอนุกรรมการด้านความมั่นคงได้จัดทำขึ้นโดยมีวัตถุประสงค์ในเบื้องต้น ดังนี้

1. เป็นแนวทางศึกษาการดำเนินการให้เกิดความมั่นคงปลอดภัยในการประกอบธุรกรรม ทางอิเล็กทรอนิกส์ ซึ่งมาตรฐานดังกล่าวอ้างอิงจากมาตรฐานสากล ISO 17799 / IEC 17799 : 2000 และมาตรฐานที่ใช้ในประเทศสหรัฐอเมริกา NIST (National Institute of Standards and Technology) Special Publication800-52 และมาตรฐานที่ประเทศออสเตรเลีย นิวซีแลนด์ AS/NZS (BS) 7799 ซึ่งครอบคลุม Information Security Management System (ISMS)
2. เพื่อเป็นแนวทางเสริมสร้างการรักษาความมั่นคงปลอดภัยให้กับองค์กรหรือหน่วยงานที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์โดยเริ่มต้นจากการสร้างความมั่นปลอดภัยให้กับองค์กรในระดับพื้นฐาน และเมื่อองค์กรมีความพร้อมในระดับเบื้องต้นจึงได้ก้าวขึ้นสู่ระดับกลาง และสูงเพื่อองค์กรจะได้มีความมั่นคงปลอดภัยมากยิ่งขึ้นและเป็นพื้นฐานไปสู่การได้รับมาตร

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

ฐานในระดับสากลต่อไปซึ่งปัจจุบันได้มีองค์กรหรือหน่วยงานที่มีความตระหนักในด้านความมั่นคงปลอดภัยได้ก้าวล้ำไปสู่กระบวนการสร้างความมั่นคงปลอดภัยให้กับองค์กรในระดับ Best Practice แล้ว

สำหรับองค์กรเหล่านั้นไม่จำเป็นต้องกลับมาเริ่มต้นดำเนินการตามแนวทางแห่งมาตรฐานนี้สำหรับองค์ประกอบของมาตรฐานนี้ประกอบด้วยสิ่งจำเป็นสำหรับการเริ่มต้นสร้างมาตรฐานความมั่นคงปลอดภัยให้กับองค์กรในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งแบ่งเป็น 10 หัวข้อ ดังนี้

1. นโยบายความมั่นคงปลอดภัยขององค์กร
2. โครงสร้างความมั่นคงปลอดภัยภายในองค์กร
3. การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร
4. มาตรฐานของบุคลากรเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร
5. ความมั่นคงปลอดภัยทางด้านกายภาพและสิงแวดล้อมขององค์กร
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
7. การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร
8. การพัฒนาและดูแลระบบสารสนเทศ
9. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
10. การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบาย

โดยในแต่ละหัวข้อจะระบุวัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องกับหัวข้อและมีข้อปฏิบัติ แยกตามวัตถุประสงค์ในแต่ละหัวข้อ เพื่อให้องค์กรเริ่มต้นทำความเข้าใจกับแนวทางปฏิบัติเหล่านี้ คณะอนุกรรมการฯ จึงแบ่งระดับความอยากง่ายในการเริ่มต้นสร้างความมั่นคงปลอดภัยให้กับองค์กรเป็น 3 ระดับ โดยพิจารณาจากความจำเป็นเบื้องต้นในการสร้างความมั่นคงปลอดภัยเกี่ยวกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์ และได้ให้ความหมายของแต่ละระดับไว้ดังนี้

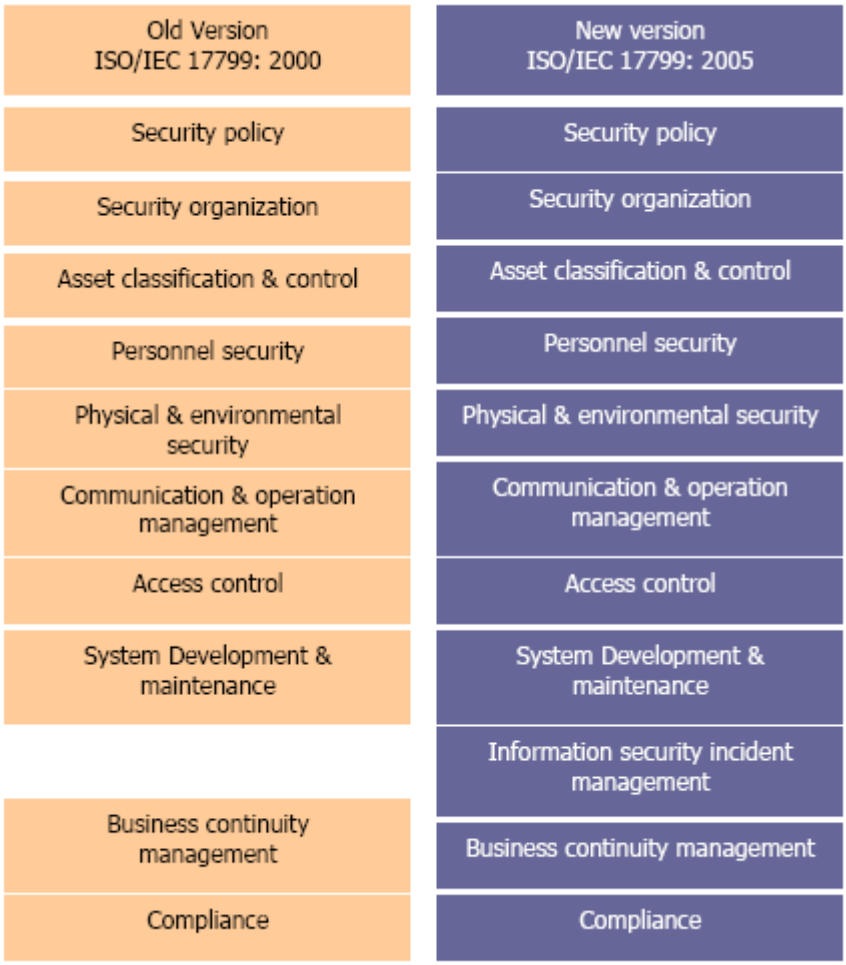
- ความมั่นคงปลอดภัยพื้นฐาน หมายถึง หัวข้อปฏิบัติที่คณะอนุกรรมการฯ ได้พิจารณาแล้วและเห็นว่าเหมาะสมกับองค์กรที่ต้องการระดับความมั่นคงปลอดภัยพื้นฐาน
- ความมั่นคงปลอดภัยปานกลาง หมายถึง หัวข้อปฏิบัติที่คณะอนุกรรมการฯ ได้พิจารณาแล้วและเห็นว่าเหมาะสมกับองค์กรที่ต้องการระดับความมั่นคงปลอดภัยปานกลาง

DRAFT

- ความมั่นคงปลอดภัยสูง หมายถึง หัวข้อปฏิบัติที่คณะอนุกรรมการฯ ได้พิจารณาแล้วและเห็นว่าเหมาะสมกับองค์กรที่ต้องการระดับความมั่นคงปลอดภัยสูง

2. มาตรฐาน ISO/IEC 17799:2005 (เวอร์ชั่น 2)

มาตรฐาน ISO/IEC 17799:2005 เป็นการปรับปรุงมาจากมาตรฐาน ISO/IEC 17799:2000 เพื่อให้ทันสมัยมากยิ่งขึ้นโดยให้ความสำคัญต่อประเด็นการตอบรับเหตุการณ์ละเมิดความมั่นคงปลอดภัย ประเด็นเทคโนโลยีที่เปลี่ยนแปลง และประเด็นการเสริมสร้างความมั่นคงปลอดภัยให้กับกระบวนการทางธุรกิจมากยิ่งขึ้น เนื้อหาและประเด็นที่เปลี่ยนแปลงไปจากมาตรฐาน ISO/IEC 17799:2000 มาตรฐานฉบับเดิมสรุปเป็นแผนภาพได้ดังนี้



รูปที่ 3.1 แสดงหัวข้อในมาตรฐานการรักษาความมั่นคงปลอดภัย ฉบับสากลเปรียบเทียบระหว่าง ISO/IEC 17799:2000 กับ ISO/IEC 17799:2005

DRAFT

จากรูปที่ 3.1 แสดงถึงจำนวนหัวข้อหลักด้านความมั่นคงปลอดภัย (Security Domain) สำหรับเวอร์ชันเดิมปี ค.ศ. 2000 (ทางซ้ายมือ) ทั้งหมด 10 หัวข้อ และสำหรับเวอร์ชั่นใหม่ปี ค.ศ. 2005 ทั้งหมด 11 หัวข้อ โดยมีหัวข้อที่เพิ่มขึ้นมาใหม่คือ หัวข้อ Information Security Incident Management



รูปที่ 3.2 แสดงการเปรียบเทียบจำนวนมาตรการ (Control) และวัตถุประสงค์ของมาตรการความมั่นคงปลอดภัย (Control Objective) ระหว่างมาตรฐาน ISO/IEC 17799:2000 (เวอร์ชั่นเดิม) กับ ISO/IEC 17799:2005 (เวอร์ชั่นใหม่)

รูปที่ 3.2 แสดงให้เห็นถึงจำนวนมาตรการความมั่นคงปลอดภัยที่คงเดิมไว้ 116 ข้อ มาตรการในเวอร์ชั่นเดิมได้ถูกตัดทิ้งไป จำนวน 9 ข้อ และในเวอร์ชันใหม่มีมาตรการเพิ่มจำนวน 17 ข้อ มีวัตถุประสงค์ของมาตรการความมั่นคงปลอดภัยใหม่จำนวน 8 ข้อ และมีวัตถุประสงค์ของมาตรการความมั่นคงปลอดภัยเดิมจำนวน 5 ข้อ ที่ได้รับการแก้ไขโดยถูกนำไปรวมกับวัตถุประสงค์ของมาตรการความมั่นคง

มาตรฐานความมั่นคงปลอดภัยให้กับองค์กรในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ มาตรฐาน ISO/IEC 17799:2005 ซึ่งแบ่งเป็น 11 หัวข้อ ดังนี้

1. นโยบายความมั่นคงปลอดภัย (Security policy)
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)
3. การบริการจัดการทรัพย์สินขององค์กร (Asset Management)
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management)
7. การควบคุมการเข้าถึง (Access control)
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems acquisition, development and maintenance)
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)
10. การความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)
11. การปฏิบัติตามข้อกำหนด (Compliance) ข้อกำหนดทางกฎหมาย นโยบาย ข้อกำหนดทางเทคนิค และการตรวจประเมินระบบสารสนเทศ

ถึงแม้ว่าการนำมาตรฐาน ISO/IEC 17799 มาประยุกต์ใช้กับองค์กร ไม่จำเป็นต้องได้รับการรับรองมาตรฐาน BS7799 จาก Certification Body แต่องค์กรที่ต้องการความน่าเชื่อถือและการยอมรับจากคู่ค้าในระดับมาตรฐานโลกก็อาจจะต้องผ่านกระบวนการเตรียมการและการตรวจสอบ ซึ่งในประเทศไทยมีเพียงไม่กี่องค์กรที่ได้รับรองมาตรฐาน BS7799 ส่วนที่2 (part 2)

สำหรับ IT Control Framework ที่สามารถนำมาอ้างอิงและประยุกต์การใช้งานร่วมกับมาตรฐานดังกล่าวได้แก่ COBIT Framework (Control Objectives for Information and Related Technology) และ COSO Framework ซึ่งเป็นมาตรฐานที่ธนาคารพาณิชย์ และ บริษัทหลักทรัพย์นิยมนำมาใช้อ้างอิง สำหรับ COSO Framework นั้นประกอบด้วย 5 หัวข้อหลัก ได้แก่ Control Environment, Risk Assessment, Control Activities, Information and Communication และ Monitoring

3.2 ผลการสำรวจสถานภาพด้านความมั่นคงปลอดภัยของประเทศไทย

3.2.1 การสำรวจสัมภาษณ์กลุ่มหน่วยงานด้านความมั่นคงปลอดภัย

ผลการสำรวจข้อมูลด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรกลุ่มด้านความมั่นคงปลอดภัยจากข้อมูลการสำรวจสัมภาษณ์และแบบสอบถาม มีดังนี้

1. ด้านประสบการณ์ความมั่นคงปลอดภัยขององค์กร (Security Experience) ทุกหน่วยงานประสบกับความเสี่ยงต่อการรักษาความมั่นคงปลอดภัยสารสนเทศในองค์กร โดยมีการโจมตีจากภายนอกหรือผู้ไม่ประสงค์ดีในการพยายามเข้าสู่ระบบ และการโจมตีจากไวรัสที่มีผล

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

กระทบต่อการทำงานของหน่วยงาน ดังนั้นหน่วยงานจะต้องมีมาตรการด้านความมั่นคงปลอดภัยขององค์กร

2. ด้านนโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy) ผลการสำรวจพบว่าองค์กรส่วนใหญ่ มีการจัดทำเอกสารนโยบายความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร (Information Security Policy Document) รวมทั้งมีการเผยแพร่ให้พนักงานได้รับทราบในรูปแบบต่างๆ อาทิ หนังสือเวียน, เผยแพร่บน Internet/Intranet, จัดพิมพ์เป็นรูปเล่ม แต่ในแง่ความมั่นคงปลอดภัยนั้นถึงแม้จะมีการจัดทำนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร แต่ก็ไม่ได้แบ่งเป็นไปตามทางที่เป็นมาตรฐาน นอกจากนั้นยังไม่ได้มีการนำไปปฏิบัติอย่างเป็นระบบ
3. ด้านความมั่นคงปลอดภัยภายในและระหว่างองค์กร หน่วยงานส่วนใหญ่จะมีบุคลากรหรือกลุ่มงานที่ได้รับมอบหมายให้จัดการดูแลด้านความมั่นคงปลอดภัยของระบบงานเท่านั้น แต่เรื่องความมั่นคงปลอดภัยภายในองค์กรและระหว่างองค์กรนี้เป็นเรื่องที่องค์กรต่างๆ ต้องมีการดูแลโดยฝ่ายเครือข่าย และฝ่ายบริหารระบบ ซึ่งบุคลากรของหน่วยงานมีระดับความเข้าใจในเรื่องเทคโนโลยีการรักษาความมั่นคงปลอดภัยนั้นยังมีในระดับต่ำ
4. ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร ผลการสำรวจพบว่าองค์กรหรือหน่วยงานส่วนใหญ่ มีการอบรมและวางแผนสำหรับการจัดหลักสูตรด้านความมั่นคงปลอดภัยให้แก่พนักงาน โดยส่วนมากเน้นหนักไปที่เจ้าหน้าที่ผู้รับผิดชอบด้าน ICT เป็นหลัก หลายองค์กรเรียกร้องให้มีการจัดการเกี่ยวกับค่าฝึกอบรม ซึ่งมีค่าใช้จ่ายต่อหัวที่สูงมากจากทางบริษัทเจ้าของผลิตภัณฑ์ ถึงแม้ข้อมูลความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากรในเบื้องต้นที่ได้นั้นระบุว่ามีการฝึกอบรมในระบบความมั่นคงปลอดภัยแต่ข้อเท็จจริงมีว่า ทั้งหมดเป็นการไปเข้าฟังการสัมมนา ซึ่งไม่ได้มีการฝึกอบรมอย่างเป็นระบบ
5. ด้านความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อมขององค์กร ในทุกหน่วยงานมีการดำเนินการเรื่อง Access Control ที่มีการนำ Technology ในด้านการตรวจสอบลายนิ้วมือ และ การตรวจสอบบัตรในการควบคุมการผ่านเข้าออกซึ่งไม่มีปัญหาแต่อย่างไร แต่ก็ยังขาดกระบวนการในเรื่องการบริหารจัดการสิทธิและติดตามรายงานการเข้าใช้อย่างเป็นระบบ
6. ด้านการบริหารจัดการการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร ผลการสำรวจพบว่าทุกองค์กรในกลุ่มตัวอย่าง มีการติดตั้งอุปกรณ์บริหารป้องกันและจัดการความมั่นคงปลอดภัยบนเครือข่าย การสำรองข้อมูล หรือ Backup รวมทั้งมีการมีการติดตั้งซอฟท์แวร์ป้องกันไวรัส หนอนซึ่งส่วนมากได้ติดตั้งมาพร้อมกับเครื่องที่จัดซื้อ ในเรื่องของการทำพาณิชย์อิเล็กทรอนิกส์ มีเพียงส่วนน้อยที่มีการจัดทำระบบพาณิชย์อิเล็กทรอนิกส์ นอกจากนี้องค์กรส่วนใหญ่เรียกร้องให้มีการกำหนด ROOT CA กลางรวมถึงการจัดการด้าน

DRAFT

PKI จากองค์กรกลางผู้รับผิดชอบ อย่างไรก็ตามบางหน่วยงานมีความกังวลถึงผลกระทบต่อการใช้ ROOT CA จากองค์กรกลางกับการทำงานร่วมกับ CA ที่องค์กรหรือหน่วยงานมีอยู่ ดังนั้นเรื่องการดูแลระบบและเครื่องให้มีความมั่นคงปลอดภัยนั้น เป็นเรื่องที่จะต้องมีความเข้าใจเป็นเบื้องต้นและได้มีการปฏิบัติบ้าง แต่ยังขาดการประยุกต์แนวทางที่กำหนดเป็นมาตรฐาน ในส่วนที่เกี่ยวกับธุรกรรมอิเล็กทรอนิกส์ ก็ไม่ได้มีความพยายามอย่างจริงจังในด้านนี้ เนื่องจากติดขัดที่กฎหมายและการประสานงานกับหน่วยงานอื่น

7. ด้านการควบคุมการเข้าถึง การสำรวจพบว่าทุกองค์กรหรือหน่วยงานที่สำรวจ มีการควบคุมการเข้าถึงระบบสารสนเทศภายในองค์กร โดยมีการกำหนดสิทธิตามระดับการใช้งาน มีการกำหนด User/Password ให้กับผู้ใช้ ซึ่งหน่วยงานมีความเข้าใจและมีแนวทางในการดำเนินการแต่ยังขาดกระบวนการที่เป็นมาตรฐานสากล โดยเฉพาะอย่างยิ่งในการควบคุมการเข้าถึงข้อมูลโดยอาศัยสถาปัตยกรรมข้อมูลที่มั่นคง
8. ด้านการพัฒนาและดูแลระบบสารสนเทศ องค์กรยังไม่มีความเข้าใจเรื่องการใช้สถาปัตยกรรมซอฟต์แวร์ที่มีความมั่นคงในแนวทางของ Web Service และการพัฒนาซอฟต์แวร์ที่ตรวจสอบได้ เช่น ไม่มีการทำ Code Audit เป็นต้น
9. ด้านการบริหารความต่อเนื่องของการดำเนินงานขององค์กร ผลการสำรวจพบว่าทุกองค์กรหรือหน่วยงานที่สำรวจมีการจัดทำแผนสร้างความต่อเนื่อง (Business Continuity Plan) ตามข้อกำหนดของ สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) แต่ ยังขาดการประเมินและปรับปรุงแผนและการนำแผนมาทดสอบใช้งาน ดังนั้นการบริหารความต่อเนื่องของการดำเนินงานจะต้องมีการจัดทำแผนในเรื่องนี้ แต่การดำเนินการยังอยู่ในขั้นเริ่มต้น นอกจากนี้ยังไม่มีการวางแผนฉุกเฉินของหน่วยงาน และการฝึกอบรมเชิงปฏิบัติการเพื่อเตรียมความพร้อม
10. ด้านข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร ในหลายองค์กรหรือหน่วยงานไม่มีข้อกำหนดและบทลงโทษโดยเฉพาะสำหรับการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร ซึ่งในปัจจุบันมีเพียงข้อบังคับตามระเบียบข้าราชการซึ่งไม่สามารถครอบคลุมการทำผิดในลักษณะนี้โดยตรงได้ และมีเพียงส่วนน้อยที่มีการควบคุมลิขสิทธิ์ทรัพย์สินทางปัญญาอย่างถูกต้อง ซึ่งในส่วนนี้ต้องการงบประมาณในการแก้ไขปัญหา มีหลายองค์กรหรือหน่วยงานที่หันไปใช้ซอฟต์แวร์ Open Sources แทนเพื่อหลีกเลี่ยงปัญหานี้แต่ยังประสบกับปัญหาคุณภาพของผลิตภัณฑ์และความเข้ากันได้ ประเด็นเรื่องนี้เป็นเรื่องที่มีความสัมพันธ์กับเรื่องอื่น ๆ และเกี่ยวข้องกับความเข้าใจและการปฏิบัติตามนโยบายและกฎหมาย ขณะนี้จะต้องรอให้มีกฎหมาย และนโยบายที่ชัดเจน เพื่อหน่วยงานจะได้นำไปปฏิบัติได้

DRAFT

จากข้อมูลการสัมภาษณ์และแบบสอบถามเป็นที่เห็นได้ชัดในประเด็นหลัก

- หน่วยงานไม่มีความเข้าใจเรื่องความมั่นคงปลอดภัยสารสนเทศ
- หน่วยงานยังไม่มีความรู้การนำมาตรฐานสากลว่าด้วยความมั่นคงปลอดภัยสารสนเทศมาใช้
- หน่วยงานยังไม่เข้าใจเรื่องระบบการลงโทษของผู้ละเมิดนโยบายความมั่นคง
- หน่วยงานยังไม่มีแผนเรื่องความมั่นคงปลอดภัยสารสนเทศ

3.2.2 การสำรวจสถานภาพความปลอดภัยของเครือข่ายในประเทศไทย

ผลการศึกษานโยบายความปลอดภัยของเครือข่ายสำหรับประเทศไทย ที่เป็นการรักษาปลอดภัยของเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต นำมาจากผลรายงานการวิจัยสถานภาพปลอดภัยของเครือข่ายในประเทศไทยจากการสำรวจในกลุ่มของอุดมศึกษาสถานบันการศึกษาจากผู้เข้าร่วมสัมมนาในงาน “Thai IT Security 2001” โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ข้อมูลการสำรวจมีดังนี้

1. การใช้ไฟร์วอลล์กลุ่มของอุดมศึกษา
2. การใช้ระบบซอฟต์แวร์หรือฮาร์ดแวร์สำหรับตรวจจับการบุกรุก
3. การบันทึกการเข้าใช้ระบบเพื่อวิเคราะห์ตรวจหาปัญหาปลอดภัยจากการบันทึก
4. เอกสารกำหนดนโยบายปลอดภัยเพื่อแจ้งให้ผู้ใช้ได้ทราบว่าสิ่งใดอนุญาตหรือไม่อนุญาตหรือไม่ให้กระทำ
5. การตรวจสอบปัญหาความปลอดภัยล่วงหน้า
6. แผนปฏิบัติการที่เป็นเอกสารกำหนดขั้นตอนการปฏิบัติการเมื่อตรวจพบปัญหาความปลอดภัย
7. ผู้รับผิดชอบด้านรักษาความปลอดภัย
8. ลำดับความสำคัญของปัญหาความปลอดภัยในหน่วยงาน
9. หัวข้อการฝึกอบรมด้านความปลอดภัยที่สนใจ

3.2.3 การวิเคราะห์และสรุปประเด็นหลักผลการสำรวจ

ประเด็นหลักด้านความปลอดภัยในกลุ่มเครือข่ายสถาบันการศึกษาจากการสำรวจทั้ง 9 ประเด็นจากข้างต้น มีดังนี้

1. สถาบันการศึกษาส่วนใหญ่ยังขาดแคลนอุปกรณ์พื้นฐานที่จำเป็นในการรักษาและเฝ้าระวังความปลอดภัย ไม่ว่าจะเป็นไฟร์วอลล์หรือระบบตรวจจับผู้บุกรุก สาเหตุประเด็นของ

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

ปัญหาเนื่องจากหน่วยงานหลายแห่งยังขาดความรู้ความเข้าใจด้านเครื่องพื้นฐานในการรักษาความปลอดภัย ดังนั้นควรมีการจัดฝึกอบรมด้านเทคโนโลยีให้อย่างแพร่หลายและทั่วถึง

2. สถาบันการศึกษาส่วนใหญ่ไม่มีกระบวนการและข้อกำหนดในการเฝ้าระวังและรักษาความปลอดภัย และมาตรการดำเนินเมื่อพบปัญหา กระบวนการและข้อกำหนดในการเฝ้าระวังรักษาความปลอดภัยและมาตรการเป็นสิ่งสำคัญที่ผู้บริหารหน่วยงาน จากผลการสำรวจได้ชี้ให้เห็นว่าผู้บริหารเครือข่ายในระดับนโยบายขาดความรู้ความเข้าใจและยังมิได้ให้ความสำคัญในเรื่องการรักษาความปลอดภัย ดังนั้นควรมีการจัดสัมมนาผู้บริหารหน่วยงานเพื่อสร้างความเข้าใจและตระหนักถึงความสำคัญของการจัดทำนโยบายและข้อกำหนดด้านความปลอดภัย
3. สถาบันการศึกษาส่วนใหญ่ไม่มีการแจ้งให้ผู้ใช้ทราบถึงนโยบายการใช้เครือข่าย ผู้ใช้เครือข่ายส่วนใหญ่เป็นนิสิตนักศึกษาซึ่งมีความสามารถพื้นฐานในการใช้คอมพิวเตอร์ ขณะที่โปรแกรมหรือเครื่องมือที่ใช้เจาะระบบหรือสร้างปัญหาความปลอดภัยในเครือข่ายมีเผยแพร่อย่างเปิดเผย และใช้งานได้ง่ายโดยไม่ต้องอาศัยความเชี่ยวชาญพิเศษ ดังนั้นการประกาศใช้นโยบายให้ผู้ใช้ทราบอย่างทั่วถึงย่อมเป็นการสร้างความเข้าใจ และแจ้งเตือนให้ผู้ใช้ทราบถึงขอบเขตที่พึงปฏิบัติและมาตรการดำเนินการของหน่วยงานในการใช้เครือข่ายเพื่อช่วยลดปัญหาที่อาจตามมาภายหลัง
4. สถาบันการศึกษาบางส่วนยังไม่มีผู้เชี่ยวชาญที่รับผิดชอบด้านความปลอดภัยของเครือข่ายโดยตรง ปัญหาขาดแคลนผู้เชี่ยวชาญด้านความปลอดภัย เป็นปัญหาที่ยังไม่ได้รับการแก้ไขอย่างเป็นทางการ ดังนั้นงานรักษาความปลอดภัยของเครือข่ายจะเป็นงานที่มอบหมายให้ผู้ดูแลเครือข่ายซึ่งไม่ได้รับการฝึกอบรมให้มีความเชี่ยวชาญโดยตรง หรือให้เป็นภาระของผู้ได้รับมอบงานทำหน้าที่ศึกษาความรู้เพิ่มเติมเอง ซึ่งประเทศไทยยังขาดแคลนผู้เชี่ยวชาญและยังไม่มีการวางแผนสร้างบุคลากร แผนการฝึกอบรม หรือตั้งเป้าหมายในการผลิตบุคลากรในกลุ่มนี้ ที่เป็นประเด็นสำคัญที่จะต้องวางแผนและกำหนดเป้าหมายเพื่อผลิตบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยให้เพียงพอ และมีมาตรการสนับสนุนในการกำหนดค่าตอบแทนวิชาชีพเฉพาะให้เหมาะสม

3.3 สถานภาพด้านความมั่นคงปลอดภัย การใช้เทคโนโลยีสารสนเทศและการสื่อสารของต่างประเทศ

วัตถุประสงค์ของการศึกษาสถานภาพด้านความมั่นคงปลอดภัยของต่างประเทศ ที่จะนำมาเป็นกรณีศึกษาในการสร้างแผนที่นำทาง และแผนแม่บทฯ สำหรับประเทศไทย ซึ่งจะประกอบด้วย

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

- ประเทศสหรัฐอเมริกา
- ประเทศออสเตรเลีย
- ประเทศสิงคโปร์

3.3.1 สถานภาพด้านความมั่นคงปลอดภัยของประเทศสหรัฐอเมริกา

กรอบการดำเนินงาน (Frameworks) เพื่อการศึกษาเปรียบเทียบสถานภาพของแต่ละประเทศจะพิจารณาจากองค์ประกอบหลัก 3 ประการของ ความมั่นคงปลอดภัยฯ ได้แก่ “Process, People and Technology” ซึ่งแยกออกเป็นหัวข้อ ดังนี้

- ด้านนโยบายและการบริหารจัดการ (Process)
- ด้านการควบคุมและการปฏิบัติงานตามนโยบาย (People)
- ด้านเทคโนโลยี (Technology)

3.3.1.1 ด้านนโยบายและการบริหารจัดการ

ในส่วนนี้จะศึกษากระบวนการในการดำเนินนโยบายและการบริหารจัดการของประเทศสหรัฐอเมริกา เพื่อการรักษาความมั่นคงปลอดภัยด้านไอซีทีของชาติ ในภาครัฐหรือภาคสาธารณะ และในภาคธุรกิจเอกชน ทั้งนี้จะไม่รวมรายละเอียดในเรื่องที่เกี่ยวกับความมั่นคงปลอดภัยของชาติ ซึ่งเป็นข้อมูลปกปิดของรัฐบาล

แรงขับเคลื่อนของการกำหนดให้มีนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศในระดับประเทศ ซึ่งถือว่าเป็นตลาดเสรีทางการแข่งขันในระบบเศรษฐกิจนั้น จะประกอบด้วยประเด็นสำคัญได้แก่

- ความมั่นคงปลอดภัยในชีวิตและทรัพย์สินของประชาชน (Public Safety)
- ความมั่นคงปลอดภัยด้านเศรษฐกิจ (Economic Security)
- นวัตกรรม (Technological Advances/Innovation)
- ความต้องการของผู้บริโภค (Consumer Demand)
- โลกาภิวัฒน์ (Globalization)
- รัฐบาลอิเล็กทรอนิกส์ (e-Government)

สหรัฐอเมริกาต้องเผชิญภัยคุกคามจากการก่อการร้าย ดังเช่นกรณี “9/11” ในวันที่ 11 เดือนกันยายน 2544 ซึ่งกระทบกระเทือนต่อความมั่นคงปลอดภัยของชาติในวงกว้าง การปกป้องโครงสร้างพื้นฐานด้านสารสนเทศต่อการก่อการร้ายจึงเป็นอีกกรณีหนึ่งของการป้องกันความมั่นคงปลอดภัยที่จำเป็นยิ่ง

เดือนกุมภาพันธ์ พ.ศ. 2546 รัฐบาลจึงได้กำหนดแผนกลยุทธ์แห่งชาติ เรียกว่า “The National Strategy to Secure Cyberspace” ซึ่งมีรายละเอียดดังต่อไปนี้

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

1.1 ยุทธศาสตร์ชาติต่อความมั่นคงปลอดภัยด้านไซเบอร์ (The National Strategy to Secure Cyberspace)

<u>วัตถุประสงค์ (Objectives)</u>

1. เพื่อป้องกันการโจมตีด้านไซเบอร์ต่อโครงสร้างพื้นฐานวิกฤตของชาติ
2. บรรเทาความไม่มั่นคงของชาติด้านไอทีต่อการโจมตีด้านไซเบอร์
3. ลดความเสียหายที่อาจเกิดขึ้นและเวลาฟื้นตัวจากการโจมตี ด้านไซเบอร์

<u>โครงการเร่งด่วนเพื่อความมั่นคงปลอดภัยด้านไซเบอร์สเปซ</u>

มีจำนวนทั้งสิ้น 5 โครงการ คือ

1) ระบบโต้ตอบความมั่นคงปลอดภัยด้านไซเบอร์ระดับชาติ
2) โครงการบรรเทาภัยคุกคามและความไม่มั่นคงต่างๆ ด้านไซเบอร์ระดับชาติ
3) โครงการฝึกอบรมและกระตุ้นความรู้ของความมั่นคงปลอดภัยด้านไซเบอร์ระดับชาติ
4) การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของภาครัฐบาล และ
5) โครงการความร่วมมือเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ระดับนานาชาติ

โครงการข้างต้นยังสามารถแบ่งตามภารกิจสำคัญได้ 3 กลุ่ม คือ โครงการเร่งด่วนอันดับแรกจะมุ่งปรับปรุงการรับมือต่อเหตุการณ์บนไซเบอร์สเปซ (อินเทอร์เน็ต) และลดความเสียหายร้ายแรงที่อาจเกิดขึ้นจากเหตุเหล่านั้น โครงการลำดับที่ 2 3 และ 4 มุ่งจะบรรเทาภัยคุกคาม (Threats) และทรัพยากรสำคัญที่มีความเสี่ยง (Vulnerabilities) ทั้งหลาย จากการโจมตีทางไซเบอร์ (Cyber Attacks) และโครงการลำดับที่ 5 เป็นการป้องกันการโจมตีทางอินเทอร์เน็ต ซึ่งอาจเป็นภัยต่อทรัพยากรด้านความมั่นคงปลอดภัยของชาติ และเพื่อที่จะปรับปรุงการจัดการและการโต้ตอบภัยคุกคามต่างๆ เหล่านี้ที่เกิดขึ้นระหว่างประเทศ

<u>การปฏิบัติการและโครงการริเริ่มต่างๆ ด้านความมั่นคงปลอดภัย (Actions and Initiatives</u>

การจัดทำแผนปฏิบัติการและโครงการที่เกี่ยวเนื่องกันกับแผนกลยุทธ์แห่งชาตินี้มีดังนี้

1. เสริมสร้างสถาปัตยกรรมระบบระหว่างภาครัฐและเอกชนสำหรับตอบโต้เหตุจาก
   ไซเบอร์ (Cyber Incidents) ในระดับชาติ

DRAFT

2. จัดให้มีการพัฒนาการวิเคราะห์ทางยุทธการและยุทธวิธีต่อการโจมตีทางไซเบอร์และการค้นหาความไม่มั่นคงปลอดภัยของระบบสารสนเทศ
3. ส่งเสริมภาคเอกชนให้พัฒนาความสามารถที่จะแบ่งปัน มุมมองของสาระสำคัญด้านสุขภาพของไซเบอร์สเปซ
4. ขยายการเตือนภัยด้านไซเบอร์และเครือข่ายสารสนเทศเพื่อที่จะสนับสนุนบทบาทของ กระทรวงความมั่นคงปลอดภัยของมาตุภูมิ (DHS) ในการประสานงานการจัดการเหตุการณ์วิกฤตด้านความมั่นคงปลอดภัยบนไซเบอร์สเปซ
5. ปรับปรุงการจัดการเหตุระดับชาติ
6. ประสานงานในกระบวนการสำหรับความมีส่วนร่วมของอาสาสมัครในการพัฒนาของแผนสนับสนุนการทำงานอย่างต่อเนื่องของระบบระหว่างรัฐและเอกชน
7. การฝึกปฏิบัติของแผนรับมือให้ระบบทำงานได้อย่างต่อเนื่องของรัฐบาลจากเหตุความมั่นคงปลอดภัยด้านไซเบอร์
8. ปรับปรุงและส่งเสริมการแลกเปลี่ยนสารสนเทศที่เกี่ยวข้องกันการโจมตีทางไซเบอร์ ภัยคุกคาม และความไม่มั่นคงของระบบ

1.2 โครงการด้านความมั่นคงปลอดภัยอื่น ๆ (Security Programs)

1) Guidelines and Standards (800 Series)

Special Publications 800 Series

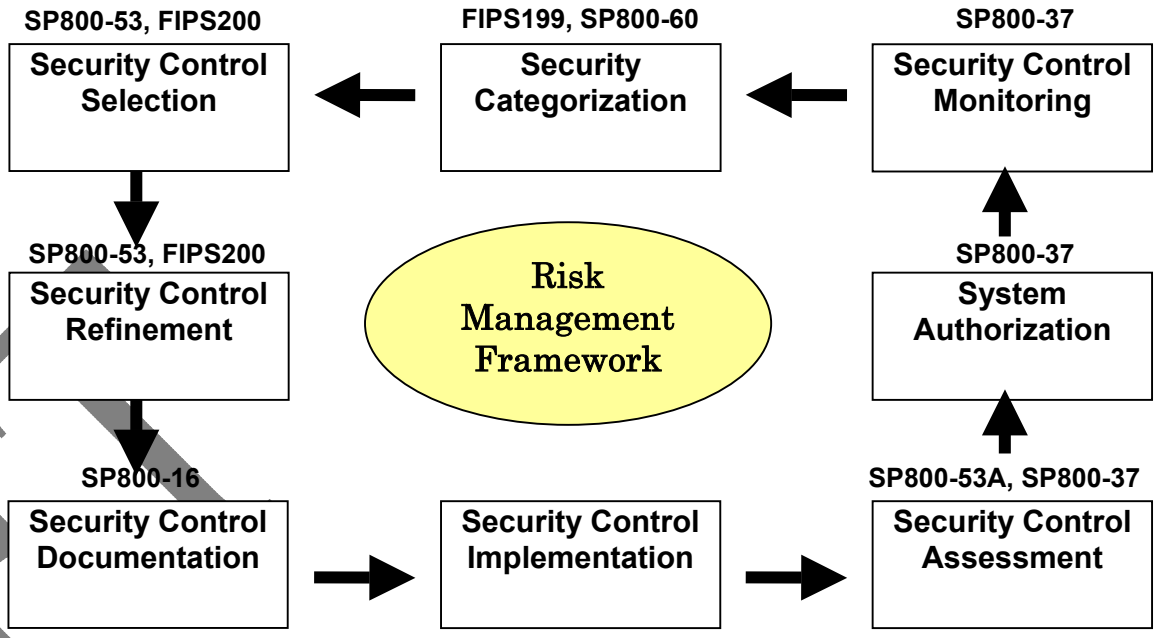
(http://csrc.nist.gov/publications/nistpubs/index.html)

- SP800-26 (Security Self-Assessment)
- SP800-30 (Risk Management)
- SP800-37 (Certification and Accreditation)
- SP800-53 (Recommended Security Controls)
- SP800-53A (Verifying Effective Security Controls)
- SP800-60 (Information Types Mapped to Controls)

2) Federal Information Processing Standards (FIPS)

- FIPS199 (Security Categorization)
- FIPS200 (Minimum Security Controls)

DRAFT



รูปที่ 3.3 The Risk management framework under SP800 and FIPS199

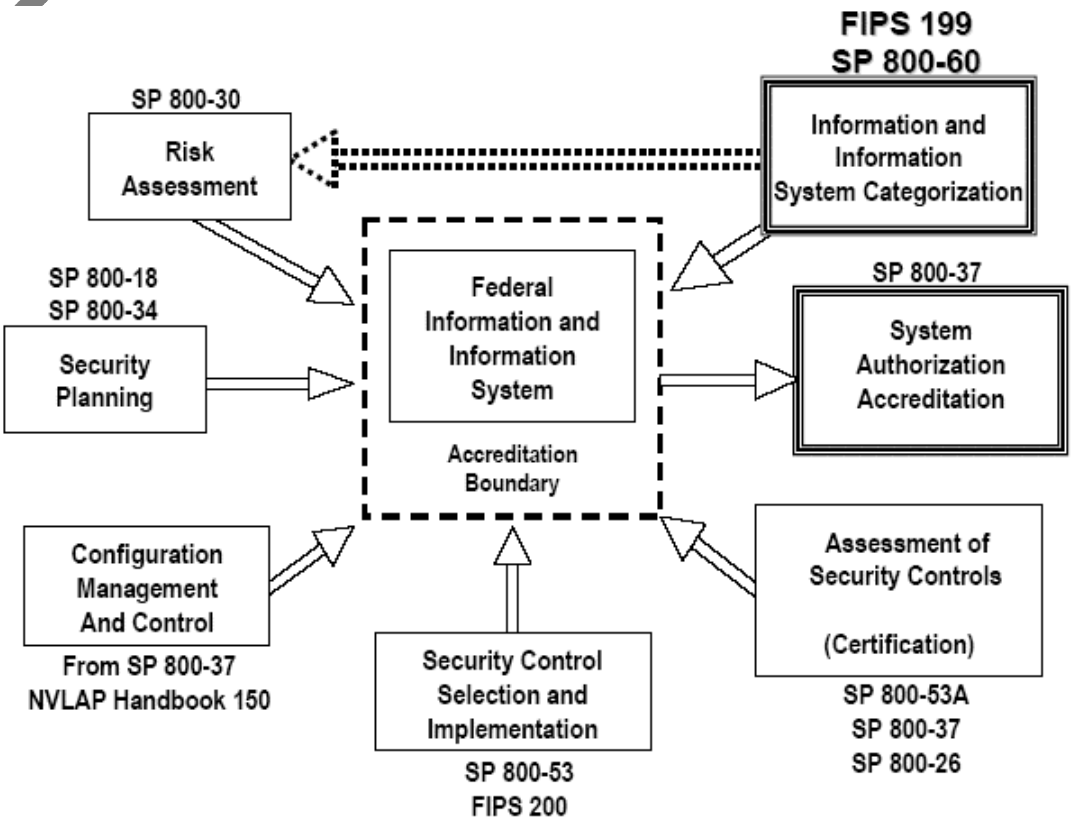
3) Federal Information Security Management Act (FISMA)

- FISMA, Title III, public Law 107-347, December 17, 2002
- เพื่อจัดให้มีความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) แทนกฎหมายเดิม คือ "Government Information Security Reform Act" และ "Computer Security Act"
- หน่วยงานของรัฐบาลกลางทั้งหลายต้องรับผิดชอบต่อการจัดให้มีป้องกันสารสนเทศที่เก็บรักษาหรือรวบรวมโดยหน่วยงานนั้นๆ ไม่ว่าโดยทางตรงหรือทางอ้อม รวมถึงการรักษาความมั่นคงปลอดภัยของงานระบบสารสนเทศที่ใช้ในการปฏิบัติงานโดยตรงหรือผ่านตัวแทน เพื่อให้การดำเนินงานในภาพรวมของรัฐทำได้อย่างมีประสิทธิภาพ ดังนั้น NIST (National Institute of Standard and Technology) จึงได้รับมอบหมายให้พัฒนามาตรฐานและแนวทางปฏิบัติ รวมถึงความต้องการขั้นต่ำที่จะต้องมี เพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับการปฏิบัติงานและการดูแลทรัพย์สินทั้งหมด (all agency operations and assets) ของหน่วยงานรัฐ

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

บาลกลาง อย่างไรก็ตามมาตรฐานและแนวทางปฏิบัตินี้จะไม่รวมถึงระบบรักษาความมั่นคงปลอดภัยของประเทศ (National Security Systems)

- นอกจากนี้ยังมีข้อบังคับที่ออกให้หน่วยงานของรัฐบาลกลางต้องรายงานผลการปฏิบัติงานในดำเนินนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ กระบวนการทำงาน และการปฏิบัติงานตามแผน ต่อรัฐสภา ทุกๆ สามเดือน และรายงานสรุปประจำปีด้วย



รูปที่ 3.4 ความสัมพันธ์ระหว่างแนวปฏิบัติของ NIST และ FISMA[1]

[1] Blueprint Technologies, Inc 2005

4) Personal Identity Verification (PIV)

- Personal Identity Verification of Federal Employees and Contractors
- (http://csrc.nist.gov/piv-program/)

5) National Vulnerability Database (NVD)

เป็นฐานข้อมูลด้านความไม่มั่นคงของระบบ หรือความเสี่ยงของความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงแหล่งข้อมูลสาธารณะของรัฐบาลทั้งหมดและอ้างถึงแหล่งข้อมูลด้านอุตสาหกรรมด้วย

3.3.1.2 ด้านการควบคุมและการปฏิบัติงานตามนโยบาย

1.1 NIST (National Institute of Standards and Technology)

National Institute of Standards and Technology จัดตั้งขึ้นในปี 1901 โดยเป็น หน่วยงานภายใต้ฝ่ายบริหารเทคโนโลยีของกระทรวงพาณิชย์ (a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration.) มีภารกิจในการสนับสนุนและส่งเสริม ความสามารถในการแข่งขันทางอุตสาหกรรมและนวัตกรรมของประเทศ โดยใช้ วิทยาศาสตร์ ด้านมาตรวิทยาชั้นสูง มาตรฐาน และเทคโนโลยี ด้วยวิธีการที่เสริมสร้างความมั่นคงปลอดภัยทางเศรษฐกิจและการปรับปรุงคุณภาพชีวิต ประกอบด้วย

1. บทบาทที่สำคัญ (NIST Role) ได้แก่
   - กำหนดมาตรฐานและแนวปฏิบัติ
   - กำกับด้านงานวิจัย
   - ช่วยเหลือภาคเอกชน
2. CSD- Computer Security Division

   Computer Security Division (CSD), NIST เป็นผู้พัฒนามาตรฐานต่างๆ ได้แก่
   - ความต้องการขั้นต่ำของมาตรฐานและแนวทางปฏิบัติ เพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ภาครัฐ ได้แก่ การควบคุมความมั่นคงปลอดภัยด้าน ก) การบริหารจัดการ ข) การปฏิบัติงาน และ ค) ด้านเทคนิค ทั้งนี้จะรวมทั้งสารสนเทศและระบบสารสนเทศในแต่ละประเด็น
   - มาตรฐานของการจัดประเภทสารสนเทศและระบบสารสนเทศ โดยคำนึงถึงระดับความเสี่ยงต่างๆ เพื่อกำหนดระดับที่เหมาะสมของความมั่นคงปลอดภัยด้านสารสนเทศในแต่ละประเภท นั้นๆ

DRAFT

1.2 องค์การและหน่วยงานภาคเอกชนอื่นๆ

รายชื่อองค์การและหน่วยงานภาคเอกชนอื่นๆ ที่มีกิจกรรมต่อเนื่องในด้านเครือข่ายและความมั่นคงปลอดภัยฯ ในสหรัฐอเมริกา (รวมถึงในระดับนานาชาติ) เพื่อส่งเสริมการพัฒนาบุคลากรและหลักปฏิบัติด้านความมั่นคงปลอดภัยในภาคเอกชน อาทิเช่น

1. ISC^2 (International Information Systems Security Certification Consortium)

ถือได้ว่าเป็นองค์กรริเริ่มในการออกประกาศนียบัตรด้าน Information Security ระดับนานาชาติ (www.isc2.org) ประกาศนียบัตรที่ออกโดย ISC2 จะไม่ขึ้นอยู่กับยี่ห้ออุปกรณ์ และแบ่งเป็นสองประเภทหลัก คือ CISSP (Certified Information Systems Security Professional) และ SSCP (Systems Security Certified Practitioner)

CISSP จะครอบคลุมความรู้ด้าน Information Security แบบกว้างๆ แต่ไม่ลงลึกในรายละเอียด อาทิ เช่น

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Nnetwork Security

SSCP จะครอบคลุมความรู้ด้าน Computer Security อาทิ เช่น

- Access Control
- Administration
- Audit and Monitoring
- Cryptography
- Data Communications
- Malicious Code/Malware
- Risk, Response and Recovery

DRAFT

2. ISACA (Information Systems Audit and Control Association)
   - CISA (Certified Information Security Auditor)
   - CISM (Certified Information Security Manager)
3. ISSPCS (International Systems Security Professional Certification Scheme)
   - ISSEA (International Systems Security Engineering Associations)
4. SANS (SysAdmin, Audit, Network, Security Institute, 1989)
   - SANS GIAC (Global Information Assurance Certification, 1999)

3.3.1.3 ด้านเทคโนโลยี

1.1 ภารกิจที่สำคัญของ CSD (CSRC Focus Areas)

ได้แก่

- มาตรฐาน Cryptographic และแอพพลิเคชัน
- การทดสอบความมั่นคงปลอดภัย
- การวิจัยด้านความมั่นคงปลอดภัย หรือ เทคโนโลยีสำคัญในอนาคต
- การจัดการและแนวปฏิบัติด้านความมั่นคงปลอดภัย

1.2 โครงการสำคัญในปี ค.ศ. 2005-2006 ของ NIST (NIST Major Focus Areas 2005-2006)

- FISMA
- HSPD-12/PIV
- CMVP (The Cryptographic Module Validation Program)
- Emerging Technology
  - Media Sanitization
- Cryptographic Protocols
  - Digital Signature
  - Cryptographic Algorithm
  - Configuration Checklists (XP)

1.3 เป้าหมายระยะสั้นด้านมาตรฐานและแนวปฏิบัติของความมั่นคงปลอดภัย ค.ศ. 2005-2006[2] มีดังนี้

1. SP800-37

[2] http://csrc.nist.gov/

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

เพื่อนำเสนอแนวปฏิบัติของ การออกใบรับรองและประกาศนียบัตรด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่สนับสนุนงานของผู้บริหารหน่วยงานในรัฐบาลกลาง ไม่ใช้บังคับทั่วไป แต่องค์กรอื่นๆ ในภาคเอกชน สามารถเลือกนำไปปฏิบัติในเรื่องที่เกี่ยวข้องได้

2. FIPS PUB 199

   FIPS Publication 1999 เป็นระเบียบที่กำหนดประเภทต่างๆ ของความมั่นคงปลอดภัยให้พัฒนาเป็นมาตรฐานของสารสนเทศและระบบสารสนเทศ

3. SP800-60

   Mapping Guidance (to be updated 2006)

   (Guide for Mapping Types of Information and Information Systems to Security Categories. That publication defines information security categories for Unites States Federal government agencies.)

4. SP800-53

   Minimum Security Controls

   (Recommended Security Controls for Federal Information Systems)

5. SP800-53A

   Assessment Methods

6. FIPS 200

   Minimum Security Requirements

7. HSPD-12

   Homeland Security Presidential Directive/Hspd-12

   (The Policy for a common identification standard for Federal employees and contractors, August 27, 2004)

8. FIPS 201/201-1

   เกี่ยวข้องกับโครงการ Personal Identity Verification (PIV) มีดังนี้

   - Part I

     Common Identification and Security Requirements

   - Part II

     Common Interoperability Requirements

DRAFT

9. SP800-16
   (Information Technology Security Training Requirements: A Role- and Performance-Based Model)

3.3.2 สถานภาพด้านความมั่นคงปลอดภัยของประเทศสิงคโปร์

กรอบการดำเนินงาน (Frameworks) เพื่อการศึกษาเปรียบเทียบสถานภาพของสิงคโปร์จะพิจารณาจากองค์ประกอบหลัก 3 ประการของ ความมั่นคงปลอดภัยฯ ได้แก่ “Process, People and Technology” ซึ่งแยกออกเป็นหัวข้อ ดังนี้

- ด้านนโยบายและการบริหารจัดการ (Process)
- ด้านการควบคุมและการปฏิบัติงานตามนโยบาย (People)
- ด้านเทคโนโลยี (Technology)

3.3.2.1 ด้านนโยบายและการบริหารจัดการ

การศึกษา วิจัยและพัฒนาด้าน Information Security (IS) เริ่มจากกระบวนการพัฒนาการบริการของรัฐโดยใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) เป็นเครื่องมือ รัฐบาลได้จัดทำนโยบายระดับชาติอย่างต่อเนื่องนับสิบปี รวมถึงแนวปฏิบัติที่มีเป้าหมายสำคัญเป็นภารกิจของชาติที่ต้องไปให้ถึง

1.1 แผนยุทธศาสตร์ด้านไอซีทีระดับชาติ

แผนยุทธศาสตร์ด้านไอซีทีของสิงคโปร์แบ่งได้เป็น 2 แผน[3] คือ แผนงานรัฐบาล (Government Infocom Plans) และแผนงานระดับประเทศ (National Infocom Plans) มีวัตถุประสงค์เพื่อการบริหารจัดการที่มีประสิทธิภาพ ระหว่างหน่วยงานในกำกับของรัฐบาลที่ให้บริการกับประชาชนและธุรกิจเอกชน โดยอาศัยไอซีที และเพื่อเป็นแนวทางปฏิบัติให้กับ องค์กรภาคเอกชนและภาคธุรกิจสามารถวางแผนงานที่สอดคล้องกันทั้งประเทศ มุ่งไปสู่เป้าหมายเดียวกัน คือ ยุทธศาสตร์ชาติ นั่นเอง แผนที่ยุทธศาสตร์ด้านไอซีทีของสิงคโปร์สามารถสรุปได้ในรูปของตาราง ดังต่อไปนี้

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

ตาราง 1 Singapore's six strategic ICT Plans

กลยุทธ์[4]	ช่วงเวลา	National Infocomm Plans	Government Infocomm Plans
ประยุกต์ใช้เทคโนโลยีฯสำหรับ “Innovation, Integration and Internationalization”	2010 - 2015	iN2015	
	2006 - 2010		iGov2010
นำศักยภาพของเทคโนโลยีฯมาใช้ให้ได้อย่างเต็มที่ เพื่อที่จะสร้างคุณค่าใหม่ สร้างฝันให้เป็นจริงและสร้างความอยู่ดีกินดีให้กับประชาชน	2003 - 2006	Connected Singapore	e-Government Action Plan II
พัฒนาสิงคโปร์ให้เป็น “global Infocomm Capital, e-Economy and e-Society”	2000 - 2003	Infocomm 21	e-Government Action Plan
ปรับเปลี่ยนสิงคโปร์ให้เป็น “an Intelligent Island”	1992 - 1999	IT2000	Civil Service Computerization Programmed
ขยายระบบต่างๆ ของรัฐบาลให้เอกชนใช้ประโยชน์ด้วย เช่น TradeNet, MediNet, LawNet เป็นต้น	1986 - 1991	The National IT Plan	
โครงการนำคอมพิวเตอร์มาใช้กับการบริการประชาชน เพื่อพัฒนาอุตสาหกรรมไอทีและกำลังคนด้านไอที	1980 - 1985	The National Computerization Plan	

1.2 Infocomm Security Master Plan

แผนแม่บทด้านความมั่นคงปลอดภัยฯ ของรัฐบาลฉบับปัจจุบัน เรียกว่า “Infocomm Security Master Plan” มีวัตถุประสงค์เพื่อสร้าง แผนที่นำทาง (Roadmap) ในระยะ 3 ปี สำหรับป้องกันโครงสร้างพื้นฐานวิกฤต การรักษาความมั่นคงปลอดภัยของรัฐ ธุรกิจและประชาชน ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีสาระสำคัญ ดังต่อไปนี้

3 www.ida.gov.sg 2006

4 2006 iDA Singapore

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

- การป้องกันประชาชน (Securing the People Sector)
- การป้องกันหน่วยงานภาคเอกชน (Securing the Private Sector)
- การป้องกันหน่วยงานภาครัฐ (Securing the Public Sector)
- การพัฒนาศักยภาพด้านความมั่นคงปลอดภัยของชาติ (Developing National Capability)
- การพัฒนาให้ความรู้ด้านเทคโนโลยีและการวิจัย (Cultivating Technology and R&D)
- การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานด้านสารสนเทศของชาติ (Security National Infrastructure)

ปัจจัยสำคัญของความสำเร็จอาจจะพิจารณาได้จากการบริหารจัดการโครงการ รัฐบาลสิงคโปร์ได้มอบหมายให้ IDA (Infocomm Development Authority) เป็นองค์กรที่รับผิดชอบการดำเนินการของโครงการนี้ เพื่อประสานความร่วมมือระหว่างหน่วยงานอื่นๆ ในระดับกระทรวง ส่วนการผลักดันนโยบายและการควบคุมดูแลแผนแม่บทจะดำเนินการในรูปของคณะกรรมการติดตามและกำกับดูแลฯ (Project Steering Committee) ซึ่งประกอบด้วยผู้บริหารระดับสูง ของรัฐบาล(ปัจจุบันประธาน คกก. เป็นรองปลัดกระทรวงการคลัง)

ในส่วนของ Infocomm Security Initiatives นั้น คกก. ได้กำหนดนโยบายเป็นโครงการริเริ่ม อาทิ เช่น

- โครงการพัฒนา Cyber security โดยขยายขีดความสามารถในปัจจุบันของ IDA
- โครงการ Incident management ผ่านหน่วยงาน SingCERT และ GITSIR (Government IT Security Incident Response) Team
- โครงการ Threat Management เพื่อป้องกันโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure)

3.3.2.2 ด้านการควบคุมและการปฏิบัติงานตามนโยบาย

หน่วยงานหลักที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสิงคโปร์ คือ IDA (Infocomm Development Authority) ทั้งนี้ไม่นับรวมหน่วยงานด้านความมั่นคงปลอดภัยแห่งชาติ เช่น กระทรวงกลาโหม กระทรวงมหาดไทย เป็นต้น

1.1 Infocomm Development Authority of Singapore (IDA)

IDA เกิดจากการรวมตัวของหน่วยงานสองหน่วย คือ NCB (National Computer Board) และ TAS (Telecommunications Authority of Singapore) เมื่อ 1 ธันวาคม ค.ศ. 1999 อยู่ภายใต้การกำกับของ MICA (Ministry of Information, Communications and the Arts) ซึ่งกำกับดูแลหน่วยงาน 6 หน่วยงาน ได้แก่

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

- IDA (Infocomm Development Authority)
- MDA (Media Development Authority)
- National Arts Council
- NLB (National Library Board)
- National Heritage Board
- Preservation of Monuments Board

IDA ซึ่งมีโครงสร้างการบริหารงานโดยคณะกรรมการกำหนดนโยบาย มีหน้าที่ที่สำคัญ คือ

- พัฒนาและส่งเสริมการแข่งขันเสรีด้านเทคโนโลยีสารสนเทศฯ โดยเฉพาะอย่างยิ่งในอุตสาหกรรมโทรคมนาคม
- พัฒนาการวางแผนและนโยบายด้านเทคโนโลยีสารสนเทศฯ
- พัฒนาอุตสาหกรรมด้านเทคโนโลยีสารสนเทศฯ ให้สามารถแข่งขันได้ในระดับโลก และ
- ทำหน้าที่ เป็น CIO (Chief Information Officer) ให้กับรัฐบาลในการนำ Infocomm ไปประยุกต์ใช้

1.2 การจัดการเหตุ ด้านความมั่นคงปลอดภัยของไซเบอร์ (Cyber Security Incident Management)

มีการจัดตั้งหน่วยงานเพื่อจัดการเหตุฯ บนไซเบอร์ขึ้นสองหน่วยโดยภาครัฐ และยอมให้ภาคเอกชนตั้งศูนย์ปฏิบัติการเฝ้าระวัง (Security Operation Center) เพื่อตอบสนองความต้องการเฉพาะ ของธุรกิจ

1.) Singapore Computer Emergency Response Team (SingCERT)

SingCERT ทำหน้าที่เป็น National cyber security incident management and response center โดยเป็นตัวแทนของประเทศสิงคโปร์ในระดับภูมิภาคและระดับประเทศในการร่วมมือและประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น Forum of Incident Response and Security Teams (FIRST) หรือ Asia Pacific CERT (APCERT) forum

การบริหารงานของ SingCERT ปัจจุบันอยู่ภายใต้การกำกับดูแลของ Infocomm Security and Trust Division, IDA Singapore

2.) Government IT Security Incedent Response Team (GITSIR)

GITSIR ทำหน้าที่เฝ้าระวังเหตุทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานของรัฐบาล เตรียมความพร้อมให้กับหน่วยงานอื่นๆ ในการรับมือกับเหตุการณ์ฉุกเฉิน โดยการเตรียมการอย่างเป็นระบบ มีระเบียบปฏิบัติที่ชัดเจน ช่วยเหลือหน่วยงานอื่นๆ ในการจัดตั้งทีมงานทำหน้าที่รับมือกับ

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

เหตุฯ ในหน่วยงานนั้นๆ ทั้งนี้ก็เพื่อการบริหารจัดการภาครัฐสามารถเฝ้าระวังเหตุได้อย่างมีประสิทธิภาพ

3.) National Cyberthreat Monitoring Centre (NCMC)

เป็นหน่วยงานอยู่ภายใต้การกำกับดูแลของ IDA เพื่อพัฒนาขีดความสามารถในการเฝ้าระวังและ ตอบโต้กับภัยคุกคาม บรรเทาผลจากภัยคุกคามทางไซเบอร์ ทำหน้าที่เฝ้าระวังและวิเคราะห์เหตุการณ์ตลอด 24 ชั่วโมง มีการขยายและจัดตั้งเครือข่ายของศูนย์เฝ้าระวังในรูปแบบต่างๆ ขึ้นในสิงคโปร์ เช่น Cyber-Watch Centre (CWC), Threat Analysis Centre (TAC) หรือ Outsource IT Security Monitoring ที่เราเรียกว่า MSS (Managed Security Service) เป็นต้น คาดว่าจะเปิดดำเนินการได้ในปี ค.ศ. 2007

3.3.2.3 *ด้านเทคโนโลยี (Technological Control)*

การดำเนินการตามแผนแม่บท Infocomm Security นั้น รัฐบาลสิงคโปร์ได้ริเริ่มโครงการต่างๆ ตามลำดับความสำคัญ มีหลายโครงการที่ต้องจัดจ้างภาคเอกชนและธุรกิจให้ดำเนินการแทน (Outsourcing Programmed) และหลายโครงการที่ภาครัฐจะต้องดำเนินการเอง โดยมีโครงการนำร่องไปแล้ว ได้แก่

- CII-SA (Critical Infocomm Infrastructure Surety Assessment) เพื่อประเมินขีดความสามารถและความพร้อมของ National Critical Infocomm Infrastructure (CII) สามารถวิเคราะห์และกำหนดระบุ CII ต่อภัยคุกคามทางไซเบอร์ได้ นอกจากนี้ยังเป็นแนวทางปฏิบัติของการประสานงานระหว่างหน่วยงานกำกับดูแลตามกฎหมายหรือระเบียบ และผู้ที่เป็นเจ้าของ CII นั้นๆ
- Infocomm Security Health Scorecard เพื่อประเมินความพร้อมของหน่วยงานบริการภาคสาธารณะด้านความมั่นคงปลอดภัยของสารสนเทศ ช่วยให้หน่วยงานภาครัฐสามารถระบุจุดอ่อนภายในการปฏิบัติงานของตนเพื่อการปรับปรุงคุณภาพ และจะเป็นตัวชี้วัดด้าน “Security health” ประจำปีของหน่วยงาน
- National Infocomm Security Awareness Programmed เพื่อให้ความรู้และความเข้าใจแก่ประชาชน ภาคเอกชนและภาคสาธารณะเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศและการสื่อสาร และ
- National Trust Framework เป็นโครงการต่อเนื่องจาก iN2015 เพื่อผลักดันนโยบายระดับยุทธศาสตร์ 4 ด้าน คือ
    - Infrastructure (National Authentication Framework, Security Measurement and Benchmarking and Product assurance)

DRAFT

- Manpower development (Building a critical pool of competent IS professionals, IS Professional Roadmap, Code of Conduct within Singapore)
- Education and adoption (focus on end-uses computers, public awareness) และ
- Regulation (the need to safeguard digital assets through regulatory measures, Study for a National Cyber Security & Privacy Act)

3.3.3 สถานภาพด้านความมั่นคงปลอดภัยของประเทศออสเตรเลีย

นอกจากมาตรฐานความมั่นคงปลอดภัยสากล ซึ่งประเทศออสเตรเลียนำมาประยุกต์ใช้โดยทั่วไป เช่น ISO/IEC17799, ISO/IEC27001 แล้ว รัฐบาล ได้พัฒนาคู่มือปฏิบัติงาน “ACSI 33” (2000-2004)[5] เป็นคู่มือด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ซึ่งออกแบบมาเพื่อช่วยให้หน่วยงานของรัฐบาลทำงานโดยใช้เทคโนโลยีสารสนเทศ ในสภาพแวดล้อมที่มีความมั่นคงปลอดภัย เอกสารชุดนี้สร้างขึ้นในปี 2000 และตั้งเป้าไว้ว่าหน่วยงานของรัฐบาลจะนำไปปฏิบัติได้ครบทุกหน่วยงานในปี 2004

การศึกษาสถานภาพด้านความมั่นคงปลอดภัยของประเทศออสเตรเลียจะแบ่งออกเป็น 3 ด้านดังนี้

- ด้านนโยบายและการบริหารจัดการ
- ด้านการควบคุมและการปฏิบัติงานตามนโยบาย
- ด้านเทคโนโลยี

3.3.3.1 ด้านนโยบายและการบริหารจัดการ

ในคู่มือ “Part 1 ACSI33 and ICT Security” กำหนดแนวทางการดำเนินงานของความมั่นคงปลอดภัยของหน่วยงานของรัฐบาล ในรูปของ แผนปฏิบัติการนำไปใช้งาน (Implementation Plan) แสดงขั้นตอนการปฏิบัติงานในระดับนโยบายของหน่วยงาน ที่จะนำคู่มือไปใช้งาน ดังนี้

1. การพัฒนานโยบายประจำหน่วย (Policy development) ประกอบด้วยหัวข้อสำคัญ คือ
   - แสดงนโยบายเดิมที่เกี่ยวข้องและมีใช้อยู่แล้ว
   - พัฒนานโยบายใหม่ (ถ้าจำเป็น) เพื่อที่จะให้ครอบคลุมความต้องการทั้งหมดของแต่ละระบบ

5 Australian Government Information Technology Security Manual (the Defense Signals Directorate, Department of Defenses) which are designed to enable government agencies to achieve an assured information technology security environment.

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

2. การจัดทำการบริหารความเสี่ยง (Conduct risk management) ประกอบด้วยหัวข้อสำคัญ คือ
   - แสดงขอบเขตของระบบที่ต้องการป้องกัน
   - พัฒนาแผนบริหารความเสี่ยง (Risk Management Plan- RMP) เบื้องต้น
3. การพัฒนาแผน (Plan development) ประกอบด้วยหัวข้อสำคัญ คือ
   - พัฒนาแผนความมั่นคงปลอดภัยไอซีทีระดับสูง สำหรับการใช้งานระหว่างหลายๆ ระบบ
   - พัฒนาหรือปรับแก้ไขแผนความมั่นคงปลอดภัยของระบบ (Systems Security Plan- SSP) เพื่อให้ครอบคลุมแต่ละระบบ
4. การนำไปประยุกต์ใช้ (Implementation) ประกอบด้วยหัวข้อสำคัญ คือ
   - การปฏิบัติตามแผน SSP รวมถึงการจัดซื้อฮาร์ดแวร์และซอฟต์แวร์
   - พัฒนาและสร้างเอกสารด้าน Security Standard Operating Procedures (SOPs)
5. Certification ประกอบด้วยหัวข้อสำคัญ คือ
   - กำหนดว่าอะไรบ้างที่ต้องการทำใบรับรองการใช้งาน (Certification)
   - จัดหาใบรับรองฯ จากองค์กรหรือบุคคลที่เกี่ยวข้อง
6. Accreditation ประกอบด้วยหัวข้อสำคัญ คือ
   - จัดหาใบรับรอง Accreditation จากผู้ที่ออกใบรับรองได้ตามระเบียบ
7. การบำรุงรักษา (Maintenance) ประกอบด้วยหัวข้อสำคัญ คือ
   - เริ่มประยุกต์ใช้งานตามกระบวนการควบคุมการเปลี่ยนแปลง
   - ตรวจสอบความถูกต้องครบถ้วน
8. ทบทวนกระบวนการ (Review)

3.3.3.2 ด้านการควบคุมและการปฏิบัติงานตามนโยบาย

1.1 ASCI33 Part 2

ด้านการควบคุมการปฏิบัติงานตามนโยบาย ได้แก่ระบุไว้ใน คู่มือ ASCI33 คือ “Part 2 ICT Security Administration” ซึ่งแสดงรายละเอียดของกระบวนการเป็น 9 บท ดังนี้

- Chapter 1 - ICT Security Roles and Responsibilities

  เป็นการกำหนดบทบาทของผู้ที่มีส่วนได้เสีย (Roles)

  - DSD (the Defense Signals Directorate)
  - Other Organizations

DRAFT

- Appointing an IT Security Adviser (ITSA)
- IT Security Adviser Responsibilities
- System Manager
- System Users

- Chapter 2 - Security Documentation
- Chapter 3 - Identifying and Developing an ICT Security Policy (ICTSP)
- Chapter 4 - Risk Management: Risk Management Plan (RMP)
- Chapter 5 - Developing a System Security Plan (SSP)
- Chapter 6 - Developing and Maintaining Security: Standard Operating Procedures (SOPs)
- Chapter 7 - Certifying and Accrediting ICT Systems
- Chapter 8 - Maintaining ICT Security and Managing Security
- Chapter 9 - Reviewing ICT Security: Infosec-Registered Assessor Program (I-RAP)[6]

1.2 หน่วยงานและบุคลากรระดับชาติอื่นๆ ที่ดำเนินงานด้านความมั่นคงปลอดภัยของเครือข่ายและสารสนเทศ (National authorities in network and IS)

การจัดกลุ่มผู้มีส่วนได้เสียของเครือข่ายและสารสนเทศ (National authorities in network and IS) ได้แก่

- IT Security Advisers (ITSAs)
- Agency Security Advisers (ASAs)
- Agency ICT security administrators, system administrators, and network administrators,
- Agency security policy staff
- Infosec Registered Assessors (under the Infosec-Registered Assessor Program (I-RAP))
- Technical personnel with some ICT security responsibilities, and
- Security personnel with some understanding of and responsibility for ICT security.

องค์กรอื่น ๆ ที่เกี่ยวข้อง (Other Organizations) ได้แก่

- Protective Security Coordination Centre – Attorney - General's Department
    - Risk management and general protective security.

6 The Infosec-Registered Assessor Program (I-RAP) is a DSD initiative designed to register suitably qualified information security assessors to carry out specific types of ICT security assessments to Australian Government standards

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

- The PSCC's Training Centre provides protective security training. URL: http://www.ag.gov.au/

- Protective Security Section - Australian Security Intelligence Organization
  - Protective security risk reviews and advice, and equipment testing. URL: http://www.asio.gov.au/
- National Archives
  - Advice and guidelines on archives legislation and its application to ICT systems. URL: http://www.naa.gov.au/
- Department of Finance (Australian Government Information Management Office)
  - Development, coordination and oversight of Government policy on electronic commerce, online services and the Internet, URL: http://www.finance.gov.au/
- The Office of the Federal Privacy Commissioner
  - Advice on how to comply with the Privacy Act and related legislation, URL: http://www.privacy.gov.au/
- Department of Foreign Affairs and Trade
  - Policy and advice for security overseas, URL: http://www.dfat.gov.au/
- Australian National Audit Office
  - Performance audits and "Better Practice" guides for areas including information security, URL: http://www.anao.gov.au/
- High Tech Crime Centre -Australian Federal Police
  - Law enforcement in relation to e-crime and other high tech crimes, URL: http://www.ahtcc.gov.au/
- Australian Computer Emergency Response Team
  - Computer incident prevention, response and mitigation strategies, URL: http://www.auscert.org.au/

DRAFT

3.3.3.3 ด้านเทคโนโลยี

1.1 ASCI33 Part 3 ICT Security Standards

ด้านการควบคุมการปฏิบัติงานตามนโยบาย ได้แก่ระบุไว้ใน คู่มือ ASCI33 คือ “Part 3 ICT Security Standards” ซึ่งแสดงรายละเอียดของกระบวนการเป็น 10 บท ดังนี้

Chapter 1 - Physical Security

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- ASIO T4 Protective Security
- Fundamentals
- Removable Media
- Servers and Communication Equipment
- Server Rooms
- Workstations and Network Infrastructure
- Area Security
- Tamper Evident Seals
- Physical Security Incidents
- Emergency Procedures

Chapter 2 – Personnel

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- User Training and Awareness
- Training Resources
- Clearances and Briefings

Chapter 3 - ICT Product Lifecycle

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- DSD Approved Products
- Product Selection
- Acquiring Products
- Installing and Using Products
- Disposing of Products

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

Chapter 4 - Hardware Security

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- Classifying, Labeling and Registering
- Repairing and Maintaining Hardware
- Disposing of Hardware
- Media Sanitization
- Media Destruction
- Portable Computers and Personal Electronic Devices

Chapter 5 - Software Security

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- Software Fundamentals
- Software Development
- Database Security
- Web Application Security
- Electronic Mail Security
- Electronic Mail - Protective Marking Policy
- Malicious Code and Anti-Virus Software

Chapter 6 - Logical Access Control

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- User Identification and Authentication
- Privileged and System Accounts
- Access and Authorization

Chapter 7 - Active Security

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- Intrusion Detection Systems
- Event Logging
- Other Logs
- Auditing
- Vulnerability Analysis

เอกสารฉบับนี้อยู่ระหว่างการพิจารณาปรับปรุงแก้ไข ห้ามนำไปเผยแพร่ ตัดต่อ คัดลอก ทำซ้ำ ดัดแปลง
ก่อนได้รับอนุญาตเป็นลายลักษณ์อักษร (ร่างแก้ไข 2.5 24-11-06)

Chapter 8 - Communications Security (Comsec)

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- About Comsec
- Cabling
- Cable Distribution Systems
- Labeling and Registration
- Wireless Communications
- Telephones and Telephone Systems
- IP Telephony
- Facsimile Machines

Chapter 9 – Cryptography

ประกอบด้วยหัวข้อสำคัญ ดังนี้

Cryptographic Requirements

- DSD Approved Cryptographic Algorithms (DACAs)
- DSD Approved Cryptographic Protocols (DACPs)
- Secure Sockets Layer and Transport Layer Security (SSL/TLS)
- Secure Shell (SSH)
- Secure Multipurpose Internet Mail Extension (S/MIME)
- FIPS 140
- Key Management

Chapter 10 - Network Security

ประกอบด้วยหัวข้อสำคัญ ดังนี้

- Network Management
- Internet work Connections
- Gateways
- Firewalls
- Diodes
- Data Transfer
- Remote Access

DRAFT

- Peripheral Switches
- Virtual LANs
- Multifunction Devices

3.4 สรุป

ในบทนี้ได้ศึกษากรณีการสร้างและกำหนดนโยบายความมั่นคงปลอดภัยด้านไอซีทีและไซเบอร์สเปซ (Cyber Security) ของไทยและในต่างประเทศ ได้แก่ สหรัฐอเมริกา สิงคโปร์ และออสเตรเลีย โดยพิจารณาจากกรอบการทำงาน (Frameworks) ที่เป็นประเด็นหลักของความมั่นคงปลอดภัย ได้แก่ “Process, People and Technology” ซึ่งแยกออกเป็นหัวข้อย่อย คือ ด้านนโยบายและการบริหารจัดการ (Process) ด้านการควบคุมและการปฏิบัติงานตามนโยบาย (People) และ ด้านเทคโนโลยี (Technology) ทั้งนี้เพื่อให้เป็นกรณีศึกษาเปรียบเทียบกับประเทศไทย จากนี้จึงจะวิเคราะห์สภาพแวดล้อมจากยุทธศาสตร์และนโยบายในประเทศ สร้างเป้าหมายเฉพาะด้านความมั่นคงปลอดภัย แล้วจึงกำหนดเป็นแผนที่นำทาง และเป็นร่างแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีต่อไป

DRAFT