แผนแม่บท ICT Security แห่งชาติ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ลงวันที่ 8 กุมภาพันธ์ 2550

คำนำ

การจัดทำแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติ National ICT Security Plan Best Practices ได้มาจากการศึกษาวิเคราะห์ จากสถานภาพปัจจุบันด้านความมั่นคงปลอดภัยของประเทศจากการสำรวจสัมภาษณ์ผู้ที่เกี่ยวข้อง (Focus Group) และจากกลุ่ม CII (Critical Information Infrastructure) โดยวิเคราะห์ตามมาตรฐาน ISO17799 รวมถึงศึกษากรณีศึกษาแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีของต่างประเทศ ได้แก่ ออสเตรเลีย สิงคโปร์ เพื่อมากำหนด วิสัยทัศน์ พันธกิจ วัตถุประสงค์ เป้าหมายและแผนงาน ที่มีความเหมาะสมสำหรับประเทศไทย

แผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติ จะประกอบไปด้วยแผนงานโครงการที่จะต้องดำเนินการ การกำหนดลำดับความสำคัญของแผนให้สอดคล้องกับยุทธศาสตร์ของประเทศ โครงการที่ประเทศต้องรีบดำเนินการเร่งด่วน ตามผลการวิเคราะห์สถานภาพปัจจุบันด้านความมั่นคงปลอดภัยของประเทศ การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยด้านไอซีที ความต้องการหลักสูตรฝึกอบรม ที่เหมาะสมสำหรับประเทศไทย การจัดการด้าน Security Professional Certification สำหรับหน่วยงานต่าง ๆ ของประเทศ พร้อมด้วยแผนงานในการจัดตั้งองค์กรที่กำกับดูแล ความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติ ซึ่งประกอบด้วยโครงสร้างของหน่วยงาน บทบาทหน้าที่ที่รับผิดชอบ เพื่อทำหน้าที่จัดการด้านความมั่นคงปลอดภัยด้านไอซีทีของประเทศต่อไป

สารบัญ

บทที่ 1
บทนำ

ปัจจัยพื้นฐานสำคัญในการลดความเสี่ยงต่ออาชญากรรมคอมพิวเตอร์ เพื่อมุ่งสู่การพัฒนาเศรษฐกิจและสังคมให้ทัดเทียมกับนานาชาติ โดยอาศัยเทคโนโลยีสารสนเทศและการสื่อสาร ประเทศไทยมีความจำเป็นอย่างยิ่งที่จะต้องมีนโยบายการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายสำหรับองค์กรและหน่วยงานต่าง ๆ ตลอดจนผู้ใช้งานระบบและเครือข่ายทั่วไป เพื่อให้การดำเนินการดังกล่าวมีกระบวนการขั้นตอนอย่างเป็นระบบ จึงจำเป็นต้องมีการจัดทำแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติเพื่อกำหนดขอบเขตหรือข้อกำหนดในการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์และเครือข่ายให้กับองค์กรและหน่วยงานต่าง ๆ ในระดับชาติ

ด้วยเหตุนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในฐานะที่เป็นหน่วยงานของภาครัฐที่รับผิดชอบทางด้านนโยบายและแผนแม่บทด้านเทคโนโลยีสารสนเทศของประเทศ จึงได้ดำเนินการจัดทำนโยบาย และแผนแม่บทการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย (ICT Security) สำหรับประเทศไทย เพื่อเป็นกรอบ แนวทางให้องค์กรและหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน รวมถึงประชาชนผู้ใช้ระบบทั่วไป นำไปบังคับใช้ เพื่อให้ข้อมูลและระบบเครือข่ายคอมพิวเตอร์ของประเทศมีความมั่นคงและปลอดภัยโดยรวม

เอกสารฉบับนี้เป็นรายงานแผนแม่บทความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ National ICT Security Master Plan ตามแนวทางของมาตรฐานสากลและความต้องการด้านการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศและการสื่อสารของประเทศ ต่อไปในแผนแม่บทความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติจะเรียกเป็นแผนแม่บท ICT Security แห่งชาติ

เนื่องจากจุดมุ่งหมายของนโยบายในการรักษาความมั่งคงปลอดภัย คือ การกำหนดแนวทางและการดูแลรักษาความปลอดภัยของข้อมูลซึ่งเกี่ยวข้องกับข้อบังคับและกฎหมาย การปฏิบัติงานบางขั้นตอนเกี่ยวข้องกับการพัฒนานโยบายระบบรักษาความปลอดภัย มีส่วนสำคัญที่เป็นการกำหนดแบบแผนนโยบายในการรักษาความปลอดภัย แนวนโยบาย มาตรฐานให้ตรงกับความต้องการที่แท้จริงและลำดับความสำคัญก่อนหลัง โดยการกำหนดแบบแผนจำเป็นต้องครอบคลุมถึงรายละเอียดของการสอดคล้องกันระหว่างการออกกฎหมาย นโยบาย และการควบคุมตามความต้องการ ดังต่อไปนี้

- รูปแบบการศึกษาในส่วนของระบบรักษาความปลอดภัย จัดฝึกอบรม
- การสนับสนุนให้มีการดำเนินการปฏิบัติการอย่างต่อเนื่อง
- การให้ความสำคัญกับการฝ่าฝืนต่อการรักษาความปลอดภัยของข้อมูล

- กระบวนการรับผิดชอบต่อสถานการณ์ทั่วไปและสถานการณ์จำเพาะสำหรับการจัดการรักษาความมั่นคงปลอดภัย
- การควบคุมดูแลกระบวนการต่าง ๆ เพื่อเสถียรภาพของนโยบาย
- วิธีการกำหนดข้อยกเว้นให้แก่นโยบาย และมาตรฐาน
- ระบบจัดการต่าง ๆ เพื่อสร้างความมั่นใจให้แก่ระบบว่า นโยบาย, มาตรฐาน, ระบบการแนะแนว และกระบวนการต่าง ๆ มีการดูแลอย่างสม่ำเสมอ

นโยบายการรักษาความมั่นคงปลอดภัยจักต้องคำนึงถึงประเด็นสำคัญต่อไปนี้

1. โครงสร้างการบริหารระบบรักษาความปลอดภัย

โครงสร้างการบริหารและจัดการมีความสำคัญอย่างยิ่งในการกำหนดรูปแบบการติดตั้งระบบรักษาความปลอดภัย ระบบรักษาความปลอดภัยต่างๆที่สามารถถูกควบคุมและบริหารจัดการตามมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ทั้งนี้ต้องมีการกำหนดและนิยามกระบวนการต่าง ๆ ในการรักษาความปลอดภัยอย่างชัดเจน นอกจากการประสานงานจากองค์กรต่างๆ ที่มีส่วนเกี่ยวข้องตามแผนนโยบายรักษาความปลอดภัยจะต้องดำเนินการตามมาตรฐานสากล

2. ระบบรักษาความปลอดภัยด้านบุคลากร

บุคลากรเป็นส่วนที่เป็นจุดอ่อนที่สุดในสายการทำงานในระบบรักษาความปลอดภัย ซึ่งทำให้นโยบาย มาตรฐาน ข้อแนะนำและแนวทางไม่สามารถทำงานได้อย่างมีประสิทธิภาพหากผู้ใช้งาน และผู้ดูแลระบบนั้น ๆ ไม่สามารถปฏิบัติได้ตรงตามความต้องการของระบบรักษาความปลอดภัย ดังนั้นระบบรักษาความปลอดภัยด้านบุคลากรจึงมีความจำเป็นอย่างมากในแผนแม่บท ICT Security แห่งชาติ การจัดฝึกอบรมในเรื่องของการรักษาความปลอดภัยและการใช้งานระบบอย่างถูกต้องและมีประสิทธิภาพ โดยบุคลากรต้องมีความรู้ความสามารถอยู่ในระดับที่เหมาะสมกับงานที่ตนรับผิดชอบ โดยการจัดทำหลักสูตรการอบรมและพัฒนาบุคคลากรที่มีประสิทธิภาพ

3. การดูแลจัดการระบบคอมพิวเตอร์และเครือข่าย

ระบบเครือข่ายจะต้องมีการควบคุมจัดการด้านความมั่นคงปลอดภัยที่ดี เพื่อให้เกิดความปลอดภัยจากการโจมตี และต้องสามารถดูแลระบบและโปรแกรมต่าง ๆ ผ่านระบบเครือข่าย ความสามารถของระบบรักษาความปลอดภัย ระดับการให้บริการ และการจัดการดูแลของทุกเครือข่ายจะต้องใช้กรรมวิธีมาตรฐานและอุปกรณ์ที่ได้รับการทดสอบด้านความมั่นคงปลอดภัยตามมาตรฐานสากลการต่อเชื่อมเครือข่ายจะต้องมีมาตรฐานความปลอดภัยกำกับเพื่อให้ความมั่นใจกับความปลอดภัยข้อมูลและความเป็นส่วนตัวของข้อมูล

ในการจัดส่งกันในเครือข่ายทั่วไป หรืออินเทอร์เน็ตนอกจากนี้ การกำหนดรูปแบบการแลกเปลี่ยนข้อมูลซึ่งกันและกันถือเป็นเรื่องหลักที่ต้องจัดทำขึ้นเพื่อเป็นมาตรฐานในการแลกเปลี่ยนข้อมูลที่มีการกำกับดูแล

การรักษาความปลอดภัยของการทำธุรกรรมที่มีส่วนเกี่ยวข้องกับระบบอิเล็กทรอนิกส์ รวมถึงการทำธุรกรรมบนเครือข่ายอินเทอร์เน็ต จำเป็นต้องมีการกำหนดการควบคุมดูแล การจำเพาะเจาะจงข้อมูลที่ต้องผ่านเครือข่ายสาธารณะจำเป็นต้องมีกฎหมายด้านความปลอดภัยสารสนเทศตลอดจนมาตรฐานและรูปแบบการรักษาความมั่นคงปลอดภัยต่อรวมกับระบบการค้นหา ป้องกันแก้ไข และการกู้คืนข้อมูลจำเป็นต้องมีการติดตั้งเพื่อให้ความมั่นใจแก่ทุกฝ่านที่เกี่ยวกับธุรกรรมอิเล็กทรอนิกส์

4. การให้สิทธิการใช้และการเข้าถึงข้อมูล

การเข้าถึงข้อมูลจำเป็นต้องมีการควบคุมบนพื้นฐานของการรักษาความปลอดภัย การกำหนดสิทธิการทำงานและเข้าถึงข้อมูลของผู้ใช้จะต้องมีการกำหนดที่ชัดเจนบนนโยบายของหน่วยงาน ผู้ใช้ควรจะได้รับการกำหนดสิทธิให้เข้าถึงข้อมูลหรือระบบเฉพาะส่วนที่จำเป็นและอนุญาตให้ใช้เท่านั้น การให้สิทธิพิเศษในการใช้งานและเข้าถึงข้อมูลควรจะมีเฉพาะในส่วนเหตุการณ์ที่จำเป็นเท่านั้นและจะต้องยกเลิกสิทธินั้นเมื่อเหตุการณ์พิเศษสิ้นสุดแล้ว

เทคนิคและวิธีการให้สิทธิแก่ผู้ใช้งานจำเป็นต้องมีการตัดสินใจที่ดีเพื่อให้สามารถรองรับกับการกำหนดสิทธิต่าง ๆ แก่ผู้ใช้งานได้ การนำเทคโนโลยีต่าง ๆ มาทำให้ระบบมีความเข้มแข็งได้ย่อมมีความสำคัญอย่างยิ่ง อาทิเช่น การเข้ารหัส(Encryption) สมาร์ทการ์ด(Smartcard) การใช้ระบบชีวภาพ(Biometric) สามารถสนับสนุนการสร้างระบบควบคุมการเข้าถึงข้อมูล ดังนั้นการบูรณาการหลาย ๆ เทคโนโลยีเข้าด้วยกันย่อมส่งผลให้การกำหนดสิทธิมีความเข้มแข็งมากขึ้น

นโยบายต่าง ๆ ควรมีการกำหนดตามการใช้งานของการเข้ารหัส โดย Key Management ควรถูกนำมาใช้งานเพื่อควบคุมดูแลการเข้ารหัส ในขั้นตอนการติดตั้งระบบการเข้ารหัส ควรตรึกตรองถึงกฎข้อบังคับของประเทศ ร่วมกันกับการเข้ารหัสของนานาประเทศ ที่เราจะต้องทำธุรกรรมร่วมกัน ดังนั้นการนำผู้เชี่ยวชาญในส่วนนี้มาจัดการจึงมีความจำเป็นอย่างยิ่ง

5. การจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ

ระบบเทคโนโลยีสารสนเทศและการสื่อสารประกอบด้วย ฮาร์ดแวร์ เครือข่าย ซอฟต์แวร์ และบุคลากร กระบวนและขั้นตอนงานต่างๆ ดังนั้นจะต้องคำนึงถึงระบบสารสนเทศทั้งระบบในการรองรับกับเหตุการณ์ต่างๆที่เกิดให้ไม่ว่าจากภายนอกหรือภายในดังนั้นจะต้องสร้างระบบที่ทรงประสิทธิภาพในการรักษาความปลอดภัยโดยสามารถตอบสนองต่อเหตุการณ์ต่างๆ ที่อาจจะเกิดขึ้น เมื่อเกิดช่องโหว่ของการติดต่อสื่อสาร โดยระบบจะต้องสามารถเข้าไปแก้ไขจัดการได้ทันท่วงที

6. การบริหารจัดการธุรกรรมอย่างต่อเนื่อง

การดำเนินธุรกรรมอย่างต่อเนื่อง และแผนการกู้คืนข้อมูลการดำเนินการมีความสำคัญต่อการดำเนินงานเป็นอย่างยิ่งโดยเฉพาะส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานวิกฤตของประเทศ(Critical Infrastructure) เช่น โรงกลั่นน้ำมัน ที่ทำการรัฐบาลและโครงสร้างพื้นฐานวิกฤตด้านสารสนเทศ(Critical Information Infrastructure) เช่น ศูนย์ข้อมูลกรมสรรพากร ระบบสื่อสารดาวเทียมเครือข่ายโทรทัศน์ เป็นต้น โครงสร้างเหล่านี้ถือเป็นโครงสร้างที่สำคัญมากของประเทศที่จำเป็นต้องมีการทำงานอย่างต่อเนื่องในสภาวะปกติและในสภาวะที่ถูกโจมตี การบริหารจัดการในระดับประเทศนี้จะต้องมีการวางแผนให้มีผลกระทบในการสูญเสียให้น้อยที่สุดและอยู่ในระดับที่สามารถควบคุมดูแลได้

นอกจากนี้การวิเคราะห์ค่าความเสียหายจากการถูกคุกคาม ความล้มเหลวในการรักษาความปลอดภัย ความขัดข้องในการให้บริการ ตลอดจนการวิเคราะห์ความเสี่ยงจำเป็นต้องมีการวางแผนการวิเคราะห์โดยประเมินค่าจากการดำเนินกิจการในระดับประเทศเป็นหลัก การดูแลแก้ไขและกู้คืนข้อมูลสำคัญต่าง ๆ ที่บกพร่องไปจะต้องมีการดำเนินการอย่างเพียงพอ โดยสอดรับกับแผนแม่บท ICT Security แห่งชาติและแผนปฏิบัติการที่เกี่ยวข้องเช่นแผนเตรียมความพร้อมแห่งชาติด้านการสื่อสาร เป็นต้น

การจัดทำแผนแม่บท ICT Security แห่งชาตินั้นจะต้องคำนึงถึงประเด็นสำคัญที่กล่าวมาแล้วนอกจากนั้นยังต้องกำหนดแผนให้สอดคล้องกับมาตรฐานด้านความมั่นคงปลอดภัยสากลได้แก่มาตรฐานชุด ISO 27000 ทั้งนี้การจัดทำโครงการแผนแม่บท ICT Security แห่งชาติจะมีวัตถุประสงค์และเป้าหมายดังนี้

- **วัตถุประสงค์**
  - เพื่อสำรวจแนวทางการจัดทำแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติในต่างประเทศ(National ICT Security Plan Best Practices)
  - เพื่อสำรวจและวิเคราะห์สถานภาพปัจจุบันของประเทศไทยด้านความมั่นคงปลอดภัย
  - เพื่อกำหนดกรอบนโยบาย แนวทางดำเนินการ และมาตรการเพื่อการบริหารจัดการ ICT Security ของประเทศ
  - เพื่อจัดทำแนวทางบริหารจัดการดำเนินการ เพื่อพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยด้านไอซีทีของประเทศ

- **เป้าหมาย**
  - การทำธุรกรรมทางอิเล็กทรอนิกส์มีความปลอดภัย
  - หน่วยงานภาครัฐและสังคมมีความปลอดภัยตามมาตรฐานที่ได้กำหนด
  - อุปกรณ์ที่ใช้ในระบบเครือข่าย ต้องมีการจัดมาตรฐานความปลอดภัย

- มีโครงสร้างองค์กรที่รับผิดชอบในเรื่อง ICT Security แห่งชาติ ในการผลักดันให้เป็นไปตามแผนแม่บท ICT Security แห่งชาติ

ดังนั้นแผนแม่บทความมั่นคงปลอดภัยด้านไอซีที (ICT Security Master Plan) เป็นแผนที่นำทางทางกลยุทธ์ (a Strategic Roadmap) ซึ่งจำเป็นสำหรับการริเริ่มโครงการระดับชาติเพื่อที่จะคุ้มครองโครงสร้างพื้นฐานวิกฤตของชาติ (Critical Information Infrastructure) จากภัยคุกคามทางไซเบอร์ เพื่อที่จะลดผลกระทบจากเหตุ ตลอดจนการฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว แผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติจะช่วยจัดตั้งรูปแบบและลำดับความสำคัญในบริบทของ ความมั่นคงปลอดภัยด้านไอซีทีเมื่อคำนึงถึงสถานการณ์ปัจจุบันและการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องทั้งหลาย ทั้งที่จะเกิดต่อภาคประชาชน ภาคเอกชนและภาครัฐบาล การออกแบบแผนแม่บทฉบับนี้ต้องการที่จะจัดให้มีองค์การที่มีกรอบการทำงานและเครื่องมือที่จำเป็นอย่างพอเพียง เพื่อที่จะสนับสนุนกิจกรรมต่างๆ ที่จะเกิดขึ้นมาหลังจากการนำแผนไปปฏิบัติแล้ว เป็นแผนแม่บทฯ ในระยะสามปี

แผนแม่บท ICT Security แห่งชาติจะประกอบด้วยหัวข้อสำคัญแบ่งได้เป็น 7 บทดังต่อไปนี้คือ

1 บทนำ

2 การศึกษานโยบายความมั่นคงและปลอดภัย ICT ของประเทศไทย เพื่อศึกษาถึงนโยบายระดับชาติ ในส่วนที่เกี่ยวข้อง เพื่อให้แผนแม่บท ICT Security แห่งชาติ สอดคล้องและสนับสนุนกับยุทธศาสตร์ชาติ ในด้านต่าง ๆ

- นโยบายจากกรอบการพัฒนา ICT 2010
- นโยบายการร่างประมวลกฎหมายด้าน ICT
- นโยบายเตรียมความพร้อมแห่งชาติด้านข้อมูลสารสนเทศ เป็นต้น
- นโยบาย ICT ด้านสนับสนุน

3 การกำหนดยุทธ์ศาสตร์

- วิสัยทัศน์พันธกิจและวัตถุประสงค์
- SWOT และยุทธศาสตร์
- ยุทธศาสตร์ เป้าหมาย แผนงาน และโครงการ
- โครงการริเริ่ม (Initiative Programmers) เพื่อส่งเสริม ICT Security แห่งชาติ
- การกำหนดความเร่งด่วนของโครงการ
- การกำหนดงบประมาณ
- ผู้รับผิดชอบโครงการ

4 แผนปฏิบัติการ โครงการเร่งด่วน

นำเสนอโครงการเร่งด่วน ลำดับต้น ที่จะต้องดำเนินการก่อนในช่วงแรกของแผนปฏิบัติงานได้แก่

- การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ
- ประเมินความพร้อมด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงานภาครัฐ
- ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ
- โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ
- โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ
- โครงการฝึกอบรม ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

5 แผนงานพัฒนาบุคลากรและถ่ายทอดเทคโนโลยี

- ความต้องการการฝึกอบรม
- หลักสูตรฝึกอบรมและหลักสูตรระดับปริญญาบัตร

- การบริหารจัดการด้าน Security Professional Certification สำหรับหน่วยงานภาครัฐและเอกชน

6 แผนการจัดตั้งองค์กรกำกับดูแลด้าน ICT Security

- สำนักงานนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และการสื่อสาร (Office of the ICT Security Policy)
- โครงสร้างหน่วยงาน

7. การติดตามผลประเมินผล

- ดัชนีชี้วัดเพื่อการติดตามประเมินผล
- ความสัมพันธ์ของดัชนีชี้วัด ลิขิตสมดุลย์ เป้าหมาย และแผนงานด้านการสื่อสาร

บทที่ 2
สถานภาพนโยบายและการปฏิบัติด้าน ICT Security

ในบทที่ 2 นี้จะสรุปถึง นโยบาย กฎหมาย หลักปฏิบัติด้าน ICT Security ในประเทศไทยโดยเริ่มที่พิจารณากรอบของ IT 2010 ซึ่งเป็นฐานในการกำหนดแผนแม่บทไอซีทีแห่งชาติฉบับปี 2544-2549 จากนั้นก็ทบทวนกฎหมายไอซีทีที่อยู่ในสถานภาพต่างๆ ในด้านการเตรียมพร้อมแห่งชาติก็พิจารณาการเตรียมการด้านการสื่อสารและด้านเทคโนโลยีสารสนเทศจากนั้นก็พิจารณาแนวนโยบายสำหรับแนวปฏิบัติด้านการวิจัยพัฒนาเทคโนโลยีการบริหารจัดการและการบริหารโครงการด้าน ICT Security ซึ่งเป็นสิ่งที่ประเทศไทยยังไม่เริ่มหรือได้ดำเนินการแล้วเป็นบางส่วนแต่ไม่บูรณาการหัวข้อที่จะอธิบายประกอบด้วย

- นโยบายจากกรอบการพัฒนา IT 2010
- นโยบายการร่างประมวลกฎหมายด้านไอซีที
  - กฎหมายประกอบนโยบายด้านเทคโนโลยีสารสนเทศ
  - กฎหมายลำดับรองภายใต้ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ
- นโยบายเตรียมความพร้อมแห่งชาติด้านข้อมูลสารสนเทศ
- นโยบาย ICT ด้านสนับสนุนอื่นๆ
  - การวิจัยและพัฒนา
  - เทคโนโลยี
  - การบริหารจัดการ
  - การบริหารโครงการ

2.1 นโยบายจากกรอบการพัฒนา IT 2010

นโยบายกรอบพัฒนา IT 2010 ตามรูป 2.1 เน้นการพัฒนาเทคโนโลยีสารสนเทศใน 5 ด้าน ได้แก่

- e – Industry
- e – Commerce
- e – Education
- e – Government
- e – Society

บนฐานของการวิจัยและพัฒนาองค์ความรู้ การพัฒนาบุคลากรและสร้างโครงสร้างพื้นฐานด้วย ไอซีที เพื่อนำไปสู่เป้าหมายของการสร้างเศรษฐกิจกับสารสนเทศ สำหรับสังคมที่มีความพร้อมด้านการใช้ไอซีทีในกรอบนโยบายนี้ เป้าหมายคือการสร้างประเทศที่ใช้ไอซีที อย่างมีประสิทธิภาพและมีประสิทธิผลกรอบ

IT2010 ไม่ได้เน้นความปลอดภัยในการใช้ ไอซีที และการรักษาความเป็นส่วนบุคคลซึ่งจะต้องได้รับความคุ้มครองอย่างเต็มที่ตามแนวทางที่กำหนดในแผนแม่บท ICT Security แห่งชาติ

e-Industry **e-Commerce**	**e-Government**	**e-Society** **e-Education**
Science & Technology ,R&D ,Knowledge		
Information Development ,IT Literacy ,IT HR		
Telecommunication Infrastructure		
Quantity		**Quality**

รูปที่ 2.1 กรอบนโยบายการพัฒนา ICT IT2010 (ICT Development Policy Framework)

อย่างไรก็ตาม ในกรอบ IT2010 ยังไม่มีการเน้นประเด็น ICT Security ดังนั้น แผนแม่บท ICT Security แห่งชาติจักต้องปรับกรอบ IT2010 ให้ครอบคลุมเรื่องความมั่นคงปลอดภัยสารสนเทศเนื่องจากการพัฒนาระบบสารสนเทศ ในปัจจุบันล้วนแต่ทำงานบนอินเตอร์เน็ตทำให้ทุกระบบเชื่อมกันหมดและเปิดโอกาสให้มีการโจมตีทั้งระบบได้ง่าย ดังนั้น จะต้องมีการกำหนดกรอบ กรรมวิธี เทคโนโลยีเพื่อเสริมสร้างความปลอดภัยให้แก่ระบบสารสนเทศ

e-Industry **e-Commerce**	**e-Government**	**e-Society** **e-Education**	**Nation ICT Security OP.Center** **ICT Security Management**
Science & Technology ,R&D ,Knowledge			**ICT Security R&D, ICT Security Standards**
Information Development ,IT Literacy ,IT HR			**ICT Security System Development** **HRD, Capacity Building**
Telecommunication Infrastructure			**Security Infrastructure**
Quantity		**Quality**	

รูปที่ 2.2 การเสริมสร้างกรอบ IT2010 โดยแผนแม่บท ICT Security แห่งชาติ

ในการนี้กรอบ IT2010 จะต้องมีการประกอบด้วยโครงสร้างตามรูป 2.2 ชั้นต่อชั้นได้แก่ ICT Security Management Information System (ISMS) พร้อมกับศูนย์ปฏิบัติการ ICT Security แห่งชาติซึ่งจะได้รับการสนับสนุนสำหรับวิจัยพัฒนาด้านความมั่นคงปลอดภัยชั้นองค์ความรู้ด้านความมั่นคงปลอดภัย เช่น มาตรฐานด้านความมั่นคงปลอดภัยต่างๆ เทคโนโลยีอุปกรณ์ด้านรักษาความมั่นคงปลอดภัยถัดลงไปก็

เป็นขั้นการพัฒนาระบบสารสนเทศที่มั่นคงปลอดภัยและพัฒนาบุคลากรด้าน ICT Security ในชั้นล่างสุดจะเป็นเรื่องความมั่นคงปลอดภัยเครือข่ายทั้งหมดนี้เฉกเช่นกับกรอบIT2010 ต้องมีการพัฒนาทั้งปริมาณและคุณภาพเพื่อให้เพียงพอกับความต้องการของประเทศไทยในอนาคต

2.2 นโยบายการร่างประมวลกฎหมายด้านไอซีที

ในการกฎหมายที่จะสนับสนุนการพัฒนาไอซีที ของประเทศได้มีการดำเนินการมาแล้วเป็นลำดับ แต่ยังอยู่ในกระบวนการออกกฎหมายอีกหลายฉบับ ซึ่งกฎหมายเหล่านี้จะเป็นการให้ความมั่นใจและกำหนดกฎกติกาการดำเนินการโดยใช้ไอซีที อย่างปลอดภัย ยุติธรรม และตั้งอยู่บนพื้นฐานของความเท่าเทียมกัน สถานภาพกฎหมายไอซีที ในขณะนี้สรุปได้ดังนี้

2.2.1 กฎหมายประกอบนโยบายด้านเทคโนโลยีสารสนเทศ

- กฎหมายเทคโนโลยีสารสนเทศฉบับแรก ชื่อว่า กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งตราขึ้นเมื่อปี 2544 แต่มีผลบังคับใช้เมื่อเมษายน 2545 กฎหมายฉบับนี้ตราขึ้นเพื่อรองรับผลทางกฎหมายของข้อความหรือนิติกรรมสัญญาที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ รวมทั้งลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายที่แน่นอนเทียบเท่ากับนิติกรรมสัญญาหรือผลผูกพันที่ตกลงหรือทำการผ่านกระดาษ
- กฎหมายเทคโนโลยีสารสนเทศฉบับที่สอง คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เห็นชอบร่างพระราชกฤษฎีกาว่าด้วยการกำกับดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ... ไปเมื่อวันที่ 30 กันยายน 2548
- กฎหมายเทคโนโลยีสารสนเทศฉบับที่สาม เป็นกฎหมายที่ตราขึ้นเพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรืออาชญากรรมทางคอมพิวเตอร์ จึงชื่อว่าร่างพระราชบัญญัติการกระทำความผิดเกี่ยงกับคอมพิวเตอร์ พ.ศ. ...
- กฎหมายเทคโนโลยีฉบับที่สี่นั้น เป็นกฎหมายที่ตราขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคล
- กฎหมายเทคโนโลยีสารสนเทศฉบับที่ห้าที่ได้มีการพัฒนามาพร้อมๆกันตั้งแต่ปี 2541 ก็คือ การผลักดันการจัดทำกฎหมายลำดับรองภายใต้มาตรา 78 ของรัฐธรรมนูญ เพื่อจัดทำให้มีการพัฒนาโครงสร้างพื้นฐานสารสนเทศที่ทั่วถึงและเท่าเทียมกัน อันเป็นการสร้างความเข้มแข็งให้กับชุมชนในการยืนหยัดต่อสู้แข่งขันในภาวะที่โลกมีการปรับเปลี่ยนหรือมีพัฒนาการและการเปลี่ยนแปลงที่รวดเร็วเช่นนี้ได้

2.2.2 กฎหมายลำดับรองภายใต้ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ จำนวน 5 ฉบับ

- พ.ร.ฎ.กำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ มาบังคับใช้

- ร่าง พ.ร.ฎ.กำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ... โดยความจำเป็นในการตรา เพราะปัจจุบันมีการทำธุรกรรมทางอิเล็กทรอนิกส์มากขึ้นทั้งการดำเนินกิจกรรมของหน่วยงาน นอกหน่วยงานและประชาชนในรูปแบบต่างๆ ในขณะที่หน่วยงานภาครัฐยังไม่มีความพร้อม อันอาจจะเป็นปัญหาและอุปสรรคสำคัญ
- ร่าง พ.ร.ฎ.ว่าด้วยการกำกับดูแลธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ... โดยร่างกฎหมายฉบับนี้ ออกตามความในมาตรา 32 แห่ง พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ เนื่องจากธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ถือเป็นหนึ่งในประเภทธุรกิจที่คณะอนุกรรมการกำกับฯ มีนโยบายที่จะกำกับดูแล เพราะเป็นธุรกิจที่มีผล กระทบต่อสาธารณะชนและยังเป็นธุรกรรมที่มีผลกระทบต่อความมั่นคงทางการเงินและการพาณิชย์
- ร่าง พ.ร.ฎ.ว่าด้วยการกำกับดูแลธุรกิจให้บริการออกใบรับรองอิเล็กทรอนิกส์ พ.ศ... โดยร่างกฎหมายฉบับนี้ ออกตามความในมาตรา 32 แห่ง พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ เนื่องจากการออกใบรับรองทางอิเล็กทรอนิกส์ถือเป็นหนึ่งในประเภทธุรกิจที่คณะอนุกรรมการกำกับฯ มีนโยบายที่จะกำกับดูแลเช่นเดียวกับธุรกิจบริการประเภทการชำระเงินทางอิเล็กทรอนิกส์ เพราะส่งผลโดยตรงต่อความน่าเชื่อถือในข้อมูลอิเล็กทรอนิกส์
- ร่าง พ.ร.ฎ.กำหนดวิธีการแบบปลอดภัย พ.ศ... โดยร่างกฎหมายฉบับนี้ ออกตามความในมาตรา 25 แห่ง พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ โดยเป็นการกำหนดวิธีการแบบปลอดภัยที่จะทำให้ธุรกรรมนั้นๆ เป็นธุรกรรมที่เชื่อถือได้ตามข้อสันนิษฐานของกฎหมาย ขณะเดียวกันยังเป็นความจำเป็นที่จะต้องมีการกำหนดเกี่ยวกับวิธีการแบบปลอดภัยตามมาตรฐานสากลเพื่อใช้เป็นกรอบในการทำธุรกรรมทางอิเล็กทรอนิกส์ทั่วไป

ในปัจจุบันประมวลกฎหมายด้านไอซีทียังเป็นกระบวนการที่อยู่ในช่วงพัฒนาอย่างต่อเนื่อง การนำแผนแม่บท ICT Security แห่งชาติมาใช้นั้นจะต้องมีกฎหมายที่รองรับในการรับรองทางอิเล็กทรอนิกส์ กฎหมายที่รับรองความเป็นส่วนบุคคลเพื่อให้ความมั่นใจแก่ประชาชนชาวไทยในการไม่ถูกล่วงละเมิดสิทธิเสรีภาพพื้นฐานส่วนบุคคลนอกจากนั้นยังต้องมีกฎหมายที่กำหนดบทลงโทษอย่างจริงจังต่ออาชญากรรมด้านที่เกี่ยวข้องกับระบบและด้านสารสนเทศต่างๆ

2.3 นโยบายเตรียมความพร้อมแห่งชาติด้านข้อมูลสารสนเทศ

คณะรัฐมนตรีมีมติเมื่อวันที่ 4 กุมภาพันธ์ 2535 ให้ความเห็นชอบแผนเตรียมพร้อมแห่งชาติ พ.ศ. 2535 เพื่อใช้เป็นแผนหลักในการเตรียมพร้อมของชาติในเรื่องทรัพยากรด้านต่างๆ 14 ด้านตั้งแต่ภาวะปกติ ในอันที่จะให้ประเทศมีความพร้อมรับสถานการณ์ในภาวะไม่ปกติ อันเนื่องมาจากภัยคุกคามจากภัยธรรมชาติ ผู้ก่อการร้าย และกำลังทหารจากภายนอกประเทศได้อย่างมีประสิทธิภาพ โดยสามารถรักษาความต่อเนื่องในการบริหารราชการ รักษาความสงบเรียบร้อยเพื่อความอยู่รอดปลอดภัยของชาติและประชาชน ซึ่งแผนเตรียมความพร้อมในด้านต่างๆ รวม 14 ด้าน จะต้องดำเนินการทุกด้านอย่างบูรณาการเพื่อสามารถสนับสนุน การป้องกันประเทศและรักษาความอยู่รอดของบ้านเมือง และเสถียรภาพของเศรษฐกิจไว้ได้

ตารางที่ 2.1 การเตรียมพร้อมด้านต่างๆ (พ.ศ. 2535)

การเตรียมพร้อมด้านต่างๆ	
1) การจัดระเบียบบริหารราชการในภาวะไม่ปกติ	8) การขนส่ง
2) การป้องกันภัยฝ่ายพลเรือน	9) การสื่อสาร
3) การประชาสัมพันธ์และควบคุมข่าวในภาวะไม่ปกติ	10) น้ำ
4) การระดมสรรพกำลังเพื่อการทหาร	11) เชื้อเพลิงและพลังงาน
5) การจัดเสถียรภาพทางเศรษฐกิจ	12) การแพทย์และการสาธารณสุข
6) อาหาร วัตถุดิบ วัสดุอุปกรณ์การเกษตร	13) กำลังคน
7) อุตสาหกรรมและปัจจัยการผลิต	14) พื้นที่

ในส่วนที่เกี่ยวข้องกับการเตรียมความพร้อมด้านการสื่อสารนั้น สภาความมั่นคงแห่งชาติได้ จัดทำแผนเตรียมพร้อมด้านสื่อสารที่ 1/2541 ขึ้นในปี พ.ศ .2541 โดยได้กำหนดเป็นกรอบนโยบายและแนวทางดำเนินการเพื่อเสริมสร้างศักยภาพด้านการสื่อสาร ให้สามารถสนองความต้องการของทหารและพลเรือนในการป้องกันภัยคุกคามจากภายนอกประเทศ รวมทั้งยังสามารถใช้แผนเตรียมพร้อมฉบับนี้ในการป้องกันและบรรเทาสาธารณภัยและภัยธรรมชาติ ซึ่งมีแนวโน้มจะทวีความรุนแรงยิ่งขึ้นด้วย

รัฐบาลซึ่งได้ให้ความสำคัญกับการเตรียมความพร้อมในการจัดการสถานการณ์ฉุกเฉินอันเกิดจากภัยด้านสาธารณภัยและภัยด้านความมั่นคงให้ได้อย่างทันท่วงทีและมีประสิทธิภาพ จึงได้ปรับปรุงนโยบายเตรียมพร้อมแห่งชาติใหม่ใน พ.ศ. 2548 เมื่อวันที่ 20 ธันวาคม 2548 คณะรัฐมนตรีได้มีมติเห็น

ชอบกับนโยบายการเตรียมพร้อมแห่งชาติ และให้ยกเลิกแผนเตรียมพร้อมแห่งชาติ พ.ศ. 2535 โดยให้ใช้นโยบายการเตรียมพร้อมแห่งชาติ เป็นกรอบการกำหนดยุทธศาสตร์ มาตรการ แผนปฏิบัติการ เพื่อให้บริการจัดการสาธารณภัย ภัยด้านความมั่นคง และสถานการณ์ฉุกเฉินได้อย่างมีประสิทธิภาพ โดย ให้หน่วยงานที่เกี่ยวข้องเร่งจัดทำแผนปฏิบัติการให้สอดคล้องตามนโยบายการเตรียมพร้อมแห่งชาติดังกล่าว และซักซ้อมการปฏิบัติตามแผนเป็นระยะตามความเหมาะสมด้วย

ทั้งนี้ ความสำคัญของนโยบาย การเตรียมพร้อมแห่งชาติ มีวัตถุประสงค์หลักที่สำคัญ เพื่อใช้เป็นแผนหลักของชาติในการเตรียมความพร้อมด้านมาตรการและด้านทรัพยากรต่าง ๆ ให้มีความพร้อมในอันที่จะป้องกัน บรรเทาภัยและช่วยเหลือประชาชนให้สามารถอยู่รอดปลอดภัยในภาวะปกติและไม่ปกติ ประกอบกับสถานการณ์ในปัจจุบันได้เปลี่ยนแปลงไป โดยเฉพาะภัยจากสาธารณภัยขนาดใหญ่มีแนวโน้มขยายพื้นที่มากขึ้น และเพิ่มระดับการเกิดบ่อยครั้งขึ้น ดังนั้น เพื่อให้ประเทศไทยมีความพร้อมรับสถานการณ์ในภาวะดังกล่าวได้อย่างมีประสิทธิภาพ สามารถรักษาความต่อเนื่องในการบริหารราชการ รักษาความสงบเรียบร้อยของประเทศและเสถียรภาพทางเศรษฐกิจไว้ได้ รวมทั้งสามารถสนับสนุนการป้องกันประเทศและรักษาความอยู่รอดปลอดภัยของชาติและประชาชน ทั้งนี้ นโยบายการเตรียมพร้อมแห่งชาติมีดังกล่าว ได้เน้นให้ความสำคัญ 4 ประการ ดังนี้

1) การเตรียมความพร้อมด้านทรัพยากร ทุกภาคส่วนได้มีการเตรียมความพร้อมในการป้องกันภัย การบรรเทาภัย การระงับภัย และการฟื้นฟูภายหลังจากการเกิดภัย ให้พร้อมเผชิญสาธารณภัย ภัยด้านความมั่นคง และสถานการณ์ฉุกเฉิน
2) การมีส่วนร่วมของทุภาคส่วน ให้ หน่วยงานภาครัฐ รัฐวิสาหกิจ ภาคเอกชน องค์กรเอกชน และภาคประชาชน มีส่วนร่วมและสนับสนุนแผนป้องกันภัยฝ่ายพลเรือนแห่งชาติ และแผนป้องกันประเทศ
3) การจัดทำแผนให้ หน่วยงานได้ยึดถือสำหรับจัดทำแผนรองรับในการป้องกันภัย การบรรเทาภัย การระงับภัย และการฟื้นฟูภายหลังจากการเกิดภัย ภัยด้านความมั่นคง และสถานการณ์ฉุกเฉินที่เกิดขึ้นให้ประสานสอดคล้องและเชื่อมโยงกันอย่างเป็นระบบ
4) การบริหารจัดการให้ การบริหารจัดการในการเตรียมพร้อมทั้งระบบมีเอกภาพ ประสิทธิภาพ และทันท่วงที ในทุกสถานการณ์

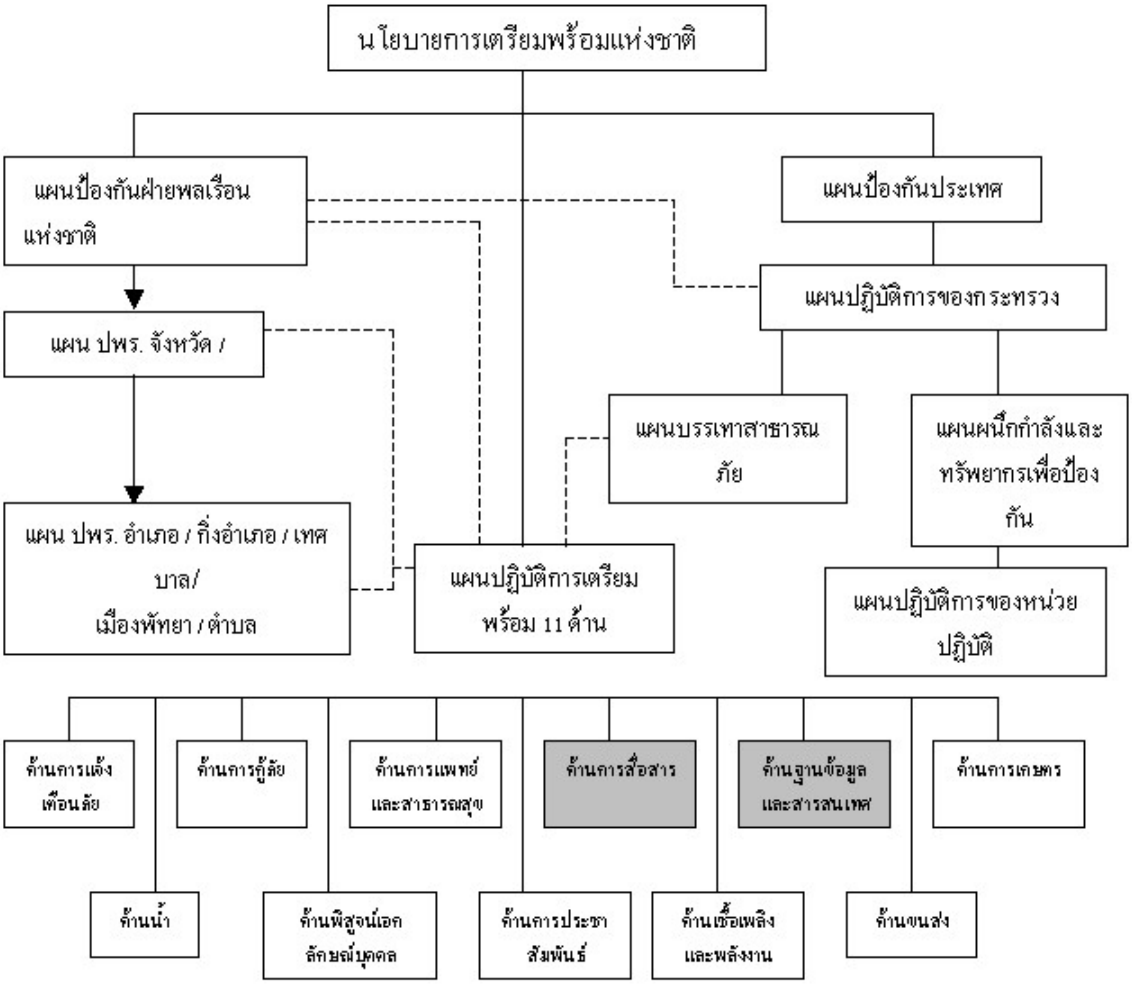
พร้อมกันนี้ได้มีการแบ่งมอบหมายการปฏิบัติตามนโยบายการเตรียมความพร้อมแห่งชาติ ออกเป็น 4 ส่วน และแบ่งหน้าที่รับผิดชอบให้มีหน่วยงานหลักและหน่วยงานรองรับผิดชอบไว้ด้วย สำหรับในการจัดทำแผนปฏิบัติการเตรียมความพร้อมด้านต่าง ๆ โดยที่หน่วยงานจะต้องจัดทำแผนปฏิบัติการเตรียมความพร้อมภายใต้ความรับผิดชอบของหน่วยงานมารองรับ กรณีเมื่อเกิดสถานการณ์ภัยพิบัติ โดยในขั้นต้นจะ

กำหนด การเตรียมความพร้อมด้านต่าง ๆ ไว้รวม 11 ด้าน ตามตาราง 2.2 และภาพรวมในรูป 2.3 โดยที่การปฏิบัติการเตรียมความพร้อมด้านการสื่อสารนั้น เป็นหน้าที่ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ตารางที่ 2.2 การเตรียมพร้อมด้านต่างๆ (พ.ศ. 2549)

การเตรียมพร้อมด้านต่างๆ (2549)	
1) ด้านการแจ้งเตือนภัย (ตพ.1) 2) ด้านการกู้ภัย (ตพ.2) 3) ด้านน้ำ (ตพ.3) 4) ด้านการแพทย์และสาธารณสุข (ตพ.4) 5) ด้านพิสูจน์เอกลักษณ์บุคคล (ตพ.5) 6) ด้านการสื่อสาร (ตพ.6)	7) ด้านการประชาสัมพันธ์ (ตพ. 7) 8) ด้านฐานข้อมูลและสารสนเทศ (ตพ.8) 9) ด้านเชื้อเพลิงและพลังงาน (ตพ.9) 10) ด้านการเกษตร (ตพ.10) 11) ด้านการขนส่ง (ตพ.11)

แผนแม่บท ICT Security แห่งชาติจะต้องเนื่องกับการเตรียมระดับฐานข้อมูลสารสนเทศ ตลอดจนการเตรียมด้านการสื่อสาร โดยจะต้องผลักดันให้ฐานข้อมูลสารสนเทศ และการสื่อสารมีความมั่นคงปลอดภัยจากการโจมตี การปลอมแปลง และการตัดทอนในระหว่างการปฏิบัติงานในภาวะฉุกเฉิน และจะต้องกำหนดมาตรการการเตรียมพร้อมที่ลดความเสี่ยงและเพิ่มความปลอดภัยด้านเทคโนโลยีสารสนเทศเพื่อให้การดำเนินการทางองค์กรสามารถทำได้อย่างต่อเนื่องในช่วงเกิดสภาวะฉุกเฉินและหลังจากสภาวะฉุกเฉินผ่านพ้นไปแล้ว นอกจากนั้นการเตรียมความพร้อมในด้านอื่นๆ ที่กำหนดถ้ามีการใช้ระบบเทคโนโลยีสารสนเทศ แล้วก็จะต้องดำเนินการให้มีความมั่นคงปลอดภัยตามแนวทางที่กำหนดในแผนแม่บท ICT Security แห่งชาติ



รูปที่ 2.3: ภาพรวมของแผนปฏิบัติการเตรียมพร้อม 11 ด้าน

2.4 นโยบาย ICT ด้านสนับสนุนอื่น ๆ

2.4.1 การวิจัยและพัฒนา

การวิจัยและพัฒนาด้าน ICT Security ในประเทศไทยยังไม่ได้เริ่มต้น หน่วยงานที่สนับสนุนด้านการวิจัย เช่น สำนักงานกองทุนวิจัยไทย (Thai Research Fund) ก็ให้การสนับสนุนโครงการวิจัยที่เกี่ยวกับ ICT Security เพียงโครงการเดียว[1] ส่วนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) แม้จะมีการจัดตั้งโครงการ Thai CERT ซึ่งสนับสนุนการเผยแพร่ความรู้ด้าน ICT Security แต่ก็มิได้มีภารกิจในการวิจัยและพัฒนาด้าน ICT Security แต่อย่างใด สำหรับงานวิจัยในระดับมหาบัณฑิต และดุษฎีมหาวิทยาลัยในประเทศไทย ยังไม่ปรากฏกิจกรรมการวิจัยในด้านนี้อย่างชัดเจน

ตามแนวนโยบายของกรอบ IT2010 และแผนแม่บท ICT Security แห่งชาติ ฉบับ 2544-2549 ได้กำหนดยุทธศาสตร์สำหรับประเทศไทยที่จะพัฒนาขีดความสามารถด้านสารสนเทศเพื่อการแข่งขันกับนานาชาติ แต่ในทศวรรษที่ผ่านมาก็ขาดการสนับสนุนด้านการพัฒนาพื้นฐานความรู้เทคโนโลยีสารสนเทศและการสื่อสารอย่างจริงจัง และยังไม่มีการสนับสนุนการวิจัยและพัฒนาด้าน ICT Security ซึ่งใช้เป็นฐานในการดำเนินการบริการและสร้างอุตสาหกรรม ICT Security

เพื่อให้ประเทศไทยสามารถพึ่งพาตนเองทางด้านเทคโนโลยี แผนแม่บท ICT Security แห่งชาติ มีแนวนโยบายและปฏิบัติการชัดเจนในการสนับสนุนให้อาจารย์ในมหาวิทยาลัยภาครัฐและเอกชนดำเนินการวิจัยและพัฒนาด้าน ICT Security ตามตาราง 2.3

ตารางที่ 2.3 หัวข้อวิจัยด้าน **ICT Security**

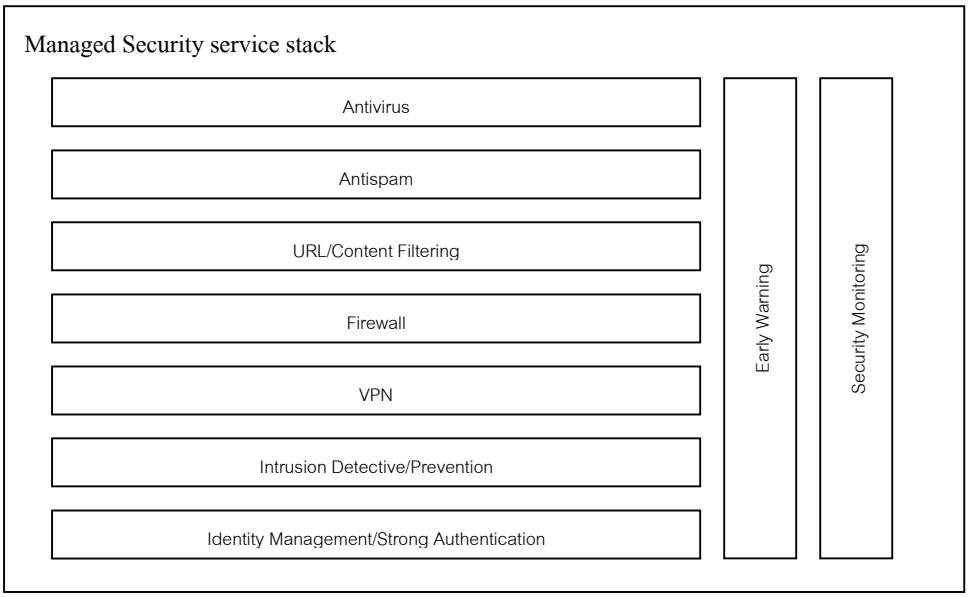
หัวข้อวิจัยที่เร่งด่วน	คำอธิบาย	หัวข้อย่อย
เทคโนโลยีด้าน Authentication	- การระบุตัวตน - การอนุมัติ - การตรวจสอบความถูกต้อง ฮาร์ดแวร์, ซอฟต์แวร์	- การกระจาย public key - การจัดการ Certificate และการยกเลิก Certificate - การใช้ร่วมกับ Token และ biometric - การแยกของการระบุตัวตน เพื่อความเป็นส่วนตัว
โปรโตคอลพื้นฐานที่มั่นคงปลอดภัย	- การทำให้โปรโตคอลที่ใช้ในปัจจุบันมีความมั่นคงปลอดภัย	- โปรโตคอล VoIP และ VPN - การ Trade off ระหว่างความปลอดภัยและ

หัวข้อวิจัยที่เร่งด่วน	**คำอธิบาย**	**หัวข้อย่อย**
		สมรรถนะ
การประกันความมั่นคงปลอดภัยของกิจกรรมซอฟต์แวร์ และฮาร์ดแวร์	- การพัฒนาขบวนการและกรรมวิธีที่อยู่บนพื้นฐานของวิทยาศาสตร์และการควบคุมที่เข้มข้น	- ภาษาโปรแกรมที่มีขีดความสามารถของความมั่นคงปลอดภัย - Code ที่มั่นคงปลอดภัยที่ใช้ซ้ำได้
ความมั่นคงปลอดภัยแบบเต็มรูปแบบ	- การบูรณาการความปลอดภัยเข้าไปในระบบเพื่อลดความซ้ำซ้อน	- สภาพแวดล้อมที่มีอุปสรรค์และระบบเก่าที่ไม่ปลอดภัยกับระบบใหม่ - การโจมตีจากภายใน - ข้อผิดพลาดในระบบที่ซ้ำซ้อน
สอดส่องและตรวจจับ	ติดตามและวิธีตอบสนองการโจมตีแบบใหม่	- การสอดส่องแบบ Real Time - การตรวจจับการโจมตีในระดับบนสุด
กรรมวิธีการลดความเสี่ยงและการกู้ฟื้น	รูปแบบและขั้นตอนการตอบสนองอย่างรวดเร็วต่อภัยที่จะเกิดขึ้น	- วิธีรักษาระบบด้วยตนเอง (Self Healing) - วิธีต้านข้อผิดพลาด (Fault Tolerant)
ไซเบอร์ฟอเร็นสิกส์	การควบคุมอาชญากรรมแบบ Online เพื่อที่จะป้องกันการเกิดอาชญากรรม และการจับผู้ต้องสงสัย	- การสืบค้นย้อนกลับ - การทำ delimiting
การทำโมเดลและต้นแบบทดสอบ	การทำโมเดลที่สมจริงและมีโครงการนำร่องเพื่อที่จะพิจารณาสินค้าด้านความปลอดภัยอย่างต่อเนื่อง	- การจัดทำต้นแบบ - การ Update ผ่านเครือข่าย
ตัวชี้วัดการเปรียบเทียบและ	กระบวนการขั้นตอนมาตรฐาน	- ตัวชี้วัด

หัวข้อวิจัยที่เร่งด่วน	**คำอธิบาย**	**หัวข้อย่อย**
การดำเนินการที่ Best Practice	ในการประเมินเทคโนโลยีใหม่	- การนำ Certificate อย่างอัตโนมัติ - การวิเคราะห์ความเสี่ยง
ประเด็นที่ไม่เกี่ยวกับเทคโนโลยี	- ด้านจิตวิทยา - เศรษฐศาสตร์ - สังคม	- ข้อแนะนำการพิจารณา - การประเมินผลส่วนตัว - ตระหนักถึงประเด็นเศรษฐกิจและความปลอดภัย

2.4.2 เทคโนโลยี

การใช้เทคโนโลยีด้านรักษาความมั่นคงปลอดภัยของหน่วยงานในไทยทำในรูปแบบที่นำอุปกรณ์ด้าน ICT Security เท่าที่จำเป็นมาใช้โดยส่วนใหญ่แล้วจะไม่มีการนำมาใช้อย่างเป็นระบบหรือเต็มรูปแบบ และยังไม่ได้นำเทคโนโลยีกระบวนการบริหารจัดการด้าน ICT Security ที่เป็นมาตรฐานมาใช้ในองค์กร เทคโนโลยี ICT Security แบ่งเป็น 3 ส่วน เทคโนโลยีด้านฮาร์ดแวร์ เทคโนโลยีซอฟต์แวร์ และเทคโนโลยีด้านกระบวนการ (ส่วนบริการ) ในการนี้ การจัดการกับ ICT Security อย่างเป็นระบบตาม



รูปที่ 2.4 การจัดการป้องกันเทคโนโลยีอย่างเป็นระบบ

รูปแบบการโจมตีต่างๆ ที่กำหนดในกรอบการใช้เทคโนโลยีด้านความมั่นคงปลอดภัยอย่างเป็นระบบในรูปที่ 2.4 ซึ่งเน้นเทคโนโลยีฮาร์ดแวร์และระบบซอฟต์แวร์ที่จำเป็นต้องมีในการสร้างระบบความมั่นคงปลอดภัย ทั่วไปแล้วจะต้องพิจารณาให้ครบทุกด้าน ดังนี้

- การปฏิบัติงานของเจ้าหน้าที่ทุกระดับ
- การออกแบบสถาปัตยกรรมที่รักษาความมั่นคงปลอดภัย
- การใช้เทคโนโลยีเข้ารหัส
- การพิสูจน์ตัวตนและการอนุมัติสิทธิ
- การจัดการระบบและเครือข่าย
- การสอดส่องและตรวจสอบ
- การรับมือกับเหตุการณ์
- การมีระบบสำรองและการกู้ภัย
- การรักษาความปลอดภัยเชิงกายภาพ

ส่วนการบริหารจัดการการโจมตีรูปแบบต่างๆ นั้นในปัจจุบันจะอิงมาตรฐานตระกูล ISO 27000 แต่โดยทั่วไปแล้วจะต้องมีนโยบายที่ชัดเจนในประเด็นต่างๆ ดังนี้

- ระเบียบและนโยบายด้านรักษาความมั่นคงปลอดภัย
- การดำเนินการด้านรักษาความมั่นคงปลอดภัย
- การจัดการด้านการรักษาความมั่นคงปลอดภัยอย่างเป็นระบบและร่วมกัน
- การมีกลยุทธตามแนวปฏิบัติที่เป็นเลิศด้านการรักษาความมั่นคงปลอดภัย
- การพัฒนาบุคลากรให้มีความรู้ ทักษะและความสามารถด้านการรักษาความมั่นคงปลอดภัย
- การพัฒนาบุคลากรในองค์กรให้มีความรู้ และจิตสำนึกด้านการรักษาความมั่นคงปลอดภัย

2.4.3 การบริหารจัดการ

ในระดับองค์กรขนาดใหญ่ ทั่วไปแล้วจะต้องบริหารจัดการเพื่อให้พันธกิจ และธุรกิจขององค์กรดำเนินการไปได้อย่างต่อเนื่อง (Business Continuity) และในกรณีที่เกิดภาวะฉุกเฉินด้านความมั่นคงปลอดภัย แล้วสามารถฟื้นคืนสู่สภาพเดิมได้อย่างรวดเร็ว (Disaster Recovery) ตามโครงสร้างตามรูป 2.5 ซึ่งแสดงถึงการบริการใน 3 ระดับได้แก่ การให้บริการที่ปรึกษาด้านบริหารจัดการ การให้บริการที่ปรึกษาด้านระบบ และการพัฒนาระบบ IT ที่สนับสนุนการดำเนินการอย่างปลอดภัย และมีความพร้อมรองรับการโจมตีด้าน ICT และพร้อมรับภัยพิบัติด้านอื่นๆ

ในระดับองค์กร สิ่งที่ต้องการเตรียมพร้อมด้าน ICT Security คือการนำ ISMS (Information Security Management System) มาใช้กับองค์กร ตามมาตรฐานชุด ISO/IEC 27000 ซึ่งประกอบด้วย

ISO/IEC 27000 Fundamental and Vocabulary

มาตรฐาน ISO/IEC 27001 ISMS Requirement

มาตรฐาน ISO/IEC 27002 ISMS Code of practice

มาตรฐาน ISO/IEC 27003 ISMS Implementation Guideline

มาตรฐาน ISO/IEC 27004 ISMS Measurements

มาตรฐาน ISO/IEC 27005 ISMS Risk Management

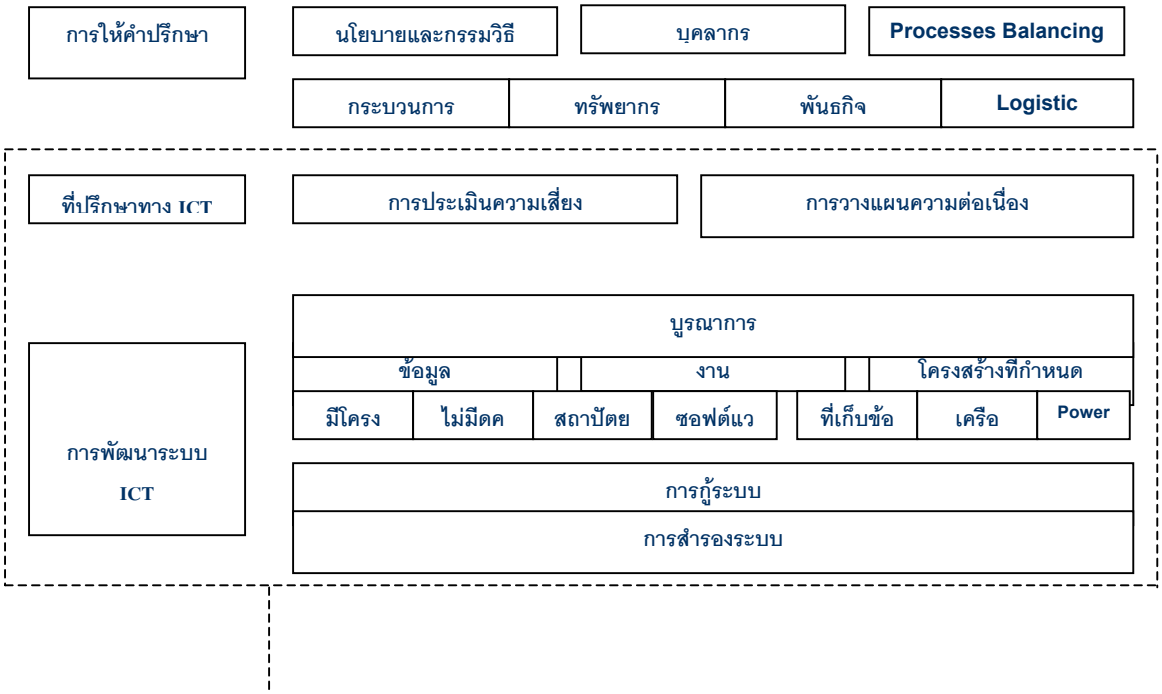
มาตรฐาน ISO/IEC 27006 ISMS Accreditation Guideline

ทั้งนี้จะต้องมีการพัฒนาบุคลากรกำหนดทรัพยากรที่ต้องใช้และการกำหนดกระบวนงานที่มาตรฐานต่างๆ บุคลากรภายในหรือจากภายนอกจำนวนหนึ่งต้องได้รับ Certification ด้าน ISMS เพื่อการประกันคุณภาพในการดำเนินการด้าน ICT Security ทั้งนี้การนำ ISMS มาใช้ โดยรับบริการที่ปรึกษาจากหน่วยงานที่ใช้ ISMS Certification ได้ จะช่วยให้

- ลดความเสี่ยงจากการโจมตีทาง ICT
- นำไปสู่การดำเนินงานที่โปร่งใสตรวจสอบได้ และมีประสิทธิภาพ

เพื่อให้การนำมาตรฐาน ISO 27000 จะต้องมีนโยบายที่ชัดเจนว่าหน่วยงานภาครัฐ และภาคเอกชนที่เกี่ยวเนื่องการทำงานกับภาครัฐจะต้องมีการดำเนินการ Certification ตามกรรมวิธี ISMS หรือมาตรฐานอื่นตามธุรกิจนั้น

- ต้องสนับสนุนให้มีบริษัทให้บริการด้านฝึกอบรม ISMS และให้ใบรับรอง
- ต้องสนับสนุนให้สถาบันการศึกษาเปิดหลักสูตรด้าน ICT Security

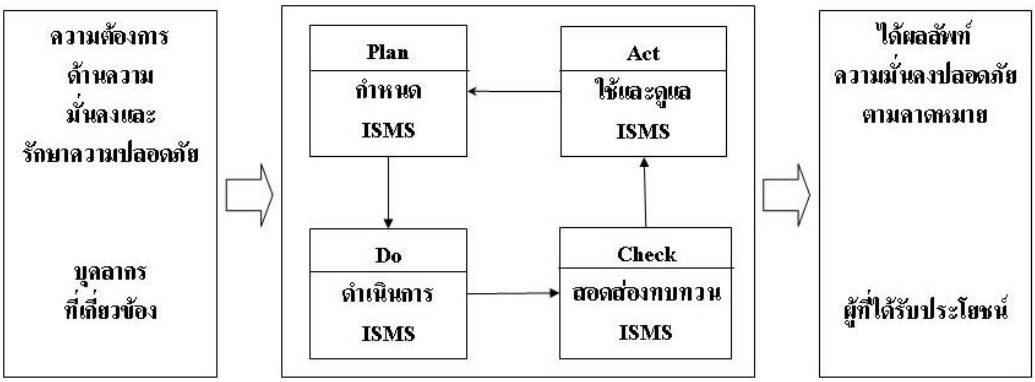


รูปที่ 2.5 กรอบการให้บริการด้าน ICT Security

2.4.4 การบริหารโครงการ

หน่วยงานที่ดำเนินการเตรียมความพร้อมด้าน ICT Security เพื่อสร้างความมั่นใจจะสามารถป้องกันการโจมตี และเมื่อมีการโจมตีเกิดขึ้นแล้วสามารถตอบสนองทันท่วงที และยังต้องมีความพร้อมและกรรมวิธีการสำรองระบบ เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง โดยที่ข้อมูลและระบบบริการมีความมั่นคงปลอดภัยและสมบูรณ์

กรรมวิธีบริหารโครงการด้าน ICT Security จะต้องทำตามกรรมวิธีมาตรฐาน ISMS เริ่มที่มาตรฐาน ISO/IEC 27001 จะต้องตรงกับความต้องการด้าน ICT Security แล้วเดินตามโมเดล PDCA ตามรูปแบบที่กำหนดใน มาตรฐาน ISO 27001 ตามรูป 2.6



รูปที่ 2.6 PDCA ใช้ในมาตรฐาน ISO 27001

ซึ่งการใช้กรรมวิธีนี้จะช่วยให้สามารถดำเนินการปรับปรุงความปลอดภัยสารสนเทศได้อย่างต่อเนื่อง ทั้งนี้การบริหารโดย ISMS จะทำใน 10 ขั้นตอน ดังนี้

ขั้นตอน	การดำเนินงาน	ผลลัพธ์
1	นิยามขอบเขตของ ISMS	ขอบเขตงาน ISMS
2	นิยามนโยบาย ISMS	นโยบาย ISMS
3	นิยามความเสี่ยงต่อระบบสารสนเทศ	บันทึกวิธีการประเมินความเสี่ยงประเภทต่าง
4	หาความเสี่ยงที่ได้	รายการของความเสี่ยง , โอกาสที่ถูกโจมตีสำหรับแต่ละความเสี่ยงและผลกระทบ
5	ดำเนินการประเมินความเสี่ยง	รายงานผลกระทบ และโครงการที่อาจเกิดขึ้น

ขั้นตอน	การดำเนินงาน	ผลลัพธ์
6	การจัดการกับความเสี่ยง	ประเมินวิธีการจัดการความเสี่ยงทางเลี่ยงและความเสี่ยง และวิธีการควบคุม
7	เลือกวัตถุประสงค์ควบคุม และวิธีการ	รายการวัตถุประสงค์ควบคุมและวิธีควบคุม
8	ขออนุมัติความเห็นชอบจากผู้บริหารในเรื่องความเสี่ยงที่เหลือที่ยังไม่ได้จัดการ	รายงานความเสี่ยงที่เหลืออยู่ที่ยังไม่ได้จัดการ
9	ขออนุมัติให้ดำเนินการ ISMS ได้	คำอนุมัติของผู้บริหารให้ดำเนินการ ISMS ได้
10	เตรียมรายงานวัตถุประสงค์การควบคุม วิธีควบคุม และ/หรือเขตที่ไม่ควบคุม	รายงานการจัดการความเสี่ยง

บทที่ 3
การกำหนดยุทธศาสตร์ ICT Security

3.1 วิสัยทัศน์พันธกิจและวัตถุประสงค์

วิสัยทัศน์

ประเทศไทยมีระบบรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายสำหรับองค์กรและหน่วยงานต่าง ๆ ตลอดจนผู้ใช้งานระบบและเครือข่ายทั่วไปตามมาตรฐานสากล และประเทศไทยเป็นผู้นำด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

พันธกิจ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในฐานะที่เป็นหน่วยงานของภาครัฐที่รับผิดชอบทางด้านนโยบายและแผนแม่บทด้านเทคโนโลยีสารสนเทศของประเทศ จึงเป็นผู้จัดทำนโยบาย และนำแผนแม่บท ICT Security แห่งชาติ และนำไปปฏิบัติเพื่อให้องค์กรและหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน รวมถึงประชาชนผู้ใช้ระบบทั่วไป นำไปบังคับใช้ เพื่อให้ข้อมูลและระบบเครือข่ายคอมพิวเตอร์ของประเทศมีความมั่นคงและปลอดภัยโดยรวม ทั้งสนับสนุนการพัฒนาฐานวิจัยและพัฒนาด้านรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

วัตถุประสงค์

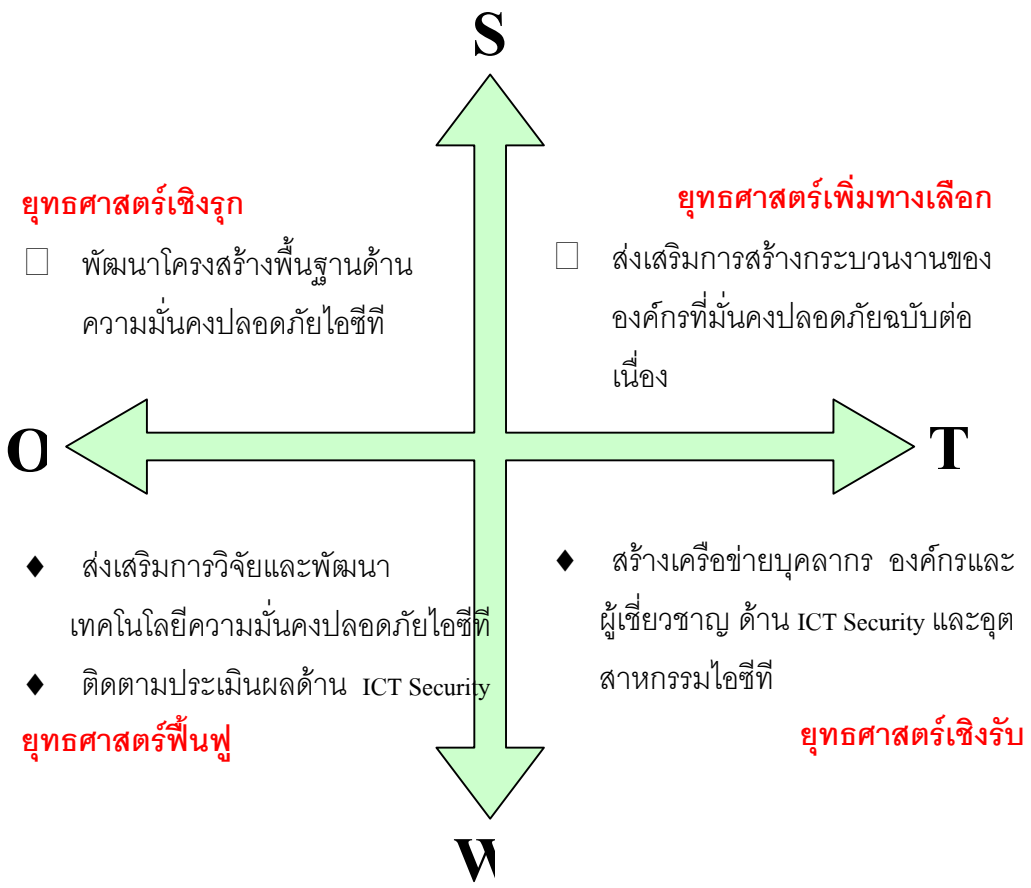
1. เพื่อกำหนดแนวทางการพัฒนาขีดความสามารถด้าน ICT Security
2. เพื่อดำเนินการพัฒนากระบวนการรักษาความมั่นคงปลอดภัยอย่างเป็นระบบ
3. เพื่อให้หน่วยงานและภาครัฐสามารถดำเนินการเตรียมความพร้อมการดำเนินงานอย่างต่อเนื่องภายใต้สถานการณ์ฉุกเฉิน
4. เพื่อส่งเสริมการพัฒนาบุคลากรและอุตสาหกรรมด้าน ICT Security
5. เพื่อกำหนดกรอบนโยบาย แนวทางดำเนินการ และมาตรการเพื่อการบริหารจัดการ ICT Security ของประเทศ
6. เพื่อจัดทำแนวทางบริหารจัดการดำเนินการ เพื่อพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยด้านไอซีทีของประเทศ

เป้าหมาย

1. การทำธุรกรรมทางอิเล็กทรอนิกส์มีความปลอดภัย
2. หน่วยงานภาครัฐและสังคมมีความปลอดภัยตามมาตรฐานที่ได้กำหนด
3. อุปกรณ์ที่ใช้ในระบบเครือข่าย ต้องมีการจัดมาตรฐานความปลอดภัย

3.2 SWOT และยุทธศาสตร์

ในการวิเคราะห์ SWOT (Strength Weakness Opportunity Threat) เพื่อหาจุดแข็ง จุดอ่อน โอกาสและภัยคุกคามด้าน ICT Security นั้นได้จัดทำโดยผ่านการประชาพิจารณ์และรับฟังข้อแนะนำจากผู้ชำนาญการด้านต่างๆซึ่งเพื่อพิจารณาถึงตัวประกอบหลัดที่มีผลต่อแต่ละด้านแล้วก็ได้วิเคราะห์หาแนวยุทธศาสตร์ 4 แบบได้แก่ ยุทธศาสตร์เชิงรุก ยุทธศาสตร์เพิ่มทางเลือก ยุทธศาสตร์ฟื้นฟู และยุทธศาสตร์เชิงรับ โดยมีแผนงานที่สอดคล้องรองรับแต่ละยุทธศาสตร์ตามรูป 3.1 ส่วนรูป 3.2 นั้นแสดงรายละเอียดของตัวประกอบหลักของแต่ละมิติที่วิเคราะห์ได้แก่ มิติโอกาส มิติภัยคุกคาม มิติจุดแข็ง และมิติจุดอ่อน



รูปที่ 3.1 รูปแสดงความสัมพันธ์ระหว่าง SWOT กับ แผนยุทธศาสตร์

	จุดแข็ง (S)	**จุดอ่อน (W)**
	• รัฐบาลกำหนดนโยบายอย่างชัดเจนที่จะเตรียมความพร้อมด้านความมั่นคงปลอดภัยฯ • ประเทศไทยมีการพัฒนาด้านไอซีทีอย่างต่อเนื่อง ทำให้สามารถระดมบุคลากรด้านไอซีทีได้จำนวนมาก • การบริหารงป.ภาครัฐ และธุรกิจในประเทศ เป็นระบบใหม่ที่มุ่งผลสัมฤทธิ์ตามเป้าหมายที่ชัดเจน เช่น ด้านความมั่นคงปลอดภัยฯ เป็นต้น	• ระบบไอซีทีภายในประเทศไม่มีความพร้อมในการบริหารจัดการด้านความมั่นคงปลอดภัยฯ ทั้งในด้านงบประมาณและองค์การ • การขาดแคลนองค์ความรู้ กระบวนการและบุคลากรด้านความมั่นคงปลอดภัยฯ • กฎหมาย ระเบียบ ข้อบังคับ ทั้งหลายที่เกี่ยวข้องยังไม่พร้อมใช้บังคับ • ประชาชนยังไม่มีความรู้และความเข้าใจในด้านความมั่นคงปลอดภัยอย่างพอเพียง
โอกาส(O) • ปัจจุบันทั่วโลกได้ตระหนักถึงผลกระทบจากความไม่มั่นคงที่เกิดแก่ไอซีที ทำให้ประเทศไทย ซึ่งต้องพึ่งพาการค้ากับประชาคมโลก จำเป็นต้องลงทุนมากขึ้นในการพัฒนาระบบไอซีที โดยเฉพาะอย่างยิ่งเพื่อให้เกิดความมั่นคงปลอดภัยฯ ในระดับมาตรฐานนานาชาติ • ประเทศไทยสามารถพัฒนามาตรฐานความมั่นคงปลอดภัยฯ ได้ในเวลาสั้นและด้วยต้นทุนที่ประหยัด	**ยุทธศาสตร์เชิงรุก** • พัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไอซีที	**ยุทธศาสตร์ฟื้นฟู** • ส่งเสริมการวิจัยและพัฒนาเทคโนโลยีความมั่นคงปลอดภัยไอซีที • ติดตามประเมินผลด้าน ICT Security
ภัยคุกคาม (T) • มีความเสี่ยงเพิ่มขึ้นเนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ ทั้งในประเทศ และระหว่างประเทศ • การเชื่อมต่อระบบงานผ่านอินเตอร์เน็ต ทำให้การโจมตีจากภายนอกประเทศหรือภายนอกระบบสามารถทำได้ง่ายและขยายผลความเสียหายไปได้อย่างรวดเร็ว	**ยุทธศาสตร์เพิ่มทางเลือก** • ส่งเสริมการสร้างกระบวนงานขององค์กรที่มั่นคงปลอดภัยอย่างต่อเนื่อง	**ยุทธศาสตร์เชิงรับ** • สร้างเครือข่ายบุคลากร องค์กรและผู้เชี่ยวชาญ ด้าน ICT Security และอุตสาหกรรมไอซีที

รูปที่ 3.2 รูปแสดงความสัมพันธ์ระหว่าง SWOT กับ แผนยุทธศาสตร์

3.3 ยุทธศาสตร์ เป้าหมาย แผนงาน และโครงการ

ยุทธศาสตร์เชิงรุก (Aggressive)

<u>ยุทธศาสตร์ 1</u> พัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไอซีที

การเสริมสร้างความเข้มแข็งของ ICT Security ของประเทศจะต้องดำเนินการทั้งด้านนโยบายและการปฏิบัติการโดยองค์กรหรือหน่วยงานใหม่หรือดั่งเดิมที่เกี่ยวข้องจะต้องดำเนินการกำจัดความเสี่ยงต่างๆ ที่เกิดจากการใช้ ICT โดยต้องมีศูนย์กลางการดำเนินการมีกระบวนการขั้นตอนและใช้เทคโนโลยีด้าน ICT Security ตามมาตรฐานสากล

เป้าหมาย

- สามารถสร้างศูนย์ปฏิบัติการภายใน 3 ปี และสนับสนุนให้มีการใช้
- สามารถดำเนินการจัดทำโครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติได้ภายใน 3 ปี
- สามารถดำเนินการจัดทำโครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย (Lawful Interception)ได้ภายใน 3 ปี

แผนงาน

- ส่งเสริมการจัดการความเสี่ยงจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

โครงการ

- ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ
- โครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติ
- โครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย (Lawful Interception)

ยุทธศาสตร์ฟื้นฟู (Turnaround)

<u>ยุทธศาสตร์ที่ 2</u> ส่งเสริมการวิจัยและพัฒนาเทคโนโลยีความมั่นคงปลอดภัยไอซีที

การดำเนินการตั้งรับด้าน ICT Security จะต้องดำเนินการอย่างต่อเนื่องทั้งติดตามเทคโนโลยีใหม่ๆ ที่ต้องนำมาประยุกต์ใช้และต้องดำเนินการวิจัยพัฒนากระบวนการขั้นตอนเทคโนโลยีตลอดจนนำแนวทางปฏิบัติที่เป็นเลิศและมาตรฐานด้าน ICT Security มาปรับใช้กับสภาพแวดล้อมของประเทศไทยโดยอาศัยบุคลากรและผู้เชี่ยวชาญจากหน่วยงานภาครัฐและมหาวิทยาลัยทั้งภาครัฐและเอกชนมาร่วมดำเนินการด้านวิจัยพัฒนาและประยุกต์ใช้เทคโนโลยีด้าน ICT Security ระดับสากล

เป้าหมาย

- สามารถดำเนินการได้ภายใน 1 ปี
- สามารถกำหนดมาตรฐานได้ภายใน 2 ปี
- สามารถมีระบบการเข้ารหัสได้ภายใน 3 ปี

แผนงาน

- พัฒนาเทคโนโลยีการจัดการระบบสารสนเทศและเครือข่าย

โครงการ

- ประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- การจัดทำมาตรฐานและการรับรองผลิตภัณฑ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยด้านไอซีที
- โครงการวิจัยและพัฒนาระบบการเข้ารหัสข้อมูลเพื่อเป็นมาตรฐานของชาติ

ยุทธศาสตร์ 4 ติดตามประเมินผลด้าน ICT Security

การดำเนินการ ICT Security จะต้องมีการตื่นตัวและปรับตามกลยุทธ์ใหม่ๆที่ใช้โจมตีระบบ ICT ดังนั้นการประเมินผลแผนงาน โครงการ การดำเนินงานในระดับต่างๆอย่างต่อเนื่องจึงมีความสำคัญอย่างยิ่งยวด เพื่อให้ความมั่นใจว่า สามารถตอบสนองต่อเหตุการณ์ที่ไม่คาดคิดได้ทันเวลาและสามารถเรียนรู้จากบทเรียนที่เกิดจากความผิดพลาดที่เกิดขึ้นแล้ว

เป้าหมาย

- สามารถจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยได้ภายใน 1 ปี

แผนงาน

- การบังคับใช้กฎ ระเบียบและการวัดผล (Compliance and Measurement)

โครงการ

- โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ

ยุทธศาสตร์เชิงเพิ่มทางเลือก (Diversification)

ยุทธศาสตร์ 3 ส่งเสริมการสร้างกระบวนงานขององค์กรที่มั่นคงปลอดภัยอย่างต่อเนื่อง

เมื่อเกิดเหตุการณ์ฉุกเฉินด้าน ICT Security ด้านภัยธรรมชาติ ด้านผู้ก่อการร้ายซึ่งอาจมีผลกระทบต่อการดำเนินการธุรกิจภาคเอกชน เช่น ตลาดหลักทรัพย์ ธนาคาร ธุรกิจส่งออก ธุรกิจการบิน และการดำเนินงานภาครัฐ เช่น ระบบ e-Service ต่างๆ จำเป็นต้องมีมาตรการที่ทำให้ธุรกิจและพันธกิจดำเนินต่อได้ภายใต้

สภาวะความเสียหายที่กำลังเกิดขึ้นหรือได้เกิดขึ้นแล้วในการนี้ทุกภาคส่วนจะต้องมีการจัดทำแผนงานรองรับในเรื่องความต่อเนื่องของธุรกิจและกำหนด นโยบาย อุปกรณ์ กระบวนการ ขั้นตอนต่างๆที่ต้องดำเนินการในสภาวะฉุกเฉินต่างๆ

<u>เป้าหมาย</u>

- สามารถจัดทำกรอบได้ภายใน 2 ปี
- สามารถกำหนดนโยบายได้ภายใน 2 ปี
- มีหน่วยงานไม่ต่ำกว่า 30 แห่งที่จัดทำนโยบาย ICT Security ต่อปี
- สามารถจัดทำได้ไม่ต่ำกว่า 50 แห่งต่อปี

แผนงาน

- พัฒนาระบบการบริหารจัดการด้านความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)
- ส่งเสริมนโยบายด้านความมั่นคงปลอดภัยและการจัดองค์กร

โครงการ

- กรอบโครงสร้างด้านความต่อเนื่องในการดำเนินงานขององค์กร
- การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ (National Security Policy)
- จัดทำนโยบาย ICT Security ประจำหน่วยงาน
- จัดทำร่างคำของบประมาณด้าน ICT Security ประจำหน่วยงาน

ยุทธศาสตร์เชิงรับ (Defense)

<u>ยุทธศาสตร์ที่ 5</u> สร้างเครือข่ายบุคลากร องค์กรและผู้เชี่ยวชาญ ด้าน ICT Security และอุตสาหกรรมไอซีที

ในการเตรียมความพร้อมด้าน ICT Security และสร้างกลไกต่างๆที่เสริมความแข็งแกร่งเข้าประเทศไทยด้าน ICT Security จำเป็นต้องให้ประชาชนและหน่วยงานทุกส่วนภาค ตระหนักถึงความสำคัญของเรื่องนี้ เพื่อที่จะเป็นพลังหนุนในการพัฒนาบุคคลากรที่มีความเชี่ยวชาญด้าน ICT Security ในทุกระดับของการใช้งานเทคโนโลยี และจะต้องมีบุคคลากรที่ผ่านการรับรองวิทยฐานะด้านมาตรฐาน ICT Security ที่ยอมรับกันทั่วโลก

<u>เป้าหมาย</u>

- มีผู้เข้าร่วมโครงการไม่ต่ำกว่า 5,000 คนต่อปี
- มีบุคลากรที่สอบผ่านการรับรองความสามารถการดำเนินการด้านความมั่นคงปลอดภัยไม่ต่ำกว่า 50 คนต่อปี

- สามารถจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security ได้ภายใน 3 ปี
- มีผู้ที่ผ่านการอบรมหลักสูตรวุฒิบัตรไม่ต่ำกว่า 2,000 คนต่อปี

<u>แผนงาน</u>

- พัฒนาบุคลากรด้าน ICT Security
- แผนงานส่งเสริมการพัฒนายุทธศาสตร์ICT Security

โครงการ

- โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ
- โครงการส่งเสริมการสร้างวิชาชีพด้านความมั่นคงปลอดภัยแห่งชาติ
- โครงการจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security
- โครงการฝึกอบรมด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Training)

ตาราง 3.1 แสดงข้อมูลสรุปของแผนยุทธศาสตร์รวมถึงแผนงานโครงการและเป้าหมายของแต่ละโครงการ

ตาราง 3.1 สรุปยุทธศาสตร์ แผนงาน เป้าหมายและโครงการ

ยุทธศาสตร์	แผนงาน	โครงการ	เป้าหมาย
ยุทธศาสตร์ 1 พัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไอซีที *"การเสริมสร้างความเข้มแข็งของ ICT Security ของประเทศจะต้องดำเนินการทั้งด้านนโยบายและการปฏิบัติการ โดยองค์กรหรือหน่วยงานใหม่หรือดั่งเดิมที่เกี่ยวข้องจะต้องดำเนินการกำจัดความเสี่ยงต่างๆที่เกิดจากการใช้ ICT โดยต้องมีศูนย์กลางการดำเนินการมีกระบวนการขั้นตอนและใช้เทคโนโลยีด้าน ICT Security ตามมาตรฐานสากล"*	• ส่งเสริมการจัดการความเสี่ยงจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	• ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ	☐ สามารถจัดตั้งศูนย์ฯได้ภายใน 3 ปี
		☐ โครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติ	☐ สามารถดำเนินการได้ภายใน 3 ปี
		☐ โครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย (Lawful Interception)	☐ สามารถดำเนินการได้ภายใน 3 ปี
ยุทธศาสตร์ที่ 2 ส่งเสริมการวิจัยและพัฒนาเทคโนโลยีความมั่นคงปลอดภัยไอซีที *"การดำเนินการตั้งรับด้าน ICT Security จะต้องดำเนินการอย่างต่อเนื่องทั้งติดตามเทคโนโลยีใหม่ๆที่ต้องนำมาประยุกต์ใช้และต้องดำเนินการวิจัยพัฒนากระบวนการขั้นตอนเทคโนโลยีตลอดจน*	• พัฒนาเทคโนโลยีการจัดการระบบสารสนเทศและเครือข่าย	☐ ประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร	☐ สามารถดำเนินการได้ภายใน 1 ปี

ยุทธศาสตร์	แผนงาน	โครงการ	เป้าหมาย
นำแนวทางปฏิบัติที่เป็นเลิศและมาตรฐานด้าน ICT Security มาปรับใช้กับสภาพแวดล้อมของประเทศไทยโดยอาศัยบุคลากรและผู้เชี่ยวชาญจากหน่วยงานภาครัฐและมหาวิทยาลัยทั้งภาครัฐและเอกชนมาร่วมดำเนินการด้านวิจัยพัฒนาและประยุกต์ใช้เทคโนโลยีด้าน ICT Security ระดับสากล"		☐ การจัดทำมาตรฐานและการรับรองผลิตภัณฑ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยด้านไอซีที	☐ สามารถกำหนดมาตรฐานได้ภายใน 2 ปี
		• โครงการวิจัยและพัฒนาระบบการเข้ารหัสข้อมูลเพื่อเป็นมาตรฐานของชาติ	☐ สามารถมีระบบการเข้ารหัสได้ภายใน 3 ปี
<u>ยุทธศาสตร์ 3</u> ส่งเสริมการสร้างกระบวนงานขององค์กรที่มั่นคงปลอดภัยฉบับต่อเนื่อง *"เมื่อเกิดเหตุการณ์ฉุกเฉินด้าน ICT Security ด้านภัยธรรมชาติ ด้านผู้ก่อการร้ายซึ่งอาจมีผลกระทบต่อการดำเนินการธุรกิจภาคเอกชน เช่น ตลาดหลักทรัพย์ ธนาคาร ธุรกิจส่งออก ธุรกิจการบิน และการดำเนินงานภาครัฐ เช่น ระบบ e-Service ต่างๆ จำเป็นต้องมีมาตรการที่ทำให้ธุรกิจและพันธกิจดำเนินต่อได้ภายใต้สภาวะความเสียหายที่กำลังเกิดขึ้นหรือได้เกิดขึ้นแล้วในการนี้ทุกภาคส่วนจะต้องมีการจัดทำแผนงานรองรับในเรื่องความต่อเนื่องของธุรกิจและกำหนด นโยบาย อุปกรณ์ กระบวนการ ขั้นตอนต่างๆที่*	• พัฒนาระบบการบริหารจัดการด้านความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)	• กรอบโครงสร้างด้านความต่อเนื่องในการดำเนินงานขององค์กร	☐ สามารถจัดทำกรอบได้ภายใน 2 ปี
	☐ ส่งเสริมนโยบายด้านความมั่นคงปลอดภัยและการจัดองค์กร	• การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ (National Security Policy)	☐ สามารถกำหนดนโยบายได้ภายใน 2 ปี

ยุทธศาสตร์	แผนงาน	โครงการ	เป้าหมาย
ธุรกิจและกำหนด นโยบาย อุปกรณ์ กระบวนการ ขั้นตอนต่างๆที่ต้องดำเนินการในสภาวะฉุกเฉินต่างๆ"		● จัดทำนโยบาย ICT Security ประจำหน่วยงาน	● มีหน่วยงานไม่ต่ำกว่า 30 แห่งที่จัดทำนโยบาย ICT Security ต่อปี
		● จัดทำร่างคำของบประมาณด้าน ICT Security ประจำหน่วยงาน	☐ สามารถจัดทำได้ไม่ต่ำกว่า 50 แห่งต่อปี
<u>ยุทธศาสตร์ 4</u> ติดตามประเมินผลด้าน ICT Security *"การดำเนินการ ICT Security จะต้องมีการตื่นตัวและปรับตามกลยุทธ์ใหม่ๆที่ใช้โจมตีระบบ ICT ดังนั้นการประเมินผลแผนงาน โครงการ การดำเนินงานในระดับต่างๆอย่างต่อเนื่องจึงมีความสำคัญอย่างยิ่งยวด เพื่อให้ความมั่นใจว่า สามารถตอบสนองต่อ*	● การบังคับใช้กฎ ระเบียบและการวัดผล (Compliance and Measurement)	☐ โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ	☐ สามารถจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยได้ภายใน 1 ปี

ยุทธศาสตร์	แผนงาน	โครงการ	เป้าหมาย
เหตุการณ์ที่ไม่คาดคิดได้ทันเวลาและสามารถเรียนรู้จากบทเรียนที่เกิดจากความผิดพลาดที่เกิดขึ้นแล้ว"			
<u>ยุทธศาสตร์ที่ 5</u> สร้างเครือข่ายบุคลากร องค์กรและผู้เชี่ยวชาญด้าน ICT Security และอุตสาหกรรมไอซีที *"ในการเตรียมความพร้อมด้าน ICT Security และสร้างกลไกต่างๆ ที่เสริมความแข็งแกร่งเข้าประเทศไทยด้าน ICT Security จำเป็นต้องให้ประชาชนและหน่วยงานทุกส่วนภาค ตระหนักถึงความสำคัญของเรื่องนี้ เพื่อที่จะเป็นพลังหนุนในการพัฒนาบุคคลากรที่มีความเชี่ยวชาญด้าน ICT Security ในทุกระดับของการใช้งานเทคโนโลยี และจะต้องมีบุคคลากรที่ผ่านการรับรองวิทยฐานะด้านมาตรฐาน ICT Security ที่ยอมรับกันทั่วโลก"*	• พัฒนาบุคลากรด้าน ICT Security	• โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ	☐ มีผู้เข้าร่วมโครงการไม่ต่ำกว่า 5,000 คนต่อปี
	☐ แผนงานส่งเสริมการพัฒนายุทธศาสตร์ ICT Security	☐ โครงการส่งเสริมการสร้างวิชาชีพด้านความมั่นคงปลอดภัยแห่งชาติ	☐ มีบุคลากรที่สอบผ่านการรับรองความสามารถการดำเนินการด้านความมั่นคงปลอดภัยไม่ต่ำกว่า 50 คนต่อปี
		☐ โครงการจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security	☐ สามารถจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security ได้ภายใน 3 ปี

3.4 โครงการริเริ่ม (Initiative Programmers) เพื่อส่งเสริม ICT Security แห่งชาติ

จากข้อ 3.2 โครงการที่ต้องดำเนินการตามยุทธศาสตร์มีทั้งหมด 15 โครงการโครงการเหล่านี้จะเสริมสร้างความเข้มแข็งด้าน ICT Security แห่งชาติตลอดจนสร้างฐานการพัฒนาให้ ICT Security เป็นอุตสาหกรรมของประเทศ

1) ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ(National Info-Security Policy and Analysis Centre)
2) โครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติ (National Electronic Authentication Infrastructure)
3) โครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย (Lawful Interception)
4) ประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information Vulnerability Assessment for Critical Infrastructure)
5) การจัดทำมาตรฐานและการรับรองผลิตภัณฑ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยด้านไอซีที (Certification of information Products)
6) โครงการวิจัยและพัฒนาระบบการเข้ารหัสข้อมูลเพื่อเป็นมาตรฐานของชาติ
7) กรอบโครงสร้างด้านความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Framework)
8) การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ (National Security Policy)
9) จัดทำนโยบาย ICT Security ประจำหน่วยงาน
10) จัดทำร่างคำของบประมาณด้าน ICT Security ประจำหน่วยงาน
11) โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ (ICT Security Scorecard)
12) โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ (National Cyber Security Awareness Programmer)
13) โครงการส่งเสริมการสร้างวิชาชีพด้านความมั่นคงปลอดภัยแห่งชาติ (National Certification for Information Security Professionals)
14) โครงการจัดตั้งสำนักงานส่งเสริมอุตสากรรม ICT Security (National Certification for Information Security Professionals)
15) โครงการฝึกอบรมด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Training)

3.5 การกำหนดความเร่งด่วนของโครงการ

การกำหนดความเร่งด่วนของโครงการเพื่อดำเนินการในระยะเวลา 3 ปีโดยกรรมวิธีการให้คะแนนในเงื่อนไขต่างๆ 6 เงื่อนไขดังนี้

1. โอกาสและความสำเร็จ

มีโอกาสสำเร็จสูงหมายถึงว่ามีการใช้งานมีการดำเนินการเป็นที่ยอมรับได้คะแนนก็เป็น 10

0 10

ยอมรับต่ำ ยอมรับสูง

2. งบลงทุน

โครงการที่ต้องใช้งบลงทุนต่ำคะแนนก็เป็น 10

0 10

ลงทุนสูง ลงทุนต่ำ

3. การเชื่อมกับระบบที่อื่น

โครงการที่ไม่ต้องมีการเชื่อมโยงกับระบบอื่น คะแนนก็เป็น 10

0 10

เชื่อมโยง ไม่เชื่อมโยง

4. นโยบาย

โครงการที่กำหนดโดยนโยบายภาครัฐคะแนนก็เป็น 10

0 10

ไม่มีนโยบาย มีนโยบาย

5. ความซับซ้อน

โครงการที่ไม่มีความซับซ้อนข้อสำคัญดำเนินการได้ง่ายไม่มีข้อปัญหาที่ต้องวิเคราะห์คะแนนก็เป็น 10

0 10

ซับซ้อนสูง ซับซ้อนต่ำ

เมื่อให้คะแนนแต่ละเงื่อนไขสำหรับแต่ละโครงการแล้วก็รวมคะแนนประเมินสำหรับแต่ละโครงการหลังจากที่เรียงคะแนนจากมากไปน้อยก็จะได้ลำดับโครงการตามความเร่งด่วนตาราง 3.2 แสดงลำดับของโครงการจากโครงการที่เร่งด่วนที่สุดไปถึงโครงการที่เร่งด่วนน้อยที่สุด

ตาราง 3.2 การประเมินความเร่งด่วนโครงการ

ชื่อโครงการ	ค่าประเมิน					รวม
	โอกาสสำเร็จ	งบลงทุน	เชื่อมโยงกับระบบที่มี	นโยบาย	ความซับซ้อน	
1. การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ	10	10	8	10	8	46
2. ประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร	10	5	10	10	10	45
3. ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ	10	5	8	10	8	41
4. โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ	10	7	10	10	4	41
5. โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ	10	3	10	10	17	40
6. โครงการฝึกอบรม ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร	10	3	10	10	7	40
7. จัดทำนโยบาย ICT Security ประจำหน่วยงาน	10	8	10	5	5	38
8. จัดทำร่างคำของบประมาณด้าน ICT Security ประจำหน่วยงาน	10	8	10	2	8	38
9. โครงการส่งเสริมการสร้างวิชาชีพด้านความมั่นคงปลอดภัยแห่งชาติ	10	7	10	2	7	36
10. โครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติ	7	5	8	10	5	35
11. กรอบโครงสร้างด้านความต่อเนื่องในการดำเนินงานขององค์กร	7	7	8	10	2	34
12. การจัดทำมาตรฐานและการรับรองผลิต	8	7	10	2	2	29

ชื่อโครงการ	ค่าประเมิน					รวม
	โอกาสสำเร็จ	งบลงทุน	เชื่อมโยงกับระบบที่มี	นโยบาย	ความซับซ้อน	
ภัณฑ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยด้านไอซีที						
13. โครงการจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security	5	5	7	2	7	26
14. โครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย (Lawful Interception)	5	5	2	5	2	19
15. โครงการวิจัยและพัฒนาระบบการเข้ารหัสข้อมูลเพื่อเป็นมาตรฐานของชาติ	5	5	5	2	2	19

3.6 การกำหนดระยะการดำเนินงาน (Phasing)

โครงการ 15 โครงการที่ได้จัดเรียงตามความเร่งด่วนแล้วก็สามารถถูกแบ่งออกเป็น 3 กลุ่มโดยพิจารณาความจำเป็นและขีดความสามารถของการดำเนินการในแต่ละปีซึ่งผลลัพธ์การแบ่งระยะการดำเนินการโครงการของแต่ละปีจะเป็นดังนี้

ปีที่ 1

1. การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ
2. ประเมินความพร้อมด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงานภาครัฐ
3. ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ
4. โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ
5. โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ
6. โครงการฝึกอบรม ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ปีที่ 2

7. จัดทำนโยบาย ICT Security ประจำหน่วยงาน
8. จัดทำร่างคำของบประมาณด้าน ICT Security ประจำหน่วยงาน
9. โครงการส่งเสริมการสร้างวิชาชีพด้านความมั่นคงปลอดภัยแห่งชาติ
10. โครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติ

11. กรอบโครงสร้างด้านความต่อเนื่องในการดำเนินงานขององค์กร

ปีที่ 3

12. การจัดทำมาตรฐานและการรับรองผลิตภัณฑ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยด้านไอซีที
13. โครงการจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security
14. โครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย (Lawful Interception)
15. โครงการวิจัยและพัฒนาระบบการเข้ารหัสข้อมูลเพื่อเป็นมาตรฐานของชาติ

3.7 ผู้รับผิดชอบโครงการ

เนื่องจากแผนแม่บท ICT Security แห่งชาติจะต้องดำเนินการโดยทุกหน่วยงานของภาครัฐและเป็นแนวทางสำหรับภาคเอกชนในการดำเนินการด้าน ICT Security ในกรณีนี้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจักเป็นผู้รับผิดชอบหลักในภาพรวมและจะต้องสนับสนุนการดำเนินการตามแนวทางที่กำหนดในทุกภาคส่วน ตาราง 3.3 กำหนดผู้รับผิดชอบหลักและหน่วยงานรองที่รับผิดชอบในโครงการต่างๆตลอดจนระยะเวลาที่ต้องดำเนินการโครงการตามยุทธศาสตร์ที่กำหนด

ตาราง 3.3 ผู้รับผิดชอบหลักของโครงการ

ยุทธศาสตร์	แผนงาน	โครงการ	หน่วยงานหลัก	หน่วยงานรอง	ระยะเวลา					
					2551		2552		2553	
<u>ยุทธศาสตร์ 1</u> พัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไอซีที	ส่งเสริมการจัดการความเสี่ยงจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	1. ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ	กระทรวงไอซีที							
		2.โครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิกส์แห่งชาติ	กระทรวงไอซีที	สนง.ตำรวจแห่งชาติ กระทรวงมหาดไทย กระทรวงต่างประเทศ						
		3. โครงการพัฒนามาตรฐานการวิเคราะห์สัญญาณดิจิตอลตามกฎหมาย	กระทรวงไอซีที	กระทรวงการคลัง กระทรวงมหาดไทย กระทรวงกลาโหม						
<u>ยุทธศาสตร์ที่ 2</u> ส่งเสริมการวิจัยและพัฒนาเทคโนโลยีความมั่นคงปลอดภัยไอซีที	พัฒนาเทคโนโลยีการจัดการระบบสารสนเทศและเครือข่าย	4. ประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยฯ	กระทรวงไอซีที	ทุกกระทรวง						
		5. การจัดทำมาตรฐานและ	กระทรวงอุตสาห	ทุกกระทรวง						

ยุทธศาสตร์	แผนงาน	โครงการ	หน่วยงานหลัก	หน่วยงานรอง	ระยะเวลา					
					2551		2552		2553	
		การรับรองผลิตภัณฑ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยด้านไอซีที	กรรม กระทรวงไอซีที							
		6. โครงการวิจัยและพัฒนาระบบการเข้ารหัสข้อมูลเพื่อเป็นมาตรฐานของชาติ	กระทรวงวิทยาศาสตร์ฯ	กระทรวงไอซีที						
<u>ยุทธศาสตร์ 3</u> ส่งเสริมการสร้างกระบวนงานขององค์กรที่มั่นคงปลอดภัยฉบับต่อเนื่อง	พัฒนาระบบการบริหารจัดการด้านความต่อเนื่องในการดำเนินงานขององค์กร	7. กรอบโครงสร้างด้านความต่อเนื่องในการดำเนินงานขององค์กร	กระทรวงไอซีที	กระทรวงการคลัง กระทรวงพานิชย์ กระทรวงอุตสาหกรรม กระทรวงคมนาคม						
	ส่งเสริมนโยบายด้านความมั่นคงปลอดภัยและการจัดองค์กร	8. การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ	กระทรวงไอซีที	ทุกกระทรวง						
		9. จัดทำนโยบาย ICT Security ประจำหน่วยงาน	กระทรวงไอซีที	ทุกกระทรวง						
		10. จัดทำร่างคำของบ	กระทรวงไอซีที	ทุกกระทรวง						

ยุทธศาสตร์	แผนงาน	โครงการ	หน่วยงานหลัก	หน่วยงานรอง	ระยะเวลา					
					2551		2552		2553	
		ประมาณด้าน ICT Security ประจำหน่วยงาน								
<u>ยุทธศาสตร์ 4</u> ติดตามประเมินผลด้าน ICT Security	การบังคับใช้กฎระเบียบและการวัดผล	11. โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ	กระทรวงไอซีที	กระทรวงกลาโหม กระทรวงมหาดไทย กระทรวงอุตสาหกรรม	■	■				
<u>ยุทธศาสตร์ที่ 5</u> สร้างเครือข่ายบุคลากร องค์กรและผู้เชี่ยวชาญ ด้าน ICT Security และอุตสาหกรรมไอซีที	พัฒนาบุคลากรด้าน ICT Security	12. โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ	กระทรวงไอซีที	กระทรวงแรงงาน กระทรวงวิทยาศาสตร์ฯ	■	■				
	แผนงานส่งเสริมการพัฒนายุทธศาสตร์ ICT Security	13. โครงการส่งเสริมการสร้างวิชาชีพด้านความมั่นคงปลอดภัยแห่งชาติ	กระทรวงไอซีที	กระทรวงแรงงาน			■	■		

ยุทธศาสตร์	แผนงาน	โครงการ	หน่วยงานหลัก	หน่วยงานรอง	ระยะเวลา					
					2551		2552		2553	
		14. โครงการจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security	กระทรวงไอซีที	กระทรวงอุตสาหกรรม					■	■
		15. โครงการฝึกอบรม ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Training)	กระทรวงไอซีที กระทรวงศึกษาธิการ	ทุกกระทรวง	■	■				

บทที่ 4
แผนปฏิบัติการโครงการเร่งด่วน

แผนแม่บทความมั่นคงปลอดภัยด้านไอซีที (ICT Security Master Plan) เป็นแผนที่นำทางทางกลยุทธ์ (a Strategic Roadmap) ซึ่งจำเป็นสำหรับการริเริ่มโครงการระดับชาติที่เป็นแผนปฏิบัติการโครงการเร่งด่วนเพื่อที่จะคุ้มครองโครงสร้างพื้นฐานวิกฤตของชาติ (Critical Information Infrastructure) จากภัยคุกคามทางไซเบอร์ เพื่อที่จะลดผลกระทบจากเหตุ ตลอดจนการฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว แผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติจะช่วยจัดตั้งรูปแบบและลำดับความสำคัญในบริบทของ ความมั่นคงปลอดภัยด้านไอซีทีเมื่อคำนึงถึงสถานการณ์ปัจจุบันและการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องทั้งหลาย ทั้งที่จะเกิดต่อภาคประชาชน ภาคเอกชนและภาครัฐบาล การออกแบบแผนปฏิบัติการโครงการเร่งด่วนของแผนแม่บทฉบับนี้ต้องการที่จะจัดให้มีองค์การที่มีกรอบการทำงานและเครื่องมือที่จำเป็นอย่างพอเพียง เพื่อที่จะสนับสนุนกิจกรรมต่างๆ ที่จะเกิดขึ้นของแผนปฏิบัติการโครงการเร่งด่วนสำหรับปีที่ 1 ของการดำเนิกการตามแผนแม่บทความมั่นคงปลอดภัยด้านไอซีที จะประกอบด้วย 6 โครงการดังนี้

16. การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ
17. โครงการประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร
18. ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ(TISPAC)
19. โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ
20. โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ
21. โครงการฝึกอบรม ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.1 4.1 การจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศ (National ICT Security Policy)

โครงการริเริ่มโครงการแรก คือ การจัดทำนโยบายด้านความมั่นคงปลอดภัย โดยยึดหลัก มาตรฐานนานาชาติ เพื่อจัดให้มีทิศทางและการสนับสนุนด้านความมั่นคงปลอดภัยของสารสนเทศที่จำเป็นตามกฎหมายและระเบียบข้อบังคับที่สอดคล้องกันเป็นแผนเดียว และ เพื่อที่จะให้เป็นการยอมรับได้เมื่อต้องทำธุรกรรมทางอิเล็กทรอนิกส์ ในระดับประเทศ มาตรฐานที่มีการพัฒนาอยู่ในปัจจุบันโดย International Standard Organization คือ ISO 17799 และ ISO 27001 ฉบับปัจจุบัน (2006) ซึ่งมีการประยุกต์ใช้ในหลายประเทศแล้ว และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ ได้ร่วมกันกับเนคเทคจัดทำมาตรฐานภาคภาษาไทยขึ้นมาแล้วด้วย ในมิติของการนำแผนไปปฏิบัติงานควรที่จะยึดถือกระบวนการมาตรฐานนี้ด้วย ได้

แก่ กระบวนการ "Plan-Do-Check-Act" ในขั้นตอนของระบบการบริหารจัดการ "Information Security Management System (ISMS)" ดังนั้นโครงการการจัดทำนโยบายด้านความมั่นคงปลอดภัยของประเทศจะต้องดำเนินการดังนี้

- จัดทำนโยบายและมาตรฐานของความมั่นคงปลอดภัยด้าน ICT ระดับชาติ
- ดำเนินการปรับมาตรฐานในชุด ISO 27000 ให้เป็นภาษาไทยเพื่อใช้เป็นฐานในการกำหนดนโยบายและดำเนินการ
- จัดทำแบบ (คู่มือ) การจัดทำนโยบาย ICT Security ระดับหน่วยงาน
- จัดฝึกอบรมและสัมนาเผยแพร่นโยบายและการดำเนินการตามนโยบาย
- จัดทำเว็บไซต์นโยบาย ICT Security แห่งชาติ
- จัดตั้งกรรมการอำนวยการ ICT Security แห่งชาติ

1.2 4.2 โครงการประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2 หน่วยงานภาครัฐทุกแห่งยังไม่มีความพร้อมด้าน ICT Security ที่สามารถป้องกัน ต่อต้านการโจมตีจากภายในและภายนอกจุดอ่อนในระบบ ICT และจุดอ่อนในกระบวนงาน ที่สำคัญต้องได้รับการระบุชื่อชี้ชัด ดังนั้นโครงการประเมินความพร้อมขององค์กรภาครัฐซึ่งเป็นโครงสร้างพื้นฐานของประเทศด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารจักต้องดำเนินการดังนี้

- จัดทำกระบวนการตรวจสอบความพร้อมด้าน ICT Security
- จัดทำ checklist เพื่อประเมินความพร้อมด้าน ICT Security
    - นโยบายในการรักษาความปลอดภัย
    - โครงสร้างการจัดการรักษาความปลอดภัยข้อมูล
    - การบริหารจัดการสินทรัพย์ต่าง ๆ
    - การรักษาความปลอดภัยของทรัพยากรบุคคล
    - การรักษาความปลอดภัยทางด้านวัตถุและสภาพแวดล้อม
    - การบริหารจัดการระบบสื่อสารและการปฏิบัติงาน
    - การควบคุมและจัดการระบบการเข้าถึงข้อมูล
    - การตรวจหา, พัฒนา และดูแลรักษาระบบข้อมูล
    - การบริหารจัดการเหตุการณ์ต่าง ๆ ที่เกิดขึ้นกับระบบข้อมูล
    - การบริหารจัดการความต่อเนื่องของการทำงาน
    - การเข้ากันได้ของข้อมูลทางด้านความปลอดภัยระดับนานาชาติ

- กำหนดมาตรฐานการตรวจสอบ
- จัดทำซอฟต์แวร์สำหรับการจัดเก็บข้อมูลการตรวจสอบ
- จัดทำคู่มือการตรวจสอบ
- สร้างคณะทำงานที่สามารถทำการตรวจสอบความพร้อม ICT Security
- สนับสนุนการตรวจสอบความพร้อมด้าน ICT Security ให้กับหน่วยราชการ

4.3 ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ

โครงการนี้จะจัดตั้งองค์การที่เรียกว่า "Thailand Info-Security Policy and Analysis Center: TISPAC"โดยมีวัตถุประสงค์ดังต่อไปนี้

1) ตรวจจับ ป้องกัน ตอบโต้ และพิทักษ์ภัย ในเชิงรุก จากการโจมตีทางไซเบอร์ ที่มุ่งเป้าไปยังโครงสร้างพื้นฐานทางความมั่นคงฯ ของเครือข่ายของชาติ เช่น เครือข่ายการเงินการธนาคาร การดำเนินงานธุรกรรมที่สำคัญยิ่งของรัฐ การบริการฉุกเฉิน เป็นต้น
2) ลดจุดอ่อน การขัดจังหวะและการหยุดชะงักของธุรกรรมต่างๆ ที่อาจเกิดขึ้นจากผลของการโจมตีทางไซเบอร์ ทั้งต่อเป้าหมายที่เป็นหน่วยงานภาครัฐและภาคธุรกิจ
3) บรรเทาความเสียหายที่อาจเกิดขึ้นและลดช่วงเวลาที่จะต้องใช้ในการแก้ไขระบบให้ฟื้นคืนสภาพ อันเนื่องมาจากการโจมตีทางไซเบอร์ ให้ได้มากที่สุด
4) เสริมสร้างความแข็งแกร่งในงานข่าวกรองเพื่อต่อต้านภัยคุกคามจากไซเบอร์ โดยอาศัยการแบ่งปันข้อมูลข่าวสารจากพันธมิตร ได้แก่ หน่วยงานรัฐอื่นๆ ทั้งในประเทศ ในภูมิภาคและระดับนานาชาติ

การดำเนินการเพื่อจัดตั้งศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติจักต้องดำเนินการดังนี้

- กำหนดความต้องการด้านสถานที่และศูนย์สั่งการ
- กำหนดความต้องการด้านซอฟต์แวร์
- กำหนดความต้องการด้านอุปกรณ์สั่งการโทรคมนาคม
- กำหนดโครงสร้างองค์กรและการดำเนินการตลอดจนสายบังคับบัญชา
- กำหนดโครงสร้าง อัตรากำลังและงบประมาณ
- ออกแบบสถาปัตยกรรมของศูนย์
- ดำเนินการบูรณาการฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย
- ทดสอบการดำเนินการ

รายละเอียดเพิ่มเติมดูได้ในบทที่ 6 เกี่ยวกับโครงสร้างองค์กร TISPAC

4.4 โครงการจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยแห่งชาติ ภัยของหน่วยงานภาครัฐ (ICT Security Scorecard)

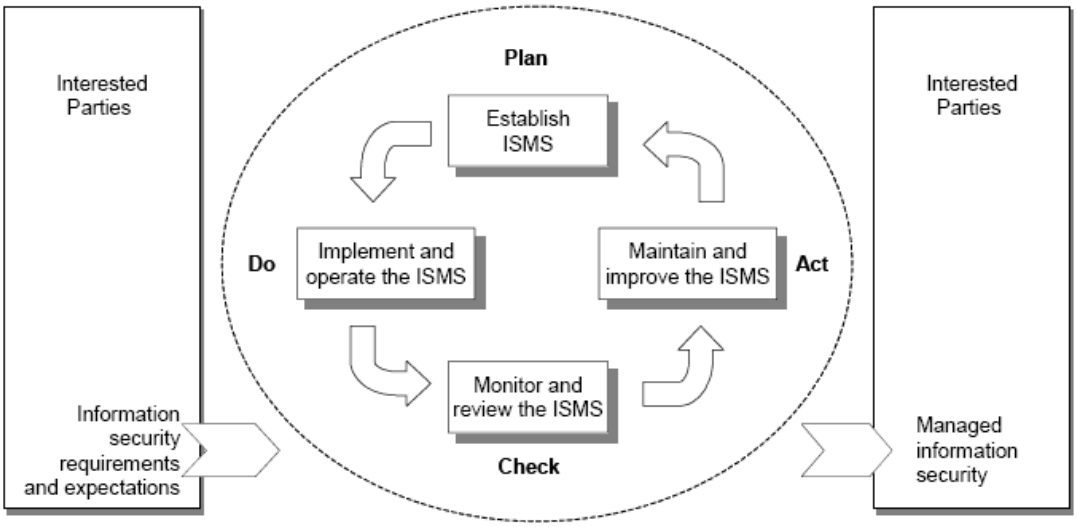
เป็นโครงการที่จะทำระเบียบเพื่อประเมินความพร้อม และความจำเป็นของภารกิจของหน่วยงานภาครัฐ ด้าน ICT Security และเป็นแนวทางปฏิบัติที่ภาคเอกชนสามารถนำไปเลือกใช้ได้ตามความเหมาะสม ในดำเนินงานควรเริ่มต้นจากส่วนที่เผยแพร่ต่อสาธารณะก่อนเป็นอันดับแรก ส่วนที่เกี่ยวข้องในส่วนย่อยต่างๆ ขององค์กร ให้ทำหลังจากส่วนที่เผยแพร่ต่อสาธารณะเสร็จสิ้นทั้งนี้แนวทางการประเมินจะต้องสอดคล้องและอ้างถึงมาตรฐาน ISO17799/ISO27001 (ได้นำเสนอมาแล้วผ่านคกก.ธุรกรรมทางอิเล็กทรอนิกส์)

ขอบเขตการดำเนินการประกอบด้วย

- ศึกษาแนวทางการจัดทำ ICT Security ในต่างประเทศ
- จัดทำโมเดล ICT Security สำหรับประเทศไทย
- ทดสอบ Validity ของ ICT Security
- ประเมิน ICT Security เพื่อให้ได้ผลลัพธ์ที่กำหนด
- จัดทำระบบ ICT สนับสนุนการจัดเก็บข้อมูลและวิเคราะห์ข้อมูล ICT Security
- จัดการฝึกอบรมกรรมวิธีรวบรวมจัดเก็บข้อมูล ICT Security

4.5 โครงการสร้างความตระหนักด้านความมั่นคงปลอดภัยแห่งชาติ

โครงการนี้จะเป็นการให้การศึกษาในรูปแบบสัมนาโดยจัดให้มีกิจกรรมร่วมนำเสนอประสบการณ์ที่เกิดจากความบกพร่องด้าน ICT Security เพื่อให้เกิดจิตสำนึกตระหนักถึงอันตรายอันเกิดจากการละเลยเรื่อง ICT Security จากนั้นจะต้องแนะนำมาตรฐาน ISO27001เพื่อให้เข้าใจกระบวนการ Plan-Do-Check-Act (PDCA) ซึ่งเป็นรูปแบบในสำหรับทุกขั้นตอนในระบบบริหารจัดการความมั่นคงปลอดภัย วิธีการดังกล่าวนี้มีความสำคัญต่อการพัฒนาระบบการจัดการความเสี่ยงที่อาจเกิดขึ้นให้มีประสิทธิภาพ แบบจำลองด้านล่างนี้แสดงถึงการทำงานของระบบ ISMS (Information Security Management System) ที่ตรงตามความต้องการของกลุ่มองค์กร (เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร) และระบบการปฏิบัติงานต่าง ๆ ที่เกิดขึ้นทำให้ระบบการรักษาความปลอดภัยต่อข้อมูลตรงต่อความต้องการ และความคาดหมายได้


Interested Parties
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Information security requirements and expectations
Interested Parties
Managed information security

การดำเนินการโครงการประกอบด้วย

- จัดการสัมนาเดือนละ 2 ครั้งโดยแต่ละครั้งเชิญผู้เข้าร่วมสัมนาไม่ต่ำกว่า 200 คน
- ให้มีการดำเนินการนำเสนอ อภิปราย และตอบคำถาม
- ให้มีการสำรวจประสพการณ์ด้าน ICT Security
- ให้จัดทำฐานข้อมูลของผู้ผ่านการสัมนา
- จัดให้การสร้างสังคมบนเว็บด้าน ICT Security

4.6 โครงการฝึกอบรม ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ในการฝึกอบรมจะต้องเน้นที่การถ่ายทอดรายละเอียดของมาตรฐาน ISO 27000 ซึ่งเน้นที่กระบวนการ Plan-Do-Check-Act โดยทีรายละเอียดดังนี้

Plan (วางนโยบายระบบ ISMS)

การจัดสร้างนโยบาย จุดประสงค์ กระบวนการ และขั้นตอนสำหรับ ISMS นั้นมีความสำคัญเป็นอย่างยิ่งในการจัดการแก้ไขปัญหาความเสี่ยงที่อาจเกิดขึ้น และยังมีความสำคัญต่อการพัฒนาศักยภาพของระบบรักษาความปลอดภัยของข้อมูล ส่งผลให้ตรงต่อนโยบายและจุดประสงค์หลักขององค์กร ซึ่งประกอบไปด้วย

- กำหนดขอบเขต (Scope and Boundaries) ของ ISMS รวมถึงแนวทางการแก้ไข (Justification) สำหรับขอบเขตที่ไม่ได้อยู่ในระบบ
- กำหนดนโยบาย ISMS เพื่อสร้างรูปแบบเฉพาะของประเทศไทย และวาระแห่งชาติ รูปแบบทางภูมิศาสตร์ สินทรัพย์ต่าง ๆ รวมถึงเทคโนโลยีที่จำนำมาใช้
- คำนวณถึงความเสี่ยงที่อาจจะเกิดขึ้น
- นิยามปัญหา
- วิเคราะห์และประเมินผลของปัญหา
- นิยามและประเมินขั้นตอนการแก้ไขปัญหา
- คัดเลือกวิธีและขั้นตอนรวมถึงเครื่องมือในการแก้ไขปัญหา
- จัดเตรียมกระบวนการและแนวทางที่สามารถใช้งานได้

Do (จัดสร้างและปฏิบัติการระบบ ISMS)

การจัดสร้างและปฏิบัติการระบบ ISMS ในขั้นตอนนี้จะเป็นการวางนโยบาย การควบคุม กำหนดขั้นตอนและกระบวนการ ซึ่งประกอบไปด้วย

- กำหนดแผนแก้ไขปัญหาความเสี่ยงที่เหมาะสมในส่วนของการบริหารการจัดการ ทรัพยากร ความรับผิดชอบ และลำดับความสำคัญ
- จัดสร้างแผนแก้ไขปัญหาความเสี่ยงเพื่อนำไปสู่การคัดสรรเครื่องมือในการจัดการและควบคุมความเสี่ยง
- ติดตั้งเครื่องมือในการจัดการและควบคุมความเสี่ยงที่คัดเลือก
- นิยามและตรวจวัดประสิทธิภาพจากเครื่องมือจัดการและควบคุมที่คัดเลือกแล้ว และกำหนดวิธีการในการตรวจวัดให้มีประสิทธิภาพสูงสุด เพื่อก่อให้เกิดความสามารถในการเปรียบเทียบและทดสอบซ้ำได้
- ติดตั้งระบบการสอนและระบบการเรียนรู้
- บริหารและจัดการกระบวนการทำงานและทรัพยากรของ ISMS
- ติดตั้งเครื่องมือจัดการที่เตรียมพร้อมสำหรับการตรวจสอบและแก้ไขความผิดพลาดต่าง ๆ ที่อาจจะเกิดขึ้นได้

Check (ค้นหาและตรวจสอบระบบ ISMS)

การเข้าถึง และการนำส่วนต่าง ๆ ที่สามารถนำไปปรับใช้ได้ไม่ว่าจะเป็น การตรวจสอบประสิทธิภาพของผลการทำงานของนโยบาย วัตถุประสงค์ และประสบการณ์ที่ตรงกับความเป็นจริง แล้วรายงานสู่ระบบจัดการเพื่อตรวจสอบ หลังการติดตั้ง ISMS แล้ว ขั้นตอนต่อไปคือการค้นหาและตรวจสอบศักยภาพในการทำงาน กระบวนการต่าง ๆ ของขั้นตอนดังกล่าว มีดังนี้

- เปิดการทำงานในส่วนการค้นหาและตรวจสอบ รวมถึงเครื่องมือในการตรวจสอบอื่นๆ ที่เกี่ยวข้องเพื่อค้นหาข้อผิดพลาด ความพยายามที่จะเจาะเข้าสู่ระบบทั้งที่สำเร็จและยังไม่สำเร็จ ค้นหาสาเหตุที่ระบบความปลอดภัยไม่สามารถทำงานได้อย่างตามประสิทธิภาพที่ต้องการ ตรวจหาเหตุการณ์ต่าง ๆ เพื่อป้องกันระบบรักษาความปลอดภัย โดยมีการสร้างระบบในการตรวจวัดอย่างชัดเจน
- เตรียมการรองรับการตรวจสอบระบบต่าง ๆ ที่เกิดขึ้นใน ISMS แล้วแยกแยะรายงานผลต่าง ๆ ตามผู้ตรวจสอบที่เกี่ยวข้อง, รองรับการตรวจเหตุการณ์ที่เกิดขึ้นในระบบ, การตรวจวัดประสิทธิภาพ, คำแนะนำและตอบกลับสู่ทุกองค์กรที่เกี่ยวข้อง
- ตรวจวัดประสิทธิภาพของเครื่องมือควบคุมเพื่อประเมินผลให้ตรงต่อความต้องการของระบบรักษาความปลอดภัย
- ตรวจสอบและประเมินผลค่าความเสี่ยงตามแผนช่วงเวลา และตรวจสอบพร้อมแยกแยะระดับค่าความเสี่ยงที่ได้
- จัดการตรวจสอบระบบภายในของ ISMS ได้ตามแผนช่วงเวลา

- รองรับและจัดการระบบการตรวจสอบของ ISMS จากรากฐานของระบบการตรวจสอบ เพื่อความมั่นใจว่าขอบข่ายของระบบทำงานมีปริมาณเพียงพอต่อความต้องการและการพัฒนาของระบบ ISMS ยังคงสามารถดำเนินการต่อไปได้อย่างมีประสิทธิภาพ
- การจัดการให้ระบบรักษาความปลอดภัยมีความทันสมัยตลอดเวลา เพื่อใช้ในการตรวจค้นและตรวจสอบกิจกรรมต่าง ๆ
- ทำการบันทึกกิจกรรมต่าง ๆ ที่มีผลต่อการทำงานหรือประสิทธิภาพของ ISMS

Act (ดูแลและพัฒนาระบบ ISMS)

ขั้นตอนนี้เป็นขั้นตอนสำหรับการปรับปรุงแก้ไขและป้องกันการทำงานที่ถูกรายงานจากการตรวจสอบระบบของขั้นตอนก่อนหน้า เพื่อใช้ในการพัฒนาศักยภาพของระบบ ISMS ทั้งนี้เพื่อสร้างความมั่นใจว่าระบบ ISMS ทำงานอย่างมีเสถียรภาพ จึงมีความจำเป็นอย่างยิ่งที่จะต้องทำให้ระบบมีความทันสมัยอยู่ตลอดเวลา ซึ่งมีกระบวนการทำงาน ดังนี้

- ติดตั้งระบบการพัฒนาที่สมบูรณ์แล้วสู่ ISMS
- นำการแก้ไขปัญหาที่มีประสิทธิภาพ และการป้องกันต่าง ๆ เข้าสู่ระบบ โดยการนำเอาเหตุการณ์ต่าง ๆ ที่เกิดขึ้นเกี่ยวกับการรักษาความปลอดภัยจากองค์กรต่าง ๆ ในประเทศ รวมถึงประเทศอื่น ๆ มาเป็นแนวทางการศึกษา(Case study)
- ติดต่อสื่อสารวิธีการแก้ไขและพัฒนาอย่างละเอียดให้แก่องค์กรที่เกี่ยวข้อง เพื่อความสมบูรณ์ในการแก้ไขหรือปรับปรุงแก่องค์กรต่าง ๆ อย่างมีประสิทธิภาพ
- ตรวจสอบองค์กรต่าง ๆ ที่ได้รับการแก้ไขและปรับปรุงแล้วว่าตรงต่อวัตถุประสงค์หรือไม่

ทั้งนี้ การนำกระบวนการ PDCA มาใช้ในแผนแม่บท ICT Security แห่งชาตินั้น สามารถระบุให้เฉพาะเจาะจงในส่วนต่าง ๆ ดังนี้

- การทำความเข้าใจในระบบรักษาความปลอดภัยของข้อมูลที่จำเป็นและตามความต้องการ เพื่อกำหนดกรอบนโยบายและวัตถุประสงค์

- การจัดเตรียมและควบคุมขั้นตอนการทำงานสำหรับการร่างโครงร่างของระบบ ISMS รวมถึงส่วนต่าง ๆ ที่เกี่ยวข้องเพื่อกำหนดรูปแบบมาตรฐานต่อการออกแผนแม่บทแห่งชาติ

- การตรวจสอบภายในและกำหนดแนวทางเพื่อค้นหาและตรวจสอบเพื่อพัฒนาเทคโนโลยีรักษาความปลอดภัยตามความเหมาะสม เพื่อกำหนดกรอบแผนนโยบายการทำงาน

- การพัฒนาศักยภาพของระบบโดยต่อเนื่องตามการประมวลศักยภาพ

การนำรูปแบบระบบ PDCA มาปรับปรุงแก้ไขเพื่อใช้งานย่อมมีข้อแตกต่างจากแผน “OECD Guidelines (2002)1 governing the security of information systems and networks”. ซึ่งการปรับปรุงนี้จะก่อ

ให้เกิดความเข้มแข็งต่อแผนนโยบายในการวางโครงสร้างและแนวทางในการดูแลจัดการความเสี่ยง การออกแบบและติดตั้งระบบรักษาความปลอดภัย การดูแลและจัดการระบบรักษาความปลอดภัยที่จะเกิดขึ้นในอนาคต

ในการดำเนินการจะมีขอบเขตดังนี้

- กำหนดโครงสร้างหลักสูตรตามที่กำหนดในบทที่ 5
- พัฒนาเนื้อหาหลักสูตรมาตรฐานบนพื้นฐานของชุดมาตรฐาน ISO 27000 ซึ่งเน้นกระบวนการ Plan-Do-Check-Act
- จัดทำ Courseware ของทุกวิชาที่ต้องฝึกอบรม
- ดำเนินการคัดเลือกผู้เข้าร่วมโครงการโดยแบ่งเป็นรุ่นตามความเหมาะสม
- กำหนดวิธีการบริหารการฝึกอบรม
- ดำเนินการฝึกอบรมและทดสอบ
- ประเมินผลการฝึกอบรม

บทที่ 5
การพัฒนาบุคลากรและถ่ายทอดเทคโนโลยี

5.1 ความต้องการฝึกอบรม

สืบเนื่องจากการพัฒนาเทคโนโลยี ICT Security เริ่มมีการใช้แพร่หลายในวงกว้างในทศวรรษที่ผ่านมาและการกำหนดมาตรฐานการบริหารความมั่นคงปลอดภัย โดย ISO/ICE 27000 เริ่มมีความเสถียรและเป็นที่ยอมรับในการจัดการด้านความมั่นคงปลอดภัย ดังนั้น บุคลากรที่มีประสบการณ์และความรู้ด้านบริหารจัดความมั่นคงและปลอดภัยอย่างเป็นระบบนั้น ยังมีจำนวนที่น้อยมากๆ ยิ่งถ้าเป็นบุคลากรระดับที่ได้รับ Certificate จากองค์กรสากลด้านความมั่นคงปลอดภัยก็มีเพียงไม่กี่คนในประเทศไทย องค์กร (ISO) ต้องเป็นองค์กรสากลแบบNon-profit ที่ทำให้ Certificate ด้านความมั่นคงปลอดภัย ในปี 1989 เมื่อนับถึงปี 2004 Certificate บุคลากรทั่วโลกกว่า 100 ประเทศ เพียง 30,000 คน สำหรับประเทศไทยสามารถคาดการณ์ได้ว่า มีความต้องการมืออาชีพด้านความมั่นคงปลอดภัยไม่ต่ำกว่า 10,000 คน ในทศวรรษหน้านี้ ดังนั้น จึงมีความจำเป็นต้องวางยุทธศาสตร์ที่มีเป้าหมายที่ชัดเจนในการดำเนินการให้มีการฝึกอบรมและจัดทำ Certificate อย่างเป็นระบบ เพื่อให้ได้บุคลากรที่สามารถดูแลเรื่องความมั่นคงปลอดภัยในองค์กร หรือสามารถให้บริการที่ปรึกษาแก่องค์กรทั้งในและนอกประเทศด้าน ICT Security

5.2 หลักสูตรฝึกอบรมและหลักสูตรระดับปริญญาบัตร

5.2.1 หลักสูตรฝึกอบรม

การฝึกอบรมด้าน ICT Security จะเป็นกลไกหลักในการพัฒนาบุคลากรให้มีความรู้ ทักษะ และความสามารถในการบริหารจัดการด้าน ICT Security ในการนี้ การจะพิจาณาดู Care Competency ด้าน ICT Security ของบุคลากร 5 ระดับ ดังนี้

ระดับ 1 : ผู้บริหารระดับสูง ผู้บริหารระดับนโยบาย และวิสัยทัศน์

ระดับ 2 : ผู้บริหารระดับกลาง ผู้บริหารด้านสารสนเทศ ระดับกระบวนงาน และกรรมวิธี

ระดับ 3 : บุคลากรระบบเครือข่าย บริหารระบบ

ระดับ 4 : บุคลากรปฏิบัติการด้านสารสนเทศ ระดับ PC และระบบงาน

ระดับ 5 : End User

ซึ่งความชำนาญและพฤติกรรม สมรรถนะของแต่ละประเภทบุคลากร จำแนกโดยตาราง

ตารางที่ 5.1 ICT Security Competency และ หลักสูตร ICT Security

ระดับ	ความชำนาญ	พฤติกรรมสมรรถนะ	ประเภทบุคลากร
1	มีความรู้ด้านความมั่นคงปลอดภัยด้านสารสนเทศในระดับปฏิบัติการ รวมทั้งมีวินัยในการใช้ ICT ตามภารกิจ และมีความซื่อสัตย์ในการค้นหา จัดเก็บและรักษาข้อมูล	1.1 สามารถใช้เทคโนโลยีสารสนเทศได้อย่างถูกต้องตามหลักความมั่นคงปลอดภัย 1.2 สามารถค้นหา จัดเก็บและรักษาข้อมูลโดยใช้ระบบเทคโนโลยีสารสนเทศความมั่นคงปลอดภัย	ระดับ 5 ระดับ 4
2	สามารถเสนอแนะและมีความชำนาญในการจัดเก็บและวิเคราะห์ข้อมูล ความมั่นคงปลอดภัย เข้าใจ และสามารถใช้อุปกรณ์ความมั่นคงปลอดภัยในระดับเครือข่าย และคอมพิวเตอร์ได้	2.1 สามารถกำหนดรูปแบบการจัดเก็บข้อมูลในองค์กรได้อย่างครอบคลุมตามความรับผิดชอบของตนเองในองค์กรได้อย่างถูกต้องสมบูรณ์ตามหลักความมั่นคงปลอดภัย 2.2 สามารถใช้โปรแกรมและอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องความมั่นคงปลอดภัยที่จำเป็นในการปฏิบัติงานในขั้นชำนาญการได้อย่างดี 2.3 บำรุงรักษาอุปกรณ์ขั้นพื้นฐานได้อย่างถูกวิธีและสามารถใช้ได้อย่างต่อเนื่อง	ระดับ 4 ระดับ 3
3	สามารถวิเคราะห์ ประมวลผล แปรข้อมูลสารสนเทศให้เกิดเป็นองค์ความรู้และสามารถถ่ายทอดสื่อสาร รวมทั้งแก้ไขปัญหาเบื้องต้นด้านความมั่นคงปลอดภัยให้กับผู้ปฏิบัติการได้	3.1 กำกับดูแลการปฏิบัติงานให้บรรลุตามเป้าประสงค์ที่กำหนดและสอดส่องการโจมตีจากภายในและภายนอก 3.2 ระบุแนวทางใหม่ๆ ในการบริหารจัดการระบบงานภายใต้ความต้องการด้านความมั่นคง	ระดับ 3 ระดับ 2

ระดับ	ความชำนาญ	พฤติกรรมสมรรถนะ	ประเภทบุคลากร
		ปลอดภัยได้ 3.3 สามารถนำข้อมูลด้านความมั่นคงปลอดภัยระหว่างหน่วยงานมาบูรณาการกัน เพื่อใช้ประโยชน์ร่วมกันได้ 3.4 สามารถวิเคราะห์และประเมินผล การถูกโจมตีหรือการเกิดปัญหาด้านความมั่นคงปลอดภัย 3.5 สามารถวิเคราะห์และดำเนินการแก้ไขปัญหาที่เกิดจากความมั่นคงปลอดภัยตามมาตรฐานการบริหารจัดการความปลอดภัย	
4	สามารถให้ข้อเสนอแนะแก่ผู้ที่เกี่ยวข้องเพื่อการตัดสินใจแก้ไขปัญหาด้านความมั่นคงปลอดภัยที่มีความซับซ้อน และสามารถพัฒนาบุคลากรให้สามารถใช้เทคโนโลยีสารสนเทศได้อย่างปลอดภัย	4.1 สามารถวิเคราะห์ระบบและให้ข้อเสนอแนะแก่ผู้ที่เกี่ยวข้องความต้องการเมื่อเกิดปัญหาความปลอดภัย ในด้านเทคโนโลยีสารสนเทศ 4.2 กำกับดูแลแนวทางปฏิบัติงานโดยใช้เทคโนโลยีสารสนเทศแก่เจ้าหน้าที่ระบบดับปฏิบัติการได้อย่างชัดเจน 4.3 สามารถสร้างระบบข้อมูลสารสนเทศที่มั่นคงปลอดภัยที่ต้องการใช้งานได้ 4.4 สามารถเชื่อมโยงเครือข่ายข้อมูลสารสนเทศระหว่างหน่วยงานได้ทุกระดับตั้งแต่หน่วยงานจนถึงระดับ ประเทศอย่างมั่นคงปลอดภัย	ระดับ 2

ระดับ	ความชำนาญ	พฤติกรรมสมรรถนะ	ประเภทบุคลากร
5	กำหนดนโยบาย สั่งการและผลักดันการใช้ระบบสารสนเทศมั่นคงปลอดภัยให้สอดคล้องกับภารกิจขององค์การจนบรรลุผลสำเร็จ เชื่อมโยงเครือข่ายในเชิงบูรณาการทั้งในระดับประเทศและสากล	5.1 มีความเป็นผู้นำในการกำหนดนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและผลักดันให้เกิดการนำไปใช้ได้จริงจนเกิดผลสัมฤทธิ์ตามวิสัยทัศน์ของหน่วยงาน 5.2 สามารถระบุความเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศจากสถานการณ์ภายนอกได้อย่างแม่นยำ 5.3 เข้าใจในเรื่องบริหารความเสี่ยง ความต่อเนื่องธุรกิจการจัดการกับภัยฉุกเฉิน และมาตรฐานสากลด้านบริหารความมั่นคงปลอดภัย	ระดับ 1

1. กลุ่มวิชาภาคบังคับ

วิชาภาคบังคับควรมี 2 วิชา ได้แก่วิชา Information Assurance and Security ซึ่งเป็นการสอนองค์

ความรู้ผู้ที่ทำงานกับ ICT เข้าใจ ส่วนอีกวิชาคือ ความเข้าใจในการดำเนินการตามมาตรฐาน ISO/IEC 17799 (หรือ ISO/IEC 27001)

1) **IAS1**. Fundamental Aspects

ในการกำหนดองค์ความรู้ด้านเทคโนโลยีสารสนเทศ (IT Body of Knowledge) โดย IEEE ซึ่งเป็นองค์กรมาตรฐานที่น่าเชื่อถือได้กำหนดองค์ความรู้ด้าน Information Assurance and Security (IAS) ได้ 11 เรื่อง ซึ่งสามารถกำหนดในเวลา 23 ชั่วโมง ดังนี้

	IAS Information Assurance and Security (23 core hours)
IAS1.	Fundamental Aspects (3)
IAS2.	Security Mechanisms (Countermeasures) (5)
IAS3.	Operational Issues (3)
IAS4.	Policy (3)
IAS5.	Attacks (2)
IAS6.	Security Domains (2)
IAS7.	Forensics (1)
IAS8.	Information States (1)
IAS9.	Security Services (1)
IAS10.	Threat Analysis Model (1)
IAS11.	Vulnerabilities (1)

ความรู้ด้าน IAS ทั้ง 11 เรื่องนี้เป็นเรื่องที่ผู้ที่ทำงานกับ ICT ต้องรู้ และเข้าใจ ดังนั้น จึงเป็นหลักสูตร

ภาคบังคับที่เจ้าหน้าที่และผู้บริหารทุกระดับต้องเข้ารับการฝึกอบรม

2) วิชา เข้าใจชุดวิชามาตรฐาน ISO 17799 & ISO 27000 สำหรับการบริหารจัดการด้านความ

มั่นคงปลอดภัย มาตรฐานความมั่นคงปลอดภัยนับว่าเป็นเทคโนโลยีสารสนเทศด้านความมั่นคงปลอดภัยที่

ประชาคมทั้งภาครัฐและเอกชนยอมรับและสามารถนำไปใช้เพื่อลดปัญหาด้านความเสี่ยงอันเกิดจากความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้องค์กรสามารถดำเนินการได้อย่างต่อเนื่อง และมีผลกระทบน้อยที่สุด

โครงสร้างหลักสูตร

1. มาตรฐาน ISO/IEC 27000
   - ภาพรวมและประวัติ
   - เปรียบเทียบ ISO/IEC 27000 กับ BS 7799-2 : 2000 ทั้งเรื่องกระบวนการ PDCA และความต้องการ
   - กระบวนการ Certificate
   - หลักการตรวจสอบ ISMS
2. การประเมินและบริหารความเสี่ยง
   - การประเมินความเสี่ยง และการใช้เครื่องมือสนับสนุนการประเมิน
   - ISO/IEC 27005 ISMS Risk Management
   - การหาความต้องการด้านความมั่นคงปลอดภัย
   - การระบุและประเมินด้านบุคลากรและจุดอ่อนระบบ
   - การเลือกวิธีการจัดการกับภัยคุกคาม
   - เลือกชุดควบคุมและกำหนดประยุกต์
3. มาตรฐาน ISO/IEC 17799
   - เวอร์ชั่นใหม่ มาตรฐาน ISO/IEC 17799 : 2005
   - นโยบายความปลอดภัย
   - การจัดโครงสร้างด้านสารสนเทศ
   - การจัดการทรัพยากร
   - การจัดการความปลอดภัยด้านบุคลากร
   - การจัดการความปลอดภัยเชิงกายภาพ และสิ่งแวดล้อม
   - การจัดการกับการสื่อสารและปฏิบัติการ
   - การควบคุมการเข้าถึง
   - การจัดหาพัฒนาและบำรุงรักษา
   - การบริหารจัดการกับการมีปัญหา
   - Compliance
4. การนำ ISO/IEC 17799 ไปประยุกต์
   - แนะนำการนำไปใช้
   - ดัชนีชี้วัด และการวัดผล
   - ISO/IEC 18044 Information Security Incident Management
   - การจัดทำกระบวนการสอดส่องปัญหา (Incident)

- สรุปและอภิปราย
- สอบ

ตารางที่ 5.2 หลักสูตร

IAS1. Fundamental Aspects Minimum core coverage time : 6 hours		IAS2. Security Mechanisms (Countermeasures) Minimum core coverage time : 10 hours	
Topics :	History and Terminology Security Mindset (reasoned paranoia) Design Principles (Defense in Depth) System/security Fife-cycle Security implementation mechanisms (gates, guards, guns ; cryptography) Information assurance and analysis model (MSR model * ; threats ; Vulnerabilities ; attacks ; countermeasures) Disaster recovery (natural and man - made) Forensics	Topics :	Cryptography Cryptosystems Keys : symmetric & asymmetric Performance (software / hardware) Implementation Authentication "Who you are, what you have, what you know" Redundancy Intrusion Detection
IAS3. Operational Issues Minimum core coverage time : 6 hours		IAS4. Policy Minimum core coverage time : 6 hours	
Topics :	Trends Auditing Cost / benefit analysis Asset Management Standards Enforcement Legal issues Disaster recovery (natural and man – made)	Topics :	Creation of Policies Maintenance of Policies Prevention Avoidance Incident Response (Forensics) Domain integration (physical, network, internet, etc.)
IAS5. Operational Issues Minimum core coverage time : 6 hours		IAS6. Security Domains Minimum core coverage time : 6 hours	
Topics :	Social Engineering Denial of Service Protocol attacks Active attacks Buffer Overflow Attacks Malware (Viruses, Trojan Horses, Worms)	Topics :	Human – Computer Interaction Information Management Integrative Programming Networking Program Fundamentals Web Systems Physical Plant

IAS7. Forensics Minimum core coverage time : 2 hours		IAS8. Information States Minimum core coverage time : 6 hours	
Topics :	Legal Systems Digital Forensics and its relationship to other Forensic disciplines Rules of Evidenced Search and Seizure Digital Evidence Media Analysis	Topics :	Transmission Storage Processing
IAS9. Security Services Minimum core coverage time : 6 hours		IAS10. Threat Analysis Model Minimum core coverage time : 6 hours	
Topics :	Availability Integrity Confidentiality Authentication (source reliability) Non – repudiation	Topics :	Risk assessment Cost benefit
IAS11. Vulnerabilities Minimum core coverage time : 6 hours			
Topics :	Perpetrators Inside attacks External attacks Black Hat White Hat Ignorance Carelessness Network Hardware (design, implementation, installation, etc,) Physical		

2. กลุ่มวิชาความมั่นคงปลอดภัย

1) ความมั่นคงปลอดภัยเครือข่ายและระบบ
2) การบริหารจัดการไฟร์วอลล์
3) การบริหารจัดการความปลอดภัยเครือข่ายไร้สาย
4) การพัฒนา Web Security
5) การสร้าง VPN ที่มั่นคงปลอดภัย
6) การใช้ระบบตรวจจับผู้บุกรุก
7) การต่อต้านการโจมตี
8) ความมั่นคงปลอดภัย Windows Server 2003
9) ความมั่นคงปลอดภัยของ UNIX และ Linux

3. กลุ่มวิชาและจุดอ่อน

1) การประเมินจุดอ่อนของระบบ (Venerability Assessment)
2) Computer Forensics and การตอบสนองต่อเหตุการณ์
3) การใช้ PKI ในองค์กร
4) การพัฒนานโยบายด้านความปลอดภัยสำหรับเครือข่าย
5) การวิเคราะห์และบริหารจัดการความเสี่ยง

4. กลุ่มวิชาการบริหารจัดการกระบวนงานอย่างมั่นคงปลอดภัย

1) หลักสูตรฝึกอบรม ISMS 2701 : ความต้องการ
2) หลักสูตรฝึกอบรม ISMS 2702 (17799) : หลักการการดำเนินการ
3) หลักสูตรฝึกอบรม ISMS 2703 : การนำไปใช้
4) หลักสูตรฝึกอบรม ISMS 2704 : การวัด
5) หลักสูตรฝึกอบรม ISMS 2705 : การบริหารความเสี่ยง
6) หลักสูตรฝึกอบรม ISMS 2706 : การรับรองวุฒิฐานะ

ตารางที่ 5.3 กลุ่มวิชา

	ผู้บริหารระดับสูง	ผู้บริหารระดับกลาง	ปฏิบัติการสารสนเทศ	ปฏิบัติการและเครือข่าย	End User
1. กลุ่มวิชาแกน					
วิชา Information Assurance and Security	/	/	/	/	
วิชาความเข้าใจในการดำเนินการตามมาตรฐาน ISO/IEC 17799	/	/	/	/	/
2. กลุ่มวิชาความมั่นคงปลอดภัย					
1. ความมั่นคงปลอดภัยเครือข่ายและระบบ			/	/	
2. การบริหารจัดการไฟร์วอลล์			/	/	
3. การบริหารจัดการความปลอดภัยเครือข่ายไร้สาย				/	
4. การพัฒนา Web Security				/	
5. การสร้าง VPN ที่มั่นคงปลอดภัย				/	
6. การใช้ระบบตรวจจับผู้บุกรุก				/	
7. การต่อต้านการโจมตี		/	/	/	
8. ความมั่นคงปลอดภัย Windows Server 2003			/	/	
9. ความมั่นคงปลอดภัยของ UNIX และ Linux			/	/	
3. วิชาและจุดอ่อน					
1. การประเมินจุดอ่อนของระบบ (Venerability Assessment)		/	/	/	
2. Computer Forensics and การตอบสนองต่อเหตุการณ์		/	/	/	
3. การใช้ PKI ในองค์กร	/	/	/	/	/
4. การพัฒนานโยบายด้านความปลอดภัยสำหรับเครือข่าย		/	/	/	/

5. การวิเคราะห์และบริหารจัดการความเสี่ยง	/	/	/	/	/
4. กลุ่มวิชาการบริหารจัดการกระบวนงานอย่างมั่นคงปลอดภัย					
1. หลักสูตรฝึกอบรม ISMS 27001 : ความต้องการ		/	/		
2. หลักสูตรฝึกอบรม ISMS 27002 (17799) : หลักการการดำเนินการ		/	/		
3. หลักสูตรฝึกอบรม ISMS 27003 : การนำไปใช้		/	/		
4. หลักสูตรฝึกอบรม ISMS 27004 : การวัด		/	/		

	ผู้บริหารระดับสูง	**ผู้บริหารระดับกลาง**	**ปฏิบัติการสารสนเทศ**	**ปฏิบัติการและเครือข่าย**	**End User**
5. หลักสูตรฝึกอบรม ISMS 27005 : การบริหารความเสี่ยง		/	/		
6. หลักสูตรฝึกอบรม ISMS 27006 : การรับรองวุฒิฐานะ		/	/		

5.2.2 หลักสูตรระดับปริญญาบัตร

ในปัจจุบันหลักสูตรมหาบัณฑิตด้านเทคโนโลยีสารสนเทศ ที่เปิดสอนตามสถาบันการศึกษาของรัฐและเอกชนจะเป็นหลักสูตรใน 3 ลักษณะ คือ

1. หลักสูตรระบบมหาบัณฑิตด้านเทคโนโลยีสารสนเทศ
   หลักสูตรประเภทนี้จะเป็นหลักสูตรในรูปแบบกว้างคือมีการเรียนในเรื่องฮาร์ดแวร์ เครือข่าย ซอฟต์แวร์ วิชาด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ เป็นวิชาเลือก 3 หน่วยกิต
2. หลักสูตรมหาบัณฑิตด้านบริหารจัดการสารสนเทศ
   หลักสูตรประเภทนี้จะเรียนในแนวบริหารที่ต้องใช้คอมพิวเตอร์ และเทคโนโลยีสารสนเทศ มีการเรียนด้านระบบสารสนเทศ การวางแผนกลยุทธ์ ด้านเทคโนโลยีสารสนเทศ และ

ซอฟต์แวร์ วิชาด้านความมั่นคงปลอดภัยก็มักเป็นวิชาเลือกหรืออาจจะเป็นหลักสูตรวิชาแกน (Core Course)

3. หลักสูตรมหาบัณฑิตด้านซอฟต์แวร์ วิศวกรรม

หลักสูตรประเภทนี้เน้นที่กระบวนการพิจารณาซอฟต์แวร์ ไม่มีการเรียน วิชาที่เกี่ยวกับความมั่นคงปลอดภัยโดยตรง

เพื่อส่งเสริมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัย สารสนเทศในระดับมหาบัณฑิต จึงสมควรจะกำหนดต้นแบบหลักสูตรในระดับมหาบัณฑิต ทั้งนี้

ต้นแบบหลักสูตรมหาบัณฑิต ด้านเทคโนโลยีสารสนเทศ	
Math Of Science in Cybersecurity	
วิชาแกน 24 หน่วยกิต	
CBC 101	เทคนิคด้านความมั่นคงปลอดภัยและการใช้รหัส
CBC 102	การดำเนินการด้านการรักษาความมั่นคงปลอดภัย
CBC 103	การโจมตีด้านสารสนเทศและการป้องกัน
CBC 104	การบริหารความเสี่ยง
CBC 105	ระบบคอมพิวเตอร์และเครือข่ายที่มั่นคงปลอดภัย
CBC 106	คอมพิวเตอร์ฟอเรนสิกส์
CBC 107	มาตรฐานการบริหารจัดการด้านความมั่นคงปลอดภัย
CBC 108	เทคนิคการจัดการภาวะฉุกเฉินและการดำเนินงานต่อเนื่อง

วิชาเลือก (ควรมีการทำวิทยานิพนธ์) หน่วยกิต : 6 วิชาเลือก (กรณีทำสาระนิพนธ์) หน่วยกิต: 9	
CBC 201	ความต้องการด้านความมั่นคงปลอดภัยสถาบันการเงิน
CBC 202	กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ
CBC 203	การออกแบบซอฟต์แวร์ที่มั่นคงปลอดภัย
CBC 204	ความปลอดภัยของเครือข่ายไร้สาย
CBC 205	เทคนิคการตรวจสอบภายใน
CBC 206	สัมมนาด้านความมั่นคงปลอดภัย
วิทยานิพนธ์ : 6 หน่วยกิต	สาระนิพนธ์ : 9 หน่วยกิต

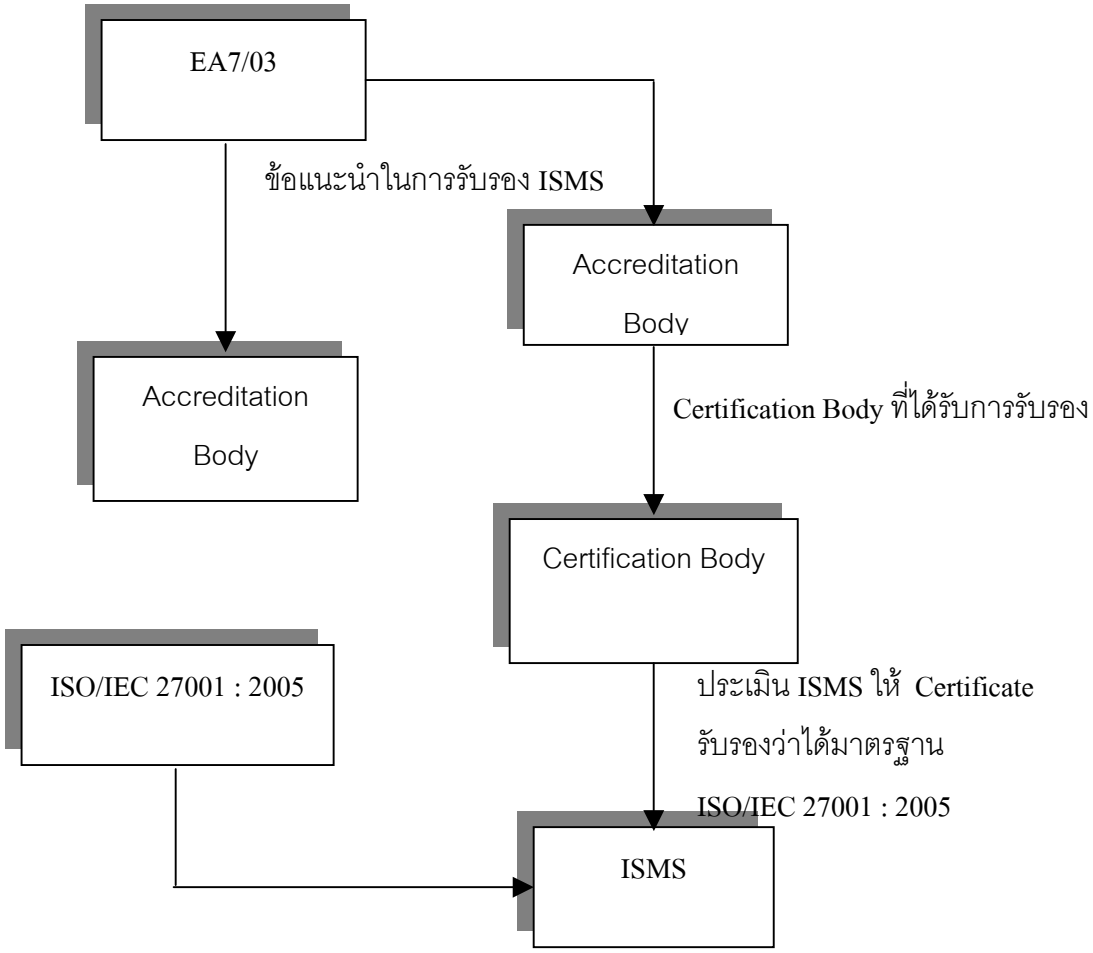
5.3 การบริหารโครงการด้าน Security Professional Certificate

ในการดำเนินการตรวจสอบความมั่นคงปลอดภัย ความเสี่ยงขององค์กรตลอดจนการนำหลักปฏิบัติที่เป็นสากลมาใช้ในองค์กร เพื่อให้องค์กรสามารถดำเนินการโดยมีความเสี่ยงน้อยที่สุดในการที่ถูกโจมตี หรือสร้างความเสียหายอันเกิดจากจุดอ่อนด้านความมั่นคงปลอดภัย ควรจะต้องทำภายใต้มาตรฐานสากลที่เป็นที่ยอมรับกันทั่วโลก เนื่องจากเป็นความจำเป็นอย่างยิ่งที่องค์กรที่ต้องทำธุรกรรมด้านนั้นจะต้องมั่นใจซึ่งกันและกันในด้านความมั่นคงปลอดภัย ทั้งนี้ในปัจจุบันมาตรฐานสากลด้านความมั่นคงปลอดภัยมาใช้ เฉพาะที่องค์กรได้รับการ Certificate การดำเนินงานเป็นไปตามมาตรฐานที่กำหนด

กระบวนการการ Certification

การให้ Certificate นั้น ได้ทำโดยองค์กรสากลหลายแห่งทั่วโลก ซึ่งองค์กรกลางเหล่านี้เป็นที่ยอมรับซึ่งกันและกัน เป็นเอกสาร EA7/03 ของ European Co-Operate for Accreditation ให้คำแนะนำในองค์กร Accreditation ระดับชาติ ในการรับรององค์กรที่ให้ Certificate ISMS ภายใต้มาตรฐาน ISO/IEC 27001 : 2005

การที่จะได้รับ Certificate จะต้องมีการตรวจสอบ ISMS ขององค์กรโดยผู้ประเมิน ISMS ผู้ประเมินจะเป็น Consultant ขององค์กรไม่ได้ มีกฎระเบียบคุมเรื่องนี้ไว้ ผู้ประเมินจะต้องทำงานให้กับ Certification Body (เป็น BSI Assessment Service Limited) Certification Body จะเป็นผู้ให้ Certificate เข้าองค์กร



รูปที่ 5.1 ความสัมพันธ์ระหว่างฝ่ายต่างๆ ที่เกี่ยวข้องกับ Certification

Certificate ที่ว่านี้จะกำหนดขอบเขต ISMS ขององค์กร Accreditation Body ที่ให้ Certificate ได้จะต้องได้รับการรับรอง Certification เช่นเดียวกัน เป็น Certification ว่าเป็น ISO/IEC 17799 Lead Assesses หรือได้รับ CISSP (Certificate Information System Professional)

CISSP

CISSP เป็น Certificate ที่ได้โดย ISCS (International formation System Security Certification Consortium) ซึ่งพบกันในปี 1989 ซึ่งสนับสนุนการสร้างมืออาชีพด้านความปลอดภัย ข้อสอบ CISSP นั้น จะประกอบไปด้วย Multiple Choice 250 ข้อ โดยให้เวลาทำใน 6 ชั่วโมง องค์ความรู้ที่สอบมี 10 ประเภท

- Accent Control System & Methodology
- Application & System Development
- Business Continuity Planning
- Cryptographic System
- Law, Investigation & Ethics
- Operator Security
- Physical Security
- Security Architecture & Models
- Security Management Practice
- Telecommunication, Network & Internet Security

ดังนั้น แผนความมั่นคงปลอดภัยจะต้องสนับสนุนให้มีจำนวนมืออาชีพด้านความมั่นคงปลอดภัย ซึ่ง

อาจ Lead Assessor หรือ CISSP ให้มีจำนวนเพียงพอ ได้รับ Certificate โดยวิธีการสนับสนุน ร่วมมือระหว่างหน่วยงานที่ให้ Certification เฉพาะหน่วยงานภาครัฐที่สามารถทำหน้าที่ดังกล่าวได้ โดยจัดให้มีงบประมาณเพียงพอ ในการดำเนินการ หรือ Certification

บทที่ 6
แผนการจัดตั้งองค์กรกำกับดูแลด้าน ICT Security

6.1 คำนำ

การพัฒนาและใช้งานเทคโนโลยีด้าน ICT Security จำเป็นต้องมีหน่วยงานดูแลอย่างต่อเนื่อง เพราะเป็นเรื่องที่มีความสำคัญต่อการปฏิบัติงานของหน่วยงานต่างๆ ในประเทศไทย ในปัจจุบันยังไม่มีหน่วยงานที่ดูแลด้านนโยบายและสนับสนุน

ชื่อหน่วยงาน	สังกัด	ภารกิจ
กระทรวงไอ ซี ที	รัฐบาลไทย	• จัดทำแผนแม่บท • กำกับดูแล • แผนเตรียมความพร้อมแห่งชาติ ด้าน IT
คณะกรรมการธุรกรรมอิเล็กทรอนิกส์	กระทรวงไอ ซี ที	• กฎหมาย
สมช.	กระทรวงมหาดไทย	• สนับสนุนการจัดเตรียมแห่งชาติด้านการสื่อสารเพื่อจัดสร้างศูนย์บริการ
ThaiCert	NECTEC กระทรวงพาณิชย์	• ระบบรวมข้อมูล

6.2 ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ (Thailand Info-Security Policy and Analysis Center : TISPAC)

1. ศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ จัดตั้งขึ้นเป็นหน่วยงานภายใต้กระทรวง ในระดับสำนักงาน โดยมีหัวหน้าหน่วยงานเป็น “เลขาธิการ” ซึ่งตำแหน่งนี้คือผู้บริหารความมั่นคงปลอดภัยระดับสูงของประเทศ (Thailand Info-Security Policy and Analysis Center : TISPAC) มีบทบาทสำคัญดังต่อไปนี้

1) ตรวจจับ ป้องกัน ตอบโต้ และพิทักษ์ภัย ในเชิงรุก จากการโจมตีทางไซเบอร์ ที่มุ่งเป้าไปยังโครงสร้างพื้นฐานทางความมั่นคงฯ ของเครือข่ายของชาติ เช่น เครือข่ายการเงินการธนาคาร การดำเนินงานธุรกรรมที่สำคัญยิ่งของรัฐ การบริการฉุกเฉิน เป็นต้น
2) ลดจุดอ่อน การขัดจังหวะและการหยุดชะงักของธุรกรรมต่างๆ ที่อาจเกิดขึ้นจากผลของการโจมตีทางไซเบอร์ ทั้งต่อเป้าหมายที่เป็นหน่วยงานภาครัฐและภาคธุรกิจ
3) บรรเทาความเสียหายที่อาจเกิดขึ้นและลดช่วงเวลาที่จะต้องใช้ในการแก้ไขระบบให้ฟื้นคืนสภาพ อันเนื่องมาจากการโจมตีทางไซเบอร์ ให้ได้มากที่สุด
4) เสริมสร้างความแข็งแกร่งในงานข่าวกรองเพื่อต่อต้านภัยคุกคามจากไซเบอร์ โดยอาศัยการแบ่งปันข้อมูลข่าวสารจากพันธมิตร ได้แก่ หน่วยงานรัฐอื่นๆ ทั้งในประเทศ ในภูมิภาคและระดับนานาชาติ

2. จัดตั้งคณะกรรมการที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อทำหน้าที่
   - เสนอแนะต่อรัฐมนตรีกระทรวง เพื่อวางนโยบายส่งเสริมการพัฒนา ICT Security ตามกรอบแผนแม่บท ICT Security แห่งชาติ
   - เสนอะแนะการจัดทำและปรับปรุงมาตรฐาน ICT Security อย่างต่อเนื่อง
   - ติดตาม และดูแลการพัฒนาอุตสาหกรรม ICT Security
   - เสนอแนะและให้คำปรึกษา เพื่อตราพระราชกำหนด และกฎหมายอื่นๆ ด้านความมั่นคงปลอดภัยที่ไม่ได้ดำเนินการโดยคณะกรรมการธุรการของอิเล็กทรอนิกส์
   - ส่งเสริมการวิจัยและพัฒนา ตลอดจนการสร้างความรู้ด้านความมั่นคงปลอดภัย
3. หน้าที่ของเลขาธิการ
   - ปฏิบัติงานตามนโยบายของรัฐมนตรีกระทรวง โดยพิจารณาจากคณะกรรมการที่ปรึกษาด้านความมั่นคงปลอดภัย
   - ส่งเสริมและสนับสนุนดำเนินการด้านความมั่นคงปลอดภัย อย่างเป็นระบบทั้งการนำเทคโนโลยีและการสร้างอุตสาหกรรมด้านความมั่นคงปลอดภัย
   - กำกับดูแลความร่วมมือและประสานงานการดำเนินการกับหน่วยงานด้านความมั่นคงปลอดภัยระดับนานาชาติ
4. บทบาทและหน้าที่ของศูนย์นโยบายและวิเคราะห์ความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ

   (4.1) งานนโยบายและส่งเสริม
   - จัดทำนโยบายและแผนภายใต้กรอบของแผนแม่บท ICT Security แห่งชาติ เพื่อส่งเสริมการจัดทำแผนแม่บทความมั่นคงปลอดภัยของหน่วยงานต่างๆ
   - ดำเนินนโยบายและส่งเสริมการพัฒนาบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัย เพื่อสนับสนุนการพัฒนาอุตสาหกรรม

- กำหนดนโยบายและแผนส่งเสริมเชิงรุก โดยการเชื่อมโยงกับผู้เชี่ยวชาญในด้านการศึกษาและอุตสาหกรรมอย่างเป็นระบบ

(4.2) งานกำกับดูแล

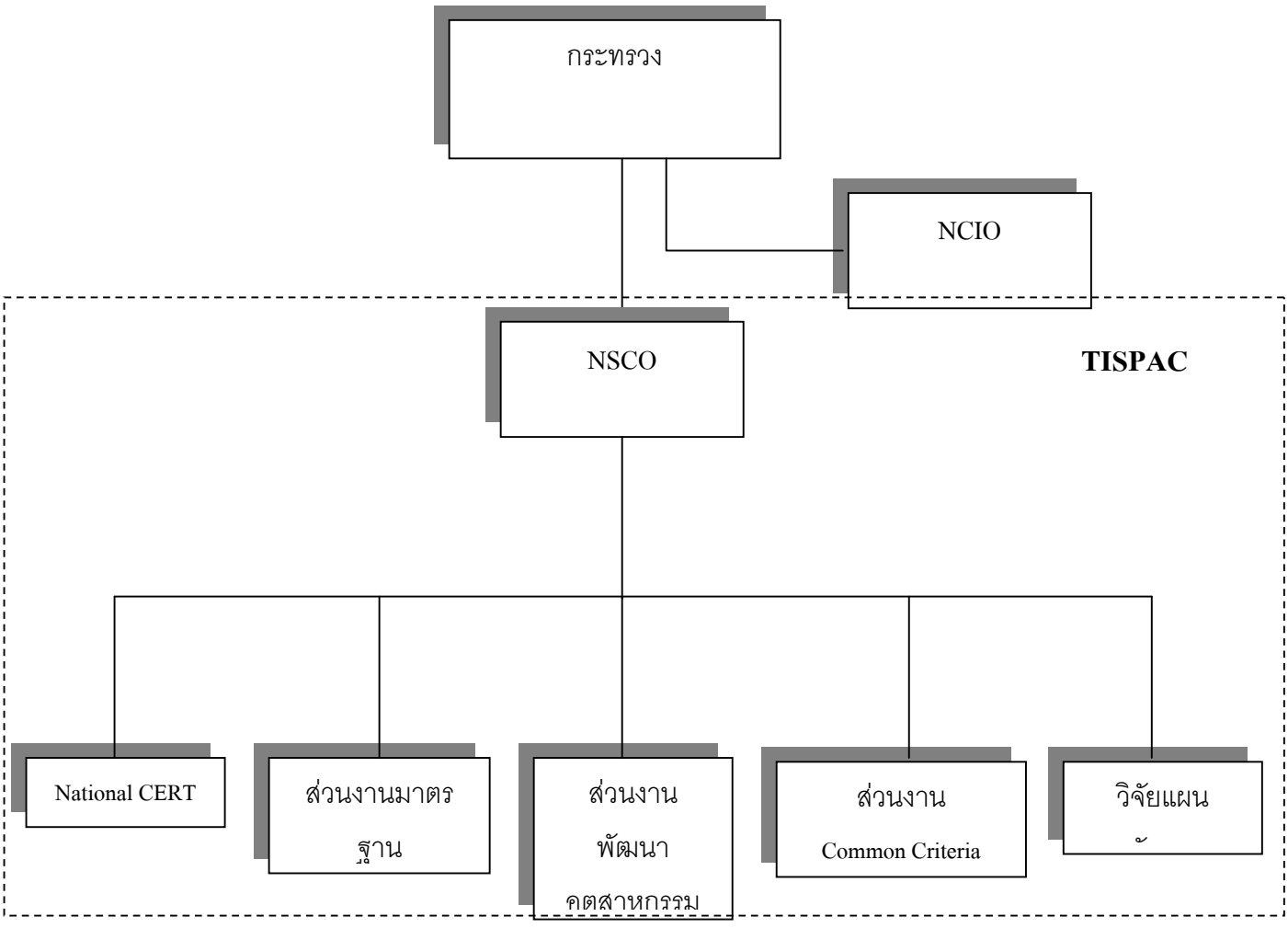
- กำกับดูแลการให้บริการให้คำปรึกษา การฝึกอบรม ที่อิงมาตรฐานสากลว่าเป็นการดำเนินการอย่างมีคุณภาพและผู้ดำเนินการมีคุณสมบัติตามที่ระบุ
- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระดับประเทศ เพื่อกำหนดนโยบายและแผนที่ลดความเสี่ยงด้านความมั่นคงปลอดภัย
- ติดตามการปฏิบัติตามแผนแม่บท ICT Security แห่งชาติ
- กำกับดูแลการปฏิบัติงานสอดส่องและตอบสนองต่อภัยคุกคาม

4.3 งานด้านกฎหมาย

- ศึกษาถึงแนวทางกฎหมายด้านความมั่นคงปลอดภัยในต่างประเทศเพื่อให้ได้กรอบความคิด เพื่อพิจารณาการประยุกต์ใช้ในประเทศไทย
- สนับสนุนและทำงานร่วมมือกับคณะกรรมการธุรการในเรื่องกฎหมายเทคโนโลยีสารสนเทศ

6.3 โครงสร้างหน่วยงาน

ศูนย์ฯบริหารโดยผู้บริหารความมั่นคงปลอดภัยระดับสูงของประเทศโดยกำกับดูแลการปฏิบัติงานของ 5 ส่วนงานได้แก่ National CERT, ส่วนงานมาตรฐาน ICT Security, ส่วนงานพัฒนาอุตสาหกรรม ICT Security, ส่วนงาน Common Criteria และ วิจัยแผนพัฒนาซึ่งแต่ละส่วนงานมีภาระหน้าที่โดยสังเขปดังนี้



รูปที่ 6.1 โครงสร้างองค์กรกำกับดูแลด้าน ICT Security

1) กลุ่มงาน National CERT

กลุ่มงานนี้มีภารกิจสอดส่องตรวจสอบ เพื่อตอบสนองต่อวิกฤตการณ์ และภาวะฉุกเฉินต่างๆ ทั้งนี้ต้องดำเนินการเป็นศูนย์กลางของ CERT ของหน่วยงานต่างๆ และดำเนินการประสานงานกับศูนย์บริการวิกฤตระดับชาติ และศูนย์บริการ

2) กลุ่มงานมาตรฐาน ICT Security

กลุ่มงานนี้มีหน้าที่ติดตาม จัดทำ และตรวจสอบมาตรฐานต่างๆ ด้าน ICT Security โดยอิงมาตรฐานความมั่นคงปลอดภัยระดับสากล

3) กลุ่มงานพัฒนาอุตสาหกรรม ICT Security

กลุ่มงานนี้ติดตาม การจัดทำแผนแม่บทความมั่นคงปลอดภัย ดำเนินการสนับสนุนพัฒนาบุคลากรด้านความมั่นคงปลอดภัย สนับสนุนการทำ Certification

4) กลุ่มงานประเมินสินค้า และบริการด้าน ICT Security

กลุ่มงานนี้มีหน้าที่ติดตาม และประเมินเทคโนโลยีด้าน ICT Security โดยเฉพาะอย่างยิ่งการประยุกต์ใช้มาตรฐาน Common Criteria ในการประเมินอุปกรณ์ด้านความมั่นคงปลอดภัย

5) กลุ่มงานวิจัยแผนพัฒนา

กลุ่มงานนี้มีหน้าที่ติดตามเทคโนโลยีใหม่ๆ ที่สามารถนำมาประยุกต์เป็นนวัตกรรมเชิงซอฟต์แวร์ หรือฮาร์ดแวร์ เพื่อสร้างฐานความรู้และพัฒนาเทคโนโลยีเชิงประยุกต์ด้านความมั่นคงปลอดภัย

บทที่ 7
การติดตามประเมินผล

7.1 คำนำ

การติดตามประเมินผล จะใช้ระเบียบวิธีลิขิตสมดุลย์ (Balanced Scorecard) เนื่องจากแผนแม่บท ICT Security แห่งชาติ เป็นแผนที่ต้องมีการบูรณาการหลายด้านในเชิงปฏิบัติ ในการนี้จึงจะพิจารณาใน 4 มิติ ได้แก่ มิติการพัฒนาองค์กรและเทคโนโลยี มิติกระบวนการขององค์กรในการสนับสนุนการดำเนินการเพื่อให้เกิดความสัมฤทธิ์ผลและสร้างความพึงพอใจแก่ภาครัฐ หน่วยงานภาคเอกชนมีระบบ ICT ที่มีความปลอดภัยต่อการโจมตีจากภายในและภายนอก ประชาชนมีความปลอดภัย และมั่นใจในความปลอดภัยด้านสารสนเทศและความเป็นส่วนตัวในสังคมไทย และธุรกิจมีความมั่นใจในการดำเนินการธุรกรรมผ่านระบบอินเตอร์เน็ต ซึ่งในที่สุดจะส่งผลให้เกิดความสำเร็จในมิติประสิทธิผลการดำเนินงานตามแผนแม่บท ICT Security แห่งชาติ

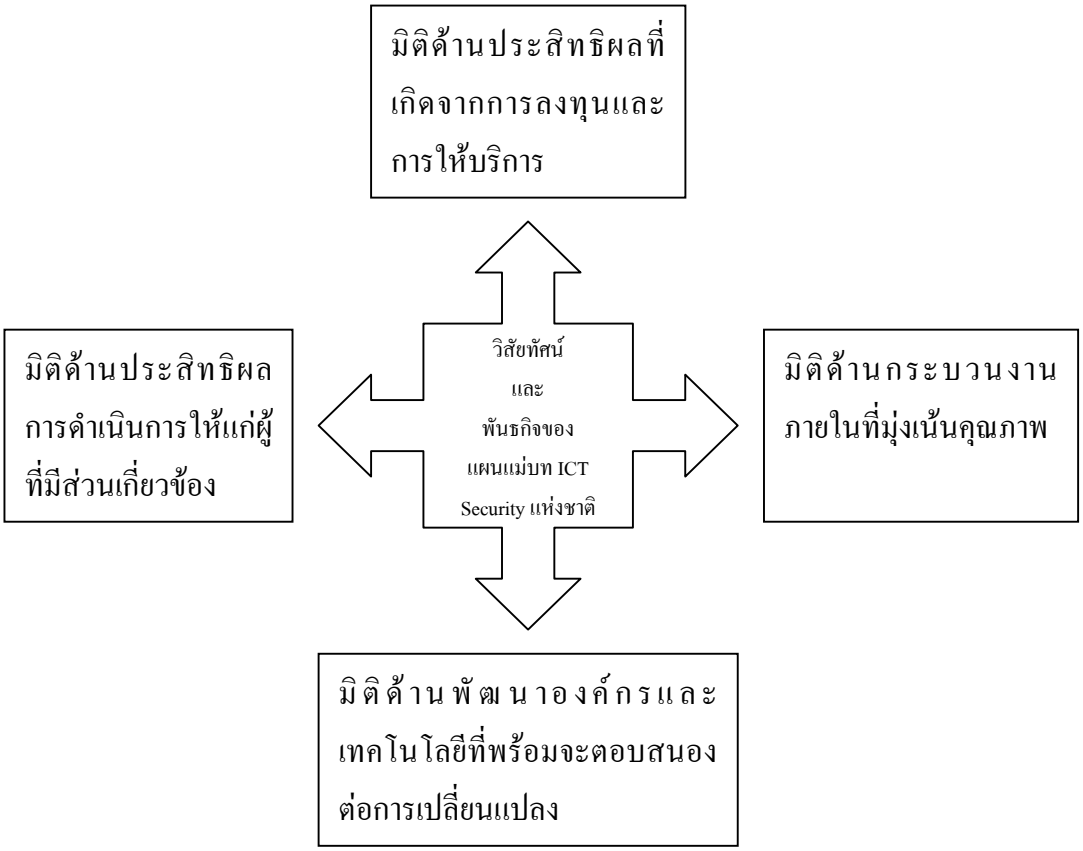
7.2 ดัชนีชี้วัดเพื่อการติดตามประเมินผล

การติดตามประเมินผลเพื่อแปลงแผนแม่บท ICT Security แห่งชาติไปสู่การปฏิบัติจะต้องดำเนินการดังนี้

1. สร้างดัชนีชี้วัดสำหรับแต่ละยุทธศาสตร์ เพื่อเป็นเครื่องมือที่บ่งบอกถึงความสำเร็จและผลกระทบของการดำเนินงานตามแผน เพื่อใช้เป็นประโยชน์ในการติดตามประเมินผล ด้านผลลัพธ์ (Output) ที่กำหนด
2. จัดทำระบบฐานข้อมูลของตัวดัชนีชี้วัดความสำเร็จ

การติดตามประเมินผลความสำเร็จของแผนแม่บท ICT Security แห่งชาติ จะประยุกต์จากระเบียบวิธีลิขิตสมดุลย์ (Balanced Scorecard: BSC) ซึ่งเป็นวิธีการที่พิจารณาผลการดำเนินงานตามเป้าประสงค์ใน 4 มิติ ได้แก่ ด้านการเงิน ด้านลูกค้า ด้านกระบวนงานภายใน และด้านการเรียนรู้ ในการนี้ สำหรับหน่วยงานภาครัฐ ที่ไม่มีพันธกิจที่แสวงหากำไร ดังนั้น BSC จะถูกปรับใช้ดังนี้

1 มิติด้านประสิทธิผลที่เกิดจากการลงทุนและการให้บริการ
2 มิติด้านประสิทธิผลการดำเนินการให้แก่ผู้ที่มีส่วนเกี่ยวข้องอันได้แก่ รัฐบาล ประชาชน
3 มิติด้านกระบวนงานภายในที่มุ่งเน้นคุณภาพ
4 มิติด้านพัฒนาองค์กรและเทคโนโลยีที่พร้อมจะตอบสนองต่อการเปลี่ยนแปลง



รูปที่ 7.1 : แนวความคิด Balanced Score card

วิสัยทัศน์

ประเทศไทยมีระบบรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายสำหรับองค์กรและหน่วยงานต่าง ๆ ตลอดจนผู้ใช้งานระบบและเครือข่ายทั่วไปตามมาตรฐานสากล และประเทศไทยเป็นผู้นำด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

พันธกิจ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในฐานะที่เป็นหน่วยงานของภาครัฐที่รับผิดชอบทางด้านนโยบายและแผนแม่บทด้านเทคโนโลยีสารสนเทศของประเทศ จึงเป็นผู้จัดทำนโยบาย และ แผนแม่บท ICT Security แห่งชาติ

ยุทธศาสตร์

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไอซีที

ยุทธศาสตร์ที่ 2 ส่งเสริมการวิจัยและพัฒนาเทคโนโลยีความมั่นคงปลอดภัยไอซีที

ยุทธศาสตร์ที่ 3 ส่งเสริมการสร้างกระบวนงานขององค์กรที่มั่นคงปลอดภัยฉบับต่อเนื่อง

ยุทธศาสตร์ที่ 4 ติดตามประเมินผลด้าน ICT Security

ยุทธศาสตร์ที่ 5 สร้างเครือข่ายบุคลากร องค์กรและผู้เชี่ยวชาญ ด้าน ICT Security และอุตสาหกรรมไอซีที

วัตถุประสงค์

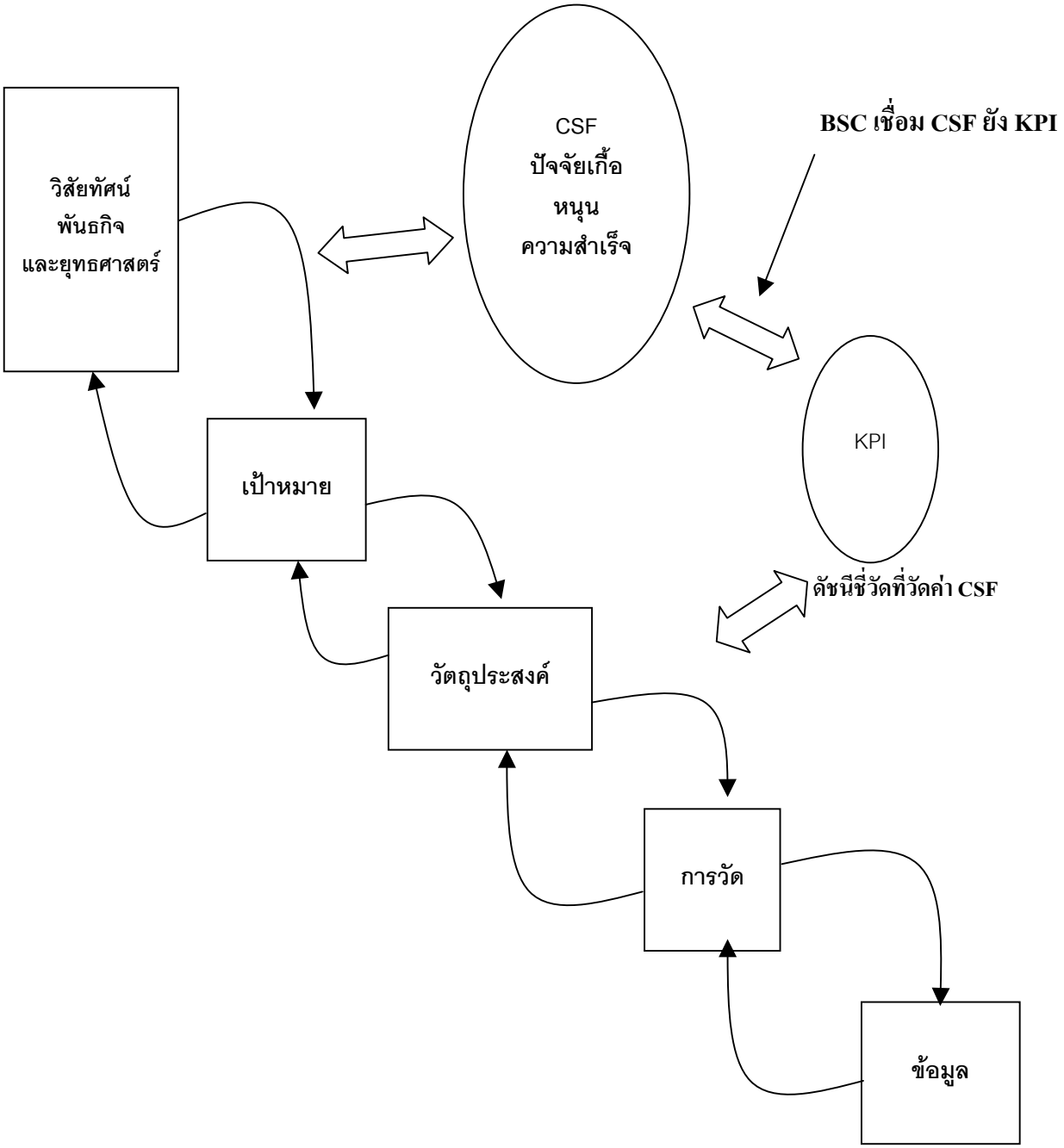
1. เพื่อสำรวจแนวทางการจัดทำแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่งชาติ National ICT Security Plan Best Practices จากต่างประเทศ
2. เพื่อสำรวจและวิเคราะห์สถานภาพปัจจุบันของประเทศไทยด้านความมั่นคงปลอดภัย
3. เพื่อกำหนดกรอบนโยบาย แนวทางดำเนินการ และมาตรการเพื่อการบริหารจัดการ ICT Security ของประเทศ
4. เพื่อจัดทำแนวทางบริหารจัดการดำเนินการ เพื่อพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยด้านไอซีทีของประเทศ

เป้าหมาย

มีแผนแม่บท ICT Security แห่งชาติ เพื่อให้

1 การทำธุรกรรมทางอิเล็กทรอนิกส์มีความปลอดภัย
2. หน่วยงานภาครัฐและสังคมมีความปลอดภัยตามมาตรฐานที่ได้กำหนด
3. อุปกรณ์ที่ใช้ในระบบเครือข่าย ต้องมีการจัดมาตรฐานความปลอดภัย
4. มีโครงสร้างองค์กรที่รับผิดชอบในเรื่องแผนแม่บท ICT Security แห่งชาติ ในการผลักดันให้เป็นไปตามแผน

ปัจจัย 4 ด้านที่มีผลต่อยุทธศาสตร์



รูปที่ 7.2 : ความเชื่อมโยงระหว่างยุทธศาสตร์, CSF, KPI และ BSC

การนำแนว BSC ไปประยุกต์ใช้สำหรับการปฏิบัติการแผนแม่บท ICT Securityแห่งชาติ ซึ่งมีเป้าประสงค์หลักตามที่กำหนด โดยมีวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ เป้าหมาย และวัตถุประสงค์ ทั้งนี้ภาพความเชื่อมโยงจากวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ไปยังเป้าหมาย วัตถุประสงค์ และการวัด ตลอดจนข้อมูลที่ต้องใช้ในการคำนวณ แสดงอยู่ในรูปที่ 9.2

โดยที่แต่ละยุทธศาสตร์จะมีการกำหนดเป้าหมายที่ต้องการ เพื่อการติดตามความสำเร็จของแผนแม่บท ICT Security แห่งชาติ สำหรับแต่ละเป้าหมายยุทธศาสตร์จะมีดัชนีชี้วัดได้หลายตัว ตาราง 9.1 แสดงดัชนีชี้วัดของเป้าหมายยุทธศาสตร์ ทั้ง 5 ยุทธศาสตร์ที่สอดคล้องกับแผนงานที่กำหนด

ดังนั้น การประเมินผลและติดตามความสำเร็จของโครงการก็จะสามารถทำได้อย่างเป็นระบบ มีหลักการที่สมดุล ในส่วนเป้าหมายการวัดผลแต่ละปีนั้น เป็นส่วนที่คณะกรรมการดำเนินการแผนแม่บท ICT Security แห่งชาติ จะต้องกำหนดและดำเนินการพัฒนาระบบรวบรวมข้อมูล เพื่อนำดัชนีชี้วัดลิขิตสมดุลย์มาใช้เป็นเครื่องมือติดตาม ประเมินผล เพื่อผลักดันให้ประสบความสำเร็จ

ตารางที่ 7.1 ความสัมพันธ์ของดัชนีชี้วัด ลิขิตสมดุลย์ เป้าหมาย และแผนงานด้านการสื่อสาร

BSC	เป้าหมาย	ตัวชี้วัด	แผนงาน
ประสิทธิผล	**<u>ยุทธศาสตร์ที่</u>** 1 พัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไอซีที ● สามารถจัดตั้งศูนย์ฯได้ภายใน 3 ปี ● สามารถดำเนินการจัดทำโครงสร้างพื้นฐานด้านการพิสูจน์ตัวตนทางอิเล็กทรอนิคส์แห่งชาติได้ภายใน 3 ปี ● สามารถดำเนินการจัดทำโครงการพัฒนามาตรฐานการวิเคราะห์สัญญาดิจิตอลตามกฎหมายได้ภายใน 3 ปี	● งบประมาณ ● บุคลากร ● จำนวนหน่วยงานที่ใช้เทคโนโลยีพิสูจน์ตัวตน □ จำนวน ISP ที่ต่อเชื่อมสัญญาณ ● ปริมาณ Traffic ที่วิเคราะห์	● ส่งเสริมการสร้างโครงสร้างพื้นฐานและศูนย์ปฏิบัติการ เพื่อจัดการความเสี่ยงจากเหตุการณ์ด้านความมั่นคงปลอดภัย

BSC	เป้าหมาย	ตัวชี้วัด	แผนงาน
ผู้ที่เกี่ยวข้อง	**<u>ยุทธศาสตร์ 3</u>** ส่งเสริมการสร้างกระบวนงานขององค์กรที่มั่นคงปลอดภัยฉบับต่อเนื่อง ● สามารถจัดทำกรอบได้ภายใน 2 ปี ● สามารถกำหนดนโยบายได้ภายใน 2 ปี ● มีหน่วยงานไม่ต่ำกว่า 30 แห่งที่จัดทำนโยบาย ICT Security ต่อปี ● สามารถจัดทำได้ไม่ต่ำกว่า 50 แห่งต่อปี	● จำนวนหน่วยงานที่ได้รับรองมาตรฐานความมั่นคงปลอดภัยของประเทศ ● มีนโยบายด้าน ICT Security ระดับชาติ จำนวนหน่วยงานที่ได้จัดทำแผนบริหารความเสี่ยงด้าน ICT Security ● จำนวนหน่วยงานที่ได้ร่างคำของบประมาณด้าน ICT Security	● พัฒนาระบบการบริหารจัดการด้านความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management) ● ส่งเสริมนโยบายด้านความมั่นคงปลอดภัยและการจัดองค์กร

BSC	เป้าหมาย	ตัวชี้วัด	แผนงาน
กระบวนการภายใน	**<u>ยุทธศาสตร์ 2</u>** ส่งเสริมการวิจัยและพัฒนาเทคโนโลยีความมั่นคงปลอดภัยไอซีที • สามารถดำเนินการประเมินความพร้อมด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารได้ภายใน 1 ปี • สามารถกำหนดมาตรฐานได้ภายใน 2 ปี • สามารถมีระบบการเข้ารหัสได้ภายใน 3 ปี	• จำนวนหน่วยงานที่ได้รับการประเมินความพร้อมด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร • มีมาตรฐานผลิตภัณฑ์ • จำนวนผลิตภัณฑ์ที่ได้รับความมั่นคงปลอดภัย □ มีระบบเข้ารหัส	• พัฒนาเทคโนโลยีประเมินผลและพัฒนาการระบบสารสนเทศและเครือข่ายที่มั่นคงปลอดภัย
	<u>ยุทธศาสตร์ที่</u> 4 ติดตามประเมินผลด้าน ICT Security • สามารถจัดทำดัชนีชี้วัดความมั่นคงปลอดภัยได้ภายใน 1 ปี	• จำนวนดัชนีชี้วัดที่ใช้ • มีระบบติดตามการประเมินผลตามความมั่นคงปลอดภัย	• การบังคับใช้กฎระเบียบและการวัดผล (Compliance and Measurement)

BSC	เป้าหมาย	ตัวชี้วัด	แผนงาน
เรียนรู้และพัฒนา	**<u>ยุทธศาสตร์ที่ 5</u>** สร้างเครือข่ายบุคลากร องค์กรและผู้เชี่ยวชาญด้าน ICT Security และอุตสาหกรรมไอซีที • มีผู้เข้าร่วมโครงการไม่ต่ำกว่า 5,000 คนต่อปี • มีบุคลากรที่สอบผ่านการรับรองความสามารถการดำเนินการด้านความมั่นคงปลอดภัยไม่ต่ำกว่า 50 คนต่อปี • สามารถจัดตั้งสำนักงานส่งเสริมอุตสาหกรรม ICT Security ได้ภายใน 3 ปี • มีผู้ที่ผ่านการอบรมหลักสูตรวุฒิบัตรไม่ต่ำกว่า 2,000 คนต่อปี	• จำนวนบุคคลากรที่ให้ความรู้ทักษะ และความสารมารถด้าน ICT Security • จำนวนบุคคลที่ได้รับ Certification ด้าน ISMS • ความก้าวหน้าในการจัดตั้งสำนักงานส่งเสริมอุตสาหกรรมความมั่นคงปลอดภัยไอซีที • จำนวนบุคลากรที่ผ่านการฝึกอบรม	• พัฒนาบุคลากรด้าน ICT Security • แผนงานส่งเสริมการพัฒนายุทธศาสตร์ ICT Security

เอกสารอ้างอิง

1. htt://thaicert.nectec.or.th ThaiCERT Nectec มาตรฐานการักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549
2. http://csrc.nist.gov
3. www.ida.gov.sg 2006
4. 2006 iDA Singapore
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
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
7. INTERNATIONAL STANDARD ISO/IEC 27001
8. กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์