140 Days Countdown for Computer Related Crime Act B.S. 2550

Prinya Hom-anek

CISSP, CISA, SSCP, CISM, SANS GIAC GCFW, Security +
(ISC)^2 Asian Advisory Board, ISACA Thailand committee

ACIS Professional Center Co., Ltd.
eMail: prinya@acisonline.net

GRC

Governance ***Risk*** ***Compliance***

Governance

- นโยบาย วัฒนธรรมองค์กร กระบวนการขั้นตอนการปฏิบัติงานซึ่งกำหนดไว้อย่างชัดเจนในการบริหารจัดการ และกำกับดูแลองค์กรโดยผู้บริหารระดับสูง เพื่อการบริหารองค์กรที่โปร่งใส ตรวจสอบได้

Corporate Governance

- รวมถึงความสัมพันธ์ และบทบาทของทุกคนในองค์กรไม่จำกัดเฉพาะผู้บริหารอย่างเดียว
- กำหนดเป้าหมายหลักโดยเน้นเรื่องความโปร่งใสในการบริหารจัดการ

Risk Management

- การบริหารจัดการความเสี่ยงที่มีเป้าหมายในการลดผลกระทบจากความเสี่ยงที่อาจมีโอกาสเกิดขึ้นได้ในองค์กร หากไม่มีการบริหารจัดการความเสี่ยงที่ดีพอ

Compliance

- การปฏิบัติตามกฎระเบียบข้อบังคับ และกฎหมาย ตลอดจนนโยบายด้านสารสนเทศและความปลอดภัยขององค์กรอย่างถูกต้อง ได้ตามมาตรฐาน เช่น
  - การปฏิบัติตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์ โดยคณะกรรมการธุรกรรมอิเล็คทรอนิกส์
  - การจัดทำแผนเพื่อรองรับ พรบ. และ พรฎ. ด้านความปลอดภัยทางอิเล็กทรอนิกส์

พรบ. และ พรฎ. ด้านความปลอดภัยทางอิเล็กทรอนิกส์

- **พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544**
  - **พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็คทรอนิกส์ภาครัฐ พ.ศ. 2549 (มาตรา 35)**
  - **(ร่าง) พรฎ. กำหนดวิธีการแบบ (มั่นคง) ปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ (มาตรา 25) ซึ่งเป็นข้อแนะนำของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ และบริษัทไทยเรทติ้ง แอนด์ อินฟอร์เมชั่นเซอร์วิส จำกัด (ทริส)**
- **พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550**
  - **ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550**

GRC

SOX Corporative Compliance

Privacy Compliance *Employment*

PCI DSS ***Corporate Governance***

IT Governance ***Strategic Risk***

Financial Risk ***Operational Risk***

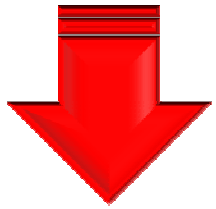
IT Risk *Basel II* Labor Compliance

GRC

Governance **Compliance**

กฎหมายธุรกรรมอิเล็กทรอนิกส์

กฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์



RISK

Good Governance

Good Governance

Risk Management

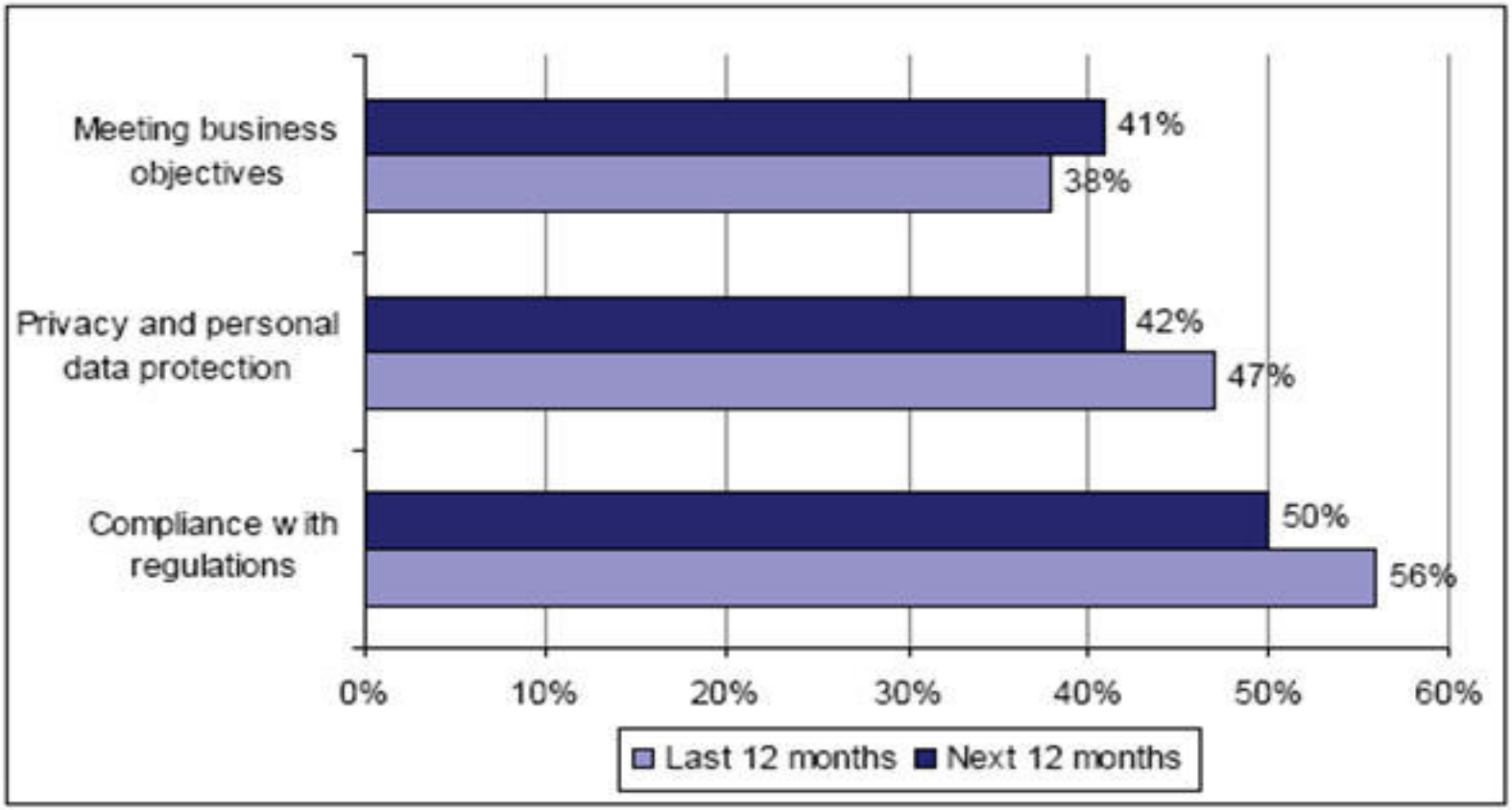
Compliance Management

The Current IT Security Management

- *Holistic Risk Management* → **การบริหารความเสี่ยงในภาพรวม**
- **นำปัจจัยด้านกฎระเบียบ ข้อกฎหมายต่าง ๆ มาพิจารณาด้วยในโครงการที่เกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ**
- **แนวทาง** “Regulatory Compliance” **เป็นเรื่องสำคัญที่มีผลกระทบต่อโครงสร้างพื้นฐานระบบสารสนเทศ** (IT Infrastructure) **ของ องค์กรอย่างหลีกเลี่ยงไม่ได้**

Top Driver of IT Security Investment

Source : Ernest and Young, Global Information Security Survey



GRC Component Definition Table

Recommended Process	Executed By
Governance (G)	The board of director, corporate secretary and governance professionals including board management
Strategy	Chief Executive Officer (CEO) or “c-suite”
Risk Management (R)	Chief Risk Officer (CRO), business line and other executives
Audit	Chief Audit Executive, internal audit, audit committee and external auditors
Legal	The general counsel and legal staff
Compliance (C)	The general counsel, chief compliance and ethics officer, compliance professionals and other legal staff
Information Technology	Chief Information Officer (CIO), privacy officer and/or security officer
Ethics & Corporate Social Responsibility	Chief Ethics Officer and Chief Responsibility Officer
Quality Management	Quality professionals throughout the organization
Human Capital & Culture	Human resource professionals and organizational design and development professionals

GRC

- แนวคิด “GRC”
  - ทำให้องค์กรแสดงถึงความเป็น “Good Governance”
  - ทำให้องค์กรเกิดความสามารถในการแข่งขัน (Competitive Advantage) ในระยะยาว
  - เสริมภาพลักษณ์ที่ดีให้กับองค์กร ตลอดจนคณะผู้บริหารระดับสูง
  - สร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับพนักงานทุกคน
  - ส่งผลให้ลูกค้าเกิดความเชื่อถือ และมีความมั่นใจในการใช้บริการต่าง ๆ ขององค์กร

GRC

- เป็นทิศทางใหม่สำหรับผู้บริหารระดับสูงขององค์กร
  - ไม่จำกัดเฉพาะผู้บริหารระบบสารสนเทศ หรือ CIO เท่านั้น
  - เป็นทิศทางของผู้บริหารในระดับ *C Level* ทั้งหมด จำเป็นต้องร่วมแรงร่วมใจกันในการผลักดันแนวคิด “GRC” ให้เป็นผลงานในเชิงปฏิบัติ
- ภาวะผู้นำ หรือ “Leadership” เป็นปัจจัยสำคัญ
  - งบประมาณ
  - ต้องมีบุคลากรที่ได้รับมอบหมายให้ทำตามแนวคิด “GRC” โดยเฉพาะ
  - ควรจัดจ้างที่ปรึกษา หรือผู้เชี่ยวชาญเฉพาะเพื่อให้คำแนะนำ และให้แนวทางปฏิบัติจาก Standard และ Best Practice ต่าง ๆ ได้อย่างถูกต้อง

กฎหมายไทยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ธุรกรรมทางอิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์

การโอนเงินทางอิเล็กทรอนิกส์

การคุ้มครองข้อมูลส่วนบุคคล

การกระทำผิดเกี่ยวกับคอมพิวเตอร์

การพัฒนาโครงสร้างพื้นฐานสารสนเทศ

สถานะกฎหมายเทคโนโลยีสารสนเทศล่าสุด

ชื่อกฎหมาย	สถานภาพ
1. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.	มีผลบังคับใช้แล้ว 10 มกราคม 2550 ใน ราชกิจจานุเบกษา ฉบับกฤษฎีกา เล่ม 124 ตอนที่ 4 ก
2. ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. .... (แก้ไขเพิ่มเติม)	- 31ตุลาคม 2550 (สำนักงาน) ผ่านการพิจารณาเห็นชอบคณะกรรมการประสานงาน สนช. เพื่อเข้าสู่การพิจารณาขอสภานิติบัญญัติแห่งชาติต่อไป - e-Document อยู่ระหว่างการเสนอเข้าพิจาณาของ สนช. ในการประชุมครั้งที่ 62/2550 (7 ธันวาคม 2550)
3. ร่างพระราชกฤษฎีกากำกับดูแลธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. .... (e-Payment)	ผ่านการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา และกำลังเข้าสู่การพิจารณาของสำนักงานเลขาธิการคณะรัฐมนตรีอีกครั้งหนึ่ง
4. ร่างพระราชกฤษฎีกาว่าด้วยการกำกับดูแลธุรกิจบริการการให้บริการออกใบรับรองอิเล็กทรอนิกส์ พ.ศ. .... (CA)	คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ให้ความเห็นชอบในหลักการเมื่อการประชุมครั้งที่ 13 เมื่อวันที่ 25 พฤษภาคม 2549 และมีการจัดให้มีการรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้องไปเรียบร้อยแล้ว 4 ครั้ง เพื่อนำข้อสังเกต ข้อเสนอแนะมาปรับแก้ร่างพ.ร.ฎ ดังกล่าว และครม.มีมติเห็นชอบเมื่อวันที่ 28 พย. 2549 ขณะนี้อยู่ระหว่างการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา
5. ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.	ครม.มีมติเห็นชอบวันที่ 1 สิงหาคม 2549 และขณะนี้อยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา
6. ร่างพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัย พ.ศ.	อยู่ในระหว่างการจัดให้มีการรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้อง เพื่อนำข้อสังเกตข้อเสนอแนะมาปรับแก้ร่างพ.ร.ฎ ดังกล่าว และขณะนี้อยู่ระหว่างการดำเนินการเพื่อเสนอต่อครม. ต่อไป

Thailand ICT Related Law Latest Update

พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ 2544
Electronic Transaction Law

พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 25 : วิธีการแบบปลอดภัย (ISO/IEC 27001)

พระราชกฤษฎีกากำหนดวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 32 : ธุรกิจบริการเกี่ยวกับธุรกรรมทาง อิเล็กทรอนิกส์

พระราชกฤษฎีกาว่าด้วยการกำกับดูแลธุรกิจบริการให้บริการออกใบรับรองอิเล็กทรอนิกส์

มาตรา 35 : ธุรกรรมภาครัฐ

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (10 มกราคม 2550)

Thailand Information Security Standard for Electronic Transaction

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
คณะอนุกรรมการด้านความมั่นคง

Electronic Transactions Commission
คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรฐานการรักษาความมั่นคงปลอดภัย
ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น1)

ประจำปี 2547

เกณฑ์การกำหนดระดับความเสี่ยง

ระดับความมั่นคงปลอดภัย	ประเภทของมาตรการป้องกัน				มาตรการป้องกันนั้นเกี่ยวข้องกับ			
	Preventive	Detective	Corrective	รวม	People	Process	Process	รวม
ระดับ 1	49	15	1	65	14	**51**	19	84
ระดับ 2	48	27	3	78	11	**53**	24	88
ระดับ 3	38	20	3	61	9	**40**	23	72
รวม	135	62	7		34	**144**	66	

ระดับ 1 หมายถึง ระดับความมั่นคงปลอดภัยพื้นฐาน มีจำนวน 51 ข้อ
ระดับ 2 หมายถึง ระดับความมั่นคงปลอดภัยขั้นกลาง มีจำนวน 104 ข้อ
ระดับ 3 หมายถึง ระดับความมั่นคงปลอดภัยขั้นสูง มีจำนวน 144 ข้อ

ตัวอย่างองค์กรที่มีความคาบเกี่ยวกับโครงสร้างพื้นฐานที่สำคัญ
ของประเทศไทยและควรจัดจัดทำมาตรฐานนี้
ในระดับความมั่นคงปลอดภัยสูงสุด (ระดับ 3)

สำหรับองค์กรที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศนั้นจัดว่าเป็นองค์กรที่มีความเสี่ยงสูง จึงต้องเร่งดำเนินการจนถึงระดับความมั่นคงปลอดภัยสูงสุดแต่เนื่องจากบางองค์กรอาจไม่ได้จัดสรรงบประมาณในส่วนนี้ไว้ จึงสามารถเริ่มต้นดำเนินงานเฉพาะบางส่วนของระบบทั้งหมดที่มีอยู่ให้เข้ามาตรฐานปลอดภัยสูงสุดก่อน การดำเนินการบางระบบ เช่น ระบบประมวลผลหลัก ระบบที่เกี่ยวข้องกับการเงิน เป็นต้น ตัวอย่างองค์กรเหล่านั้น ได้แก่

1. กลุ่มไฟฟ้าและพลังงาน ประกอบด้วย
   - การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย
   - การไฟฟ้านครหลวง
   - การไฟฟ้าส่วนภูมิภาค
   - บริษัท ปตท. จำกัด (มหาชน)
   - กรมพัฒนาและส่งเสริมพลังงาน
   - เป็นต้น

2 . กลุ่มการเงิน การธนาคารและการประกันภัย

กระทรวงการคลัง
ธนาคารแห่งประเทศไทย
ตลาดหลักทรัพย์แห่งประเทศไทย
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
กรมการประกันภัย
สมาคมประกันชีวิตไทย
สมาคมประกันวินาศภัย
ธนาคาร
บริษัทหลักทรัพย์ต่างๆ
เป็นต้น

3. กลุ่มการสื่อสาร โทรคมนาคมและขนส่ง

บริษัท การบินไทย (มหาชน) จำกัด
บริษัท ทศท คอร์ปปอเรชั่น จำกัด (มหาชน)
บริษัท กสท คอร์ปปอเรชั่น จำกัด (มหาชน)
บริษัทวิทยุการบินแห่งประเทศไทย
การท่าอากาศยานแห่งประเทศไทย
การรถไฟแห่งประเทศไทย
กรมการบินพาณิชย์
การท่าเรือแห่งประเทศไทย
กระทรวงคมมนาคม
กรมอุตุนิยมวิทยา
เป็นต้น

4. กลุ่มความสงบสุขของสังคม
   กระทรวงศึกษาธิการ
   กระทรวงสาธาณสุข
   กรุงเทพมหานคร
   กระทรวงกลาโหม
   สำนักงานตำรวจแห่งชาติ
   กระทรวงเกษตรและสหกรณ์
   การประปานครหลวง
   การประปาส่วนภูมิภาค
   เป็นต้น

มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549

จัดทำโดย

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

สิงหาคม 2549

Old Version ISO/IEC 17799: 2000	New version ISO/IEC 17799: 2005
Security policy	Security policy
Security organization	Security organization
Asset classification & control	Asset classification & control
Personnel security	Personnel security
Physical & environmental security	Physical & environmental security
Communication & operation management	Communication & operation management
Access control	Access control
System Development & maintenance	System Development & maintenance
	Information security incident management

รูปที่ 1 แสดงจำนวนหัวข้อหลักด้านความมั่นคงปลอดภัย (Security Domain) สำหรับเวอร์ชันเดิมปี ค.ศ. 2000 (ทางซ้ายมือ) ทั้งหมด 10 หัวข้อ และสำหรับเวอร์ชั่นใหม่ปี ค.ศ. 2005 ทั้งหมด 11 หัวข้อ โดยหัวข้อที่เพิ่มขึ้นมาใหม่คือหัวข้อ Information Security Incident Management

รูปที่ 1 แสดงหัวข้อในมาตรฐานการรักษาความมั่นคงปลอดภัย ฉบับสากล เปรียบเทียบระหว่างเวอร์ชันเก่าและเวอร์ชันใหม่

A	B	C	D	I	J
	Gap Analysis of Information Security Management System complied with ISO 27001:2				
	Organization :				
	นัวข้อ	ชื่อนัวข้อ	รายละเอียด,คำถาม	เผนวิธีการดำเนินการแก้ไข	ผลการปฏิบัติงาน
	1. Information Security Policy				
	1.1 นโย	ายความมั่นคงปลอดภัยสำหรับสารสนเทศ	มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง		
	1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	มีการจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ	Corporate Policy: Policy > Communication (SAT, Poster, E-mail, Web, Routing slip)> Revise (Quarterly > Procedures, 1 Year > Policies)	No
	1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร	Policy Step Procedure	No
	2. Organizational of Information Security				
	2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)		มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร		
	2.1.1	การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้าง	Corporate Policy: Recruit or Define Security Staff, Bundle Security responsibility in Registration form.	No

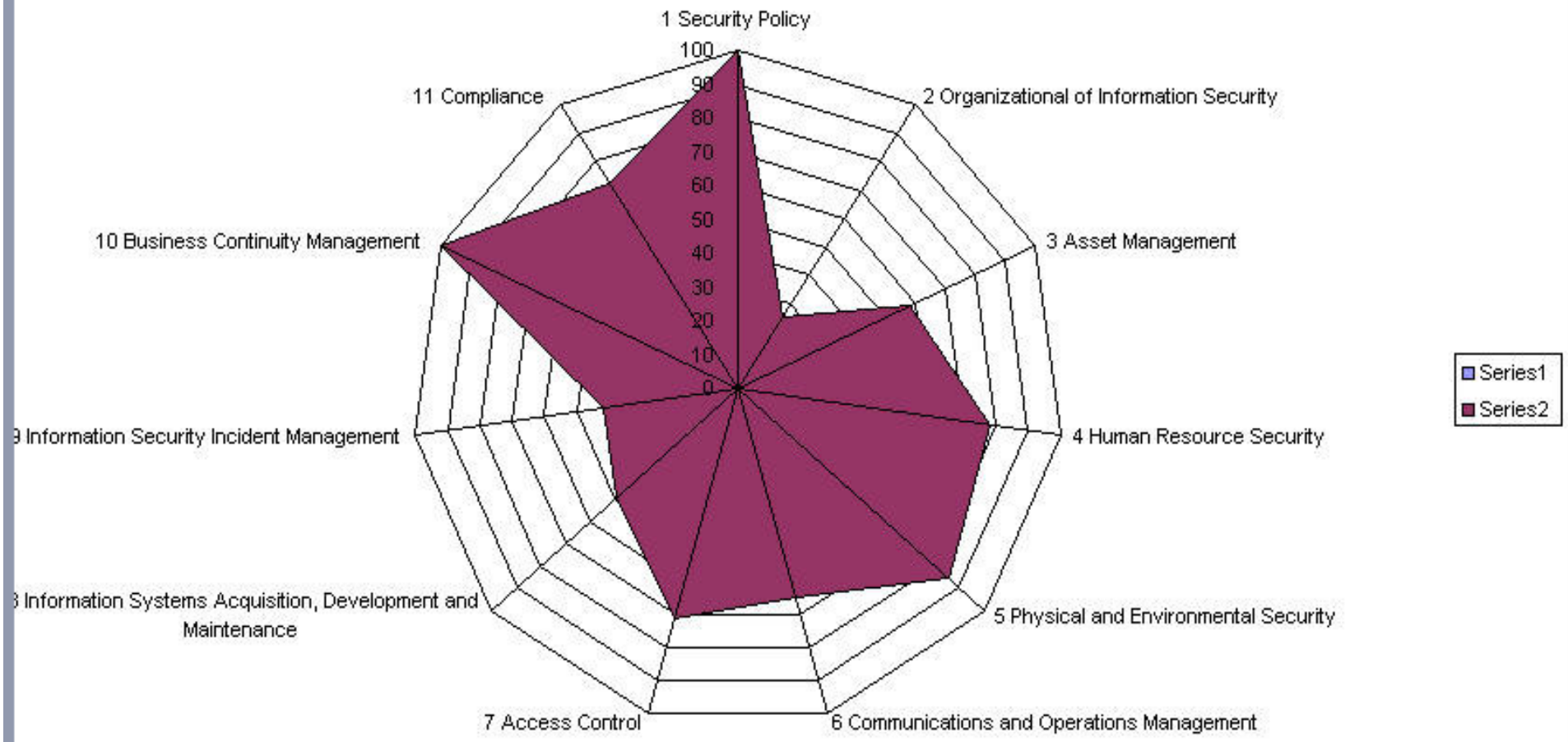
ACIS Professional Center Co., Ltd.

Checklist of Policy

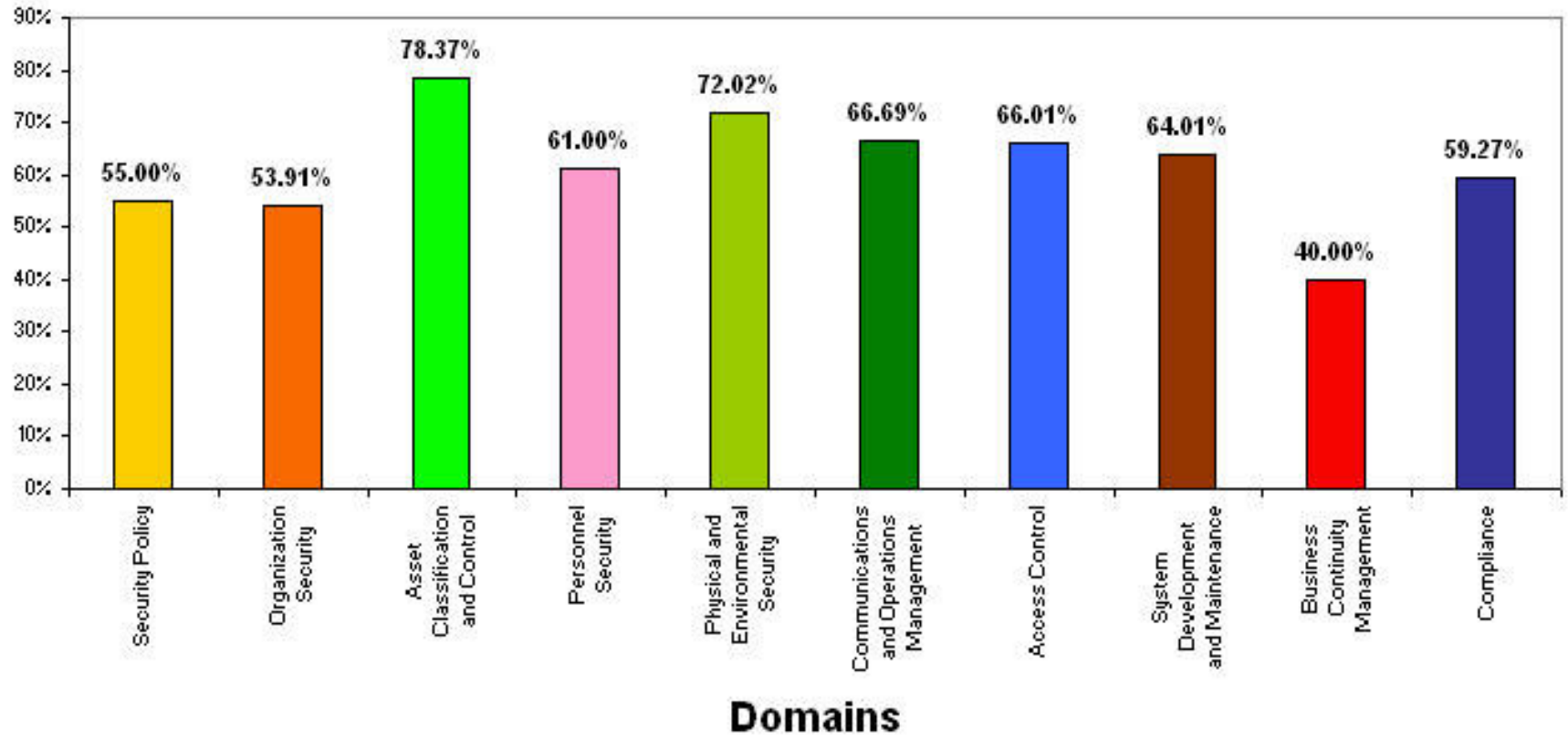
1	**Security Policy**				
	1.1	**Information Security Policy**		**Management direction and support for information security must be clearly established.**	
		1.1.1	Information Security Policy Document	Has an information security policy document been approved, published and started to use?	Yes
		1.1.2	Review of Informational Security Policy	Has an information security policy document been reviewed continuing which is developed by responder?	Yes
2	**Organizational of Information Security**				
	2.1	**Internal Organization**		**A management framework must be established to initiate and control the implementation of information security within the organization.**	
		2.1.1	Management commitment to information security	Has a response management been done clear direction, assignment and agreement for security measure?	Yes
		2.1.2	Information Security Coordination	Has a process been established to coordinate implementation of information security measures from diverse part with roles and responsibilities?	Yes
		2.1.3	Allocation of Information Security Responsibilities	Are responsibilities for accomplishment of information security requirements clearly defined?	Yes
		2.1.4	Authorization Process for Information Processing Facilities	Has a management approval process been defined for any new IT facility within the organization?	Yes
		2.1.5	Confidentiality agreements	Has confidentiality or Non-Disclosure Agreement (NDA) been clearly defined	Yes

Checklist of policy (Eng)

Summary


1 Security Policy
2 Organizational of Information Security
3 Asset Management
4 Human Resource Security
5 Physical and Environmental Security
6 Communications and Operations Management
7 Access Control
8 Information Systems Acquisition, Development and Maintenance
9 Information Security Incident Management
10 Business Continuity Management
11 Compliance
100
90
80
70
60
50
40
30
20
10
0
Series1
Series2

ISO/IEC17799 Survey Report
(from ACIS& TU MISM class) http://www.cie.th.edu/web2/



พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 25 : วิธีการแบบปลอดภัย (ISO/IEC 27001)

พระราชกฤษฎีกากำหนดวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 32 : ธุรกิจบริการเกี่ยวกับธุรกรรมทาง อิเล็กทรอนิกส์

พระราชกฤษฎีกาว่าด้วยการกำกับดูแลธุรกิจบริการให้บริการออกใบรับรองอิเล็กทรอนิกส์

มาตรา 35 : ธุรกรรมภาครัฐ

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (10 มกราคม 2550)

ความเคลื่อนไหวล่าสุดเกี่ยวกับร่างพรฎ. ภาครัฐ

เล่ม ๑๒๔ ตอนที่ ๔ ก ราชกิจจานุเบกษา ๑๐ มกราคม ๒๕๕๐

พระราชกฤษฎีกา

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

ความเคลื่อนไหวล่าสุดเกี่ยวกับร่างพรฎ. ภาครัฐ

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

อาศัยอำนาจตามความในมาตรา ๑๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๔๙ และมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙"

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มีระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ในลักษณะ ดังต่อไปนี้

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

มาตรา ๙ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

มาตรา ๑๐ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ

พลเอก สุรยุทธ์ จุลานนท์

นายกรัฐมนตรี

พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549

สาระสำคัญที่กำหนดไว้ในพระราชกฤษฎีกา (มาตรา 35)

มาตรา 3 การทำระบบเอกสารในรูปข้อมูลอิเล็กทรอนิกส์

มาตรา 4 กระบวนการพิจาณาทางปกครอง

- **กำหนดให้มีวิธีการแก้ไขปัญหาในกรณี มีเอกสารบกพร่องหรือผิดหลงโดย** (1) แจ้งประชาชนทราบว่า มีเอกสารบกพร่องหรือผิดหลง จากความไม่รู้หรือประมาทเลินเล่อ รวมทั้ง แจ้งข้อเท็จจริงเพิ่มเติม หรือวิธีการแจ้งสิทธิและหน้าที่ในกระบวนพิจารณา (2) กรณีมีความจำเป็น อาจทำข้อตกลงกับประชาชน ในการดำเนินการพิจารณาทางปกครองกับหน่วยงานภาครัฐโดยวิธีการทางอิเล็กทรอนิกส์

มาตรา 5 การรักษาความมั่นคงปลอดภัย

- **แนวนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย** (1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ 2 การสำรองข้อมูล & สภาพพร้อมใช้งาน & ทำแผนฉุกเฉิน 3 การตรวจสอบ & ประเมินความเสี่ยงอย่างสม่ำเสมอ)

มาตรา 6 การคุ้มครองข้อมูลส่วนบุคคล

- **แนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล** (หลักการ OECD 8 ข้อ)

ความเคลื่อนไหวล่าสุดเกี่ยวกับร่างพรฎ. มาตรา 25

คำอธิบาย

(ร่าง) พระราชกฤษฎีกากำหนดวิธีการแบบ (มั่นคง) ปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....

1. ความเป็นมา

สืบเนื่องจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 หมวด 1 มาตรา 25 ได้กำหนดไว้ว่า ธุรกรรมทางอิเล็กทรอนิกส์ที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ และด้วยจำเป็นที่ต้องมีการกำหนดเกี่ยวกับวิธีการแบบปลอดภัยเพื่อเป็นการสร้างมาตรฐานเบื้องต้นและเป็นบรรทัดฐานในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อันจะเป็นการสร้างความตื่นตัวให้หน่วยงานต่างๆ ตระหนักถึงความสำคัญของความมั่นคง ปลอดภัย ในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

ความเคลื่อนไหวล่าสุดเกี่ยวกับร่างพรฎ. มาตรา 25

3.3 มาตรา 8 สาระสำคัญของนโยบายด้านความมั่นคงปลอดภัย

การกำหนดนโยบายด้านความมั่นคงปลอดภัยไว้เพียงหลักการโดยกว้างนั้น เพื่อให้เกิดความยืดหยุ่นและเปิดโอกาสให้สามารถมีการประยุกต์ใช้ของมาตรฐานตามความเหมาะสมของแต่ละองค์กร ดังนั้นจึงเห็นควรให้การกำหนดรายละเอียดเกี่ยวกับมาตรฐานและเทคโนโลยีออกมาในรูปของแนวทางปฏิบัติ ในรูปประกาศจะเป็นแนวทางที่เหมาะสมที่สุด

(1) การจัดทำนโยบายหรือมาตรฐานด้านความมั่นคงปลอดภัย (Security policy)

(2)การจัดโครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร ทั้งในส่วนที่เป็นการบริการจัดการด้านความมั่นคงปลอดภัยภายในองค์กร และภายนอกองค์กร (Organisation of Information Security)

(3)การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

(4) การสร้างความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

(5)การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical security)

(6)การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบสารสนเทศและระบบคอมพิวเตอร์ขององค์กร (Information system security)

(7)การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management)

(8)การควบคุมการเข้าถึง (Access Control)

(9)การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(10)การบริหารจัดการเหตุการณ์ที่มีความเสี่ยงหรือก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)

ความเคลื่อนไหวล่าสุดเกี่ยวกับร่างพรฎ. มาตรา 25

(11) การบริหารจัดการให้มีความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

(12) การปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย (Compliance)

(13) การกำหนดเกี่ยวกับมาตรฐานของเทคโนโลยีที่เหมาะสม

3.4 มาตรา 9 การจัดทำแนวปฏิบัติ

ในการจัดทำแนวปฏิบัติเกี่ยวกับวิธีการแบบปลอดภัยที่กำหนดไว้ตามความในมาตรา 8 ได้มีการกำหนดให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายจัดทำแนวปฏิบัติเกี่ยวกับวิธีการแบบปลอดภัย โดยนำแนวทางหลักการของนโยบายด้านความมั่นคงปลอดภัย ตามร่างมาตรฐาน ISO 27001 มาปรับใช้เป็นแนวทางในการปฏิบัติ

3.5 มาตรา 10 การจัดระดับความเสี่ยงและจัดระดับของ Critical Infrastructure

ในการปรับใช้เรื่องมาตรฐานความมั่นคงปลอดภัย ได้มีการกำหนดแบ่งระดับความสำคัญในการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยเป็น 3 ระดับ กล่าวคือ ระดับสูง ระดับกลาง และระดับทั่วไป ด้วยหลักเกณฑ์พิจารณา 4 ด้าน ได้แก่

1. ด้านบุคลากรที่จะได้รับผลกระทบ
2. ด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน
3. ด้านมูลค่าความเสียหายโดยตรงของผู้ใช้บริการ
4. ด้านผลกระทบทางด้านความมั่นคงและความสงบเรียบร้อยของประเทศ

ความเคลื่อนไหวล่าสุดเกี่ยวกับร่างพรฎ. มาตรา 25

เพื่อเป็นการจัดลำดับ Rating หน่วยงานที่จัดว่าเป็นโครงสร้างพื้นฐานสาธารณะที่สำคัญของประเทศ (Critical Infrastructure) อาทิเช่น การไฟฟ้านครหลวง การประปานครหลวง ธนาคารแห่งประเทศไทยบริษัท ปตท. จำกัด (มหาชน) เป็นต้น ที่ต้องจัดให้มีการทำธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยโดยเคร่งครัดอย่างสมบูรณ์ทุกข้อ