

Information Security Management System for e-Government

June 30, 2010

Nuntana Podjananuntakul
CISSP, ITP

Agenda

- ❑ Information Security Management System
- ❑ National Critical Infrastructure: National Root CA

กฎหมายที่มีการบังคับใช้

[ใช้บังคับ 15 มี.ค. 49]

✔ มาตรา 3: พรฎ. กำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์
ที่ยกเว้นมิให้เข้ากฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาบังคับใช้ พ.ศ. 2549

[อยู่ระหว่าง Focus Group]

มาตรา 12/1: (ร่าง) หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความ
ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ (e-Document) [อยู่ระหว่างเสนอ ครม.]

✔ พรบ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 25: (ร่าง) พรฎ. กำหนดวิธีการแบบ(มั่นคง)ปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

[ใช้บังคับ 3 เม.ย. 45] +
ฉบับที่ 2 [ใช้บังคับ 14 ก.พ. 51]

[ใช้บังคับ 14 ม.ค. 52]

✔ มาตรา 32: การกำกับธุรกิจบริการ
เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

✔ พรฎ. ควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551
(ร่าง) พรฎ. ควบคุมดูแลธุรกิจบริการการให้บริการออกใบรับรองอิเล็กทรอนิกส์

✔ มาตรา 35: พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

[ใช้บังคับ 10 ม.ค. 50]

[อยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา]

✔ พรบ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

[ใช้บังคับ 18 ก.ค. 50]

พ.ร.บ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรม ทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

[ใช้บังคับ 10 ม.ค. 50]

✓ มาตรา 35: พ.ร.บ. กำหนดหลักเกณฑ์และวิธีการ
ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

มาตรา 1 ชื่อกฎหมาย

มาตรา 2 วันที่ใช้บังคับ

มาตรา 3 การทำระบบเอกสารในรูปข้อมูลอิเล็กทรอนิกส์

มาตรา 4 กระบวนการพิจารณาทางปกครอง

มาตรา 5 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

มาตรา 6 การคุ้มครองข้อมูลส่วนบุคคล

มาตรา 7 แนวทางการจัดทำนโยบาย & แนวทางปฏิบัติ

มาตรา 8 การจัดทำตัวอย่างของแนวนโยบาย & แนวปฏิบัติ

มาตรา 9 ผลบังคับใช้กับกฎหมายอื่น

มาตรา 10 ผู้รักษาการตามกฎหมาย

> e-Document System, Access Control, BCP & DRP, IT Risk Assessment, IT Audit, Privacy Policy

พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[ใช้บังคับ 18 ก.ค. 50]

✓ พรบ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

เจตนารมณ์

- เพื่อกำหนดฐานความผิดและบทลงโทษ
- เพื่อกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่
- เพื่อกำหนดหน้าที่ของผู้ให้บริการ

(ร่าง) ที่เกี่ยวข้อง

1. (ร่าง) กฎกระทรวงว่าด้วยการยึดหรืออายัดระบบคอมพิวเตอร์
2. (ร่าง) บันทึกข้อตกลงระหว่างกระทรวง ICT, กลาโหม, ยุติธรรม, สำนักข่าวกรองแห่งชาติ, สำนักงานตำรวจแห่งชาติ และ NECTEC เรื่อง การประสานงานความร่วมมือกัน
3. (ร่าง) ระเบียบว่าด้วยการประสานงานเพื่อการดำเนินการ
4. ประกาศ หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
5. ประกาศ หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่
6. ประกาศ กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่
7. ประกาศ แต่งตั้งพนักงานเจ้าหน้าที่ ตาม พรบ. 1st issue: 15, 2nd issue: 20

[ประกาศ 23 ส.ค. 50]

[ประกาศ 24 ส.ค. 50]

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ ๒๕๔๔ (มาตรา 25)

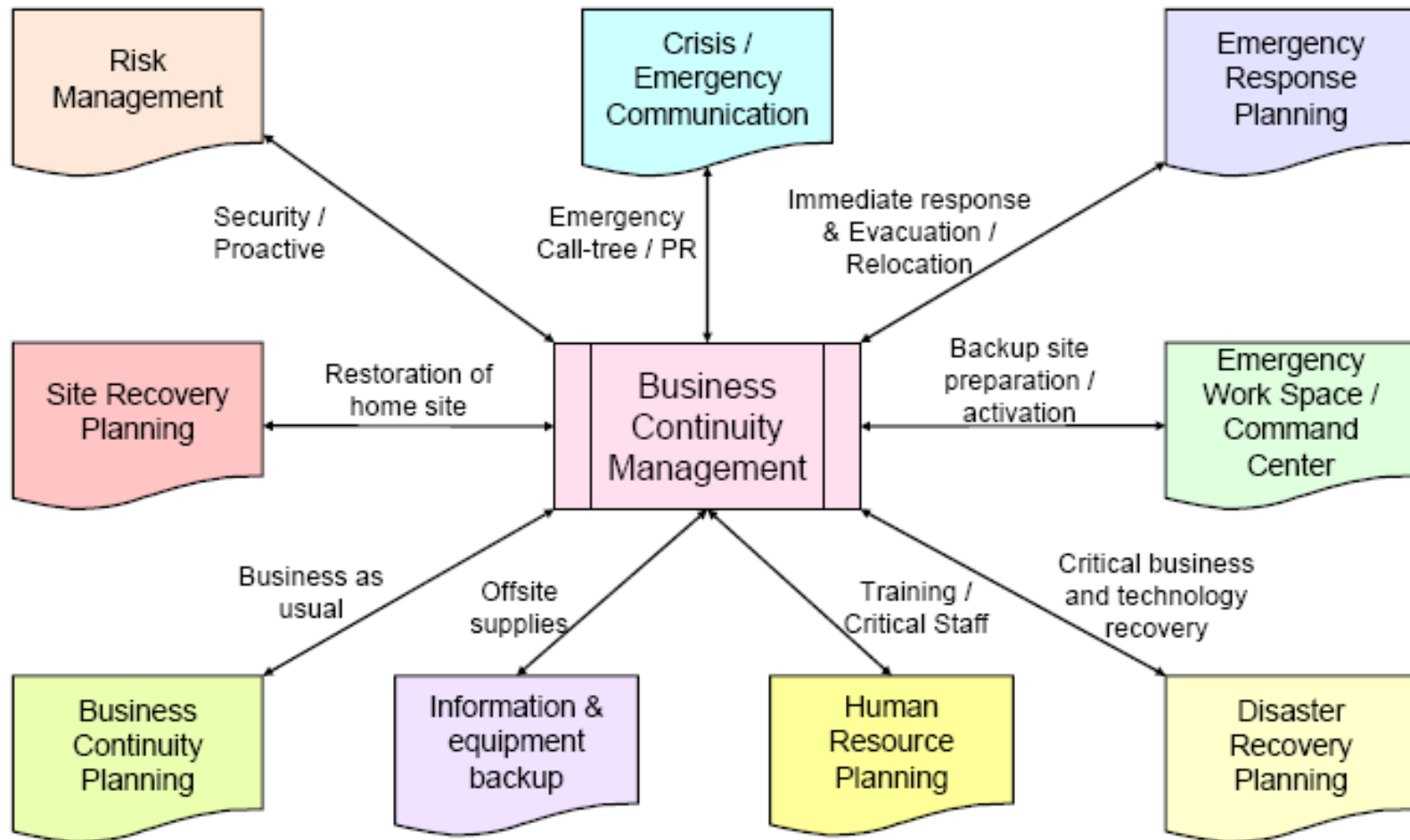
(ร่าง) พรฎ. กำหนดวิธีการแบบ (มั่นคง) ปลอดภัย
ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

- 1) SECURITY POLICY
- 2) ORGANIZATION OF INFORMATION SECURITY
- 3) ASSET MANAGEMENT
- 4) HUMAN RESOURCES 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

อ้างอิงมาตรฐาน ISO/IEC 17799: Code of practice for Information Security Management

ISO/IEC 17799:2005 was renumbered ISO/IEC 27002:2005 in the middle of 2007 to bring it into the ISO/IEC 27000 family of standards

Business Continuity Management



ISO 27000 Series

ISO/IEC 27000

Introduction to the ISO27k standards as a whole
Plus the specialist vocabulary used in ISO27k

ISO/IEC 27001:2005

Information Security Management System requirements standard (specification)

ISO/IEC 27002:2005

Code of practice for information security management (ร่าง) มาตรา 25

Describe a comprehensive set of information security control objectives and a set of generally accepted good practice security controls

ISO/IEC 27003

Implementation guidance for ISO/IEC 27001

ตัวชี้วัด กพร.

ISO/IEC 27004

Information security management measurement standard
To help improve the effectiveness of your ISMS

ISO/IEC 27005:2008

Information security risk management standard (released in June 2008)

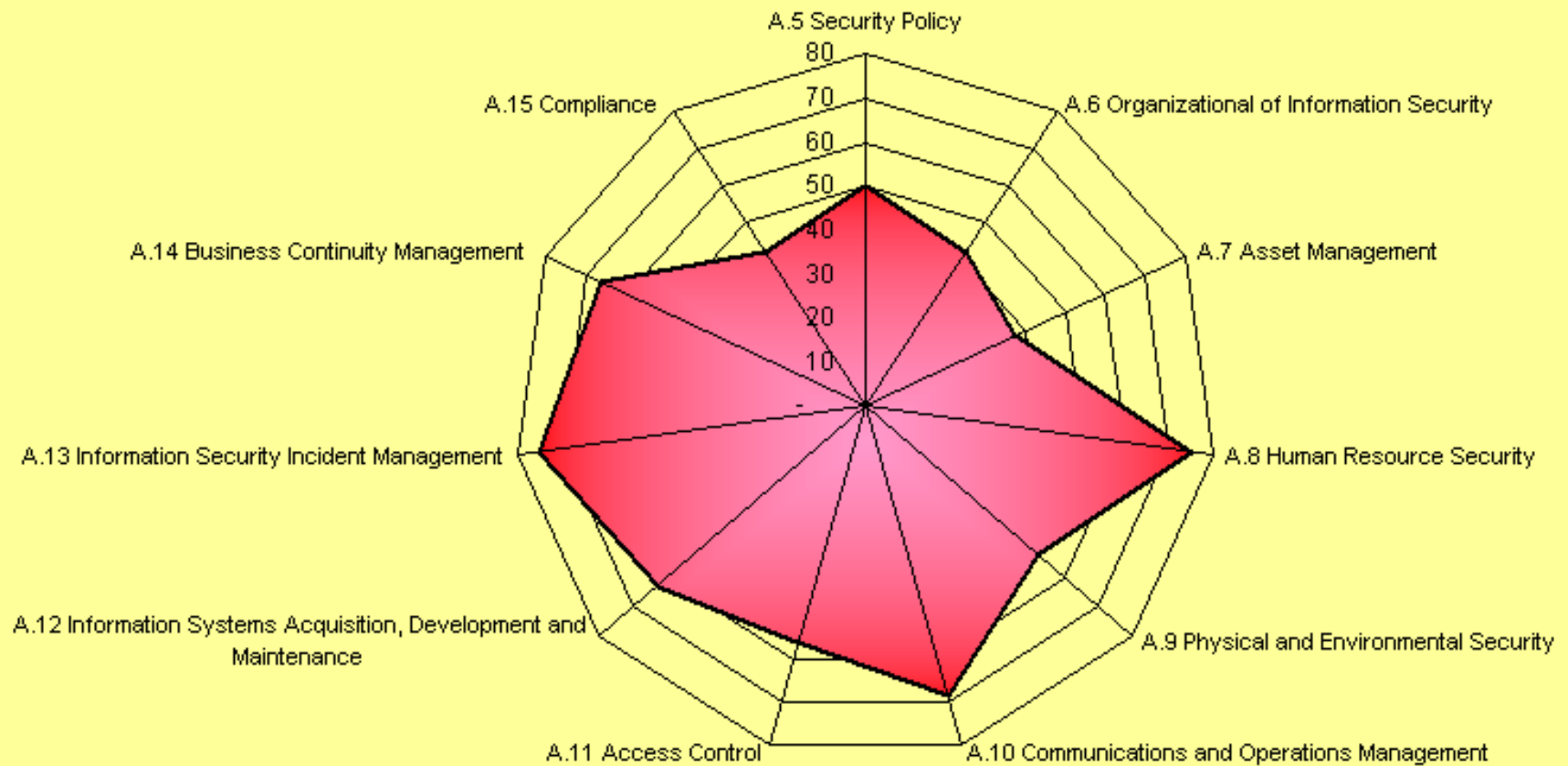
ISO/IEC 27006:2007

Guide to the certification or registration process for accredited ISMS certification

ISO/IEC 27007

Guideline for auditing Information Security Management Systems.

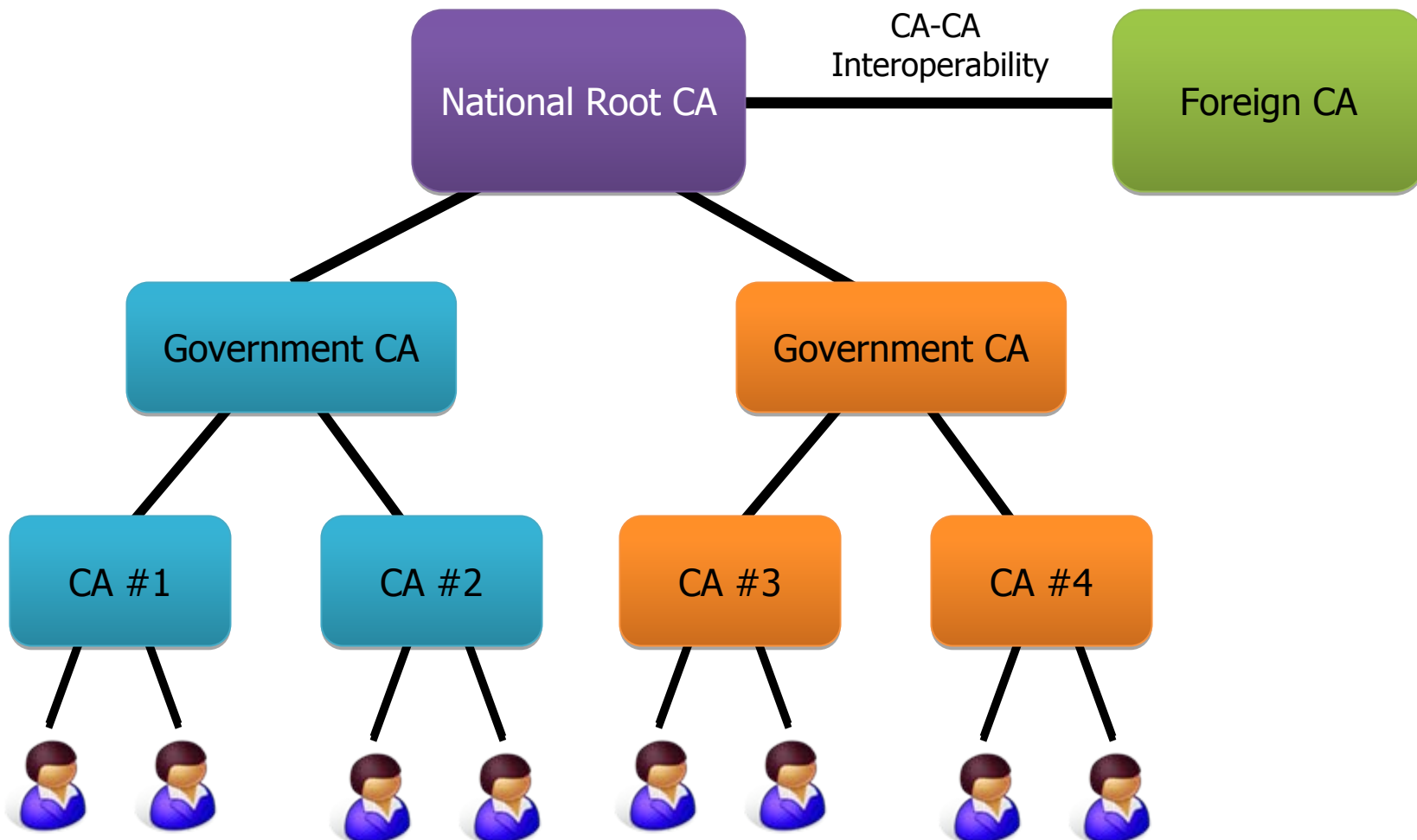
Gap Analysis



Agenda

- ❑ Information Security Management System
- ❑ National Critical Infrastructure: National Root CA

National Root CA (NRCA)



โครงการ CA to CA ภายใต้กรอบ ASEAN



Information Security Management System

PKI Service: (ร่าง) มาตรา 32 การควบคุมดูแลธุรกิจบริการการให้บริการออกใบรับรองอิเล็กทรอนิกส์

National Root CA

PKI Consulting

PKI Training

Information Security Management: (ร่าง) มาตรา 25 พรฎ. กำหนดวิธีการแบบ (มั่นคง)ปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

Gap Analysis

IT Risk Management

Vulnerability Assessment

Hardening

IT Audit

Network and Security Operation Center (NSOC): พรบ. ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์

Log Management: พรบ. ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์

G-Log

Thank you