Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

สัมมนาเชิงปฏิบัติการเพิ่มประสิทธิภาพการปฏิบัติงานของผู้ตรวจสอบภายใน หลักสูตร แนวทางการตรวจสอบระบบงานสารสนเทศ

รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
ภาควิชาการสื่อสารข้อมูลและเครือข่าย คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ (มจพ.)
pongpisit.w@it.kmutnb.ac.th

สำนักตรวจสอบภายใน
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์
6 ธันวาคม 2560

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Outline

- Audit Process
- Type of Audit
- Information Security
- Exploring Control Types and Methods
- ตัวอย่างสิ่งที่ต้องพิจารณาในการตรวจสอบ

Audit Process

มอก.19011-2556

ISO 19011 : 2011

มาตรฐานผลิตภัณฑ์อุตสาหกรรม

แนวทางการตรวจประเมินระบบการจัดการ

0. บทนำ

นับจากการตีพิมพ์มาตรฐาน ISO 19011 ครั้งแรกเมื่อปี พ.ศ. 2545 ได้มีการตีพิมพ์มาตรฐานระบบการจัดการเพิ่มเติมอีกจำนวนมาก เป็นผลให้มีความจำเป็นต้องพิจารณาขอบข่ายการตรวจประเมินระบบการจัดการให้กว้างขวางยิ่งขึ้น รวมทั้งจัดให้มีข้อแนะนำที่สามารถใช้ได้เป็นการทั่วไปมากยิ่งขึ้น

http://164.115.23.89/login/filedata/TIS19011-2556.PDF

EUROPEAN STANDARD **EN ISO 19011**

NORME EUROPÉENNE

EUROPÄISCHE NORM

October 2011

ICS 03.120.10; 13.020.10 Supersedes EN ISO 19011:2002

English Version

Guidelines for auditing management systems (ISO 19011:2011)

Lignes directrices pour l'audit des systèmes de management (ISO 19011:2011)

Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2011)

http://qic-eg.com/wp-content/uploads/2015/08/BS-EN-ISO-19011-2011.pdf

ISO 19011:2011

- มาตรฐาน ISO 19011 ไม่ได้ระบุถึงข้อกำหนดที่จะสามารถขอการรับรองได้
- แต่เป็นแนวปฏิบัติสำหรับ
  - การบริหารจัดการโปรแกรมการตรวจประเมิน และ
  - การดำเนินการตรวจประเมินระบบบริหารจัดการต่าง ๆ
  - รวมไปถึงแนวทางในการพัฒนาความสามารถ และ
  - การประเมินผลผู้ตรวจประเมินและทีมตรวจประเมิน
- แนวปฏิบัตินี้ สามารถนำไปใช้ได้กับ
  - ผู้ใช้งานต่าง ๆ ทั้งในฐานะของผู้ตรวจประเมิน หรือองค์กรที่มีการจัดทำระบบบริหารจัดการ
  - รวมถึงองค์กรที่ต้องการตรวจประเมินระบบบริหารจัดการตามข้อตกลงหรือตามช่วงเวลาที่กำหนด
  - ใช้ในการแสดงถึงความสอดคล้องตามหลักเกณฑ์ที่กำหนด และ
  - นำไปใช้ในการฝึกอบรม หรือรับรองผู้ตรวจประเมินขององค์กร

ISO 19011:2011

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- อธิบายถึงแนวคิดเกี่ยวกับ
  - ความเสี่ยงของการตรวจประเมินระบบบริหารจัดการ
  - แนวทางที่นำมาใช้ อาจทำให้เกิดความเสี่ยงที่จะไม่บรรลุวัตถุประสงค์ของกระบวนการตรวจประเมิน
  - และโอกาสที่การตรวจประเมินจะส่งผลกระทบต่อกิจกรรมและกระบวนการของผู้ถูกตรวจประเมิน

Audit

- การตรวจประเมิน (Audit) หมายถึง กระบวนการอย่างเป็นระบบ มีความเป็นอิสระ และมีการจัดทำเป็นเอกสาร เพื่อให้ได้หลักฐานของการตรวจประเมิน (Audit evidence) และการประเมินอย่างเป็นกลาง เพื่อพิจารณาถึงความสอดคล้องตามเกณฑ์การตรวจประเมิน (Audit criteria) เช่น นโยบาย ขั้นตอนการปฏิบัติงาน หรือข้อกำหนดของระบบบริหารจัดการ

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

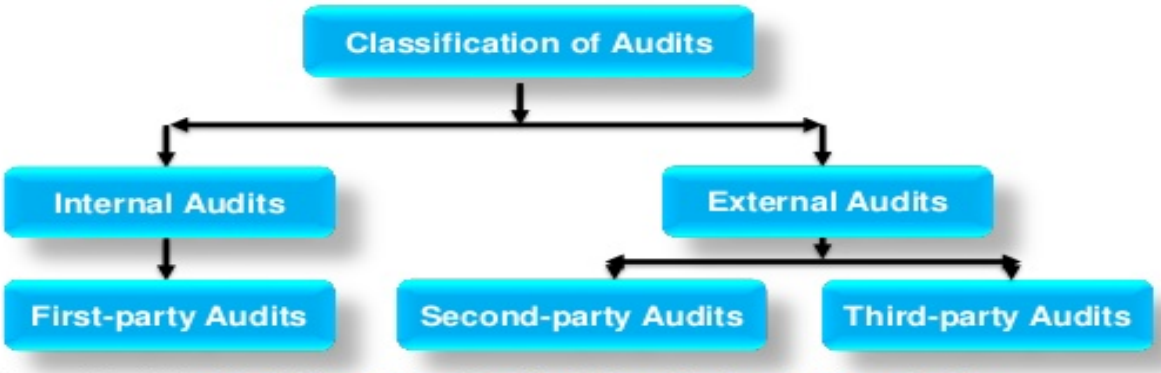
3.1
audit
systematic, independent and documented process for obtaining **audit evidence** (3.3) and evaluating it objectively to determine the extent to which the **audit criteria** (3.2) are fulfilled

http://qic-eg.com/wp-content/uploads/2015/08/BS-EN-ISO-19011-2011.pdf

Analysing results and preparing a report

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- **Classification of Audits**
  - **First-party Audit** (Internal audit)
  - **Second-party Audit** (conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf)
  - **Third-party Audit** (conducted by independent auditing organizations, such as regulators or those providing certification)



For More Details: Certified Quality Auditor Body of Knowledge

ASQ

Continues...

http://mysdvvf.com/watch?key=966c8ff6acad370aa8c9c4864a836a2b

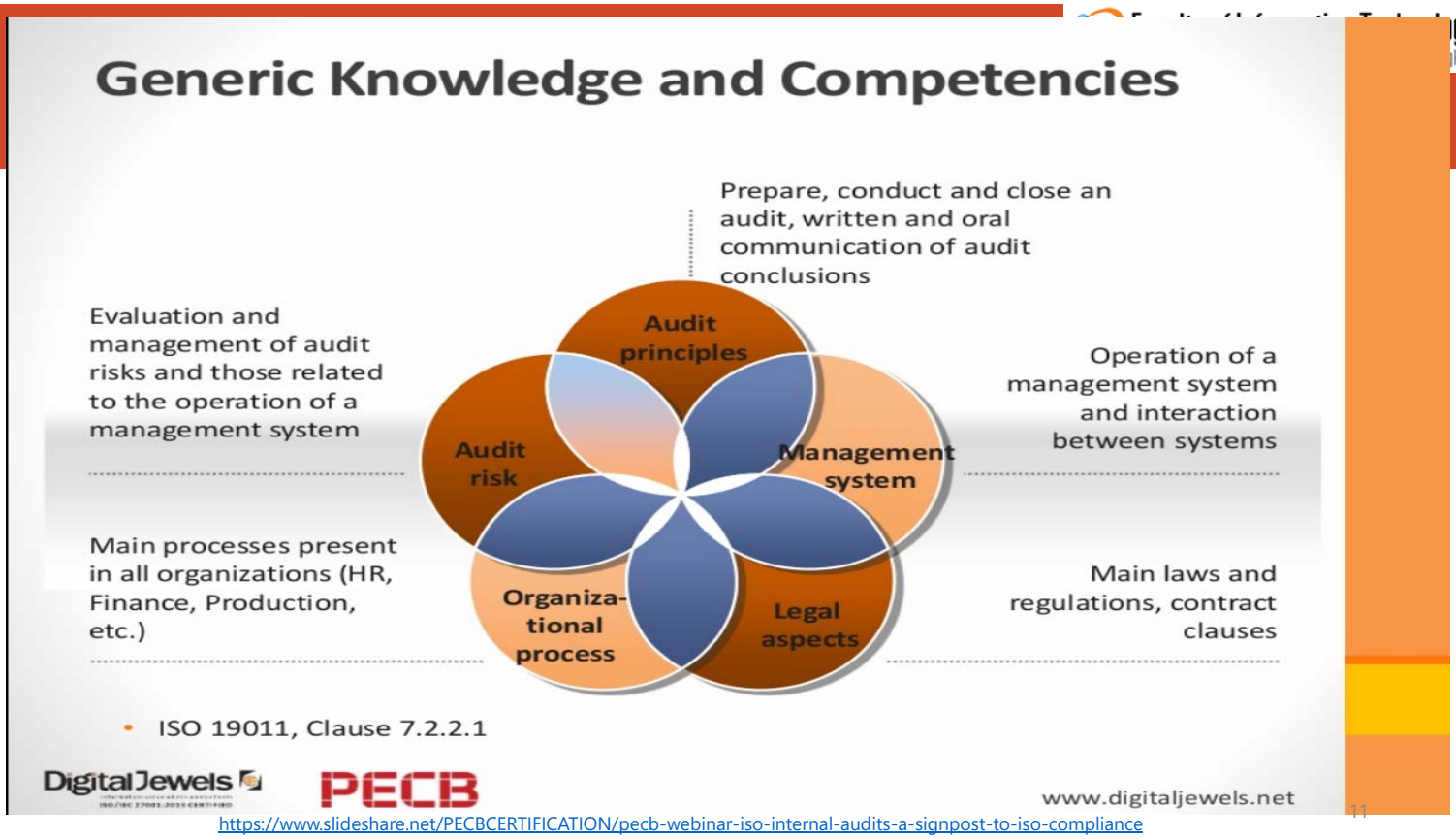
Personal Behaviours

- ISO 19011, Clause 7.2.1

DigitalJewels PECB

www.digitaljewels.net

https://www.slideshare.net/PECBCERTIFICATION/pecb-webinar-iso-internal-audits-a-signpost-to-iso-compliance



https://www.slideshare.net/PECBCERTIFICATION/pecb-webinar-iso-internal-audits-a-signpost-to-iso-compliance

Type of Audit

บทนำ

- ปัญหาส่วนใหญ่ที่เกิดขึ้นกับองค์กร ได้แก่ ปัญหาด้านการทุจริต ทางด้านการเงิน (Financial Fraud) ที่มีอัตราการเกิดอย่างต่อเนื่อง
- ปัญหาจากการบริหารองค์กรที่ไม่โปร่งใส มีต้นตอมาจากการบริหารงานที่ไม่ตรงไปตรงมาของผู้บริหารระดับสูง (Board of Director) ซึ่งสามารถหลอกลวงผ่านการตรวจสอบทั้งผู้ตรวจสอบภายใน และผู้ตรวจสอบภายนอก
- ความสำคัญของการตรวจสอบภายใน (Internal Audit) ผู้ตรวจสอบภายใน (Internal Auditor) ผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) และฝ่ายตรวจสอบภายใน (Internal Audit Department) ในองค์กรจึงกลายเป็นประเด็นสำคัญที่ผู้บริหารระดับสูงขององค์กรต้องให้ความสำคัญอย่างยิ่งยวด

Type of Audit

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- Internal Audit
- IT Audit
- Information Security Audit

Internal Audit

- หมายถึง การตรวจสอบภายใน โดยฝ่ายตรวจสอบภายในของบริษัทเอง
- "ผู้ตรวจสอบภายใน" ควรศึกษาองค์ความรู้ที่จำเป็นต้องใช้ในการปฏิบัติงานตรวจสอบภายใน
  - "Corporate Governance Framework",
  - "COSO ERM Framework" ,
  - "Risk-Based Audit"
- ผู้ตรวจสอบภายในควรสอบวัดความรู้เป็นผู้ตรวจสอบภายในที่ได้รับการรับรองแบบสากล
  - "CIA" หรือ "Certified Internal Auditor" ซึ่งได้รับการรับรองโดย The Institute of Internal Auditors หรือ IIA (สถาบันผู้ตรวจสอบภายในสากล)

Internal Audit: การสอบ "CIA"

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

วัดความรู้ทั้ง 4 ด้าน ได้แก่

1. The Internal Audit Activity's Role in Governance, Risk, and Control
2. Conducting the Internal Audit Engagement
3. Business Analysis and Information Technology (IT)
4. Business Management Skills

Internal Audit: การสอบ “CIA” (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ผู้ตรวจสอบภายในที่สอบผ่าน CIA สามารถแสดงให้เห็นถึงความแม่นยำในหลักการและองค์ความรู้ที่จะนำมาประยุกต์ใช้ในการตรวจสอบภายใน
- องค์ความรู้เฉพาะทางด้าน “Information Technology (IT)” หรือ “Information Security” นั้น ผู้สอบผ่าน CIA ยังมีความจำเป็นต้องศึกษาความรู้เพิ่มเติมเพื่อพัฒนาตัวเองเป็น “ผู้ตรวจสอบสารสนเทศ” (IT Auditor), “ผู้ตรวจสอบด้านความมั่นคงข้อมูล” (Information Security Auditor) หรือ ผู้เชี่ยวชาญด้านความมั่นคงข้อมูล (Information Security Specialist/Professional)

Internal Audit (ต่อ)

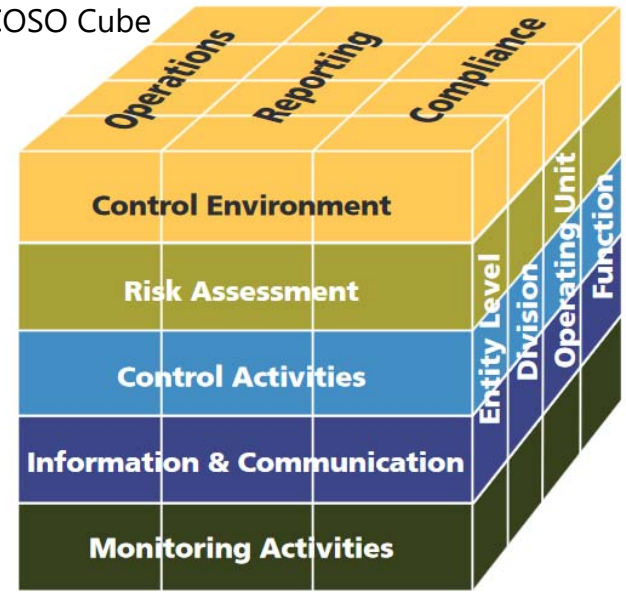
Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ผู้ตรวจสอบภายใน (Internal Auditor) จำเป็นต้องเป็น “IT Auditor” หรือ “Information Security Auditor” หรือไม่?
  - ในปัจจุบัน ทุกองค์กรมีความจำเป็นต้องนำระบบสารสนเทศมาใช้งานในแทบทุกส่วนขององค์กร
  - ดังนั้น องค์ความรู้ทางด้านการตรวจสอบระบบสารสนเทศจึงเป็นสิ่งสำคัญที่ผู้ตรวจสอบภายในจำเป็นต้องศึกษาหาความรู้เพิ่มเติม
- ถ้าหากงานที่ทำอยู่นั้นไม่มีความจำเป็นต้องใช้ความรู้ทางด้านระบบสารสนเทศหรือ ความรู้ทางด้านความมั่นคงข้อมูล เช่น การตรวจสอบเรื่อง Finance เป็นต้น
  - ผู้ตรวจสอบภายในสามารถจำกัดบทบาทของตนเป็นเพียง “ผู้ตรวจสอบภายใน” ไม่จำเป็นต้องเป็น “ผู้ตรวจสอบสารสนเทศ” หรือ “ผู้ตรวจสอบด้านความมั่นคงข้อมูล” ก็ได้

IT Audit

- ปรัชญาของ "IT Audit" แตกต่างจากปรัชญาของ "Internal Audit"
- องค์ความรู้ของ "Internal Audit" เน้นเรื่องการประยุกต์ใช้ "COSO Framework" และการมองภาพรวมในลักษณะของ "Enterprise Risk Management" หรือ "ERM" ซึ่งเป็นภาพใหญ่ขององค์กร

COSO Cube



http://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf

IT Audit (ต่อ)

- **17 internal control principles by internal control component**

CONTROL ENVIRONMENT
1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority, and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

RISK ASSESSMENT
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

CONTROL ACTIVITIES
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

INFORMATION & COMMUNICATION
13. Uses relevant information
14. Communicates internally
15. Communicates externally

MONITORING
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

http://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf

IT Audit (ต่อ)

- แต่ "IT Audit" เน้นไปที่ "CobiT Framework" หรือ อีกชื่อหนึ่งคือ "IT Governance Framework"
- โดยปรัชญา คือ การใช้งานระบบสารสนเทศให้สอดคล้อง หรือ "Align" กับวัตถุประสงค์ทางด้านธุรกิจ หรือ "Business Objective" ตลอดจน "Governance Objective"
  - "Regulatory Compliance" ต่าง ๆ

IT Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

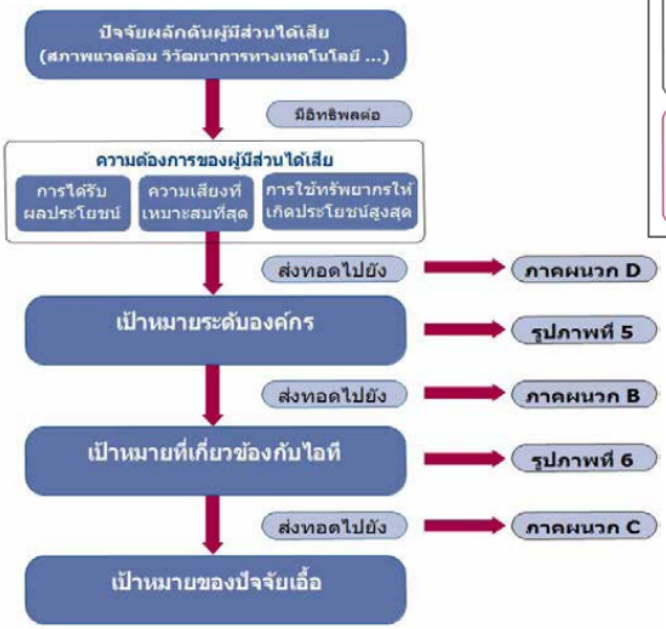
รูปภาพที่ 2—หลักการของ COBIT 5

รูปภาพที่ 12—ปัจจัยเอื้อขององค์กรใน COBIT 5

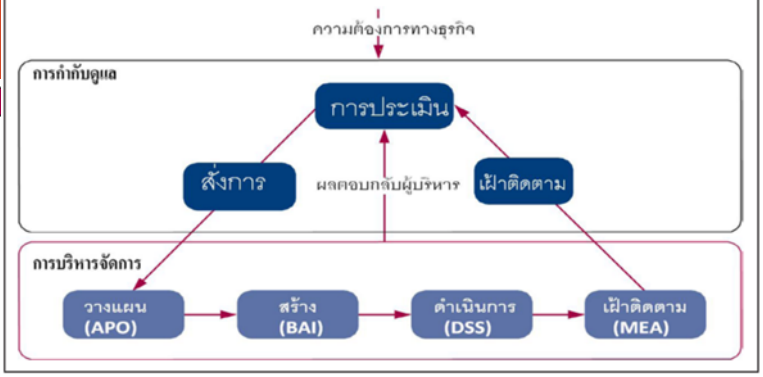
http://www.isaca.org/COBIT/

IT Audit (ต่อ)

รูปภาพที่ 4—ภาพรวมของการส่งทอดเป้าหมายใน COBIT 5

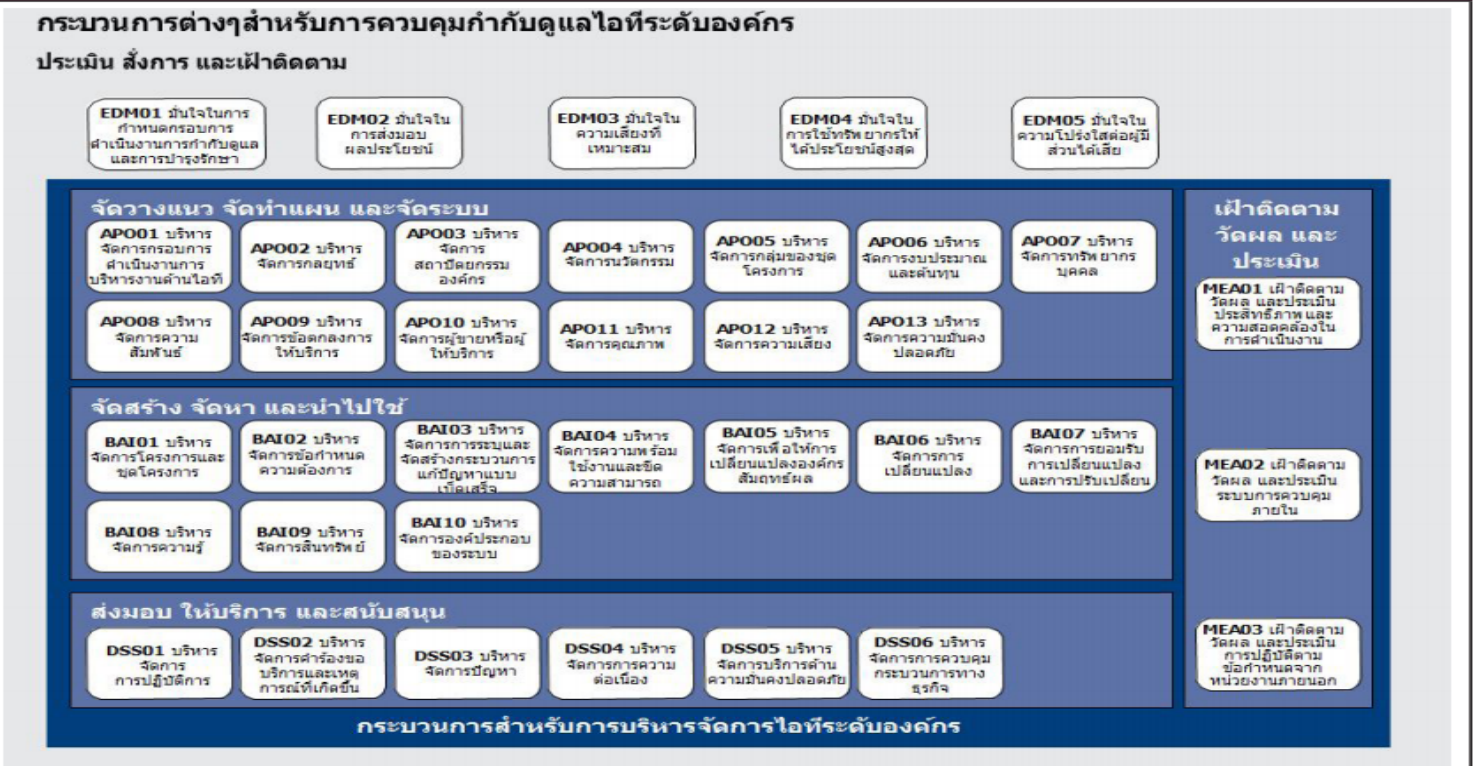


รูปภาพที่ 15—จุดสำคัญในการกำกับดูแลและการบริหารจัดการของ COBIT 5



http://www.isaca.org/COBIT/

รูปภาพที่ 16—ต้นแบบอ้างอิงของกระบวนการใน COBIT 5



http://www.isaca.org/COBIT/

IT Audit (ต่อ)

- โดยการตรวจสอบระบบสารสนเทศมีลักษณะคล้ายกับการตรวจสอบภายใน คือ
  - การนำหลักการ "GRC" หรือ "Governance , Risk Management and Compliance" มาประยุกต์ใช้
  - และมีลักษณะการตรวจสอบในแบบ "Risk-Based Approach"
  - แต่การตรวจสอบระบบสารสนเทศจำเป็นต้องมีองค์ความรู้เรื่อง "Information System Audit Process or IS Audit Process" เป็นองค์ความรู้หลัก
  - โดยมี 5 องค์ความรู้ซึ่งเป็นองค์ความรู้ที่ใช้ในการทดสอบผู้ที่ต้องการได้รับใบรับรองผู้เชี่ยวชาญด้านการตรวจสอบระบบสารสนเทศ หรือ CISA (Certified Information System Auditor) จาก ISACA (the Information Systems Audit and Control Association)

IT Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

สัดส่วนของทั้ง 5 องค์ความรู้ที่จำเป็นต้องศึกษาสำหรับสอบ CISA ตั้งแต่มิถุนายน **2016** ได้แก่

- Domain 1—The Process of Auditing Information Systems (14%)
- Domain 2—Governance and Management of IT (14%)
- Domain 3—Information Systems Acquisition, Development and Implementation (19%)
- Domain 4—Information Systems Operations, Maintenance and Support (23%)
- Domain 5—Protection of Information Assets (30%)

http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx

IT Audit (ต่อ)

- ผู้ที่สอบผ่าน"CISA" เป็นการพิสูจน์ในระดับหนึ่งว่ามีความรู้ความเชี่ยวชาญที่สามารถเป็นผู้ตรวจสอบระบบสารสนเทศที่แม่นยำในหลักวิชาการ (เหมือนผู้สอบผ่าน CIA)
- แต่ยังต้องหาความรู้เฉพาะทางเพิ่มเติมอีก เช่น
  - การตรวจสอบระบบฐานข้อมูล RDBMS เช่น Audit Oracle , Audit MS SQL Server หรือ
  - การตรวจสอบ Network และ System ต่าง ๆ เช่น การตรวจสอบ Microsoft Windows , UNIX/Linux Operating System, การตรวจสอบ Wireless, การตรวจสอบ Router และ Switching เป็นต้น

IT Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การศึกษาองค์ความรู้พื้นฐานและการสอบผ่าน CIA หรือ CISA นั้นนับเป็น "จุดเริ่มต้นที่ดี" สำหรับการเป็น "ผู้ตรวจสอบภายใน" หรือ "ผู้ตรวจสอบระบบสารสนเทศ" ที่มีประสิทธิภาพสูง

- แต่ไม่ได้หมายความว่าผู้สอบผ่าน CIA และ CISA จะปฏิบัติงานด้านการตรวจสอบได้ครบทุกเรื่อง เพราะจำเป็นต้องมีความรู้เฉพาะทางในเรื่องต่าง ๆ ดังที่กล่าวมาแล้วในตอนต้น อีกทั้งยังต้องอาศัยประสบการณ์หรือชั่วโมงบินในการตรวจสอบอีกด้วย

Information Security Audit

- องค์ความรู้ทางด้าน Information Security ก็คงหนีไม่พ้น "CBK" หรือ "Common Body of Knowledge" จาก The International Information System Security Certification Consortium, or $(ISC)^2$ ซึ่งเป็นผู้จัดสอบผู้เชี่ยวชาญด้านความมั่นคงข้อมูล หรือ "CISSP" (Certified Information System Security Professional)
- องค์ความรู้ของ "CISSP" (Certified Information System Security Professional)
  - (ตั้งแต่เดือนเมษายน 2015) ปรับเปลี่ยนเป็นมีทั้งหมด 8 โดเมน

CISSP 8x Domain Summary *(after Apr2015)*

1. **Security and Risk Management**
   (Security, Risk, Compliance, Law, Regulations, Business Continuity)
2. **Asset Security** (Protecting Security of Assets)
3. **Security Engineering** (Engineering and Management of Security)
4. **Communications and Network Security**
   (Designing and Protecting Network Security)
5. **Identity and Access Management**
   (Controlling Access and Managing Identity)
6. **Security Assessment and Testing**
   (Designing, Performing, and Analyzing Security Testing)
7. **Security Operations**
   (Foundational Concepts, Investigations, Incident Management, DR)
8. **Software Development Security**
   (Understanding, Applying, and Enforcing Software Security)

Information Security Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

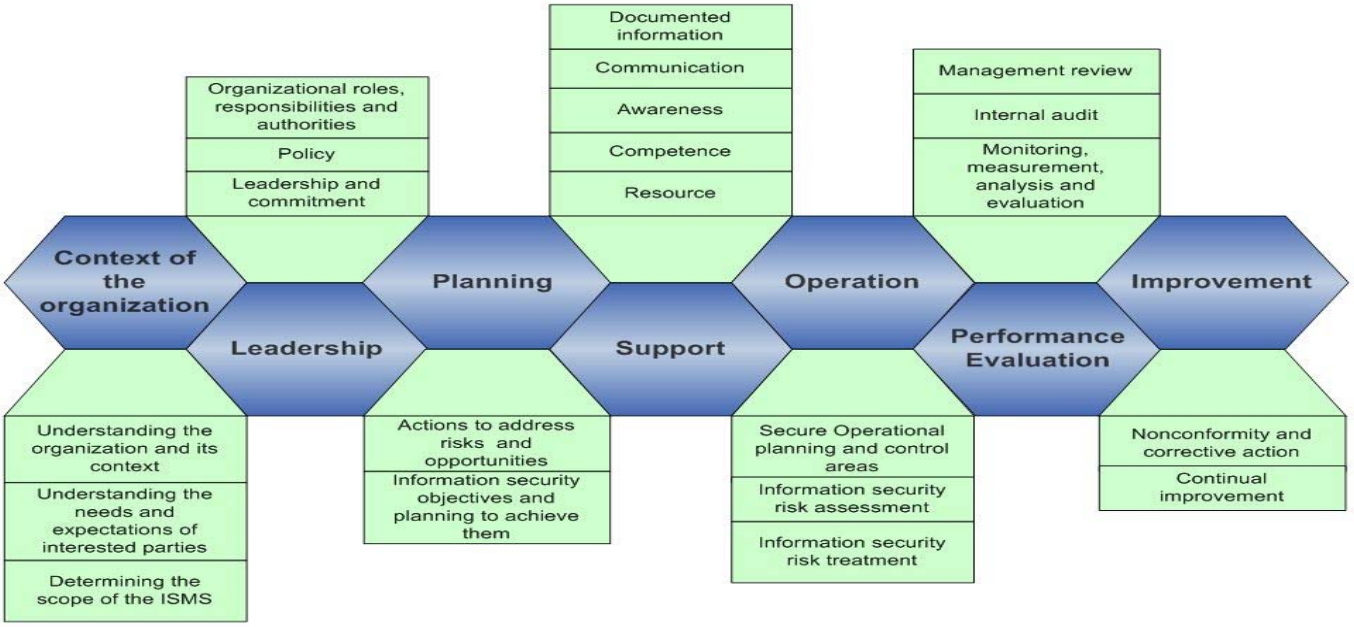
- โดยในปัจจุบัน **"IT Auditor"** จำเป็นต้องมีความรู้ด้านความมั่นคงข้อมูลเป็นความรู้เสริม
- ต้องไปตรวจเรื่อง Business Continuity Management (BCM),
- ตรวจเรื่องนโยบายด้านความมั่นคงขององค์กร (Corporate Information Security Policy),
- ตรวจเรื่องหนังสือยินยอมรับเงื่อนไขนโยบายเกี่ยวกับความมั่นคงระบบสารสนเทศ "Acceptable Use Policy" หรือ "AUP"
- ตลอดจนต้องตรวจสอบความมั่นคงของ "Network Perimeter" เช่น การตรวจสอบ Firewall , IPS/IDS , VPN หรือ Anti-Virus ซึ่งจำเป็นต้องมีความรู้ทางด้านความมั่นคงข้อมูลอย่างหลีกเลี่ยงไม่ได้

Information Security Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การตรวจสอบตามมาตรฐานการบริหารจัดการด้านความมั่นคงข้อมูลที่ได้รับการยอมรับกันในปัจจุบัน
- การตรวจสอบตามมาตรฐาน ISO/IEC 27001 Information Security Management System (ISMS)
- ISMS Lead Auditor ที่มาจาก Certification Body (CB) ผู้ตรวจสอบด้านความมั่นคงข้อมูลมีหน้าที่ในการพิสูจน์ทราบว่า องค์กรได้ปฏิบัติตาม "Control" ต่าง ๆ ที่อยู่ในมาตรฐาน ISO/IEC 27001:2013 ได้อย่างเกิดประสิทธิผล (Effectiveness) หรือไม่?

ISO 27001:2013 contents (aligned to ISO Directives)



http://laobingkaisuo.com/iso-27001-controls-spreadsheet/iso-27001-compliance-checklist-xls/

มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารส 27001:2013 (ต่อ)

มาตรการควบคุมมีทั้งหมด 14 ข้อ ได้แก่

- A5. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)
- A6. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)
- A7. ความมั่นคงปลอดภัยสำหรับบุคลากร (Human Resource Security)
- A8. การบริหารจัดการทรัพย์สิน (Asset Management)
- A9. การควบคุมการเข้าถึง (Access Control)
- A10. การเข้ารหัสข้อมูล (Cryptography)
- A11. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)
- A12. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

มาตรการควบคุม (Control) จัดการความมั่นคงปลอดภัยของสารส 27001:2013 (ต่อ)

- A13. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)
- A14. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)
- A15. ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)
- A16. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
- A17. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)
- A18. ความสอดคล้อง (Compliance)

Information Security Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- จะเห็นได้ว่ามีหลายเรื่องที่ตรงกับ CBK ของ (ISC)2 ดังนั้น ผู้ที่สอบผ่าน CISSP จึงมีพื้นฐานที่จะเป็นผู้ตรวจสอบด้านความมั่นคงข้อมูลที่ดีกว่าผู้ที่ยังไม่มีความรู้ตาม CBK ดังกล่าว
- โดยหลักการของผู้ตรวจสอบระบบความมั่นคงข้อมูลตามมาตรฐาน ISO/IEC 27001 หรือ "ISMS Lead Auditor" นั้น จะยึดหลักการ **"3E"** ได้แก่

1. **E = Existing**
2. **E = Execute**
3. **E = Effectiveness**

1. E = Existing

- เอกสารสำคัญทั้งหมดในกระบวนการ ISMS จะต้องถูกจัดทำให้เสร็จสมบูรณ์ (โดยอยู่ในรูปแบบของ Hardcopy และ/หรือ Soft-copy) ได้แก่
  - เอกสาร ISMS scope,
  - ISMS Policy,
  - Risk Assessment Methodology,
  - Risk Assessment Report,
  - Risk Treatment Plan และ
  - Statement of Applicability (SOA)

Information Security Audit (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

2. E = Execute

- องค์กรต้องปฏิบัติตามกระบวนการที่อยู่ในเอกสารในข้อหนึ่งมาในช่วงระยะเวลาหนึ่ง
- โดยปกติประมาณ 3-6 เดือน
  - เพื่อให้แน่ใจว่า เอกสารทุกอย่างที่เกี่ยวข้องได้ถูกนำมาใช้ปฏิบัติงานเป็น "Process" หรือ "Procedure" จริง ๆ
  - ไม่ใช่เป็นเพียงเอกสารที่ทำขึ้นมาแต่ไม่ได้นำมาใช้ให้เกิดประโยชน์แก่องค์กร

Information Security Audit (ต่อ)

3. E = Effectiveness

- ต้องมีกระบวนการในการวัดประสิทธิผล "Effectiveness"
  - ก่อนการปฏิบัติตามกระบวนการ ISMS (Before ISMS) เปรียบเทียบกับหลังการปฏิบัติตามกระบวนการ ISMS (After ISMS) มีประสิทธิผลเกิดขึ้นและสามารถวัดได้เป็นรูปธรรม
  - เช่น ก่อนการฝึกอบรม Information Security Awareness Training พนักงานในองค์กรทำข้อสอบ Pre-Test ได้คะแนนต่ำกว่าเกณฑ์ แต่หลังจากที่ฝึกอบรม Information Security Awareness Training ไปแล้ว กลับมาทำข้อสอบ Post-Test มีผลคะแนนที่ดีขึ้น เป็นต้น

สรุป

- ลักษณะการตรวจสอบของ "Internal Audit", "IT Audit" และ"Information Security Audit" มีลักษณะบางอย่างที่เหมือนกัน และมีหลายอย่างที่แตกต่างกัน
- "Role" หรือ "บทบาท" ของผู้ตรวจสอบจึงจำเป็นที่จะต้องกำหนดลงไปให้ชัดเจนก่อนการตรวจสอบเพื่อไม่ให้ผู้ถูกตรวจสอบ (Auditee) เกิดความเข้าใจผิดและให้ข้อมูลไม่ตรงกับรูปแบบของการตรวจสอบ ทำให้ผลลัพธ์ที่ได้จากการตรวจสอบไม่สัมฤทธิ์ผลเท่าที่ควรจะเป็นสำหรับส่วนที่เหมือนกันของการตรวจสอบทั้ง 3 ลักษณะ
- ผลการตรวจสอบ
  - สามารถถ่ายทอดในภาพรวม หรือ "Holistic Approach" และ
  - สามารถตอบโจทย์ของผู้บริหารตามหลัก "GRC" ได้อย่างชัดเจน
    - เช่น "Internal Audit" สามารถแสดงผลการตรวจสอบให้สอดคล้องกับหลัก "CG" หรือ "Corporate Governance" สามารถทำให้ Board Of Director เกิดความเข้าใจถึงต้นตอของปัญหาและทางแก้ไขที่ถูกต้องตามแนวทาง CG

สรุป (ต่อ)

- "IT Audit" สามารถนำหลัก "ITG" หรือ "IT Governance" โดยนำ "CobiT Framework" มาประยุกต์ใช้ให้เกิดผลลัพธ์จากการตรวจสอบที่มีประโยชน์ต่อการตัดสินใจของผู้บริการระดับสูงโดยอ้างอิง IT Goal กับ Business Goal ใน concept ของ Balanced Scorecard (BSC) ตามหลัก "GRC" ที่ถูกต้อง

- ถ้าหากผู้บริหารระดับสูงไม่สามารถนำข้อมูลจากการตรวจสอบไปใช้ให้เกิดประโยชน์เป็นรูปธรรม การที่ผู้บริหารระดับสูงจะกล่าวว่าองค์กรของตน "Governance" ก็คงยังไม่สามารถพูดได้เต็มปาก

สรุป (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- สำหรับในส่วนของ "Information Security Audit" ก็เช่นเดียวกัน ควรมีการนำหลักการ "Information Security Governance" มาประยุกต์ใช้เพื่อให้สามารถนำผลลัพธ์จากการตรวจสอบด้านความมั่นคงข้อมูลมาเป็นข้อมูลประกอบการตัดสินใจของผู้บริหารระดับสูง (Align with Business) ในลักษณะเดียวกับการตรวจสอบภายในและการตรวจสอบระบบสารสนเทศเช่นกัน
- ปัญหาของบ้านเราในปัจจุบันก็คือ ผู้ตรวจสอบภายในองค์กรและผู้ตรวจสอบอิสระจากภายนอกส่วนใหญ่ยังไม่สามารถนำข้อมูลผลลัพธ์จากการตรวจสอบ เช่น รายงาน Risk Assessment หรือ Risk Map มานำเสนอต่อผู้บริหารระดับสูง และ ผู้เกี่ยวข้องในองค์กรได้อย่างมีประสิทธิภาพ

สรุป (ต่อ)

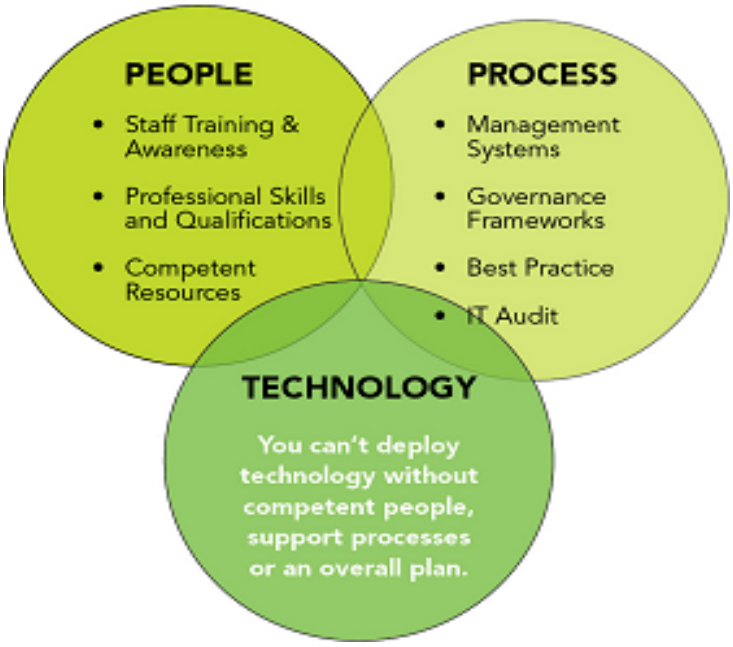
- เนื่องจากมีปัญหาด้านการ“Communication” ระหว่างผู้ตรวจสอบและผู้บริหารระดับสูง ตลอดจนการทำงานของฝ่ายต่าง ๆ ภายในองค์กรมีลักษณะเป็นเอกภาพสูงมากเสียจนไม่ค่อยได้ร่วมงานกันเท่าที่ควร เป็นปัญหาเรื่อง “Communication” ระหว่างฝ่ายเช่นกัน

- ทางแก้ปัญหา คือ การจัดประชุม โดยจัดตั้งเป็น “Steering Committee” ที่ประกอบด้วยตัวแทนจากหลายฝ่ายและมีผู้นำการประชุมที่มี “Leadership” และองค์ความรู้ที่สามารถ “นำ” หรือ “Lead” ที่ประชุมร่วมกับการทำงานของที่ปรึกษาจากภายนอก (External Consultant/Specialist) เพื่อให้องค์กรสามารถนำผลลัพธ์จากการตรวจสอบทั้ง 3 ด้านมา “บูรณาการ” ให้เกิดประโยชน์อย่างแท้จริงเป็นรูปธรรมให้แก่องค์กรในที่สุด

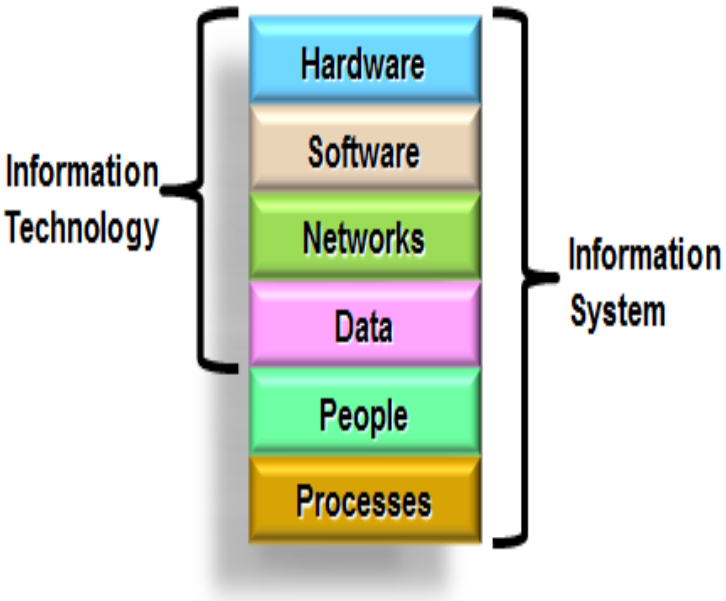
Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Information Security

THE THREE ELEMENTS FOR A SUCCESSFU ORGANIZATIONAL TRANSFORMATION



Ref: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/



https://www.emaze.com/@AFCZRLFF/MIS-Chap1

CIA triad

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ทรัพย์สิน (Asset)
  - ทรัพย์สินที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย บุคลากร
  - ทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล สารสนเทศ ความลับทางธุรกิจ
- ทรัพย์สินที่มีความมั่นคงนั้นต้องประกอบด้วยองค์ประกอบทั้ง 3 อย่างครบถ้วน
  - Confidential: เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์
  - Integrity: ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง
  - Availability: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

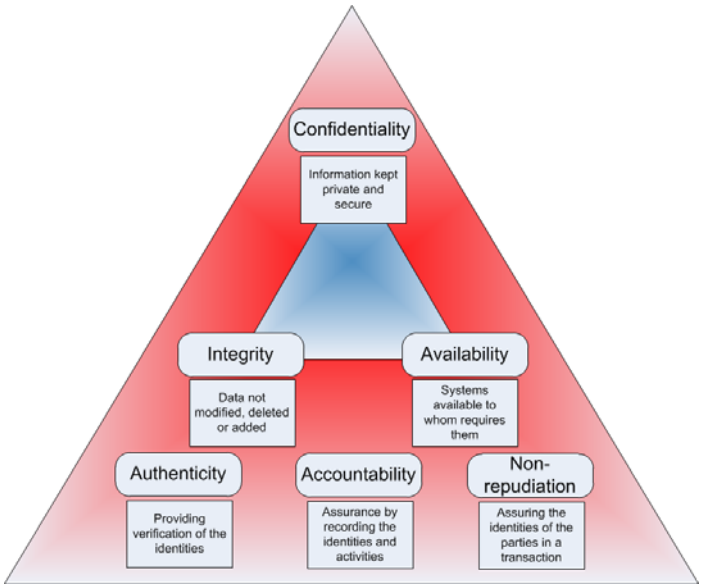
CIA triad

- ทรัพย์สิน (Asset)
  - ทรัพย์สินที่จับต้องได้ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย บุคลากร
  - ทรัพย์สินที่จับต้องไม่ได้ เช่น ข้อมูล สารสนเทศ ความลับทางธุรกิจ

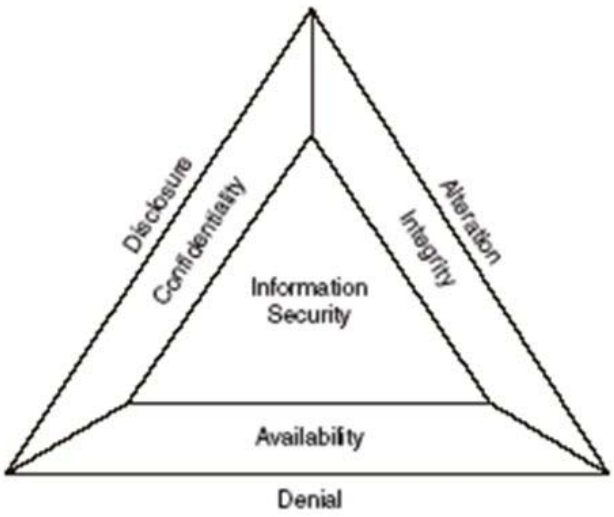
- ทรัพย์สินที่มีความมั่นคงนั้นต้องประกอบด้วยองค์ประกอบทั้ง 3 อย่างครบถ้วน
  - Confidential: เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์
  - Integrity: ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง
  - Availability: สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

http://sharemanila.com/wtf-is-cia/

CIA triad vs DAD triad



http://geraintw.blogspot.com/2012/09/cia-infosec.html



http://slideplayer.com/slide/4954666/

ความลับ (Confidentiality) (1/2)

- มาตรการตรวจสอบสิทธิก่อนเข้าถึง เพื่อยืนยันว่าผู้ที่ร้องขอนั้นมีสิทธิหรือได้รับอนุญาตให้เข้าถึงสารสนเทศ หรือระบบงานนั้นได้
- กลไกพื้นฐาน คือ การใช้รหัสผ่าน (Password) ในการพิสูจน์ตัวตนและสิทธิที่ได้รับอนุญาต
- การกำหนดชั้นความลับเป็นระดับต่าง ๆ ตามความสำคัญช่วยให้บริหารจัดการมีประสิทธิภาพมากขึ้น

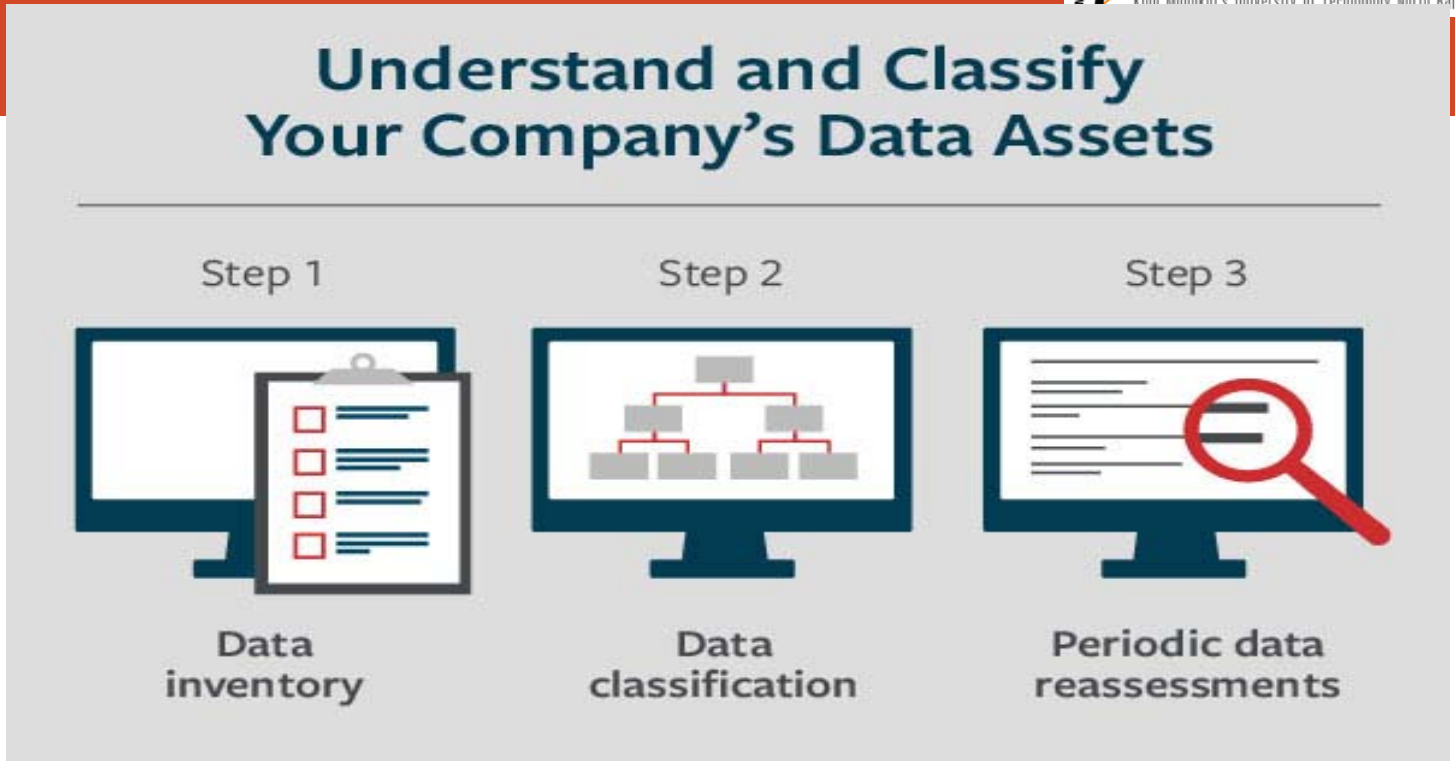
Data Classification & Monitoring - The Why

Goals of Data Classification

ENBRIDGE

- Identify WHAT information exists, and WHO needs it
- Understand how valuable the information is to each of the individuals, groups and business processes that require it
- Provide a system for protecting information critical to the organization

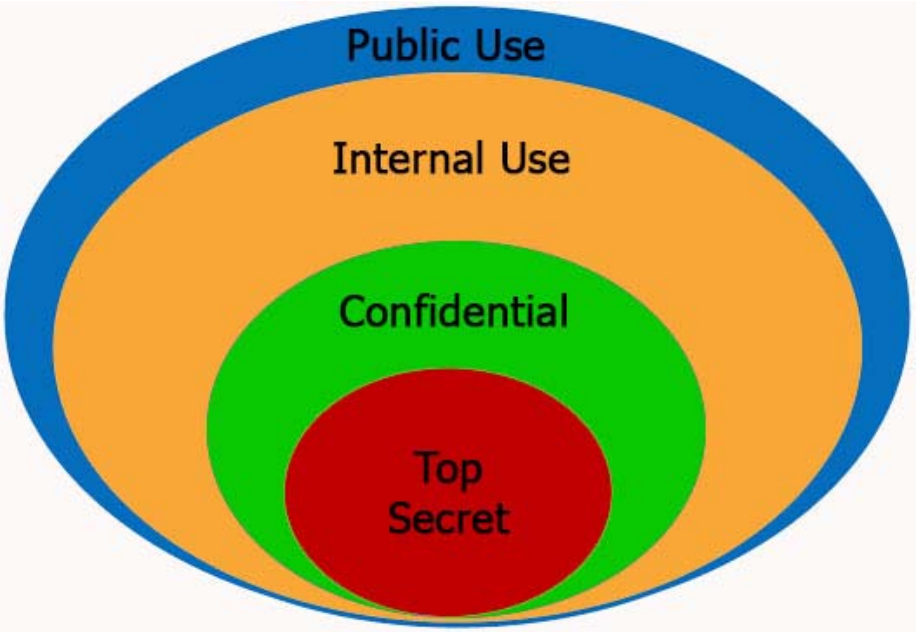
5



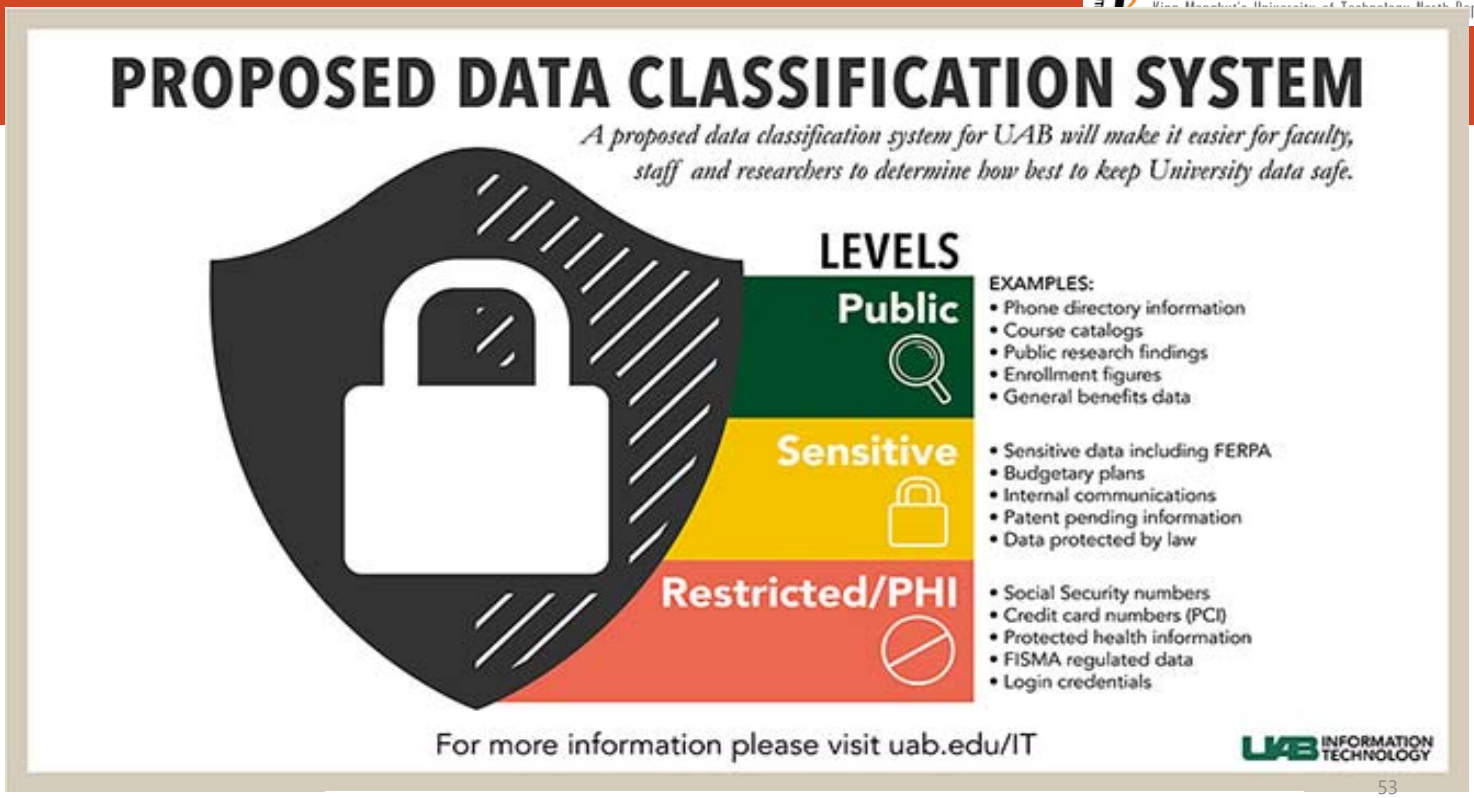
https://www.travelers.com/resources/cyber-security/data-assessment-inventory-and-classification.aspx

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

DATA CLASSIFICATION



Ref: http://www.aurorait.com/2014/06/06/importance-data-classification/



https://www.uab.edu/it/home/about-uab-it/announcements/item/819-three-levels-of-data-classification-proposed

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

SecureFirst Solutions
Data Classification

Every Organization has to segregate their Data into various categories and restrict user access based on a well-documented & maintained access control process.
Following is an depiction of Data Classification, its meaning, usage, measures to be taken during an Non-compliance and an example from each category.

Restricted
Means: Data access limited to a set of Users/Groups
Usage: Can be shared only with the relevant Users/Groups
Non-Compliance leads to: immediate termination of Employment & even legal actions
Example: Only the Board of Directors (BOD) can access the Audit Reports; etc.

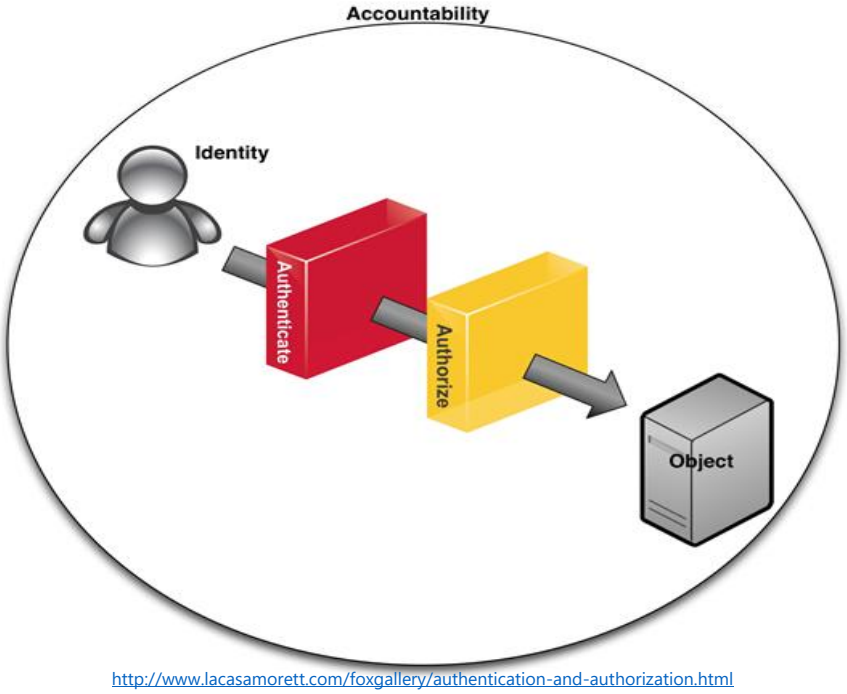
Highly Confidential
Means: Data access limited the Top Executives & Management
Usage: Can be shared only with the relevant Clients or within the Project
Non-Compliance leads to: Investigation & termination (if found guilty)
Example: Prospect Customers; Client Engagement Initiatives; Client billing details; etc.

Confidential
Means: All Company related documents unless made Public
Usage: Can be shared only with the relevant Clients or within the Organization
Non-Compliance leads to: Investigation & HR actions as directed by the Organization
Example: Client details; Company Standards, Policies & Guidelines; Client Reports; etc.

Unrestricted
Means: Documents / information already made public by the Organization
Usage: Can be shared outside the Organization without any restrictions
Non-Compliance leads to: Not Applicable (NA)
Example: Company details such as – Address; Contact number; Company acquisition; etc.

http://www.securefirstsolutions.com/blog/tag/data-classification/

AAA - Authentication, Authorization, Accounting



55

http://www.lacasamorett.com/foxgallery/authentication-and-authorization.html

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Authentication

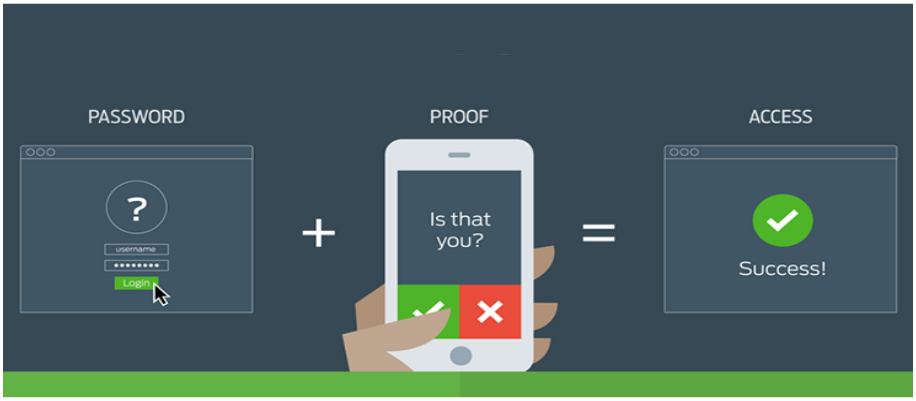
Who you are

Authorization

What you can do

https://www.soapui.org/testing-dojo/best-practices/authentication.html

https://www.vasco.com/two-factor-authentication.html



http://news.mit.edu/2015/two-factor-authentication-duo-security-0130

ความลับ (Confidentiality) (2/2)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

ชั้นความลับ

- ต้องมีเกณฑ์พิจารณาที่ชัดเจนว่าสารสนเทศลักษณะใดอยู่ในชั้นความลับที่กำหนด
- กำหนดแนวทางการ การระบุชั้นความลับ การจัดเก็บ และการสื่อสารข้อมูลสารสนเทศในแต่ละชั้นความลับอย่างชัดเจน
- มาตรการทางเทคนิคที่ใช้ในการปกป้องความลับ เช่น การเข้ารหัส (Encryption) อาจถูกนำมาใช้เสริมความแข็งแกร่งให้กับมาตรการปกป้องสารสนเทศที่ต้องการมาตรการดูแลอย่างเข้มงวด

http://www.club27001.com/2014/01/iso27001-2013-Information-Risk-Assessment.html

ความถูกต้องสมบูรณ์ (Integrity) (1/2)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) เป็นสิ่งสำคัญส่งผลถึงความน่าเชื่อถือของสารสนเทศนั้น ๆ
- ทำอย่างไรให้ข้อมูลมีความถูกต้องและน่าเชื่อถือเป็นสิ่งที่ผู้ดูแลระบบต้องหาคำตอบและดำเนินการให้เกิดขึ้น
- คำตอบในเชิงหลักการ
  - ระบบต้องมีกลไกการตรวจสอบสิทธิหรือการได้รับอนุญาตให้ดำเนินการเปลี่ยนแปลงแก้ไขหรือกระทำการใด ๆ ต่อข้อมูลนั้น

http://www.club27001.com/2014/01/iso27001-2013-Information-Risk-Assessment.html

ความถูกต้องสมบูรณ์ (Integrity) (2/2)

- บัตรประชาชนอัจฉริยะเป็นตัวอย่างใกล้ตัวที่ชี้ให้เห็นว่า ประชาชนทุกคนต้องเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเลี่ยงไม่ได้ อย่างน้อยข้อมูลส่วนตัวของเราก็ถูกจัดเก็บในฐานข้อมูลของรัฐบาล
- จะเกิดอะไรขึ้นหากชื่อของนาย A ถูกลบออกจากบัญชีทะเบียนราษฎร์
  - นาย A ไม่มีตัวตนและไม่สามารถใช้สิทธิของประชาชนในการรับบริการรัฐได้
- เห็นได้ว่าข้อมูลนี้มีความสำคัญมากเพราะเป็นหลักฐานในการพิสูจน์ตัวตนของเรา
- ข้อมูลนี้จำเป็นต้องได้รับการปกป้องดูแลความถูกต้องสมบูรณ์และความน่าเชื่อถือ หากข้อมูลถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดีย่อมส่งผลเสียต่อเจ้าของข้อมูลอย่างหลีกเลี่ยงไม่ได้

ความพร้อมใช้งาน (Availability) (1/3)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ อุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนกได้ 2 แบบ คือ

- ระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of data processing capability)
- การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service)

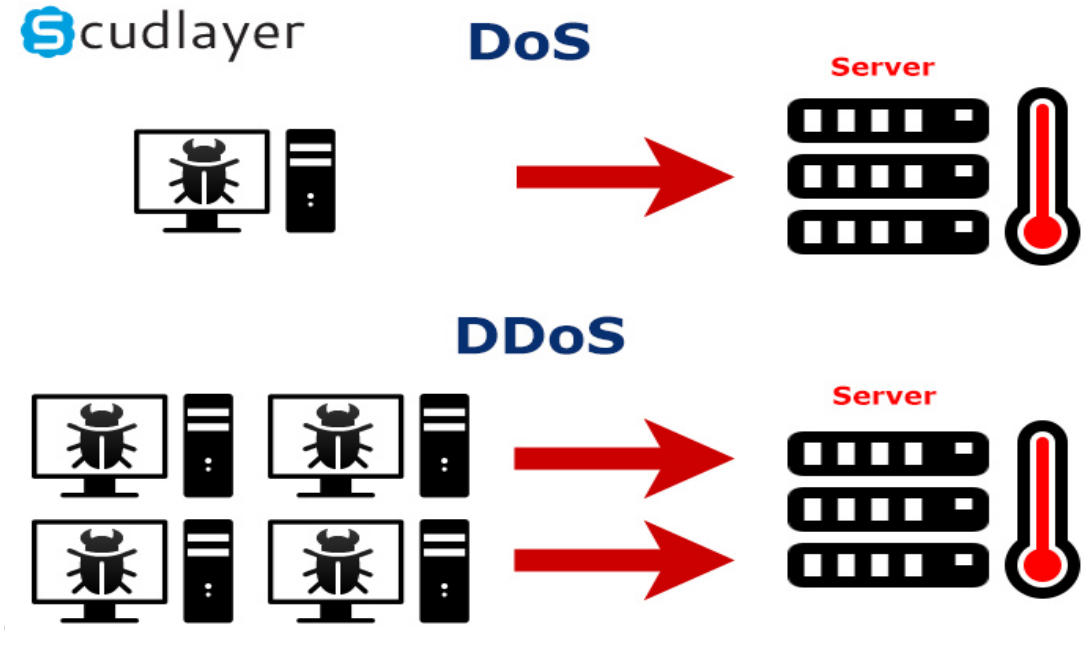
ความพร้อมใช้งาน (Availability) (2/3)

- ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ อาจเกิดจาก
  - การกระทำของผู้ใช้ระบบ ผู้บุกรุกที่มีเจตนาร้าย
  - หรือเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหวทำให้ระบบคอมพิวเตอร์เสียหายก็เป็นได้

- องค์กรที่ตระหนักถึงภัยคุกคามดังกล่าวอาจเตรียมแผนกู้คืนจากความเสียหาย (Disaster Recovery Plan) ไว้รองรับ
- หน่วยงานรัฐที่ให้บริการสารธารณะต่างใช้ระบบคอมพิวเตอร์ควบคุมการทำงาน เช่นไฟฟ้า ประปา โทรศัพท์ เป็นต้น หากคอมพิวเตอร์ที่ควบคุมระบบเหล่านี้เกิดความเสียหายไม่สามารถให้บริการได้ ทำให้บริการต่าง ๆ หยุดชะงักย่อมส่งผลเสียต่อประชาชนในวงกว้าง

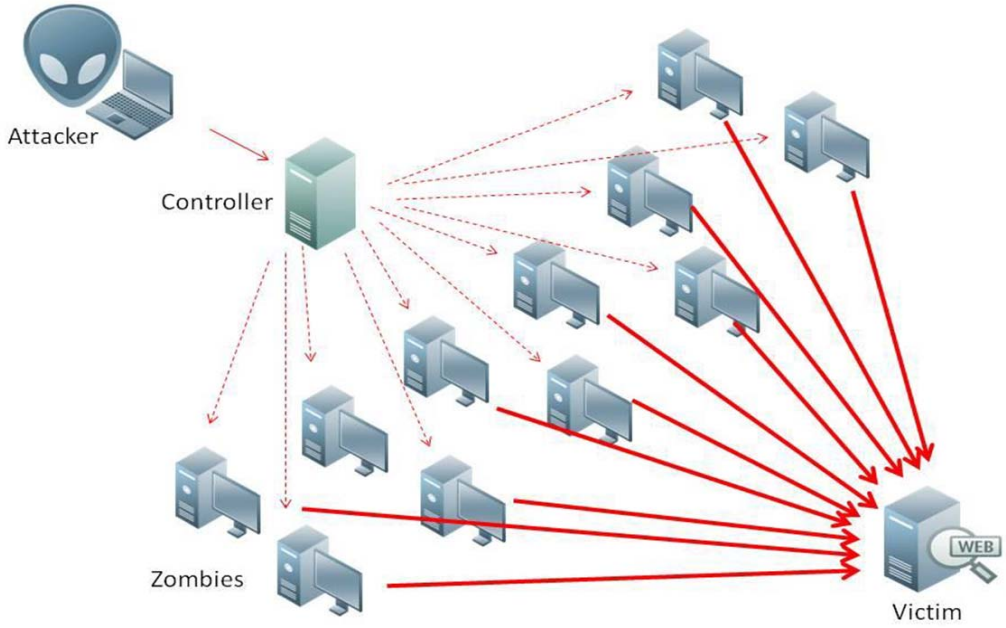
DoS (Denial of Service) and DDoS (Distributed Denial of Service)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok



https://www.scudlayer.com/blog/en/category/ddos

DDoS (Distributed Denial of Service)



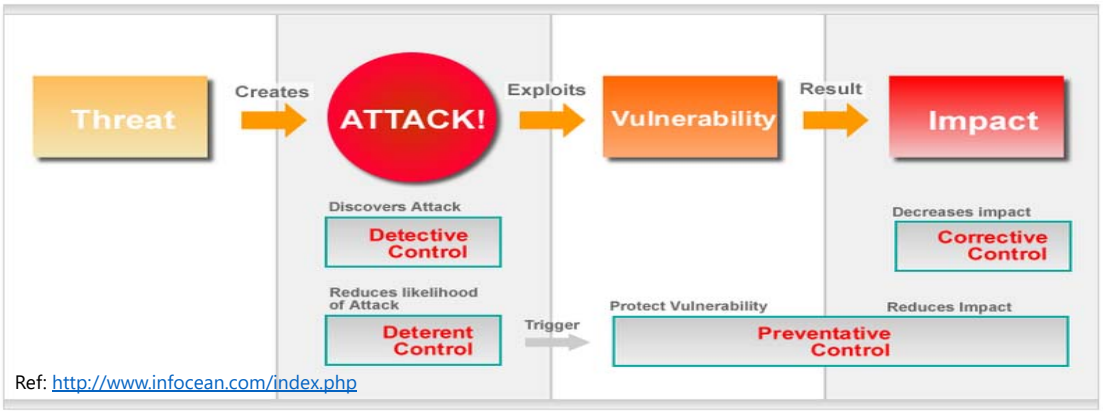
https://cyberwurx.com/ddos-protection/

ความพร้อมใช้งาน (Availability) (3/3)

- นอกจากนี้หากไฟฟ้าดับเป็นเวลานาน ระบบต่าง ๆ จะเกิดความเสียหายอย่างใหญ่หลวง
- ตัวอย่างจริงที่เคยเกิดขึ้นในต่างประเทศ เมื่อหลายปีก่อนระบบคอมพิวเตอร์ของศูนย์กระจายสินค้าเกิดความเสียหาย ไม่สามารถจ่ายกระแสไฟฟ้าไปยังคอนเทนเนอร์ที่ติดตั้งระบบทำความเย็นเป็นเวลาหลายวัน ส่งผลให้สินค้าในตู้คอนเทนเนอร์ดังกล่าวเสียหายทั้งหมด นอกจากนี้ยังทำให้ลูกค้าขอยกเลิกสัญญาเนื่องจากไม่ไว้วางใจในการบริการ เกิดความสูญเสียมูลค่ามหาศาล

- การปกป้องข้อมูล (Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับ "ความเสี่ยง (Risk)"
- หลักการคือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการปกป้องเข้มงวดกว่าข้อมูลที่มีความเสี่ยงต่ำ ตัวอย่างเช่น ข้อมูล username & password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเว็บไซต์องค์กร เป็นต้น

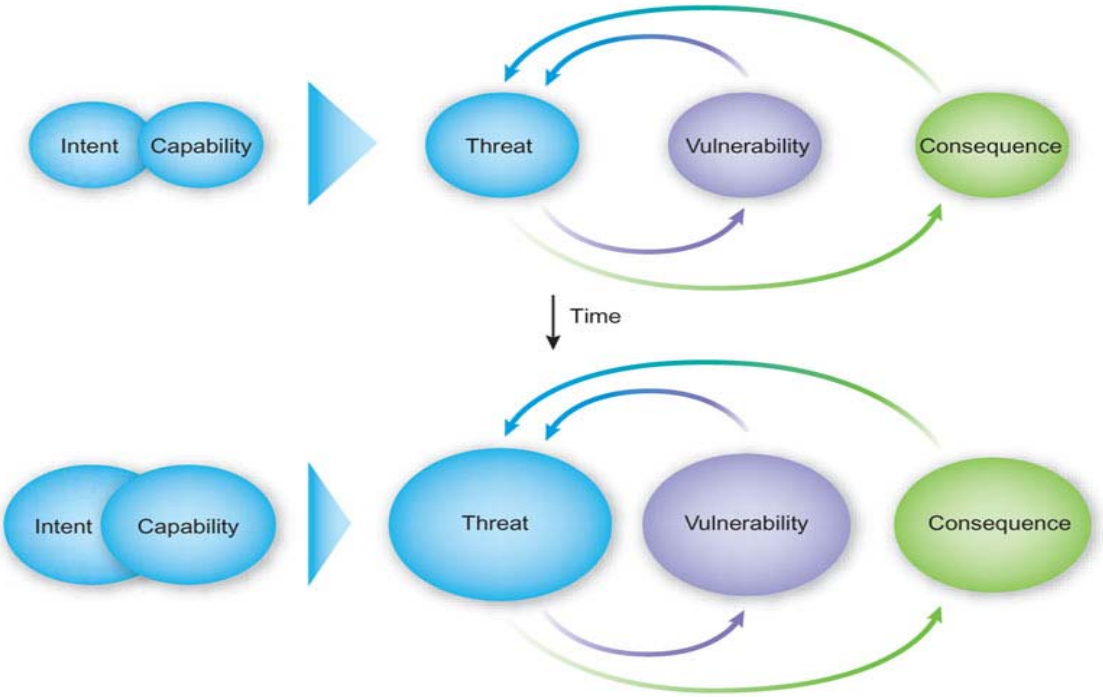
ความสัมพันธ์ของความมั่นคงและการโจมตี



Ref: http://www.infocean.com/index.php

- Threat หมายถึง “สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติองข้อมูลด้านใดด้านหนึ่งหรือมากกว่า”
- Vulnerability หมายถึง “สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ และหากถูกใช้ให้เป็นประโยชน์โดยภัยคุกคามก็อาจทำให้ทรัพย์สินสารสนเทศขององค์กรได้รับความเสียหายได้” หรือ “ช่องโหว่นั่นเอง”
- Impact หมายถึง ผลกระทบที่เกิดขึ้นหลังจากการถูกโจมตี

Ref: http://gaelrisk.com/Gael-Risk/media/Gael-Risk-Content-Images/risk-identification-vulnerabilities.jpg



Ref: http://www.suggestkeyword.com/dnVsbmVyYWJpbGl0eSB2cyB0aHJlYXQ/

ผลกระทบที่อาจเกิดขึ้นหลังจากการถูกโจมตี

- ไวรัสใช้ประโยชน์จากการไม่ได้ติดตั้งโปรแกรมป้องกันไวรัสและทำให้ข้อมูลสำคัญขององค์กรเกิดความเสียหาย
- ข้อมูลสำคัญถูกขโมยซึ่งเกิดจากการขาดการรักษาความมั่นคงทางกายภาพและทำให้องค์กรสูญเสียข้อได้เปรียบด้านการแข่งขัน
- หน้าเว็บไซต์ถูกเปลี่ยนแปลงซึ่งเกิดจากการใช้รหัสผ่านที่สั้นเกินไปและทำให้องค์กรเสียชื่อเสียง
- สูญเสียรายได้
- สูญเสียชีวิตและทรัพย์สิน
- อื่น ๆ

Countries where users faced the greatest risk of online infection

In order to assess the risk of online infection faced by users in different countries, we calculate the percentage of Kaspersky Lab users in each country who encounter detection verdicts on their machines during the quarter. The resulting data provide an indication of the aggressiveness of the environment in which computers work in different countries.

	Country*	% unique users attacked**
1	Russia	38.98%
2	Kazakhstan	37.70%
3	Ukraine	35.75%
4	Syria	34.36%
5	Belarus	33.02%
6	Azerbaijan	32.16%
7	Thailand	31.56%
8	Georgia	31.44%
9	Moldova	31.09%
10	Vietnam	30.83%
11	Armenia	30.19%
12	Kyrgyzstan	29.32%
13	Croatia	29.16%
14	Algeria	28.85%
15	Qatar	28.47%
16	China	27.70%
17	Mongolia	27.27%
18	Makedonia	26.67%
19	Bosnia and Herzegovina	25.86%
20	Greece	25.78%

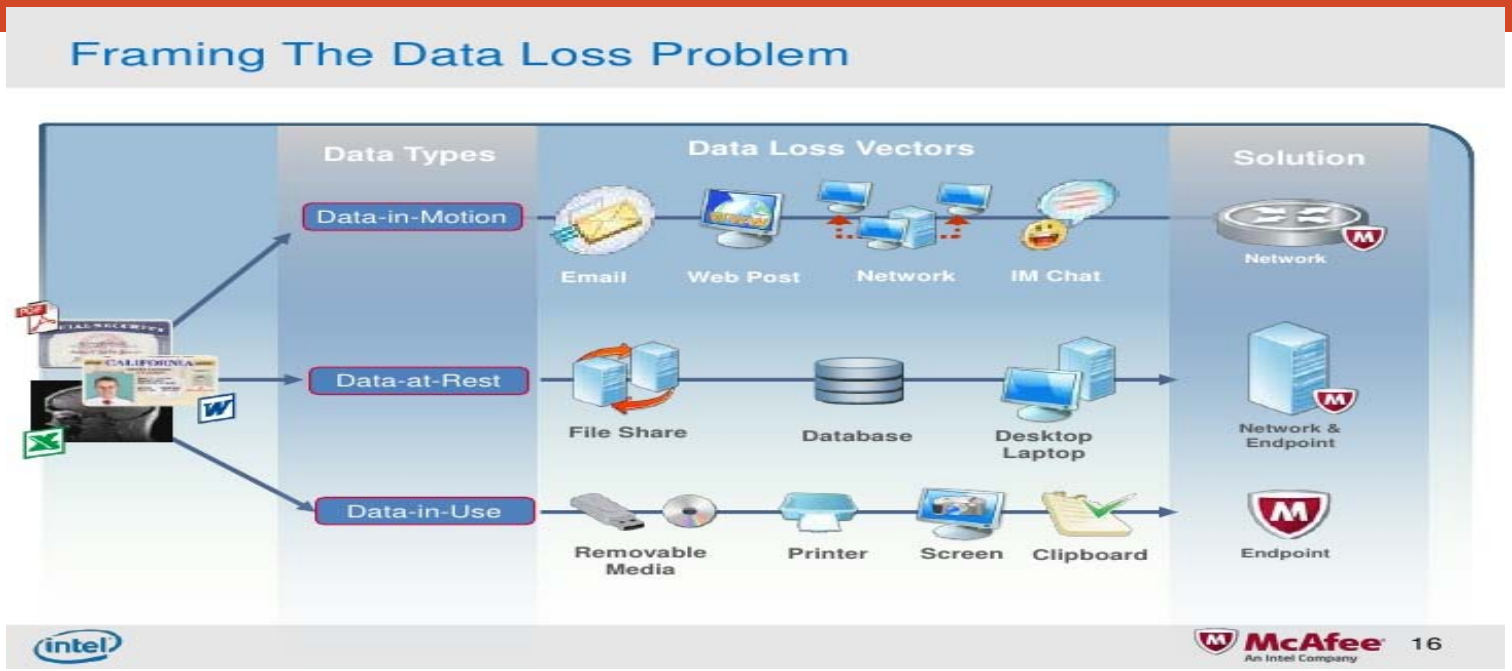
Q2 2015

https://securelist.com/analysis/quarterly-malware-reports/71610/it-threat-evolution-q2-2015/

These statistics are based on the detection verdicts returned by the web antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

การป้องกันข้อมูลที่มีความสำคัญ

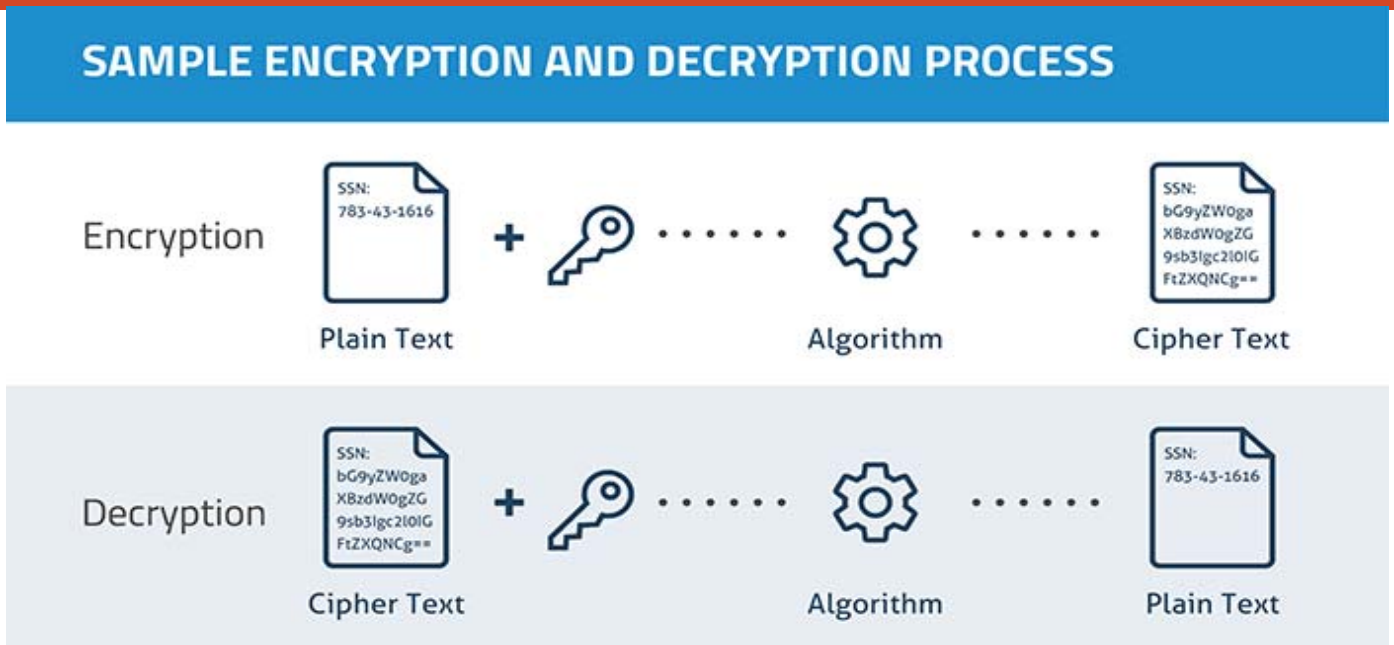


http://www.slideshare.net/Intel-ASIP/enterprise-api-security-data-loss-prevention

Understanding Core Security Goals

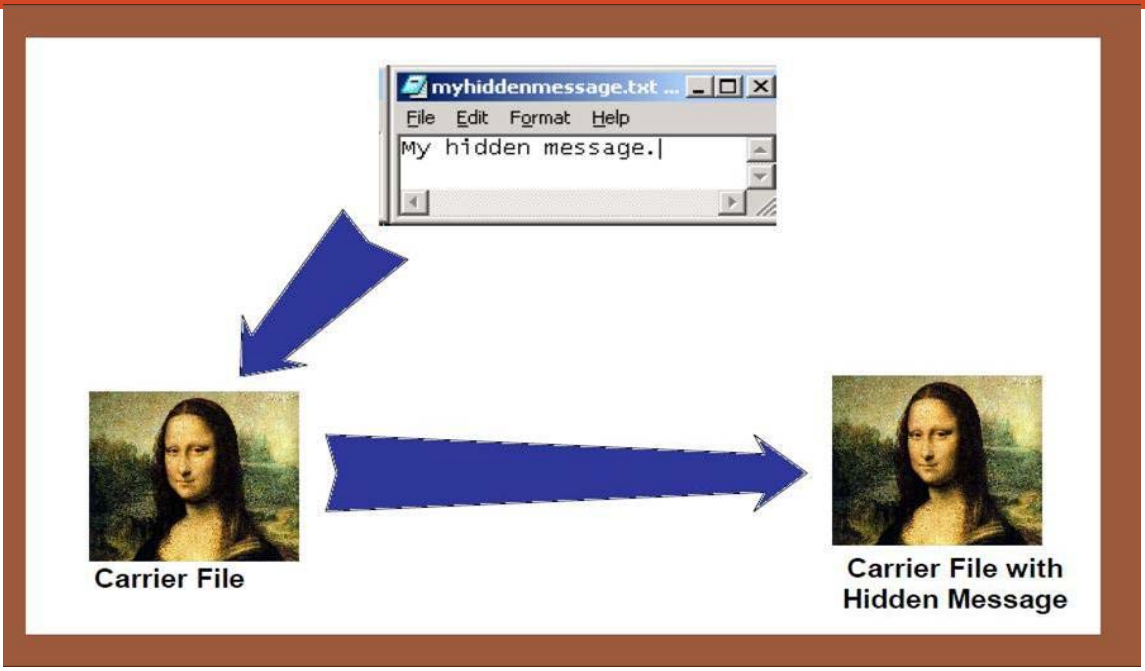
- Confidentiality
  - Encryption
  - Access controls
  - Steganography

Encryption



https://www.skyhighnetworks.com/cloud-security-university/tokenization-vs-encryption/

Steganography



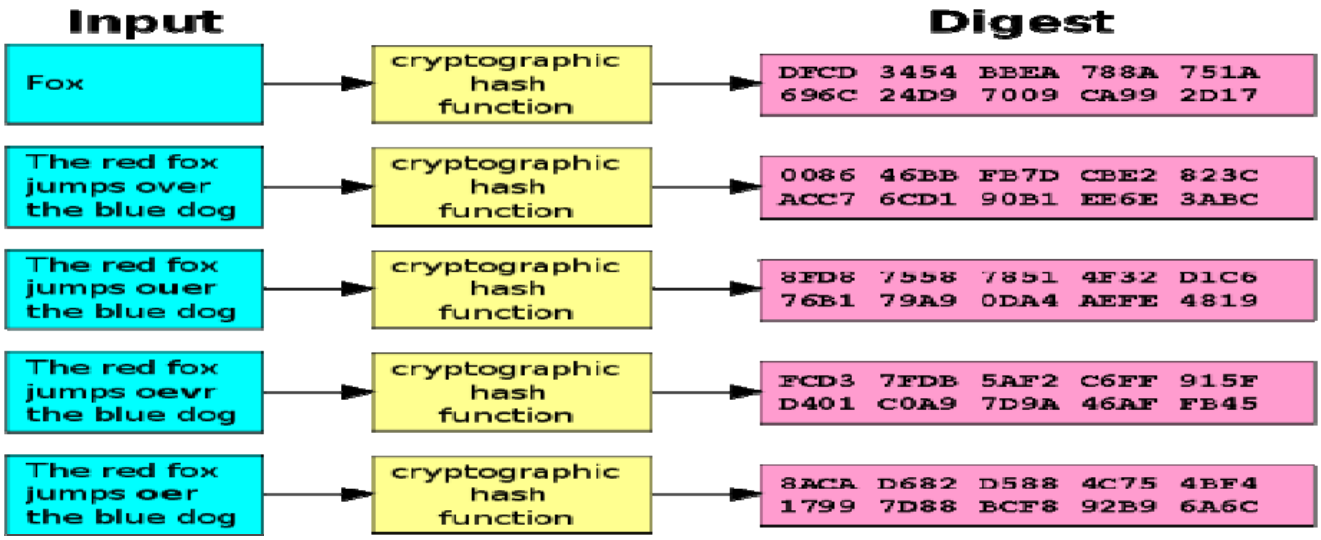
https://mgitecetech.wordpress.com/tag/steganography/

Understanding Core Security Goals

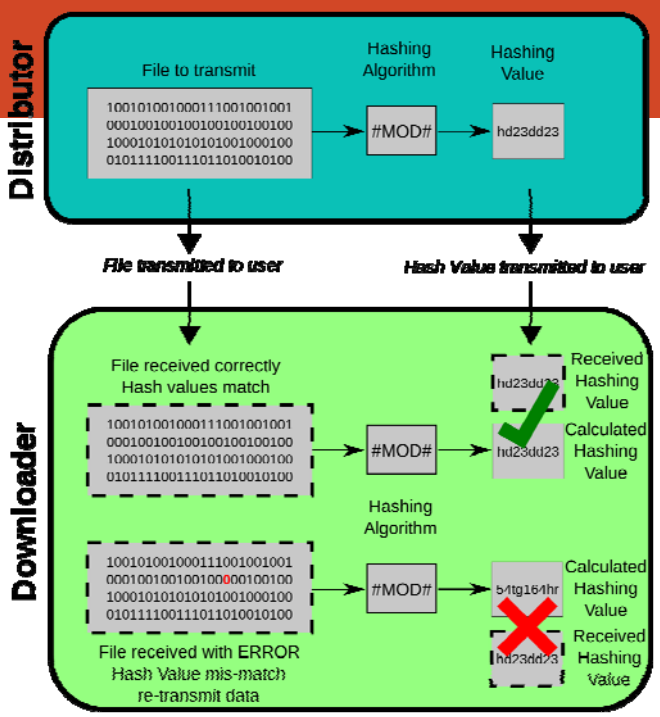
Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- Integrity
  - Hashing
  - Digital signatures
  - Certificates
  - Non-repudiation

Hashing



http://www.makeuseof.com/tag/md5-hash-stuff-means-technology-explained/



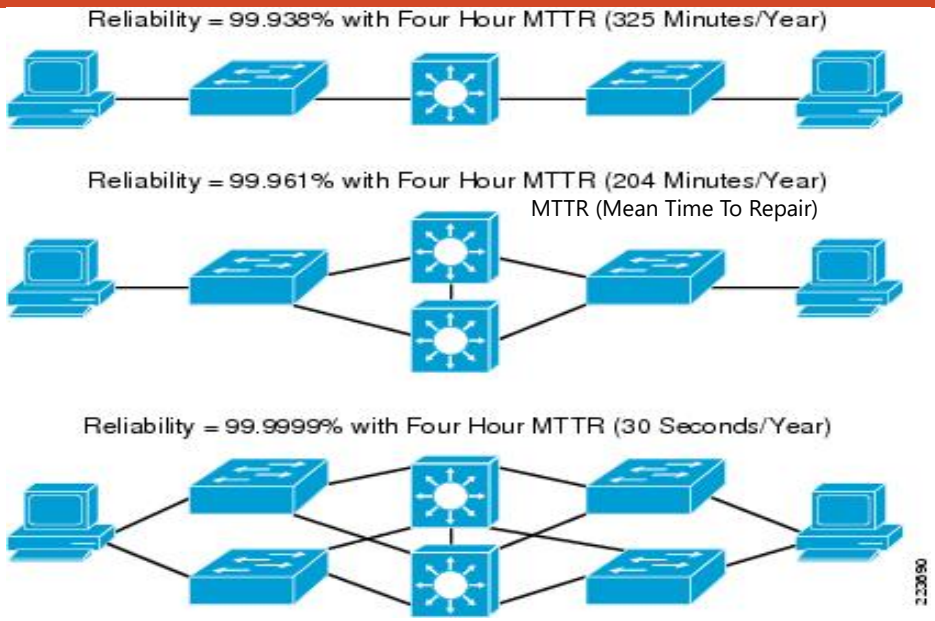
https://en.wikipedia.org/wiki/MD5

Understanding Core Security Goals

- Availability
  - Redundancy
  - Fault tolerance
  - Patching

Redundancy & Fault tolerance

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok



http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

http://serverfault.com/questions/316637/100-uptime-for-a-web-application

การปกป้อง Confidentiality Integrity Availability

- จะต้องป้องกัน Confidentiality Integrity Availability เข้มงวดแค่ไหน
- ข้อมูลมีมากมายหลายประเภท ต้องป้องกันอย่างเข้มงวดเท่ากันหมดหรือเปล่า?
- การปกป้องข้อมูล (Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับ "ความเสี่ยง (Risk)"
- หลักการ คือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการควบคุมปกป้องเข้มงวดกว่าข้อมูลที่มีความเสี่ยงต่ำ
  - เช่น ข้อมูล username & password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการควบคุมปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเว็บไซต์องค์กร เป็นต้น

ความเสี่ยงเกี่ยวกับระบบไอที

- การพัฒนาระบบสารสนเทศ
  - ไม่ทราบความต้องการของผู้ใช้
  - ระบบมีฟังก์ชันงานไม่ครบถ้วนเท่าที่ควรจะเป็น
  - ผู้พัฒนาไม่มีความรู้พอเพียง (ด้านเทคโนโลยี, การพัฒนา, การเขียนโปรแกรม)
  - ออกแบบระบบผิดพลาด
  - ระบบมีความผิดพลาดเพราะตรวจสอบโปรแกรมไม่ครบถ้วน
  - ผู้พัฒนาแอบฝังโปรแกรมอันตรายเอาไว้ เพื่อลักลอบส่งข้อมูลออก, สั่งให้คอมพิวเตอร์ทำงานผิดพลาด, สั่งให้ลบข้อมูล, ฯลฯ

Ref: การตรวจสอบไอที (IT Audit), ดร.ครรชิต มาลัยวงศ์ ราชบัณฑิต

ความเสี่ยงเกี่ยวกับระบบไอที

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การใช้ระบบ (ทั้งที่เป็นเรื่องการใช้ และ การพัฒนาไม่เหมาะสม)
  - ผู้ใช้ที่ไม่ได้รับมอบหมายให้ใช้งาน กลับสามารถเข้าใช้ระบบได้
  - การบันทึกข้อมูลไม่ครบ, ผิดพลาดหรือบกพร่อง
  - การใช้งานผิดพลาด => ต้องการอย่างหนึ่ง แต่ทำอีกอย่างหนึ่ง
  - คู่มือการใช้ผิดพลาด
  - โปรแกรมไม่สามารถถอยหลังกลับไปสู่จุดตั้งต้นก่อนทำงาน
  - ไม่สามารถตรวจสอบได้ว่าทำงานอะไรเสร็จไปบ้างแล้ว
  - การจัดทำรายงานผิดพลาด
  - ผู้ใช้ไม่สามารถค้นคืน หรือ เรียกใช้ข้อมูลที่ต้องการ

ความเสี่ยงเกี่ยวกับระบบไอที

- ความเสี่ยงเกี่ยวกับอุปกรณ์
  - คอมพิวเตอร์และอุปกรณ์ไม่สามารถทำงานร่วมกันได้
  - คอมพิวเตอร์และอุปกรณ์มีสมรรถนะต่ำ ทำให้ทำงานช้ามาก
  - คอมพิวเตอร์และอุปกรณ์เสียหายเพราะไม่ได้รับการบำรุงรักษาอย่างถูกวิธี
  - คอมพิวเตอร์และอุปกรณ์ถูกโจรกรรม
  - คอมพิวเตอร์และอุปกรณ์ถูกทำลายโดยผู้บุกรุก
  - การนำคอมพิวเตอร์และอุปกรณ์ไปจำหน่าย โดยไม่ได้ลบข้อมูลในฮาร์ดดิสก์ออกก่อน
  - **คอมพิวเตอร์และอุปกรณ์เปลี่ยนแปลงก้าวหน้าเร็วมาก แต่เราไม่ได้** ปรับปรุงเครื่องของเราทำให้ไม่สามารถใช้งานร่วมกับหน่วยงานอื่นได้

ความเสี่ยงจากภายนอก

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ระบบไอทีอาจประสบปัญหาได้หลายเรื่อง เช่น...
  - การถูกบุกรุกโดยบุคคลภายนอกเข้ามาโจรกรรมอุปกรณ์ในยามวิกาล หรือในช่วงที่ไม่มีใครดูแลห้องอุปกรณ์
  - การถูกไวรัสก่อกวนโดยไวรัสนั้นมาจากระบบอินเทอร์เน็ต, อีเมล, โปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ต, เกม, flash drive และอื่น ๆ
  - การตั้งวางอุปกรณ์ และ แผ่นซีดี ไว้บนโต๊ะทำงานโดยเปิดเผย และไม่ได้ปิดระบบก่อนลุกไปจากโต๊ะทำงาน
  - แฮคเกอร์บุกรุกเข้ามาทางระบบอินเทอร์เน็ต หรือเครือข่ายภายในเพื่อทำลายระบบ, ซอฟต์แวร์, เว็บ และ ข้อมูล หรือ แอบซุกซ่อนโปรแกรมเอาไว้เพื่อส่งข้อมูลของสำนักงานออกไปให้คนภายนอก

ความเสี่ยงจากอุบัติภัย

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- อุบัติภัยทั้งที่เกิดโดยธรรมชาติหรือโดยมนุษย์อาจจะเกิดได้...
  - เพลิงไหม้สำนักงาน ทำให้ระบบและอุปกรณ์ต่าง ๆ เสียหาย
  - น้ำท่วมสำนักงาน ทำให้ระบบและอุปกรณ์ต่าง ๆ เสียหาย
  - หลังคารั่วทำให้น้ำฝนตกลงมาบนตัวเครื่องและอุปกรณ์
  - วาตภัยอาจทำให้สำนักงานและระบบเสียหาย
  - อุบัติเหตุระหว่างขนย้ายอุปกรณ์อาจเกิดได้ เช่น รถยนต์ถูกชน, รถตกถนน, ทำเครื่องหลุดตกจากมือระหว่างการขนย้าย, เครื่องถูกโจรกรรมระหว่างการขนย้าย,

ความเสี่ยงจากบุคลากรภายใน

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- พนักงาน, ข้าราชการ, หรือผู้เกี่ยวข้องก็มีความเสี่ยง...
  - พนักงานและบุตรหลานอาจจะนำเกมจากบ้านมาเล่นในคอมพิวเตอร์
  - พนักงานอาจจะก๊อปปี้ข้อมูลไปให้บุคคลภายนอก
  - พนักงานหรือข้าราชการที่ไม่พอใจสำนักงานหรือผู้บังคับบัญชาอาจจะแอบทำลายข้อมูลหรืออุปกรณ์ภายใน
  - การใช้โปรแกรมที่ไม่ได้รับการฝึกอบรมการใช้มาอย่างดีอาจทำให้เกิดปัญหากับข้อมูลได้
  - ผู้บริหารไม่ยอมใช้คอมพิวเตอร์เอง แต่มอบอำนาจให้พนักงานใช้แทน อาจทำให้เกิดปัญหาได้มากมาย
  - พนักงานอาจจะแอบแก้ไขโปรแกรมและข้อมูลระหว่างการทำงาน

การประเมินและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

- การประเมินและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เป็นกระบวนการที่สำคัญที่องค์กรทุกระดับพึงจัดให้มีขึ้น เพื่อปกป้องธุรกิจและสร้างความสอดคล้องกับกฎหมาย รวมถึงเป็นกระบวนการพื้นฐานที่มาตรฐานสากลต่าง ๆ กำหนดให้มีการปฏิบัติใช้ภายในองค์กร เช่น ISO 27001, ISO 20000, ISO22301 เป็นต้น

- โดยวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่นิยมใช้งานอย่างแพร่หลายในองค์กรต่าง ๆ ที่ Implement ISO 27001:2005 คือวิธีการที่เรียกว่า Asset-based Risk Assessment ซึ่งประกอบด้วยขั้นตอนหลัก ๆ ดังนี้
  - จัดทำทะเบียนทรัพย์สิน (Inventory of Asset) เพื่อระบุทรัพย์สินสารสนเทศที่สำคัญที่ต้องได้รับการปกป้อง
  - พิจารณาถึงภัยคุกคาม (Threat) ที่อาจทำอันตรายต่อทรัพย์สินสารสนเทศ และจุดอ่อน (Vulnerability) ในตัวทรัพย์สิน กระบวนการ หรือมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่อาจเป็นช่องทางให้ภัยคุกคามเหล่านั้นเข้าทำอันตรายต่อทรัพย์สินได้
  - ประเมินระดับผลกระทบ (Impact) ต่อองค์กร และโอกาส (Probability) ที่จะเกิดเหตุการณ์ความเสี่ยงขึ้น
  - คำนวณระดับความเสี่ยง โดยสูตรพื้นฐานที่นิยมใช้กัน คือ
    - ผลกระทบ **(Impact) x** โอกาส **(Probability) =** ระดับความเสี่ยง **(Risk)**

http://www.acinfotec.com/2014/06/05/learn-scenario-based-risk-assessment-suitable/

ตัวอย่าง Asset-based Risk Assessment และ Scenario-based Risk Assessment

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Asset-based Risk Assessment

Asset	Threat	Vulnerability	Impact	Probability	Risk
Application Server	การโจมตีทางเครือข่าย	ไม่ได้ทำการติดตั้ง Patch อย่างเหมาะสม	High	High	High
	ฮาร์ดแวร์เสียหรือทำงานผิดพลาด	ไม่ได้ทำการบำรุงรักษาอย่างเหมาะสม	High	Low	Medium

Scenario-based Risk Assessment

Risk Scenario	Impact	Probability	Risk
ความเสี่ยงจาก Heartbleed Bug เนื่องจากมีหลายระบบงานขององค์กรที่ใช้งาน OpenSSL version ที่ได้รับผลกระทบจากช่องโหว่นี้	High	High	High

*หมายเหตุ ตัวอย่างข้างต้นเป็นการอธิบายองค์ประกอบที่เกี่ยวข้องกับการประเมินความเสี่ยงแบบง่ายเท่านั้น การประเมินความเสี่ยงในสถานการณ์จริงยังมีองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง และมีความซับซ้อนมากกว่านี้ เช่น ต้องมีการพิจารณามาตรการควบคุม (Existing Controls) ที่มีอยู่เดิมภายในองค์กรด้วย

http://www.acinfotec.com/2014/06/05/learn-scenario-based-risk-assessment-suitable/

Asset-based Risk Assessment

ข้อดี	ข้อเสีย
•เข้าใจง่าย เนื่องจากผู้ประเมินความเสี่ยงเห็นภาพที่ชัดเจนว่ากำลังพิจารณาความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินใด •มั่นใจได้ว่าการบริหารความเสี่ยงจะครอบคลุมทุกทรัพย์สิน	•ต้องใช้ระยะเวลาและทรัพยากรจำนวนมากในการประเมินความเสี่ยงให้ครอบคลุมทุกทรัพย์สิน และผลที่ได้คือข้อมูลที่มากเกินความจำเป็น และนำไปใช้งานจริงได้น้อย •การประเมินความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินจำนวนมาก เช่น การเปลี่ยน Platform ของระบบงานหลัก หรือความเสี่ยงที่ไม่เกี่ยวข้องกับทรัพย์สินโดยตรง เช่น การปรับเปลี่ยนกระบวนการทางธุรกิจ อาจทำได้ยาก หรือถึงขั้นไม่สามารถทำได้เลย

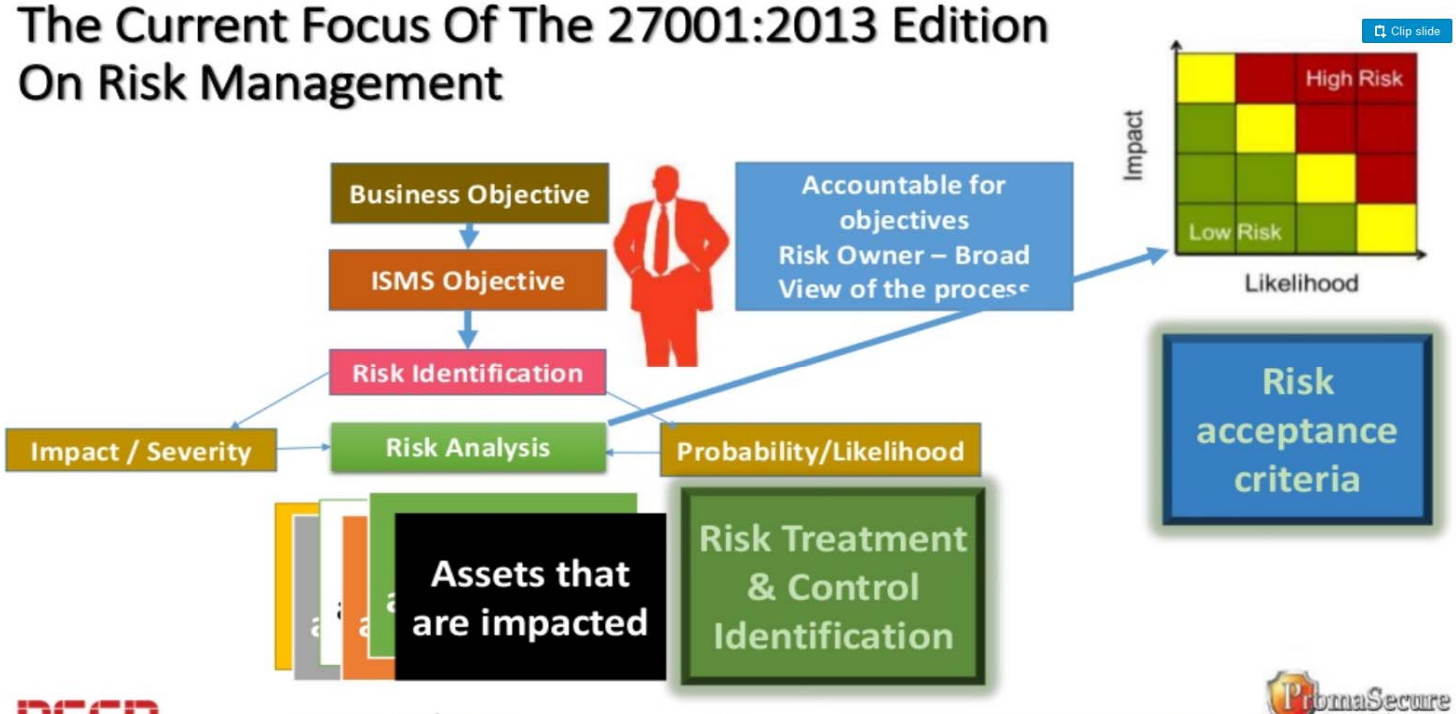
Scenario-based Risk Assessment

ข้อดี	ข้อเสีย
•ประหยัดเวลาและทรัพยากรที่ต้องใช้ในการประเมินความเสี่ยง •จำนวนข้อมูลที่ได้มีความเหมาะสมและมีคุณภาพ •สามารถประเมินความเสี่ยงได้ทุกรูปแบบ (ไม่จำกัดเฉพาะความเสี่ยงที่เกี่ยวข้องกับทรัพย์สิน)	•การระบุเหตุการณ์ความเสี่ยงทำได้ยาก โดยเฉพาะกับผู้ประเมินความเสี่ยงมือใหม่ •ไม่มีขอบข่ายที่ชัดเจน ที่จะทำให้มั่นใจได้ว่า ได้ทำการประเมินความเสี่ยงอย่างครอบคลุมแล้ว (ต่างจากการประเมินความเสี่ยงแบบ Asset-based ซึ่งจะทราบชัดเจนว่าได้ประเมินความเสี่ยงครบทุกทรัพย์สินแล้ว)

http://www.acinfotec.com/2014/06/05/learn-scenario-based-risk-assessment-suitable/

Faculty of Information Technology

The Current Focus Of The 27001:2013 Edition On Risk Management



http://www.slideshare.net/PECBCERTIFICATION/the-significance-of-the-shift-to-risk-management-from-threat-vulnerability-assessment-in-isms

Probability (Likelihood)

โอกาสที่จะเกิด

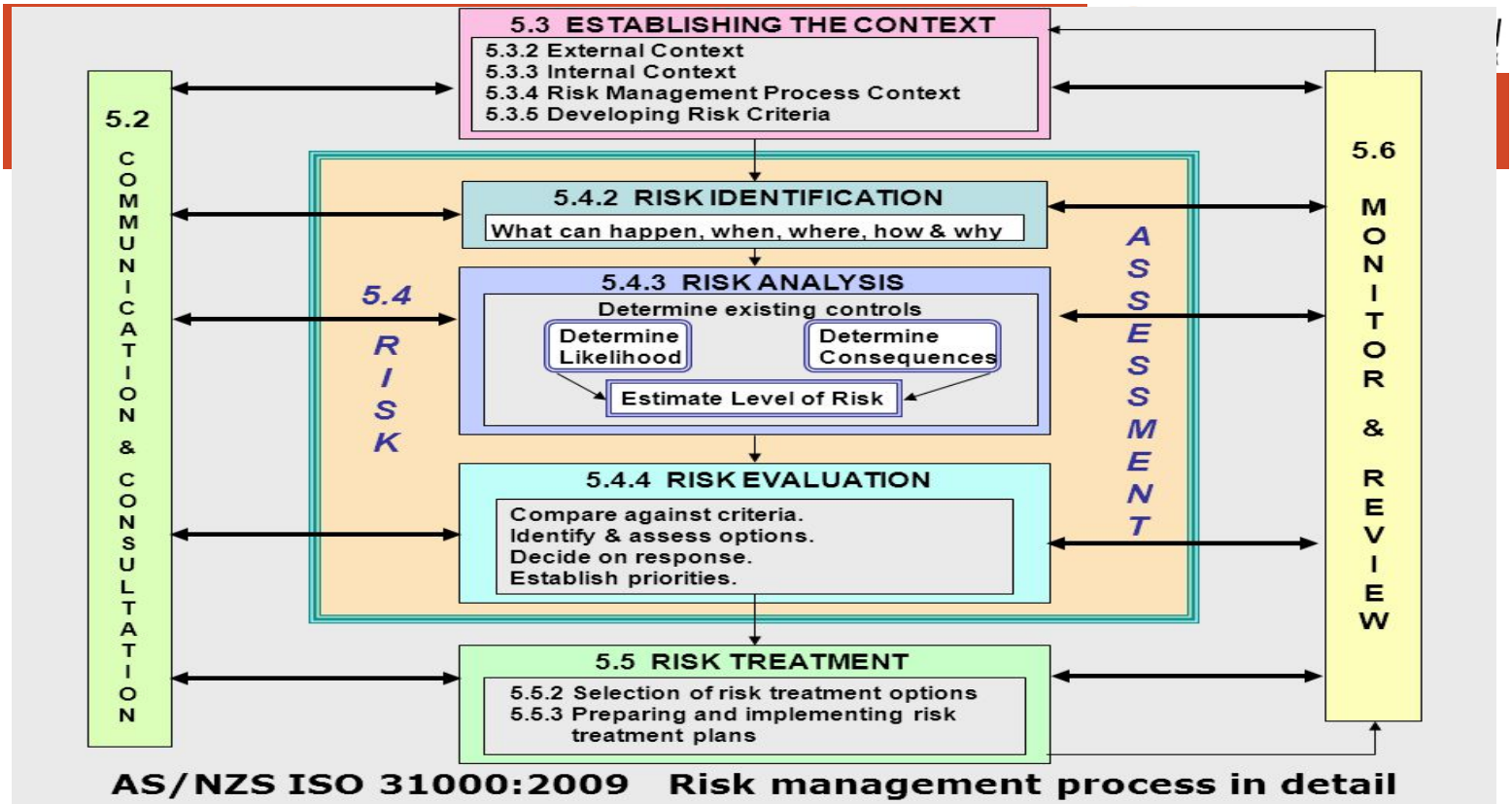
โอกาสที่จะเกิด	ความถี่โดยเฉลี่ย	คะแนน
สูงมาก	1 เดือนต่อครั้งหรือมากกว่า	5
สูง	1-6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้ง	4
ปานกลาง	1 ปีต่อครั้ง	3
น้อย	2-3 ปีต่อครั้ง	2
น้อยมาก	5 ปีต่อครั้ง	1

ผลกระทบด้านทรัพย์สิน/การเงิน

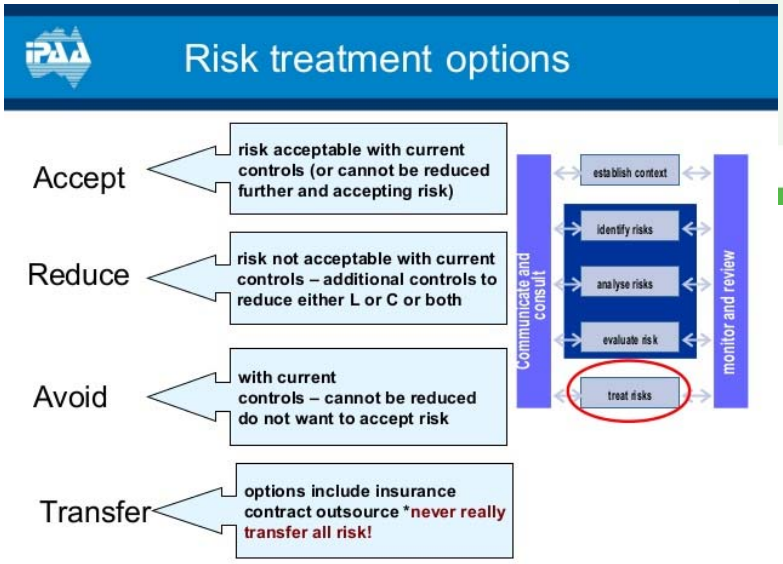
Impact

ระดับผลกระทบ	มูลค่าความเสียหาย	คะแนน
สูงมาก	มากกว่า 1,000,000 บาท	5
สูง	500,001-ไม่เกิน1,000,000 บาท	4
ปานกลาง	100,001-ไม่เกิน500,000 บาท	3
น้อย	10,001-ไม่เกิน100,000 บาท	2
น้อยมาก	ไม่เกิน 10,000 บาท	1

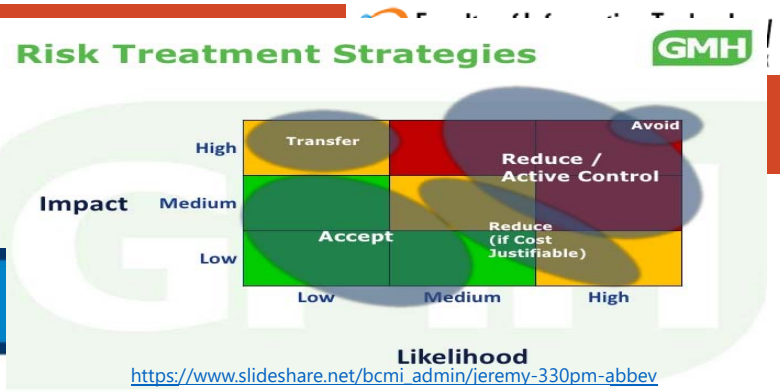
Ref: คู่มือการบริหารความเสี่ยง, องค์การสวนพฤกษศาสตร์ ปี 2551



http://slideplayer.com/slide/5917941/



https://www.slideshare.net/mikaelastafrace/beyond-compliance-37628926



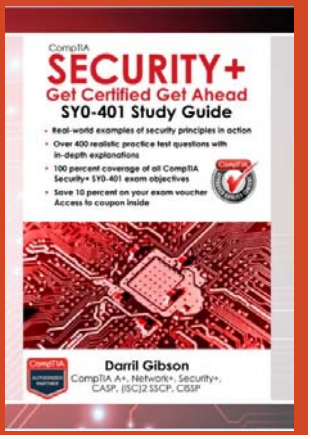
https://www.slideshare.net/bcmi_admin/jeremy-330pm-abbev

http://marketbusinessnews.com/financial-glossary/residual-risk-definition-meaning/

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Exploring Control Types and Methods

CompTIA Security+
Get Certified Get Ahead
By Darril Gibson



Introduction

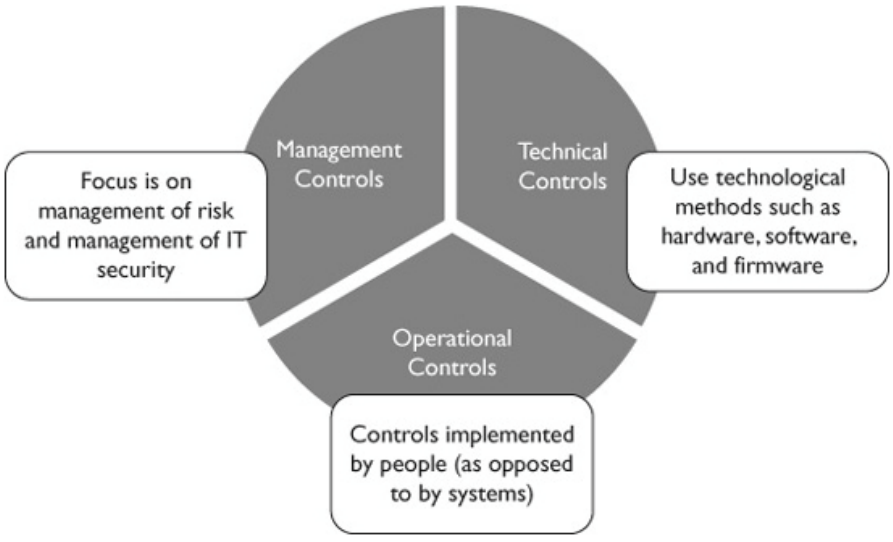
Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- Understanding control types
- Comparing physical security controls
- Implementing logical access controls
- Comparing access control models

Comparing the Classes of Controls

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

NIST Special Publication (SP) 800-53 rev 3 organizes controls into three primary classes:



https://www.safaribooksonline.com/library/view/sscp-systems-security/9780071771566/lev225.html

Faculty of Information Technology

Electrosoft

NIST SP 800-53 Rev 3

ID	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

- **Title**: Recommended Security Controls for Federal Information Systems and Organizations
- **Published:** August 2009
- **Approach**: Risk Management Framework
  - Categorize Information System
  - Select Security Controls
  - Implement Security Controls
  - Assess Security Controls
  - Authorize Information System
  - Monitor Security Controls
- **18 families** of Security Controls

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Control Goals

- Preventive controls
  - Attempt to prevent an incident from occurring
  - Hardening, training, guards, change management, disabling accounts
- Detective controls
  - Attempt to detect incidents after they have occurred
  - Log monitoring, trend analysis, security audit, video surveillance, motion detection
- Corrective controls
  - Attempt to reverse the impact of an incident
  - Active IDS (Intrusion Detection System), backups, system recovery

Control Goals

- Deterrent
  - Attempt to discourage individuals from causing an incident
  - Cable locks, hardware locks
- Compensating
  - Alternative controls used when a primary control is not feasible
  - TOTP (Time-based One-Time Password) instead of smart card

Physical Security Controls

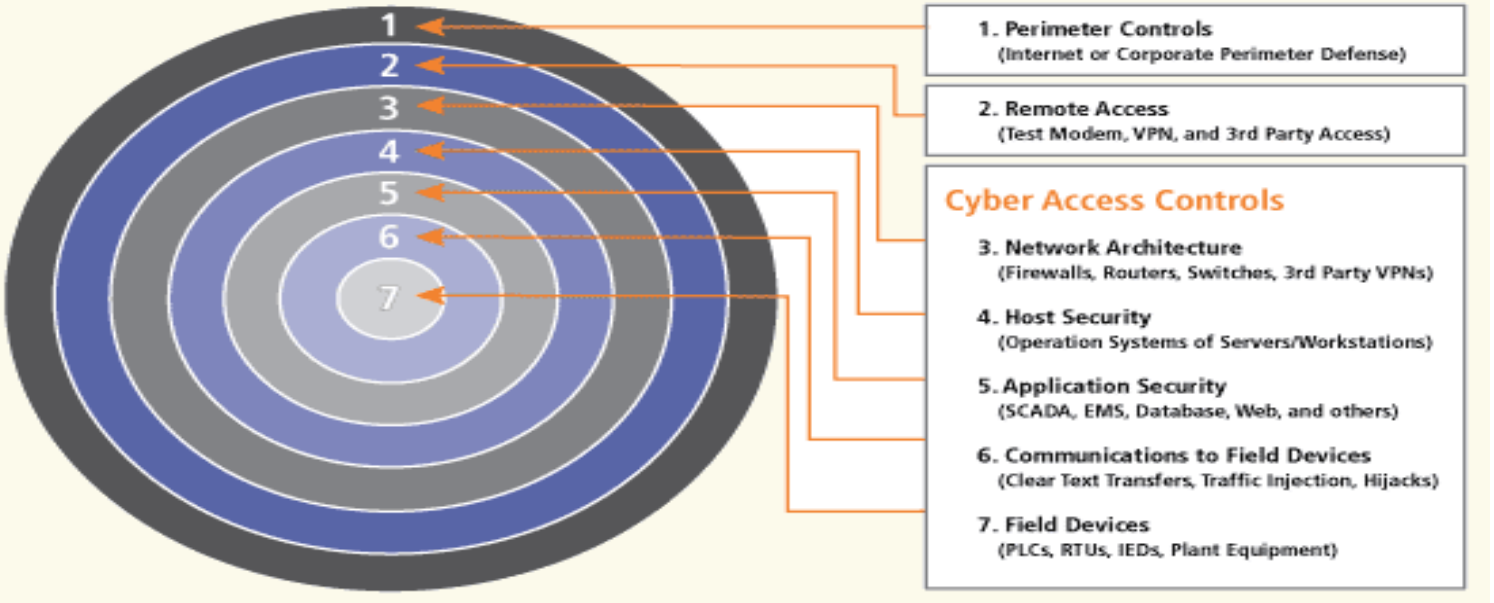
- Defense in depth with boundaries
  - Perimeter
  - Building
  - Secure work areas
  - Server and network rooms
  - Hardware (such as cable locks)

Defence in Depth

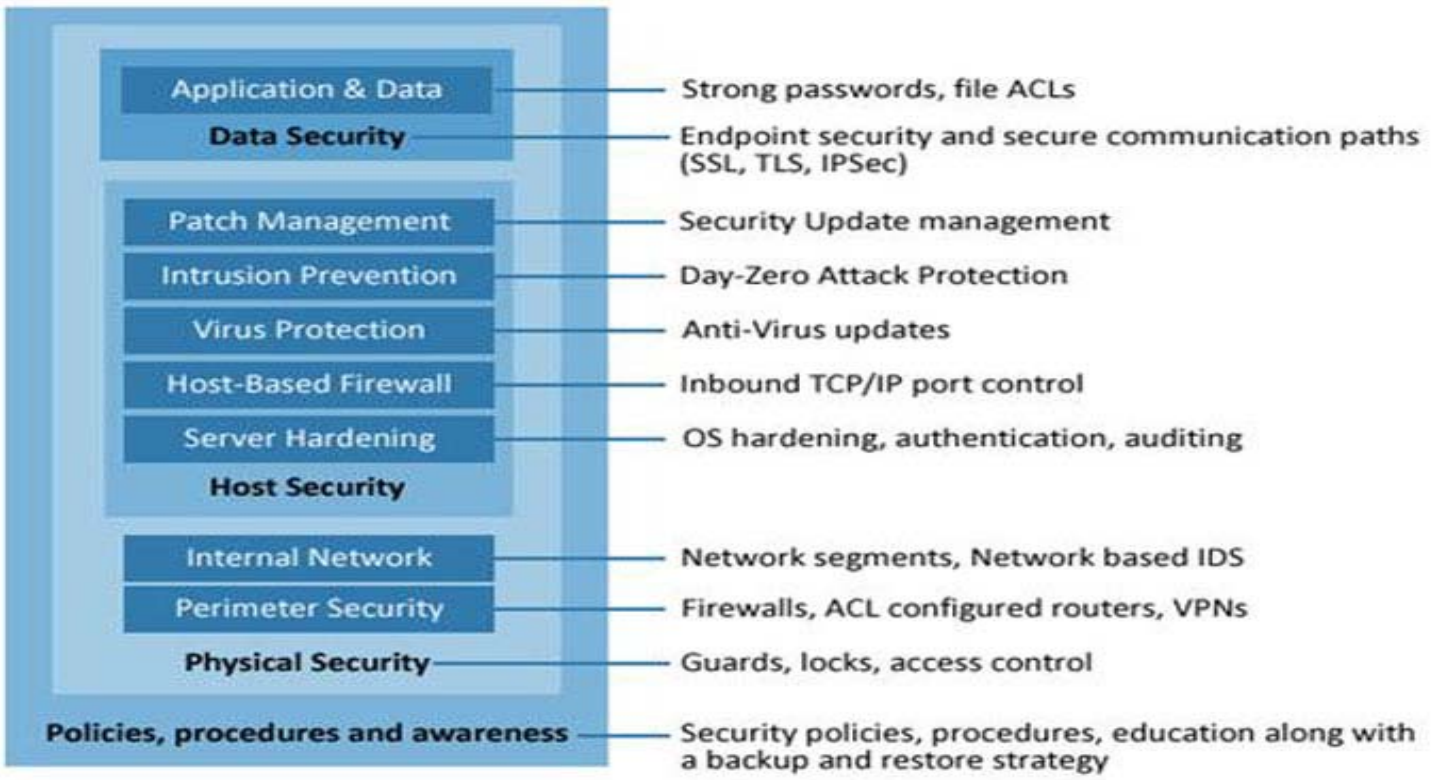
Shepherding Solution Architecture Security Decisions

http://www.slideshare.net/prawsthorne/defen

Layered Security Approach for Vulnerability Risk Assessments



http://www.remote-instruments.com/secure.html



https://www.cyberoam.com/blog/defense-in-depth/

Physical Security Controls

- Door access systems
  - Cipher locks
  - Proximity cards
  - Biometrics
- ID badges

- Tailgating and mantraps
- Security guards, access lists, and logs
- Video surveillance (CCTV)
- Fencing, lighting, and alarms
- Barricades and signs
- Hardware locks
  - Doors, locked cabinets, and safes

Tailgating (also called piggybacking)

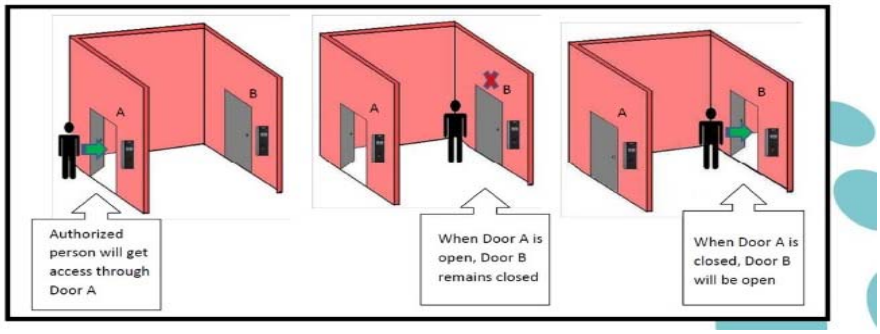
http://www.silvaconsultants.com/the-problem-of-tailgating.html

http://blogs.getcertifiedgetahead.com/tailgating-and-mantraps/

MATRIX SECURITY SOLUTIONS

Man-Trap (Deadman door)

- Useful for Multiple Doors, Arranged in a Sequence
- Regulate Opening and Closing of Doors
- Second Door will Open only After First Door has Closed
- Manage Traffic and Control Dust and Heat
- Useful to Restrict Intruder from Escaping the Premises Quickly



http://www.slideshare.net/GbsHyd1/matrix-cosec-acm-presentation-v1-r1

http://www.edsuk.com/man_trap_air_lock_cylinder_gate.html

Understanding Logical Access Controls (1/3)

Need-to-know

- Subjects should only have access to objects that enables them to perform their assigned job functions.

Least privilege

- Subjects should only have sufficient access privilege that allows them to perform their assigned work.

Understanding Logical Access Controls (2/3)

- Principle of least privilege
  - Rights identify what a user can do, such as changing the system time or rebooting a system
  - Permissions define access to resources, such as being able to read or modify a file
  - Rights and permissions combined called privileges
  - Least privilege ensures users granted only the rights and permissions needed to perform assigned tasks or functions
  - Technical control

หลักการ Least Privilege

- การให้สิทธิ์ (Authorization) เพื่อทำงานใด ๆ ไม่ว่าจะเป็นระดับผู้ใช้ (User) หรือกระบวนการ (Process) ซึ่งเราเรียกรวมกันว่าประธานหรือผู้กระทำ (ใช้ทับศัพท์ว่า Subject or Actor) กระทำการใด ๆ ต่อข้อมูล บริการ (Service) หรือแม้แต่กระบวนการ (Process) ด้วยกันเอง ซึ่งเรียกรวม ๆ กันว่ากรรม (ใช้ทับศัพท์ว่า Object) ซึ่งสามารถเขียนเป็นตัวอย่างการรวมกันของ ประธาน กริยา กรรม ได้เช่น

ประธาน **(Subject)**	กริยา **(Access)**	กรรม **(Object)**
ผู้ใช้ (User) โปรแกรม (Program) กระบวนการ(Process)	อ่าน (Read) เขียน (Write) สั่งให้ทำงาน(Execute)	แฟ้มข้อมูล (File) ฐานข้อมูล(Database) บริการ (Service) กระบวนการ(Process) ทรัพยากร(Resource)

http://narudomr.blogspot.com/2016/01/ssd101-leastprivilege.html
http://narudomr.blogspot.com/2016/01/ssd101-needtoknow.html

หลักการ Least Privilege (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การออกแบบการให้สิทธิ์มีแนวคิดเพื่อความมั่นคงปลอดภัยก็คือการให้สิทธิ์ Subject ดำเนินการต่อ Object น้อยที่สุดเท่าที่จะทำงานได้สำเร็จตามวัตถุประสงค์ หรือที่เรียกว่า Least Privilege เช่น
  - Web Application ซึ่งทำงานกับ Database เพียงแค่ insert, select, update, delete ก็ควรจะสร้าง Database User ให้กับ Web Application นั้นให้มีสิทธิ์เท่าที่ทำงานดังกล่าวได้
  - ไม่ไปล่อยให้ใช้ User ที่มีสิทธิ์สูง เช่น SA, root, SYS หรือ Schema Owner หรือ User ที่สามารถใช้คำสั่งจัดการ Schema ของข้อมูล (DDL: Data Definition Language) เช่น create, alter, drop เป็นต้น

- สิทธิ์ดังกล่าวข้างต้นเป็นสิทธิ์ในเชิงวิธีการเข้าถึง แต่ยังมีในเชิงปริมาณที่ต้องคำนึงถึงคือจำนวนและชนิดของ Object ที่เข้าใช้งาน หลักการ Lease Privilege ก็ครอบคลุมในมิตินี้ด้วย กล่าวคือหาก Subject ไม่มีความจำเป็นที่ต้องทำงานกับ Object ใด ก็ควรห้ามการเข้าถึง Object นั้น ๆ ด้วย

หลักการ Least Privilege (ต่อ)

- การให้สิทธิ์แก่ Subject มากเท่าไรก็เป็นการเพิ่มพื้นที่ในการโจมตี (Attack Surface) ต่อ Object มากเท่านั้นและเมื่อ Subject โดนยึดได้ (Compromised) Object ก็มีโอกาสถูกกระทำตามสิทธิ์ที่ให้แก่ Subject ไว้

- จำไว้เสมอว่า ให้ Subject มีสิทธิ์ยิ่งน้อยเท่าไรความเสี่ยงในการที่ Subject จะถูกสวมรอยเพื่อใช้ทำงานผิดวัตถุประสงค์หรือทำงานผิดพลาดโดยไม่ตั้งใจ (User Error) จะมีน้อยเท่านั้น

หลักการ Need to Know

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การออกแบบซอฟต์แวร์ให้มั่นคงปลอดภัยในในหัวข้อนี้ เป็นเรื่องของการเข้าถึงข้อมูล และเกี่ยวข้องกับเรื่องการรักษาความลับ (Confidentiality) โดยตรง
- หลักการ ถึงแม้ว่าใครก็ตามได้รับอนุญาตให้เข้าถึงข้อมูลไม่ว่าจะเป็นชั้นความลับระดับใดก็ตาม ก็ไม่สามารถเห็นข้อมูลนั้นได้จนกว่าจะมีความจำเป็นที่ต้องรู้ข้อมูล (Need to Know) เพื่อที่จะใช้ในการปฏิบัติงาน และไม่จำเป็นต้องเห็นข้อมูลทุกอย่าง เว้นแต่ข้อมูลที่เกี่ยวข้อง
- ตัวอย่างเช่นในระบบตรวจสอบการให้สินเชื่อ เมื่อทำการยื่นขอกู้แล้วนั้น ข้อมูลของการยื่นกู้มีหลายอย่าง เช่น
  - ข้อมูลผู้กู้ ได้แก่ชื่อ ที่อยู่ทั้งที่บ้านและที่ทำงาน หมายเลขโทรศัพท์ เงินเดือน วงเงินขอกู้ หรือแม้แต่ข้อมูลของผู้ค้ำประกันได้แก่ชื่อ ที่อยู่ เหล่านี้เป็นต้น
  - พนักงานป้อนข้อมูลได้รับอนุญาตให้เข้าถึงข้อมูลเหล่านี้ซึ่งมีชั้นความลับเป็นปกปิด (Restricted) เหมือนกันทุกคนแต่ว่าแต่ละคนจะเห็นข้อมูลเฉพาะรายที่ตนเองได้รับมอบหมายให้ป้อนเท่านั้น ไม่มีสิทธิ์ที่จะอ่านข้อมูลของการยื่นกู้ของรายอื่นที่ไม่ได้ป้อนเข้าไป

หลักการ Need to Know (ต่อ)

- จากระบบตรวจสอบการให้สินเชื่อข้างบน จะมีงานอย่างหนึ่งก็คือการตรวจสอบข้อมูลภาคสนาม พนักงานที่ทำหน้าที่นี้จะมีหน้าที่ตรวจสอบยืนยันข้อมูลบุคคลของผู้ขอกู้ว่าตรงตามที่ยื่นกู้มาหรือไม่เช่นที่อยู่ที่ให้มาได้อยู่จริงหรือไม่ สถานที่ทำงานตามที่แจ้งหรือไม่ สินทรัพย์ค้ำประกันสภาพเป็นเช่นไร พนักงานจะได้รับข้อมูลจากการยื่นกู้ของผู้ยื่นกู้เฉพาะที่ได้รับมอบหมายให้ตรวจสอบ และได้เพียงข้อมูลบางส่วนเพื่อทำงานเท่านั้น เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ ข้อมูลสินทรัพย์ค้ำประกันเป็นต้น แต่จะไม่ได้ข้อมูลวงเงินขอกู้ เงินเดือน หรือข้อมูลผู้ค้ำประกัน เป็นต้น

- Need to Know มักจะถูกใช้สับสนกับ Least Privilege เนื่องจากเป็นเรื่องการควบคุมสิทธิ์เช่นเดียวกัน โดยข้อแตกต่างจะสรุปได้ดังตาราง

ข้อเปรียบเทียบหลักการ Need to Know กับ Least Privilege

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

ข้อเปรียบเทียบ	**Need to Know**	**Least Privilege**
การเข้าถึง	อ่านเท่านั้น	อ่าน เขียน สั่งให้ทำงาน เป็นต้น
Object	ข้อมูลเท่านั้น	ข้อมูล แฟ้ม บริการ กระบวนการ เป็นต้น
Security Foundation	Confidentiality	Confidentiality, Integrity
การควบคุมการเข้าถึงข้อมูล	ระดับ Record & Field	ระดับSchema (อาจถึงระดับ Field)
สิทธิ์	ตามที่ได้รับมอบหมาย (Assignment)	ตามบทบาท(Role)

จำไว้เสมอว่า Subject ควรได้รับข้อมูลเฉพาะที่จำเป็นต้องรู้เพื่อทำงานตามหน้าที่ที่ได้รับมอบหมายเท่านั้น

Understanding Logical Access Controls (3/3)

Separation of duties

- No single person should be responsible for approving his/her own work.

Job rotation

- To reduce risk of collusion and to ensure no single point of failure.

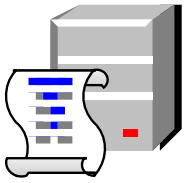
Mandatory vacation

- To allow auditors to review records.

Group Policy

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

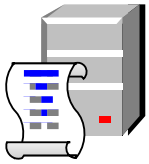
- Implemented on a domain controller
  - Local password policy
  - Domain password policy
  - Application password



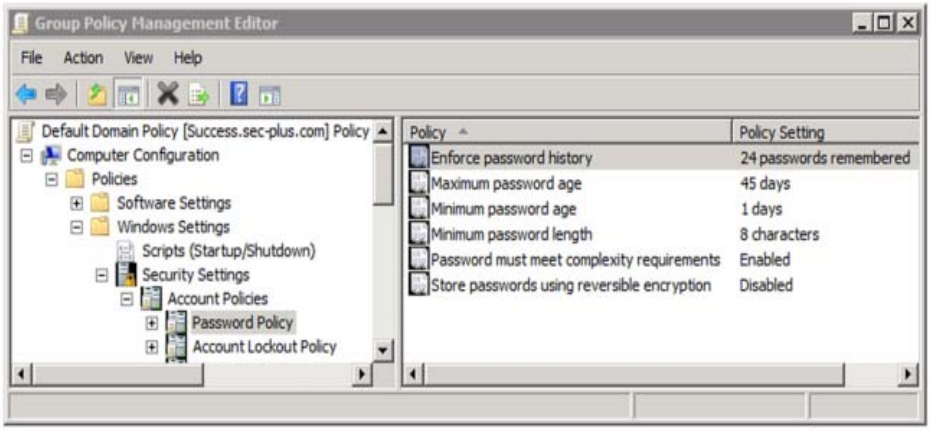
Policy

Domain Password Policy

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements



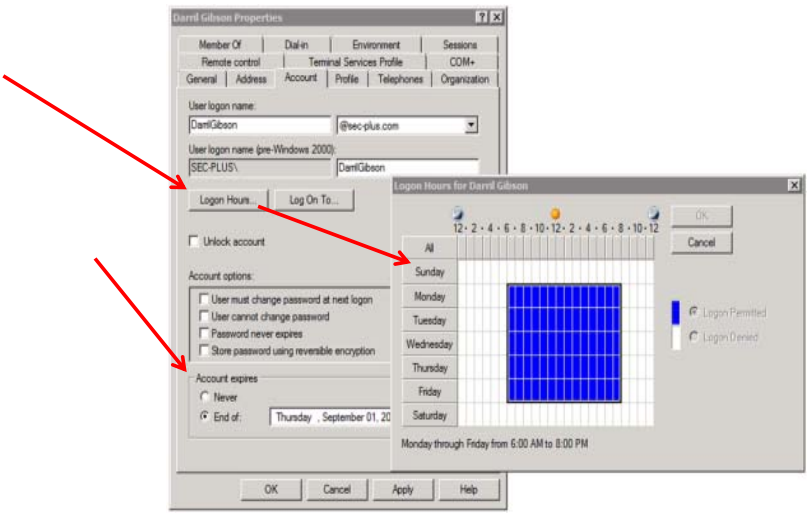
Policy



Account Management

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- Disabling and deleting accounts
- Recovering accounts
- Prohibiting generic accounts
- Time-of-day restrictions
- Account expiration
- Account access review



Comparing Access Control Models

- Role-Based Access Control (RBAC)
  - Uses roles (often implemented as groups)
  - Grant access by placing users into roles based on their assigned jobs, functions, or tasks
  - Often use a matrix

Role	Server Privileges	Project Privileges
Administrators	All	All
Executives	None	All
Project Managers	None	All on assigned projects No access on unassigned projects
Team Members	None	Access for assigned tasks Limited views within scope of their assigned tasks No views outside the scope of their assigned tasks

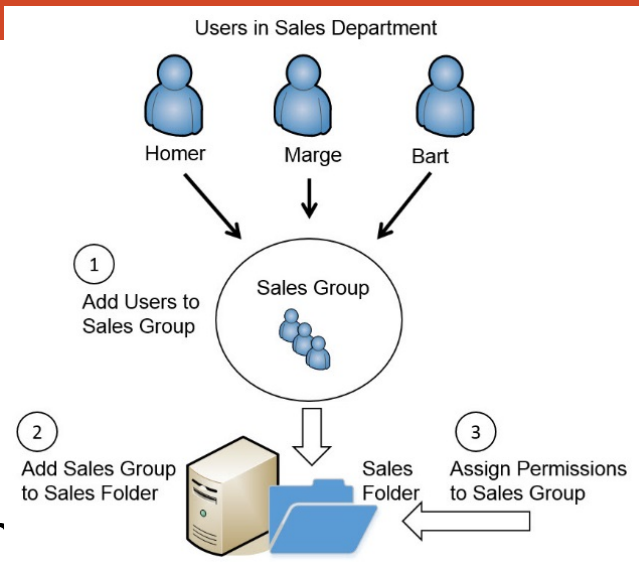
Role-Based Access Control (RBAC)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- A user account is placed into a role or group
- User inherits rights and permissions of the role
- Simplifies administration
- Helps enforce principle of least privilege
- User templates include group membership

Group-Based Privileges

1. Create a Sales group and add each of the user accounts to the Sales group
2. Add the Sales group to the Sales folder
3. Assign appropriate permissior the Sales folder



Comparing Access Control Models

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

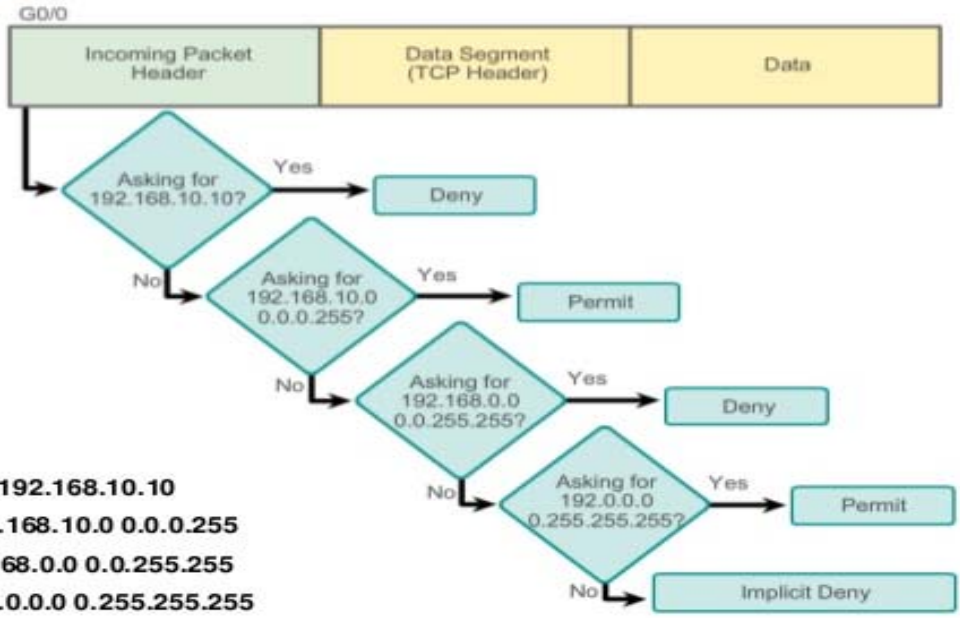
- Rule-Based Access Control
  - Based on a set of approved instructions, such as an access control list
  - Can use triggers to respond to an event

https://www.dokuwiki.org/acl

	Page/Namespace	User/Group	Permissions[1)]
#1	*	@ALL	○ None ○ Read ○ Edit ◉ Create ○ Upload ○ Delete
#2	*	bigboss	○ None ○ Read ○ Edit ○ Create ○ Upload ◉ Delete
#3	devel: *	@ALL	◉ None ○ Read ○ Edit ○ Create ○ Upload ○ Delete
#4	devel: *	@devel	○ None ○ Read ○ Edit ○ Create ◉ Upload ○ Delete
#5	devel: *	bigboss	○ None ○ Read ○ Edit ○ Create ○ Upload ◉ Delete
#6	devel: *	@marketing	○ None ◉ Read ○ Edit ○ Create ○ Upload ○ Delete
#7	devel: funstuff	bigboss	◉ None ○ Read ○ Edit ○ Create ○ Upload ○ Delete
#8	devel: marketing	@marketing	○ None ○ Read ◉ Edit ○ Create ○ Upload ○ Delete
#9	marketing: *	@marketing	○ None ○ Read ○ Edit ○ Create ◉ Upload ○ Delete
#10	start	@ALL	○ None ◉ Read ○ Edit ○ Create ○ Upload ○ Delete

Configure Standard IPv4 ACLs

Configuring a Standard ACL



Example ACL

- access-list 2 deny host 192.168.10.10
- access-list 2 permit 192.168.10.0 0.0.0.255
- access-list 2 deny 192.168.0.0 0.0.255.255
- access-list 2 permit 192.0.0.0 0.255.255.255

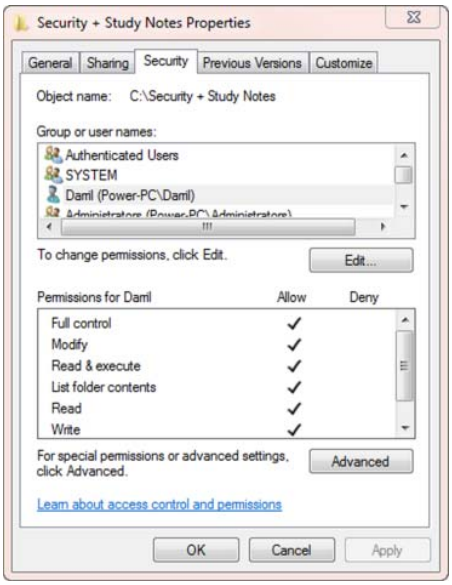
Ref: https://www.slideshare.net/vuzlego/chapter9-access-control-lists

Discretionary Access Control (DAC)

- Resources identified as objects
  - Files, folders, shares
- Specifies that every object has an owner
- Owner has full, explicit control of the object
- Beware of Trojans
  - Dual accounts for administrators

Discretionary Access Control

- Microsoft's NTFS uses the DAC model
- Discretionary access control lists (DACLs, but often shortened to ACLs) form the primary means by which authorization is determined.
  - List of access permissions
- SIDS
  - Uniquely identifies users and groups



Mandatory Access Control

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- Uses labels to determine access
- Subjects and objects are assigned labels
- Permissions granted when the labels match

- SELinux (Security-Enhanced Linux)
  - Uses MAC model
  - Helps prevent malicious or suspicious code from executing

SELinux

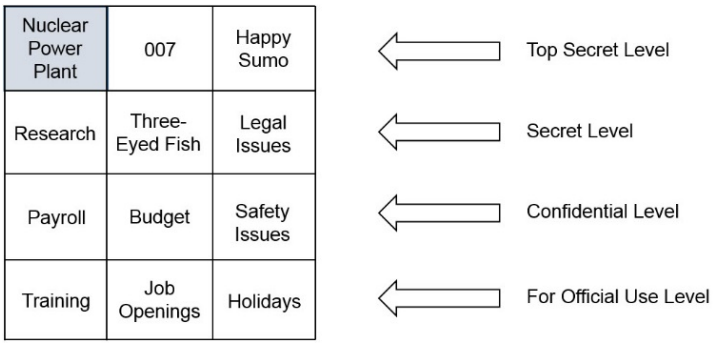
- Selinux เป็นโมดูลรักษาความปลอดภัยของ Linux ที่มีติดมากับระบบปฏิบัติการ Linux
- แต่หลายคนเลือกที่จะปิดการใช้งานเหตุผลเพราะใช้งานยาก
- SELinux ย่อมาจาก Security-Enhanced Linux
- SELinux คือ การเพิ่มประสิทธิภาพการรักษาความปลอดภัยให้กับลินุกซ์ที่ช่วยให้ผู้ใช้และผู้ดูแลระบบทำการควบคุม การควบคุมการเข้าถึง
- SELinux เป็นผลงานการวิจัยของ National Security Agency ของประเทศสหรัฐอเมริกาที่พัฒนาระบบรักษาความปลอดภัยขึ้นมาใช้เป็นการภายใน

http://www.it-know-ledge.com/Linux/

Mandatory Access Control

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- **Lattice**
- Imagine that Homer has a Top Secret clearance with a Nuclear Power Plant label.
- This gives him access to data within the Nuclear Power Plant compartment.
- However, he does not have access to data in the 007 or Happy Sumo compartment unless he also has those clearances (and associated labels).
- Higher-level clearances include lower-level clearances.
- For example, because Homer has a Top Secret clearance, he can be granted access to Secret and lower-level data.
- Again though, he will only be able to access data on these lower levels based on his need to know.



Lattice

- As another example, imagine that Lisa has a Secret level clearance.
- Administrators can grant her access to data on the Secret level and lower levels, based on her need to know.
- For example, they might grant her access to the Research data by assigning the Research label to her, but not necessarily grant her access to Three-Eyed Fish or Legal Issues data.
- However, they cannot grant her access to any data on the Top Secret level.

Summary

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- Understanding control types
- Comparing physical security controls
- Implementing logical access controls
- Comparing access control models

ตัวอย่างสิ่งที่ต้องพิจารณาในการตรวจสอบ

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

Physical Access Control กับความมั่นคงปลอดภัยตาม ISO 27001:2013

- เจ้าของสถานที่หรือผู้บริหารองค์กรจะต้องพิจารณาเลือกใช้งานอย่างรอบคอบและเหมาะสมกับสภาพแวดล้อมและเงื่อนไขของตนเอง โดยคำนึงถึงความเสี่ยงและความมั่นคงปลอดภัยเป็นหลัก

http://destinationonecounselor.blogspot.com/2015/03/physical-access-control-ISO -270012013.html

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

1. ตำแหน่งที่ติดตั้ง เป็นจุดเริ่มต้นที่สำคัญในการบริหารจัดการระบบ Physical Access Control การตัดสินใจเลือกตำแหน่งที่ติดตั้งอย่างถูกต้องเหมาะสมจะช่วยเพิ่มประสิทธิภาพในการจัดการ และเสริมความมั่นคงปลอดภัยมากยิ่งขึ้น
2. ประเภท การเลือกประเภทของระบบ Physical Access Control นั้น จะต้องพิจารณาตามความเสี่ยงของพื้นที่ และความเหมาะสมในการใช้งาน อาทิ การใช้บัตร Smart Card, การสแกนลายนิ้วมือ, การสแกนรูม่านตา เป็นต้น
3. การกำหนดสิทธิ์การเข้าถึงพื้นที่ พนักงานทุกคนไม่สมควรได้รับสิทธิ์ในการเข้าถึงพื้นที่ที่ไม่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของตนเอง ดังนั้น เพื่อให้สอดคล้องตามมาตรการด้านความมั่นคงปลอดภัย เจ้าของพื้นที่จึงควรจะมีการจำกัดสิทธิ์การเข้าถึงให้เฉพาะผู้ที่จำเป็นเท่านั้น

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

4. ระยะเวลาการจัดเก็บข้อมูล จำเป็นต้องมีการเก็บบันทึกข้อมูลการผ่านเข้าออกไว้อย่างน้อยเป็นระยะเวลา 90 วัน หรือพิจารณาให้สอดคล้องกับวัตถุประสงค์และความต้องการด้านความมั่นคงปลอดภัยขององค์กรเป็นหลัก
5. การตั้งค่าเวลา เวลาของระบบ Access Control จะต้องได้รับการตั้งค่าตามหน่วยเวลามาตรฐานสากล รวมถึงสอดคล้องกับระบบอื่นๆ ที่เกี่ยวข้อง เพื่อให้สามารถอ้างอิงและตรวจสอบได้หากมีการสืบสวนเกิดขึ้น และจะต้องได้รับการทบทวนความเที่ยงตรงของค่าเวลาอย่างสม่ำเสมอ
6. การเฝ้าระวัง การติดตั้งระบบ Access Control นั้นจะไม่เกิดประโยชน์อย่างใดเลยหากขาดการเฝ้าระวัง และจะต้องมีการกำหนดขั้นตอนการปฏิบัติงานอย่างเหมาะสม เช่น หากพบตรวจพบความผิดปกติจะต้องแจ้งไปยังใคร ผ่านทางช่องทางใด วิธีการแจ้งเป็นอย่างไร เป็นต้น

10 สิ่งสำคัญที่ต้องพิจารณาในการบริหารจัดการระบบ Access Control (ต่อ)

7. พนักงาน จะต้องมีการตระหนักรู้และมีความตื่นตัวด้านความมั่นคงปลอดภัยอยู่ตลอดระยะเวลาในการปฏิบัติงาน และจะต้องหมั่นสังเกต ตั้งข้อสงสัยอยู่เสมอ เพื่อตรวจหาความผิดปกติ
8. การสำรองข้อมูล แนวทางในการสำรองข้อมูลนั้นจะขึ้นอยู่กับความจำเป็นและความเสี่ยงของแต่ละพื้นที่ และจะต้องมีการกำหนดขั้นตอนในการสำรองข้อมูล เช่น ประเภทของสื่อบันทึกข้อมูล ระยะเวลาการจัดเก็บข้อมูลสำรอง การดูแลรักษาข้อมูลสำรอง ฯลฯ อย่างมั่นคงปลอดภัยอีกด้วย
9. โปรแกรม/ซอฟต์แวร์ ที่ใช้เพื่อจัดการระบบ Access Control นั้น จะต้องใช้งานได้ง่ายและมีความมั่นคงปลอดภัย โดยจะต้องผ่านการตรวจหาจุดอ่อนและช่องโหว่อย่างสม่ำเสมอ และจะต้องมีการจัดการผู้ใช้งาน, รหัสผ่าน รวมถึงมีการทบทวนประวัติการเข้าใช้งานอย่างรอบคอบเหมาะสม
10. สัญญาการให้บริการ องค์กรจะต้องมีการกำหนดข้อตกลงในสัญญาการให้บริการของผู้ให้บริการภายนอกที่ดูแลอุปกรณ์และระบบ Access Control อย่างเหมาะสม เช่น มีการกำหนดรอบระยะเวลาการบำรุงรักษา เงื่อนไขการแก้ปัญหาหากระบบเกิดการหยุดชะงัก เป็นต้น โดยจะต้องคำถึงความต้องการด้านความมั่นคงปลอดภัยเป็นสำคัญเสมอ

การบริหารจัดการระบบ CCTV อย่างมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ในปัจจุบันมีการใช้งานระบบ CCTV เพื่อเพิ่มความมั่นคงปลอดภัยตามสถานที่ต่าง ๆ ทั้งสถานที่ราชการ สำนักงาน เอกชน ร้านค้า รวมถึงที่พักอาศัย ซึ่งระบบ CCTV เองนั้นก็มีความหลากหลายแตกต่างกันไป ดังนั้น ผู้บริหารขององค์กรหรือเจ้าของสถานที่จึงจำเป็นที่จะต้องพิจารณาเลือกติดตั้ง CCTV ชนิดที่มีความเหมาะสมกับสภาพแวดล้อมและเงื่อนไขของตนเอง
- ข้อมูลที่น่าสนใจเพื่อประกอบการบริหารจัดการระบบ CCTV ของเราให้มีความมั่นคงปลอดภัย และสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 มีดังต่อไปนี้

http://destinationonecounselor.blogspot.com/2015/03/cctv-ISO -270012013.html

12 สิ่งที่ต้องให้ความสำคัญเมื่อมีการติดตั้งระบบ CCTV

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

1. ตำแหน่งที่ติดตั้งกล้อง เป็นสิ่งแรกสุดที่เราต้องพิจารณาให้ความสำคัญ เพราะตำแหน่งการติดตั้งที่ถูกต้องจะช่วยให้เราสามารถบันทึกภาพได้อย่างมีประสิทธิภาพ
2. ประเภทของกล้อง ควรเลือกให้เหมาะสมตามระดับความเสี่ยงของพื้นที่ เช่น กล้องปกติ, กล้องที่มีเซ็นเซอร์จับการเคลื่อนไหว, กล้องแบบที่ถูกดัดแปลงรูปลักษณ์ไม่ให้ทราบว่าเป็นกล้อง เป็นต้น
3. ความละเอียดและความคมชัด จะต้องเลือกให้สัมพันธ์กับระดับความเสี่ยงของพื้นที่
4. มุมมองของกล้อง จะต้องกำหนดว่าในพื้นที่บริเวณนั้น จำเป็นจะต้องจับภาพเป็นมุมกว้างเท่าไร ถ้าหากมุมมองของกล้องยังไม่ครอบคลุมพื้นที่ อาจจะต้องพิจารณาเพิ่มจำนวนกล้องที่ติดตั้ง

12 สิ่งที่ต้องให้ความสำคัญเมื่อมีการติดตั้งระบบ CCTV (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

5. ระยะเวลาการจัดเก็บข้อมูลภาพ ควรจะจัดเก็บข้อมูลเอาไว้อย่างน้อยไม่ต่ำกว่า 90 วัน หรือสอดคล้องตามงบประมาณขององค์กร
6. การตั้งค่าเวลา ควรจะตั้งค่าเวลาของกล้องให้สอดคล้องตามเวลาสากล รวมถึงตรวจสอบค่าเวลาของทุกระบบขององค์กรให้ถูกต้องตรงกันอีกด้วย
7. การควบคุมการเข้าถึง ต้องมีการควบคุม และตรวจสอบผู้ที่ต้องการเข้าถึงหรือใช้งานระบบอย่างเข้มงวด เพื่อปกป้องความถูกต้องของข้อมูลภาพที่ระบบ CCTV บันทึกไว้
8. การตรวจสอบและเฝ้าระวัง ข้อมูลภาพที่บันทึกไว้นั้นจะไม่มีประโยชน์ใดๆ เลย หากไม่มีการตรวจสอบและเฝ้าระวังสิ่งผิดปกติอย่างเหมาะสม ดังนั้น จึงควรจะมีการกำหนดขั้นตอนการปฏิบัติงานอย่างชัดเจน

12 สิ่งที่ต้องให้ความสำคัญเมื่อมีการติดตั้งระบบ CCTV (ต่อ)

9. การสำรองข้อมูล จะต้องมีการพิจารณาวิธีการสำรองข้อมูล ระยะเวลาการเก็บบันทึกข้อมูลสำรอง อย่างเหมาะสมตามระดับความเสี่ยง และจะต้องมีการตรวจสอบความถูกต้องและความพร้อมใช้งานของข้อมูลสำรองตามรอบระยะเวลาเพื่อความมั่นใจอีกด้วย

10. ซอฟต์แวร์หรือระบบบริหารจัดการ จะต้องได้รับการพิจารณาว่าสามารถใช้งานได้ง่ายหรือไม่ สามารถตั้งค่าให้เหมาะสมกับการใช้งานได้หรือเปล่า และมีจุดอ่อนหรือช่องโหว่ใด ๆ หรือไม่

11. บุคลากร จะต้องมีทักษะความรู้และมีความตื่นตัวเกี่ยวกับความมั่นคงปลอดภัยอยู่ตลอดเวลา และต้องหมั่นสังเกตหรือตั้งข้อสงสัยอยู่เสมอ

12. สัญญาการให้บริการ องค์กรจะต้องกำหนดข้อตกลงในการให้บริการของผู้ให้บริการภายนอกอย่างชัดเจน เช่น กำหนดรอบระยะเวลาบำรุงรักษา การจัดหาอุปกรณ์สำรอง เป็นต้น

หลากหลายคำถามที่องค์กรต้องตอบเพื่อป้องกันปัญหา “ข้อมูลรั่วไหล”

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ในปัจจุบัน “ข้อมูลรั่วไหล” กลายเป็นปัญหาพื้นฐานที่ทุกองค์กรต้องเผชิญ ไม่ว่าจะเป็นองค์กรขนาดเล็กหรือขนาดใหญ่ แม้ว่าจะมีการจัดซื้อหรือใช้งานเทคโนโลยีที่ทันสมัยและเข้มแข็งมากสักเพียงใด ก็ยังคงไม่สามารถหลีกเลี่ยงความเสี่ยงของการรั่วไหลของข้อมูลได้ เพราะสาเหตุอาจจะเกิดจากความพยายามโจมตีจากผู้มุ่งร้าย การทำงานที่ประมาทเลินเล่อของบุคลากร ฯลฯ ซึ่งล้วนแต่นำมาซึ่งผลเสียหาย

- ดังนั้น แนวทางการแก้ปัญหาข้อมูลรั่วไหลที่ดีที่สุด ก็คือการป้องกันการเกิดเหตุ และการลดผลกระทบที่อาจจะเกิดขึ้นจากเหตุนั้น - จึงนำเสนอ “รายการคำถาม” เพื่อให้ผู้บริหารของทุกองค์กรได้พิจารณา คำถามเหล่านี้จะช่วยให้เราได้ทบทวนการดำเนินการและการปฏิบัติงานต่าง ๆ ในระหว่างค้นหาคำตอบ ซึ่งจะเป็นประโยชน์ต่อการวางแผนพัฒนาและปรับปรุงต่อไป

http://destinationonecounselor.blogspot.com/2015/03/blog-post.html

คำถามที่องค์กรต้องตอบเพื่อเป็นการป้องกันหรือเตรียมการในการรับมื (ต่อ)

- องค์กรมีการจัดลำดับชั้นความลับอย่างไร
- องค์กรกำหนดวิธีในการดูแลรักษาและการใช้งานข้อมูลตามชั้นความลับอย่างไร
- องค์กรมีการควบคุมการเข้าถึงอย่างไร
- องค์กรมีมาตรฐานรหัสผ่านอย่างไร
- องค์กรมีนโยบายการนำข้อมูลหรือทรัพย์สินเข้าออกพื้นที่อย่างไร
- องค์กรมีการควบคุมการเข้าถึงพื้นที่ทางกายภาพอย่างไร
- องค์กรมีการติดตั้งระบบกล้องวงจรปิดอย่างไร
- องค์กรมีการมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศอะไรบ้าง
- องค์กรมีการกำหนดกฎระเบียบการใช้งานทรัพย์สินแต่ละประเภทอย่างไร
- องค์กรมีการควบคุมการใช้งานสื่อบันทึกข้อมูลอย่างไร
- องค์กรมีการทำลายข้อมูลอย่างมั่นคงปลอดภัยอย่างไร

คำถามที่องค์กรต้องตอบเพื่อเป็นการป้องกันหรือเตรียมการในการรับมื (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- องค์กรมีการเข้ารหัสข้อมูลสำคัญอย่างไร
- องค์กรมีการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยอย่างไร
- องค์กรมีการบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยอย่างไร
- องค์กรมีการบริหารจัดการการเปลี่ยนแปลงอย่างไร
- องค์กรมีการทบทวนประวัติการเข้าถึง ประวัติการใช้งานระบบและเหตุการณ์ต่างๆ ทางด้านความมั่นคงปลอดภัยอย่างไร
- องค์กรมีวิธีการในการคัดเลือกหรือตรวจสอบประวัติของพนักงานอย่างไร
- องค์กรมีการให้พนักงานลงนามในเอกสารสัญญาการรักษาความลับของข้อมูลอย่างไร
- องค์กรมีการสร้างความตระหนักรู้และให้ความรู้ทางด้านความมั่นคงปลอดภัยอย่างไร
- องค์กรมีบทลงโทษในกรณีมีการละเมิดความมั่นคงปลอดภัยอย่างไร

การตั้งคำถามเป็นจุดเริ่มต้นของการพัฒนาปรับปรุงที่ดีเสมอ!!

ISO/IEC 27001

- การควบคุมความมั่นคงของข้อมูลนั้นจำเป็นต้องใช้ทรัพยากรในการดำเนินการ ผู้บริหารขององค์กรย่อมคาดหวังให้วิธีการควบคุมนั้นได้ผลตามวัตถุประสงค์ และคุ้มค่ากับงบประมาณที่ได้ลงทุนไป ยกตัวอย่างเช่น การติดตั้งโปแกรมป้องกันไวรัสต้องสามารถลดอัตราความเสี่ยงที่ข้อมูลสำคัญในเครื่องคอมพิวเตอร์จะถูกโจมตีจากไวรัสต่าง ๆ โดยมีค่าบำรุงรักษาและค่าลิขสิทธิ์ของโปรแกรมอยู่ภายในงบประมาณที่ได้กำหนดไว้

- ฉะนั้น เพื่อให้ทราบว่าวิธีการควบคุมความมั่นคงของข้อมูลต่าง ๆ ที่องค์กรนำมาใช้นั้นบรรลุตามวัตถุประสงค์ และความคาดหวังหรือไม่ องค์กรจึงต้องมีการนำเครื่องมืออย่างหนึ่งมาใช้ ซึ่งก็คือ “การวัดประสิทธิผลของการควบคุมความมั่นคงของข้อมูล” (Effectiveness Measurement) นั่นเอง

http://www.acinfotec.com/2008/08/14/การควบคุมความมั่นคงของ

ISO/IEC 27001 (ต่อ)

- การวัดมีจุดประสงค์เพื่อให้ได้ผลที่มีความถูกต้องแม่นยำ และสามารถนำมาใช้ในการเปรียบเทียบได้
- การวัดที่ดีต้องมีการอ้างอิงกับมาตรฐานอย่างหนึ่งอย่างใดเสมอ ยกตัวอย่างเช่น การวัดความยาวโดยอ้างอิงมาตรฐานระบบเมตริก
- ต้องนำวิธีการ และเครื่องมือสำหรับการวัดที่เหมาะสมมาใช้งานอีกด้วย เช่น การใช้ไม้บรรทัดวัดความยาวที่ต้องการความแม่นยำในระดับเซนติเมตร หรือใช้เวอร์เนียวัดความยาวเมื่อต้องการความแม่นยำในระดับมิลลิเมตร เป็นต้น
- การวัดประสิทธิผลของวิธีการควบคุมความมั่นคงของข้อมูลอาศัยหลักการดังกล่าวข้างต้น และได้รับการบรรจุให้เป็นหนึ่งในข้อกำหนดของมาตรฐาน ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems – Requirements

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหน ISO/IEC 27001 (ต่อ)

- องค์กรจำเป็นต้องกำหนดตัววัด (Metric) สำหรับแต่ละวิธีการควบคุมที่ต้องการวัดประสิทธิผล เพื่อให้การวัดประสิทธิผลมีความถูกต้องแม่นยำ และได้ผลลัพธ์ที่ตรงกันไม่ว่าการวัดนั้นได้รับการดำเนินการโดยผู้ใดก็ตาม โดยตัววัดจะต้องประกอบไปด้วย 3 ส่วนหลัก ดังนี้

1. รายละเอียดของวิธีการควบคุมความมั่นคงของข้อมูลที่ต้องการวัดประสิทธิผล เป็นการระบุรายละเอียดที่จำเป็นเกี่ยวกับวิธีการควบคุมที่องค์กรต้องการวัดประสิทธิผล เช่น ชื่อวิธีการควบคุม วัตถุประสงค์ และขอบเขตของการวัดผลประสิทธิผล เป็นต้น
2. รายละเอียดของวิธีการที่ใช้ในการวัดประสิทธิผล เป็นการระบุรายรายละเอียดที่จำเป็นเกี่ยวกับวิธีการที่องค์กรนำมาใช้ในการวัดประสิทธิผล เช่น แหล่งข้อมูลที่จะนำมาใช้ วิธีการรวบรวมข้อมูล ตารางเวลาที่จะทำการวัดประสิทธิผล ผู้รับผิดชอบ และวิธีการประมวลผลข้อมูล เป็นต้น

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหน ISO/IEC 27001 (ต่อ)

3. การตั้งเป้าหมาย เป็นการกำหนดระดับของผลการวัด เพื่อใช้เป็นตัวชี้วัดว่าวิธีการควบคุมความมั่นคงของข้อมูลนั้นบรรลุตามวัตถุประสงค์หรือไม่ เช่น การวัดประสิทธิผลของการฝึกอบรมด้วยการทดสอบความรู้ความเข้าใจของพนักงาน หากได้คะแนนเฉลี่ยมากกว่าเป้าหมายที่ 80% หมายถึง การฝึกอบรมนั้นบรรลุตามวัตถุประสงค์ หรือ การวัดด้วยจำนวนชั่วโมงของการฝึกอบรมด้านความมั่นคงของข้อมูล โดยในปีแรกกำหนดเป้าหมายเป็น 10 ชั่วโมง/คน/ปี และปีที่สองกำหนดเป็น 15 ชั่วโมง/คน/ปี หากผลการวัดเป็นไปตามเป้าหมายนี้ ถือว่าการวางแผนและการจัดฝึกอบรมนั้นบรรลุตามวัตถุประสงค์

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหน ISO/IEC 27001 (ต่อ)

- การกำหนดตัววัดประสิทธิผลของการควบคุมความมั่นคงของข้อมูลนั้น ต้องได้รับการพิจารณาอย่างรอบคอบโดยผู้เกี่ยวข้องแต่ละฝ่ายภายในองค์กรอย่างเหมาะสม
- เพื่อให้ตัววัดนั้นสามารถสะท้อนให้เห็นประสิทธิผลของวิธีการควบคุมความมั่นของข้อมูลได้อย่างแท้จริง
- ต้องระมัดระวังไม่ให้วิธีการวัดสลับซับซ้อนจนเกินไป และไม่กำหนดเป้าหมายสูง หรือต่ำจนเกินไป ฯลฯ อันเป็นปัญหาที่พบบ่อยครั้งในการกำหนดรายละเอียดของตัววัด

การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหน ISO/IEC 27001 (ต่อ)

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- การวัดประสิทธิผลของการควบคุมความมั่นคงของข้อมูลมีประโยชน์หลายประการ เช่น การแสดงให้เห็นถึงประสิทธิผลของวิธีการควบคุมความมั่นคงของข้อมูลว่าเป็นไปตามที่ต้องการหรือไม่

- การแสดงให้เห็นถึงแนวโน้มการพัฒนาของวิธีการควบคุมความมั่นคงของข้อมูลว่าดีขึ้นหรือด้อยลงเมื่อเปรียบเทียบผลการวัดในแต่ละช่วงเวลา ซึ่งผู้บริหารสามารถนำมาใช้เป็นข้อมูลประกอบการตัดสินใจในการจัดสรรงบประมาณ และทรัพยากรสนับสนุนสำหรับแต่ละส่วนงานได้อย่างเหมาะสม

- นอกจากนี้ ผลการวัดยังสามารถยืนยันได้ว่า องค์กรมีการควบคุมความมั่นคงของข้อมูลในระดับที่ดี และมีการวัดประสิทธิผลเพื่อการปรับปรุงอยู่อย่างสม่ำเสมอ

บทสรุป

- ISO/IEC27001 (Information Security Management System: ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่าง ๆ กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO/IEC (The International Electrotechnical Commission)
- ในการจัดทำระบบบริหารจัดการ (Management System) จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง
  - การบริหารคน (ภายในองค์กรและภายนอก เช่น Outsource)
  - กระบวนการและเทคโนโลยี (เข้าใจกระบวนการทำงาน และเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน)
  - บริหารงบประมาณ (การลงทุนที่คุ้มค่า)
- ต้องเข้าใจทั้ง 3 ด้าน เพื่อที่จะหาจุดสมดุลและเกิดประโยชน์สูงสุด

อ้างอิง

Faculty of Information Technology
King Mongkut's University of Technology North Bangkok

- ปริญญา หอมเอนก, เรื่องน่ารู้เกี่ยวกับความหมาย มุมมองที่เหมือนและแตกต่างของ “การตรวจสอบภายใน” (Internal Audit), “การตรวจสอบระบบสารสนเทศ” (IT Audit) และ “การตรวจสอบด้านความปลอดภัยข้อมูล” (Information Security Audit), จุลสาร สตท. ฉบับที่ 51 ประจำเดือน มกราคม - มีนาคม 2552
- รีวิว ISO/IEC 27001: 2013 - ตอนที่1 พื้นฐานความมั่นคงปลอดภัยของสารสนเทศ, Pryn Sereepong, 14 มกราคม พ.ศ. 2557 http://www.club27001.com/2014/01/review-ISO/IEC 27001 -2013-part1.html
- รีวิว ISO/IEC 27001:2013 - ตอนที่2 ความสำคัญของการประเมินความเสี่ยงสารสนเทศ, Pryn Sereepong, 20 มกราคม พ.ศ. 2557 http://www.club27001.com/2014/01/ISO/IEC 27001 -2013-Information-Risk-Assessment.html
- Overview ข้อกำหนด ISO/IEC 27001:2013 ตอนที่ 1, Pryn Sereepong, 3 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/27001-2013-requirement-overview-part1.html
- Overview ข้อกำหนด ISO/IEC 27001:2013 ตอนที่2 (จบ), Pryn Sereepong, 5 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/ISO -27001-Requirement-overview-part2.html
- บันได 4 ขั้นสู่มาตรฐาน ISO/IEC 27001 Information Security Managment, Pryn Sereepong, 25 สิงหาคม พ.ศ. 2556 http://www.club27001.com/2013/08/4-ISO iec-27001.html
- แนวทางการทำแผนจัดการความเสี่ยง ISO/IEC 27001 (Risk Treatment Plan), Pryn Sereepong, 11 เมษายน พ.ศ. 2557 http://www.club27001.com/2014/04/risk-treatment-plan.html
- มาตรการ (Control) จัดการความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001: 2013, Pryn Sereepong, 9 กุมภาพันธ์ พ.ศ. 2557 http://www.club27001.com/2014/02/ISO -27001-2013-Controls-requirement.html