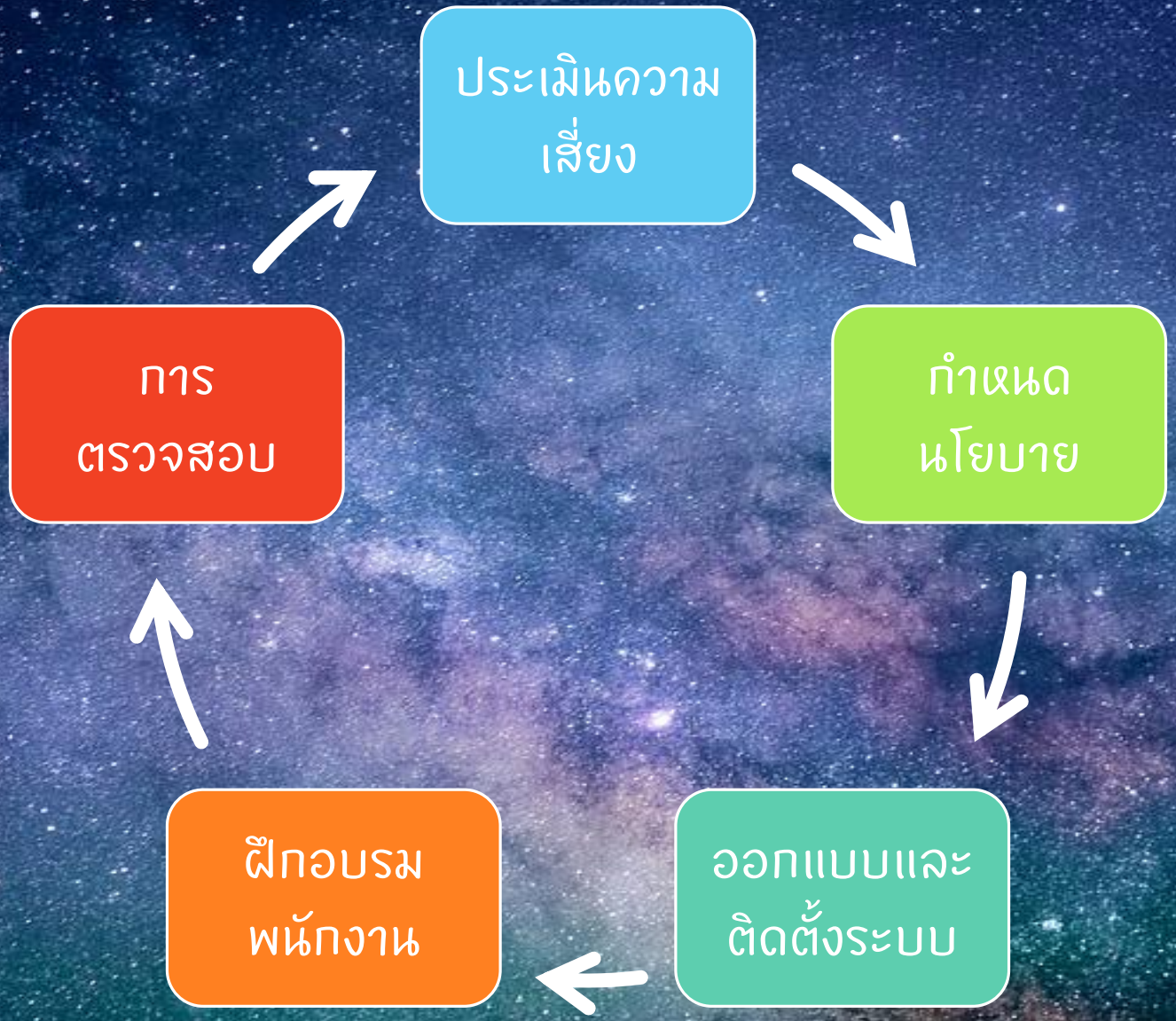
บทที่ 2 : การกำกับดูแลการรักษาความปลอดภัย (IT Security Governance)

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

กระบวนการรักษาความปลอดภัย



Outline

- มาตรฐาน COBIT, ITIL, ISO/IEC 27001
- นโยบายด้านการรักษาความปลอดภัยข้อมูล
- การสร้างความตระหนักรู้ด้านการรักษาความปลอดภัย
- การตรวจสอบด้านการรักษาความปลอดภัย
- อุปสรรคของงานด้านความมั่นคงขอ

การกำกับดูแลการรักษาความปลอดภัย (IT Security Governance)

แต่ละองค์กรสามารถดำเนินการตามกรอบมาตรฐาน เพื่อให้ครอบคลุมความปลอดภัยทุกด้าน โดยเลือกใช้กรอบมาตรฐานที่เหมาะสมกับวัฒนธรรมและธรรมชาติขององค์กร

มาตรฐานที่นิยมคือ COBIT, ITIL, ISO27001

COBIT (Control Objective for Information and Related Technology)

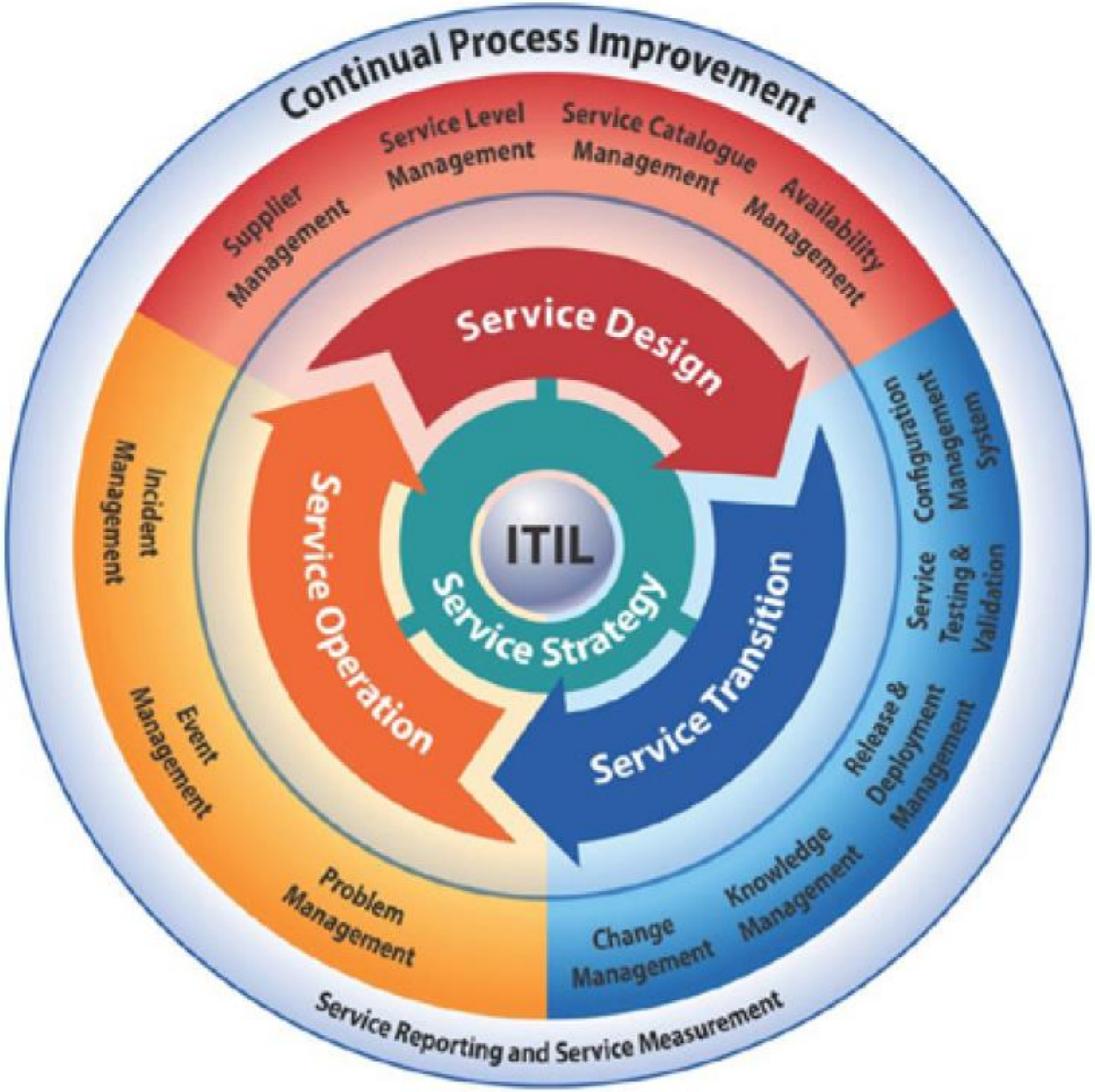
เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice)

COBIT มีหลักการ 5 ข้อ

- 1 : ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสีย (Meeting stakeholder needs)
- 2 : ครอบคลุมทั้งองค์กร (Covering the enterprise end-to-end)
- 3 : ประยุกต์ใช้กรอบแนวปฏิบัติเดียว (Applying a single integrated framework)
- 4 : หนุนแนวทางทั้งระบบ (Enabling a holistic approach)
- 5 : แยกระหว่างการอภิบาลและการบริหารออกจากกัน (Seperating governance from management)

ITIL
(The Information Technology Infrastructure Library)

- การกำหนดแนวปฏิบัติที่ดีที่สุด (Best Practices) สำหรับกระบวนการของการส่งมอบงานและการให้บริการด้านไอที ITIL เป็นมาตรฐานที่พัฒนาและกำหนดโดยรัฐบาลอังกฤษ
- เน้นการผสมผสานของวงจรชีวิตการให้บริการด้วยระบบไอที (Integrated service lifecycle approach)


Continual Process Improvement
Service Level Management
Service Catalogue Management
Availability Management
Supplier Management
Service Design
Service Strategy
Service Transition
Service Operation
ITIL
Configuration Management System
Service Testing & Validation
Release & Deployment Management
Knowledge Management
Change Management
Problem Management
Event Management
Incident Management
Service Reporting and Service Measurement

แนวทางปฏิบัติ ITIL 5 กลุ่ม

- ยุทธศาสตร์งานบริหาร (Service Strategy)
- การออกแบบงานบริการ (Service Design)
- การส่งมอบงานบริการ (Service Transition)
- การปฏิบัติงานบริการ (Service Operation)
- การปรับปรุงงานบริการอย่างต่อเนื่อง (Continual Service Improvement)

มาตรฐาน ISO/IEC 27001

- เป็นมาตรฐานเกี่ยวกับ***ระบบบริหารการรักษาความปลอดภัยข้อมูล (The Information Security Management System : ISMS)***
- เป็นมาตรฐานที่องค์กรส่วนใหญ่จะต้องทำให้ได้ตามมาตรฐานนี้ เพื่อความน่าเชื่อถือและการผ่านเกณฑ์มาตรฐานที่หน่วยงานรัฐบาลกำหนด
- ปัจจุบันใช้มาตรฐาน 2013 เน้นการวัดประสิทธิภาพขององค์กรในการบริหารความปลอดภัยข้อมูล

ความสำคัญของ ISO 27001

- ตั้งแต่ปี 2559 เป็นต้นมา รัฐบาลเริ่มออกประกาศให้องค์กรที่มีการทำธุรกรรมทางอิเล็กทรอนิกส์ จำเป็นต้องได้รับการรับรองมาตรฐาน ISO 27001 หรือมาตรฐานอื่นที่เกี่ยวข้อง เพื่อภาพลักษณ์และความน่าเชื่อถือ
- เช่น การออกประกาศให้บริษัทประกันมีการรับรองมาตรฐาน รวมถึงสถาบันทางการเงินภายในประเทศ หรือรัฐวิสาหกิจ
- การได้ใบรับรองมาตรฐานสากลจะทำให้ภาพลักษณ์ขององค์กรดีขึ้น มีความมั่นใจในการรักษาความมั่นคงปลอดภัยของระบบขององค์กรที่ได้มาตรฐาน

การประปานครหลวง
METROPOLITAN WATERWORKS AUTHORITY

IT กปน. รับ ISO/IEC 27001:2013

วันที่ 15 ก.ค. 2559

นายธนศักดิ์ วัฒนฐานะ ผู้ว่าการการประปานครหลวง (กปน.) (กลาง) รับมอบใบรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 สำหรับศูนย์คอมพิวเตอร์ของ กปน. จาก **นายประวาลทอง ทองใหญ่ ณ อยุธยา** ผู้จัดการฝ่ายรับรองระบบมาตรฐาน บริษัท Bureau Veritas Certification (ประเทศไทย) จำกัด (ที่ 2 จากซ้าย) เพื่อมั่นใจได้ว่าข้อมูลสารสนเทศของผู้ใช้บริการทุกกลุ่ม ของ กปน. จะมีความมั่นคง ปลอดภัย ปราศจากการรั่วไหล ด้วยมาตรฐานระดับสากล โดยมี **อาจารย์ปริญญา หอมเอนก** ในฐานะที่ปรึกษาคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศฯ ของ กปน. ให้เกียรติร่วมงาน

ที่มา
http://www.mwa.co.th/ewt_news.php?nid=25

[PR] 3 หน่วยงานเอ็ตด้ารับใบรับรองมาตรฐาน ISO/IEC 27001:2013 ย้ำความน่าเชื่อถือผู้พัฒนา SOFT INFRASTRUCTURE ของประเทศ

November 19, 2016 Press Release

3 พฤศจิกายน 2559 – 3 หน่วยงานภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รับใบรับรองมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems) ISO 27001:2013 ตอกย้ำภาพลักษณ์ ความน่าเชื่อถือองค์กรในฐานะผู้พัฒนา Soft Infrastructure เพื่อการดำเนินธุรกรรมทางอิเล็กทรอนิกส์สำหรับองค์กรทั้งในประเทศ-ต่างประเทศ และเพื่อรองรับแผนเศรษฐกิจดิจิทัลในภาพรวม

สุรางคณา วายุภาพ ผู้อำนวยการ ETDA กล่าวว่า 3 หน่วยงานที่ได้รับใบรับรองมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศครั้งนี้ ได้แก่ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) ศูนย์ดิจิทัลฟอเรนสิกส์ (Digital Forensics Center) และหน่วยงานผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand Root Certification Authority: Thailand NRCA) ที่ต่างมีบทบาท และหน้าที่ในการสอดส่องด้านความปลอดภัย ตลอดไปจนถึงให้บริการเพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์ให้แก่องค์กร และหน่วยงานต่าง ๆ ทั้งของภาครัฐ และเอกชน อย่างมั่งคงปลอดภัย

ศูนย์การแพทย์กาญจนาภิเษก มหาวิทยาลัยมหิดล
ผ่านการรับรองมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ISO 27001

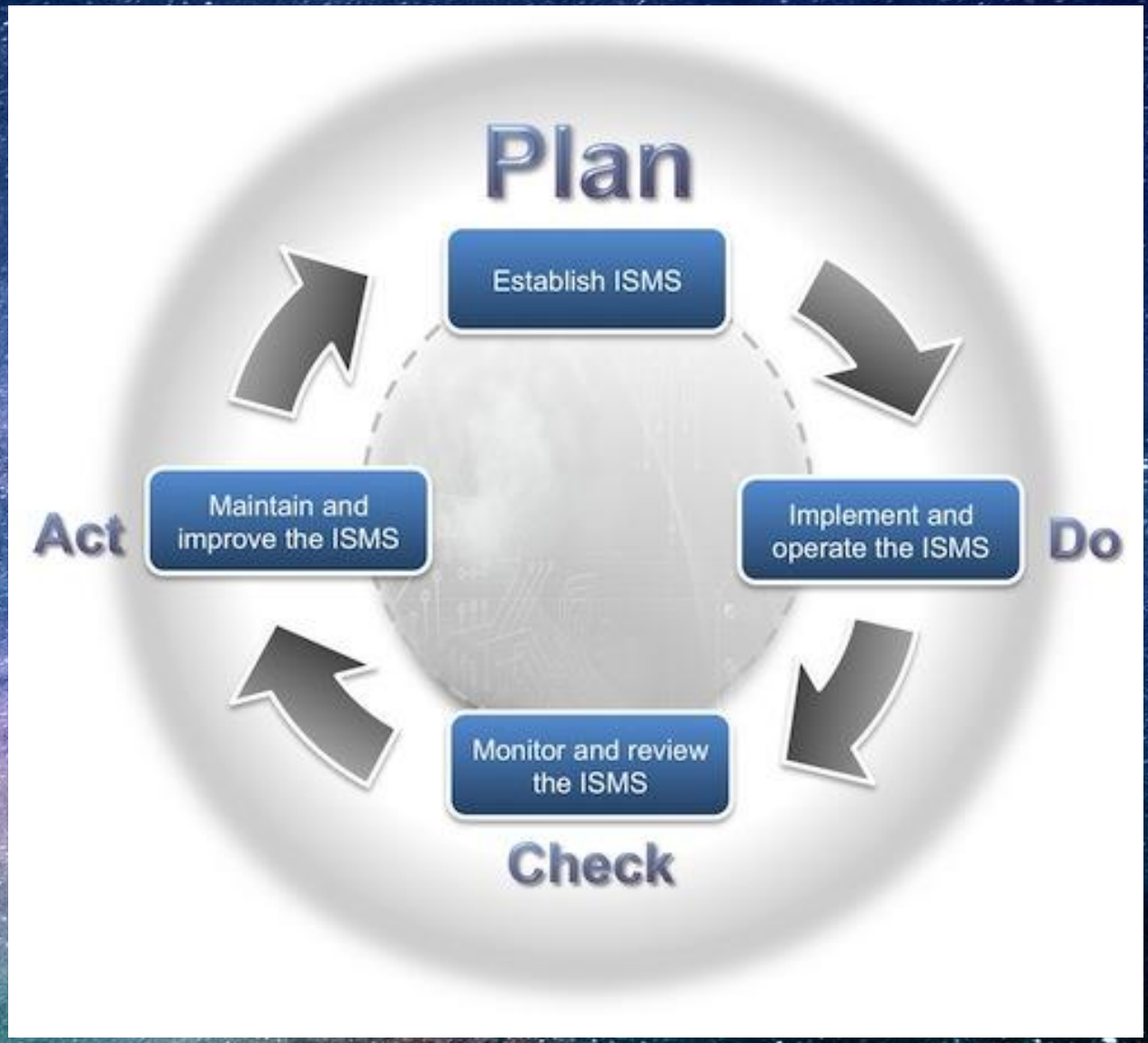
ในสังคมปัจจุบันเทคโนโลยีสารสนเทศได้มีการพัฒนาไปอย่างรวดเร็วและได้เข้ามามีบทบาทสำคัญในการดำเนินงานต่างๆขององค์กร ศูนย์การแพทย์กาญจนาภิเษก ซึ่งเป็นสถาบันทางการแพทย์แห่งหนึ่งที่ได้นำเทคโนโลยีต่างๆเหล่านี้มาเชื่อมโยงและมีการเก็บข้อมูลของผู้มาใช้บริการ ดังนั้นเรื่องของความมั่นคงปลอดภัยสารสนเทศจึงเป็นเรื่องสำคัญอย่างยิ่ง เนื่องจากภัยคุกคามคอมพิวเตอร์ในปัจจุบันมีการพัฒนาอย่างรวดเร็วและหลากหลาย ซึ่งอาจก่อให้เกิดผลกระทบต่อการดำเนินงานของศูนย์การแพทย์กาญจนาภิเษกได้

"องศาสตราจารย์นายแพทย์สรนิต ศิลธรรมผู้อำนวยการศูนย์การแพทย์กาญจนาภิเษก และคณะผู้บริหารได้มีนโยบายให้งาน เวชสารสนเทศดำเนินโครงการพัฒนามาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือ ISO/IEC 27001:2005 (Information Security Management System : ISMS) เพื่อนำมาใช้เป็นมาตรฐานในการบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศภายในศูนย์การแพทย์ฯ โดยมีหน่วยงาน ที่อยู่ภายใต้ขอบเขตของการรับรองครั้งนี้คือ งานเวชสารสนเทศ งานเวชระเบียนและงานเทคนิคการแพทย์ ซึ่งทั้ง 3 หน่วยงาน ใช้ระบบสารสนเทศและเป็นระบบสนับสนุนหลักในการให้บริการการรักษาพยาบาลผู้ป่วย"

โครงการดังกล่าวได้เริ่มดำเนินการมาตั้งแต่ต้นปี 2554 ซึ่งได้รับการสนับสนุนจากผู้บริหารศูนย์การแพทย์ฯ ใน การวางแผน กำหนดนโยบาย อนุมัติเกณฑ์ที่จะใช้ในโครงการเช่น เกณฑ์การประเมินทรัพย์สิน เกณฑ์การประเมินความเสี่ยง เป็นต้น หลังจากนั้นคณะทำงานจะนำนโยบายและเกณฑ์ที่ได้รับอนุมัติแล้วไปดำเนินการต่อ เช่น กำหนดความสำคัญทรัพย์สิน ประเมินความเสี่ยง สร้างและทดสอบแผนความต่อเนื่องทางธุรกิจ (BCP) มีการปรับกระบวนการทำงานต่างๆ ภายในศูนย์การแพทย์ฯ ให้สอดคล้องกับมาตรฐาน และมาตรฐานยังกำหนดให้ต้องดำเนินการตรวจสอบภายใน ซึ่งนับเป็นครั้งแรกที่มีการตรวจสอบภายในด้านสารสนเทศของศูนย์การแพทย์ฯ ซึ่งผลการตรวจสอบภายในต้องนำไปรายงานให้กับผู้บริหารศูนย์การแพทย์ฯ เพื่อพิจารณาและกำหนดแนวทางการดำเนินงานต่อไป และเพื่อให้มั่นใจมากยิ่งขึ้นศูนย์การแพทย์ฯ ได้ให้มีการตรวจสอบจากผู้ตรวจภายนอก โดยบริษัท ทูฟ นอร์ด (ประเทศไทย) จำกัด ซึ่งเป็นบริษัทที่ให้การรับรองมาตรฐานสากลด้านต่างๆ รวมถึงมาตรฐาน ISO/IEC 27001:2005 เข้ามาตรวจสอบการดำเนินงานตามมาตรฐาน ในการตรวจสอบครั้งนี้มีหัวหน้าคณะผู้ตรวจสอบ

ขั้นตอนหลักของ ISO/IEC 27001

PDCA



รายละเอียดเพิ่มเติม
http://www.iso.org/iso/iso27001

นโยบายด้านการรักษาความปลอดภัยข้อมูล (Information Security Policy)

นโยบายข้อมูล

นโยบายการรักษาความปลอดภัย

นโยบายการใช้งาน

นโยบายการสำรองข้อมูล

การบริหารจัดการบัญชีผู้ใช้

ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์

แผนการฟื้นฟูหลังภัยร้ายแรง

การสร้างความตระหนักด้านการรักษาความปลอดภัย (Information Awareness Training)

ผู้บริหาร	พนักงานทั่วไป	ผู้ดูแลระบบ	โปรแกรมเมอร์	เจ้าหน้าที่รักษาความปลอดภัย
• ต้องรายงานสถานการณ์และความก้าวหน้าให้ทราบ • นำข้อมูลฝึกอบรมพนักงานให้ทราบด้วย	• ได้รับการฝึกอบรมเพื่อสร้างความเข้าใจด้านความปลอดภัย • เรียนรู้วิธีการโจมตีที่กำลังเกิดขึ้น • ควรมีในหลักสูตรอบรม	• ปรับปรุงความรู้ให้ทันสมัยอยู่เสมอ • การติดตั้งแพตช์ • ควรจัดอบรมบ่อย ๆ โดยผู้เชี่ยวชาญ	• เทคนิคการเขียนโปรแกรมให้ปลอดภัย • การออกแบบโครงการพัฒนาร่วมกับฝ่ายรักษาความปลอดภัย	• ต้องปรับปรุงความรู้อยู่เป็นประจำ • ฝึกอบรมทั้งจากภายนอกและภายใน • นำเสนอข้อมูลใหม่ ๆ อยู่เสมอ

การตรวจสอบ (Audit)

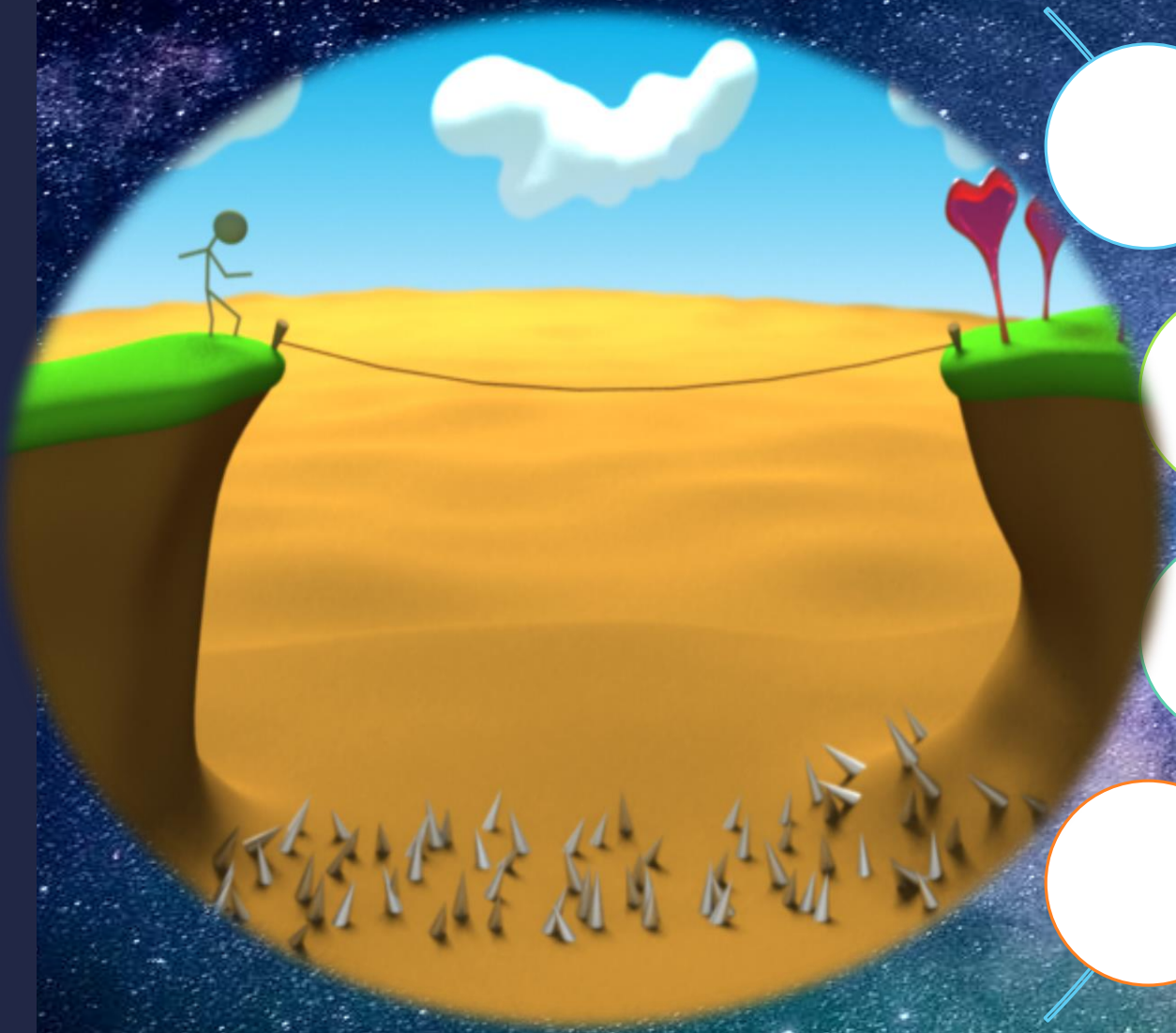
- เป็นขั้นตอนสุดท้ายของกระบวนการรักษาความปลอดภัย หลังจากดำเนินการด้านความปลอดภัยทุก ๆ อย่างแล้ว
- ปกติจะมีทั้งการตรวจสอบจากภายในและภายนอก

ตรวจสอบการปฏิบัติตามนโยบาย

การประเมินโครงการใหม่

การทดลองเจาะระบบ (Penetration Test)

อุปสรรคของงานด้านความมั่งคง



- “ความมั่นคงปลอดภัย” คือ “ความไม่สะดวก”
- ความซับซ้อนของคอมพิวเตอร์ที่ผู้ใช้ทั่วไปไม่ทราบ
- ผู้ใช้ไม่ระแวดระวัง
- การพัฒนาซอฟต์แวร์โดยคำนึงถึงความปลอดภัยในภายหลัง

อุปสรรคของงานด้านความมั่งคง

- แนวโน้มเทคโนโลยีสารสนเทศคือ “การแบ่งปัน” ไม่ใช่ “การป้องกัน”
- มีการเข้าถึงข้อมูลได้จากทุกสถานที่
- ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟต์แวร์และฮาร์ดแวร์เพียงอย่างเดียว
- มิจฉาชีพมักมีความชำนาญ
- ฝ่ายบริหารมักไม่ให้ความสำคัญแก่ความมั่นคงปลอดภัย


LET'S CROSS THE
PROBLEM