สรุปมาตรฐาน ISO 27001:2013

โดย ศิริพร เชี่ยวสมุทร

Paramount Consultant Co.,Ltd.

ชื่อมาตรฐาน ISO 27001:2013

Information Security Management System

ระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

นิยามของความมั่นคงปลอดภัยของสารสนเทศ

Confidentiality การรักษาความลับ

คุณสมบัติว่าข้อมูลจะไม่ถูกเผยแพร่หรือเปิดเผย
ให้บุคคล กิจการ หรือ กระบวนการที่ไม่ได้รับอนุญาต

Integrity ความครบถ้วนถูกต้อง

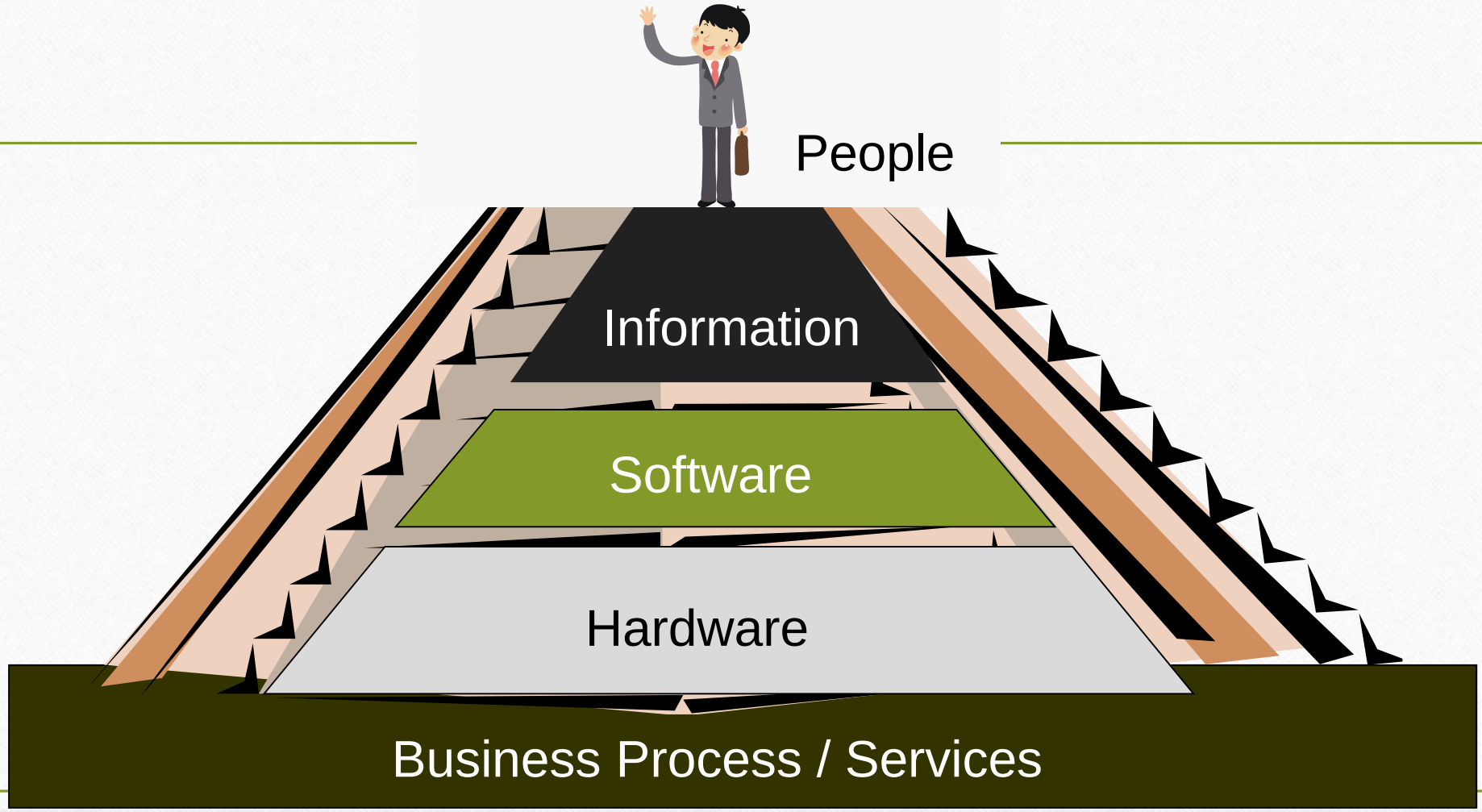
คุณสมบัติของการปกป้องความถูกต้องและ
ครบถ้วนของทรัพย์สิน

Availability ความพร้อมใช้

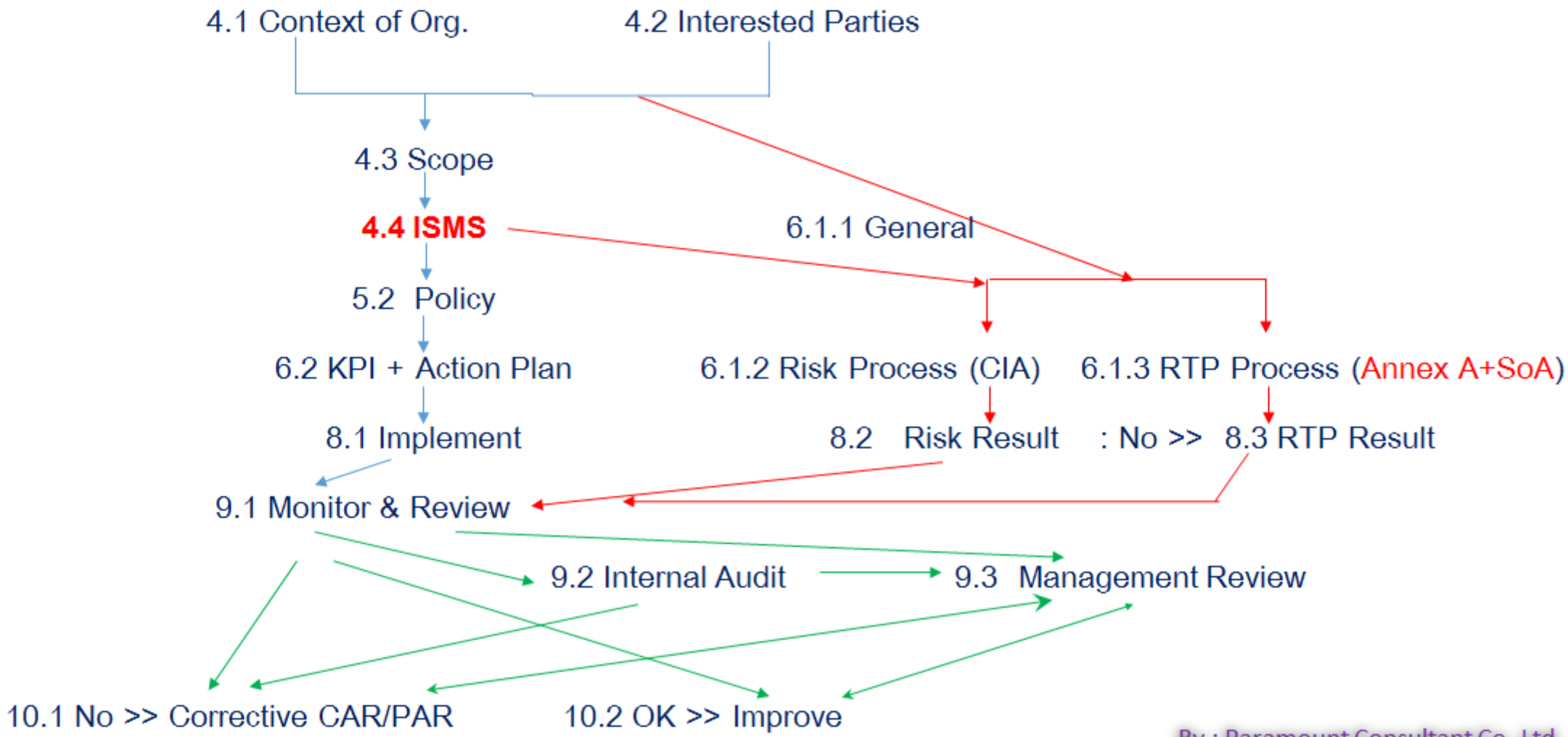
คุณสมบัติของการเป็นที่สามารถเข้าถึงและใช้งานได้
ตามความต้องการ โดยกิจการที่ได้รับอนุญาต

วิธีการจัดเก็บข้อมูลให้ปลอดภัย

สิ่งที่เกี่ยวข้องและต้องจัดการเพื่อรองรับ ISO 27001



ความสัมพันธ์ของข้อกำหนด ISO 27001:2013



By : Paramount Consultant Co.,Ltd.

5.1 Leadership and commitment 5.3 Organizational roles, Responsibilities and authorities

7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication 7.5 Documented Information

Annex A

>> A.5.1.1 Policy for IS ,A.5.1.2 Review for the IS

A.9.1.1 Access Control Policy
A.9.1.2 Access to networks and network services

Update Asset List
* A.8.1.1 Inventory of Asset
A.8.1.2 Ownership of assets

กำหนดสิทธิ User & PW
A.9.2.1 User Reregistration (User)
A.9.2.2 User access provisioning (Admin)
A.9.2.3 Management of Privileged access rights
A.9.2.4 Management of secret authentication in formation of users

เตรียมทรัพย์สินให้ตาม
A.8.1.3 Acceptable use of assets

สมัครงาน

A.7.1.1 Screening

A.7.1.2 Term & Condition
A.13.2.4 NDA

เข้าพื้นที่ทำงานตามหน้าที่ / สิทธิ
A..11.1 Secure Area
(A.11.1.1 – A.11.1.6)

อบรมมอบหมายงาน
A.6.1.1 IS Roles & Responsibilities
A.6.1.2 Segregation of duties
A.7.2.1 Management Responsibilities
A.7.2.2 IS Awareness ,EDU & Training
A.6.1.3 Contact with authorities
A.6.1.4 Contact with special Interest groups
A.7.2.3 Disciplinary Process

1

ทำงานตามหน้าที่ความรับผิดชอบ
A.12.1.1 Documented Operation procedure
A.1.2.1.2 Change management
A.12.1.3 Capacity management
A.12.1.4 Separation of development testing and operational environment

2

ต้องปฏิบัติตาม IS Policy ระหว่างทำงาน
Access Contrl
A..9.3.1 Use of Secret authentication Information
A.9.4.1 Information access restriction
A.9.4.2 Secure log-on procedure
A.9.4.3 Password management System
A.9.4.4 Use of privileged utility Program
A.9.4.5 Access control to program source code
Cryptography
A.10.1.1 Policy on the use of cryptographic Controls
A10.1.2 Key management
Equipment
A.11.2.8 Unattended User equipment
A.11.2.9 Clear desk and Clear screen policy

3

ระหว่างการทำงานแล้วพบปัญหา Incident
A.16.1 1Responsibilities & Procedure
A.16.1.2 Reporting IS Events
A.16.1.3 Reporting IS weaknesses
A.16.1.4 Assessment of and decision on IS event
A.16.1.5 Response to IS incident
A.16.1.6 Learning from IS incident
A.16.1.7 Collection of evidence

พนักงานลาออก / โอนย้าย
A..7.3.1 Termination or change of employment Responsibilities
A.8.1.4 Return of assets >> A.11.2.7 Secure disposal or re-use of equipment >> A.8.1.1 *
A.9.2.1 User De –registration

4

ระหว่างการทำงานมีการว่าจ้าง Supplier
ช่วงการว่าจ้าง Supplier
A.15.1.1 IS policy for supplier relationships
A.15.1.2 Addressing security within supplier agreements
A.15.1.3 Information and commu technology Supply chain
ช่วงติดตามการส่งมอบจาก Supplier
A.15.2.1 Monitoring and review of supplier services
A.15.2.2 Managing changes to supplier services

By : Paramount Consultant Co.,Ltd.

IT Support : A.9.2.5 Review of user access rights , A.9.2.6 Removal or adjustment of access rights , **Infra** (A.11.2 Equipment A.11.2.1 – A.11.2.6), A.12.2.1 controls against mal-ware ,A.12.3.1 Information Backup ,A.12.4.1 Event logging , A12.4.2 Protection of log information ,A.12.4.3 Administrator & operation log ,A.12.4.4 Clock Sync ,A.12.5.1 Installation of SW on OS ,A.12.6.1 Management of technical vulnerabilities ,A.12.6.2 Restriction of SW installation, A.12.7.1 Information systems and controls

BCP : A.17.1.1 Planning IS continuity ,A.17.1.2 Implement IS continuity , A.17.1.3 Verify review & Evaluate IS continuity / Redundancies A.17.2.1 Availability of information Processing facilities

Compliance : A.18.1.1 Identification. , A.18.1.2 Intellectual property rights ,A.18.1.3 Protection of records, A.18.1.4 Privacy & protection of personally identifiable info, A.18.1.5 Regulation of Crypto / A.18.2.1 Independent review of IS ,A.18.2.2 Compliance with security policies and standards , A.18.2.3 Technical compliance review

จะทำระบบ ISO27001 ได้อย่างไร

- ศึกษาข้อกำหนด
- จัดหลักสูตรฝึกอบรม
- ตั้งทีมงานในการทำระบบ สร้างแผนโครงการ
- กำหนดขอบข่ายกิจกรรมและอาณาบริเวณ
- จัดทำรายการกิจกรรม และทรัพย์สินสารสนเทศ
- ประเมินความเสี่ยง (CIA) จาก
  - มูลค่าความเสียหาย
  - ภัยคุกคาม
  - จุดอ่อน
  - ความรุนแรง
  - โอกาสเกิด
- จัดทำ / กำหนดมาตรการควบคุมความเสี่ยง จาก Annex A
  - ยอมรับความเสี่ยง
  - ควบคุมความเสี่ยง
  - ถ่ายโอนความเสี่ยง
  - หลีกเลี่ยงความเสี่ยง
- จัดทำ Statement of Applicability
- ปฏิบัติตามมาตร การควบคุมความเสี่ยง
- กำหนดตัวชี้วัด ให้ครบ รอบด้าน
- วัดผลตามตัวชี้วัด
- ทำ Internal Audit และ Management Review

เมื่อครบ 1 รอบ PDCA องค์กรพร้อมแล้วสำหรับการตรวจรับรอง

กระบวนการในการขอการรับรอง ISO 27001

- ติดต่อบริษัทที่ให้การรับรอง (Certify Body)
- ตรวจ Stage 1 (ตรวจสอบเอกสาร = ISO 27001)
- ตรวจ Stage 2 (ตรวจสอบเอกสาร = หลักฐานการดำเนินงาน >> ได้รับการรับรอง ISO 27001)
- ใบรับรองมีอายุ 3 ปี
- ระหว่างการได้การรับรอง มีการสุ่มตรวจเป็นระยะ ๆ (อย่างน้อยปีละครั้ง จนกระทั่งใบรับรองหมดอายุ)

ประโยชน์ของการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ

- ดูแลข้อมูลตามคุณค่าความสำคัญของข้อมูลที่มีต่อองค์กร
- ดูแลข้อมูลตามระดับความเสี่ยง
- ตอบสนองต่อความต้องการของผู้มีส่วนได้ส่วนเสีย
- ดูแลข้อมูลให้สนับสนุนความต่อเนื่องในการดำเนินธุรกิจในสถานะการณ์ฉุกเฉิน
- ส่งเสริมภาพลักษณ์ขององค์กร
- สามารถวัดผลความสำเร็จของวิธีการควบคุมความมั่นคงปลอดภัยของสารสนเทศ
- รู้ถึงผลตอบแทนในการลงทุนด้าน IT
- สร้างความเชื่อมั่นให้ผู้บริหาร ลูกค้า และพนักงาน
- มั่นใจในด้านความสอดคล้องต่อกฎหมาย
- ฯลฯ

กิจกรรมที่ดำเนินการแล้ว

๑	รายงานผลการกำหนด วิเคราะห์และระบุความจำเป็นของการให้บริการสารสนเทศฯ (Interested Parties)
๒	เอกสารจัดทำร่างเอกสารบริบทขององค์กร (Context of the Organization)
๓	รายงานผลการวิเคราะห์ช่องว่างมาตรการควบคุมความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO ๒๗๐๐๑: ๒๐๑๓ (Gap Analysis of Information Security Controls)
๔	ร่างนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยของสารสนเทศ (IS Policy)
๕	ร่างขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยของสารสนเทศ (Information Security Risk Assessment Methodology)
๖	ร่างแผนลดความเสี่ยงความมั่นคงปลอดภัยของสารสนเทศ (Risk Treatment Plan)
๗	ร่างแนวปฏิบัติ (Procedure) เรื่อง การควบคุมเอกสาร (Document Control Procedure)
๘	ร่างแนวปฏิบัติ (Procedure) เรื่อง การจัดระดับชั้นความลับ การบ่งชี้และการจัดการกับสารสนเทศ (Information Classification, Labelling and Handling Procedure)
๙	ร่างแนวปฏิบัติ (Procedure) เรื่อง การขอเข้าพื้นที่ควบคุม (Physical Entry Control Procedure)
๑๐	ร่างแนวปฏิบัติ (Procedure) เรื่อง การสำรองและทดสอบกู้คืนข้อมูล (Backup and Restoration Procedure)
๑๑	ร่างแนวปฏิบัติ (Procedure) เรื่อง การติดตามการใช้งานระบบสารสนเทศ (Monitoring System Use Procedure)
๑๒	ร่างแนวปฏิบัติ (Procedure) เรื่อง การลงทะเบียนผู้ใช้งาน (User Registration Procedure)
๑๓	ร่างแนวปฏิบัติ (Procedure) เรื่อง การควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change Control Procedure)
๑๔	ร่างแนวปฏิบัติ (Procedure) เรื่อง การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยของสารสนเทศ (Information Security Incident Response Procedure)

กิจกรรมที่ต้องดำเนินการต่อ

- สร้างกิจกรรมกระตุ้นความรู้ความเข้าใจ
- สร้างกิจกรรม / ทำความเข้าใจทีมงาน
- ศึกษาดูงานที่ Data Center ที่ใหญ่ที่สุดในประเทศ
- ประชุมให้ความรู้เพื่อสร้างความตระหนัก
- อนุมัติการใช้แนวทางปฏิบัติงานที่ได้จัดทำขึ้น
- จัดพิมพ์เอกสารเพื่อเป็นแนวทางในการปฏิบัติ

กิจกรรมจะดำเนินการต่อเพื่อให้การรับรอง

- ปฏิบัติตามแนวทางปฏิบัติ
- ติดตามผล KPI
- จัดทำ Internal Audit
- แก้ไขปัญหา หลังจาก การทำ Internal Audit
- ทำการประชุมทบทวนฝ่ายบริหาร
- ตรวจประเมินเพื่อขอการรับรอง