การบริหารจัดการข้อมูลส่วนบุคคลด้วยมาตรฐาน ISO/IEC 27701:2019

และ

การใช้มาตรฐาน ISO/IEC 20000:2018 เพื่อการบริหารจัดการบริการ IT อย่างมีประสิทธิผล

17.03.2020

Speaker Profile

ชื่อวิทยากร : สมบูรณ์ นิลฟุ้งขจร

ตำแหน่ง : Consulting Development Manager บริษัท ACinfotec

ประกาศนียบัตร :

- PECB Certified ISO/IEC 20000 Lead Implementer
- PECB Certified ISO/IEC 31000 Risk Manager
- PECB Certified ISO/IEC 27001 Lead Implementer
- PECB Certified ISO/IEC 27001 Lead Auditor
- PECB Certified Trainer
- ITIL 4 Foundation
- ITIL V3(2011) Intermediate

ประสบการณ์ :

- ที่ปรึกษามาตรฐาน ISO 20000 และ ISO 27001 ให้หน่วยงานภาครัฐ ภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศ

การบริหารจัดการข้อมูลส่วนบุคคลด้วยมาตรฐาน ISO/IEC 27701:2019

Agenda

- ขอบเขตข้อมูลส่วนบุคคลตามกฎหมาย
- มาตรการปกป้องข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC 27701:2019
- แนะนำ Privacy Enhanced Technology (PET)

โครงสร้างของกฎหมาย

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทบัญญัติ (มาตรา 1-7)

- หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 8-21)
- หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล (มาตรา 22-29)
- หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 30-42)
- หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 43-70)
- หมวด 5 การร้องเรียน (มาตรา 71-76)
- หมวด 6 ความรับผิดทางแพ่ง (มาตรา 77-78)
- หมวด 7 บทกำหนดโทษ (มาตรา 79-90)

บทเฉพาะกาล (มาตรา 91-96)

หมวด 2 แบ่งออกเป็น

ส่วนที่ 1 บททั่วไป

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล

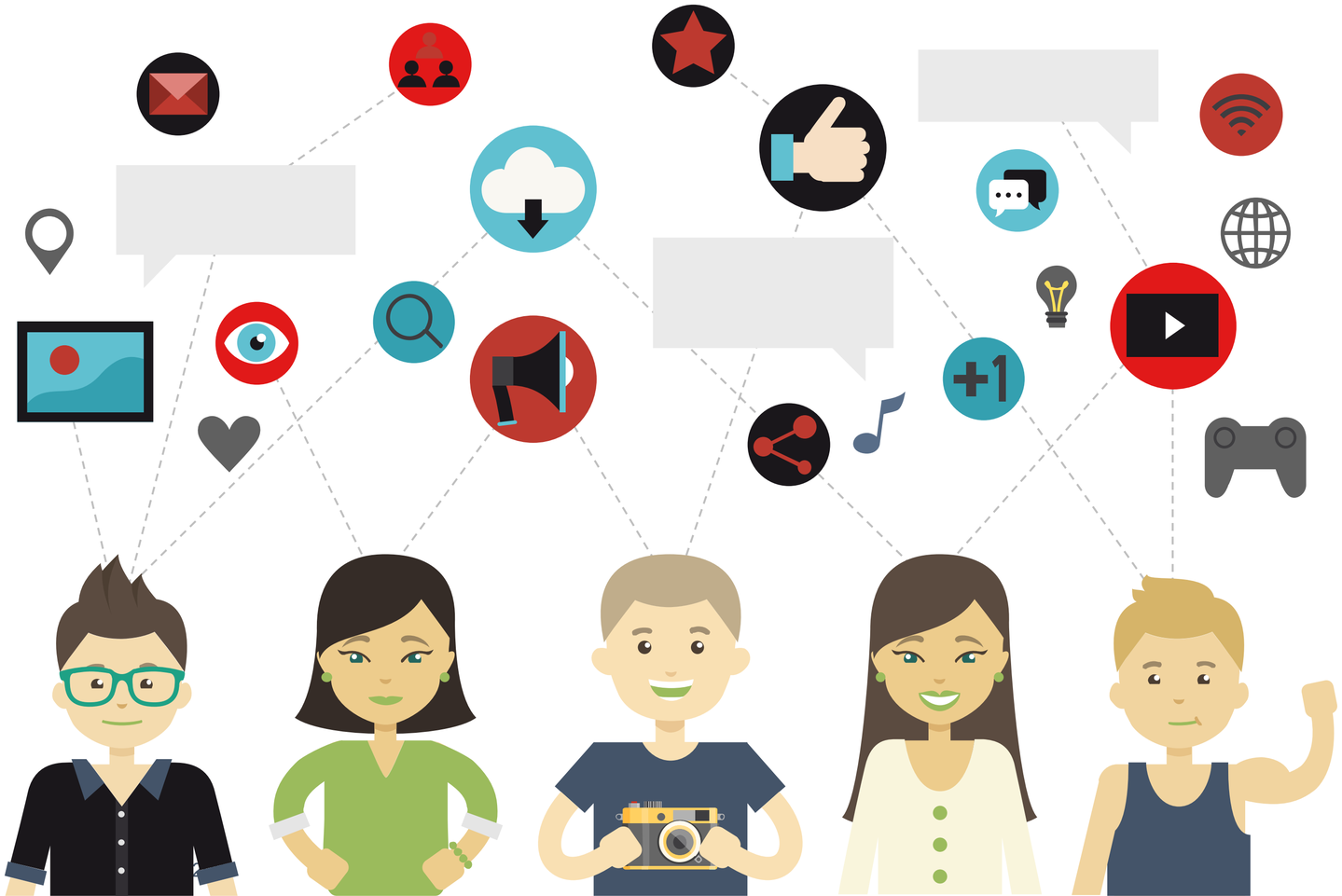
ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

Personal Data

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้
สามารถระบุตัวบุคคลนั้นได้
ไม่ว่าทางตรงหรือทางอ้อม

รวมถึงข้อมูลที่นำมารวมกันแล้ว
สามารถใช้ระบุ
อัตลักษณ์ของบุคคลได้



ข้อมูลใด ๆ ที่ระบุตัวเจ้าของข้อมูลได้ ถือเป็นข้อมูลส่วนบุคคล

ระบุทางอ้อม

เช่น
เลขทะเบียนรถยนต์
MAC Address
หมายเลขสมาชิก

ระบุจากการรวมหลาย ๆ ข้อมูล

เช่น
อายุ + อาชีพ + ที่อยู่
เพศ + รถยนต์ + บริษัท

ข้อมูลและการประมวลผลที่ไม่เข้าข่ายตามกฎหมาย

มาตรา 6

ไม่ใช่ข้อมูลส่วนบุคคล

ข้อมูลนิติบุคคล

ข้อมูลผู้ถึงแก่กรรม

ได้รับยกเว้นตามกฎหมาย

มาตรา 4

หน่วยงานความมั่นคง
ความมั่นคงไซเบอร์
บันทึกประวัติศาสตร์
สาธารณะประโยชน์
สื่อมวลชน
บริษัทข้อมูลเครดิต
เพื่อปฏิบัติตามกฎหมาย

ผู้ที่เกี่ยวข้องทั้งหมด (Stakeholders)

เจ้าของข้อมูล

บุคคลธรรมดา ที่พำนักหรือมีถิ่นที่อยู่ในประเทศไทย

ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคล ที่มีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล

Data Protection Officer

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ตรวจสอบการดำเนินงานขององค์กรให้เป็นไปตามกฎหมาย (มาตรา 41-42)

ผู้ประมวลผลข้อมูลส่วนบุคคล

บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล ตามคำสั่ง หรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคล

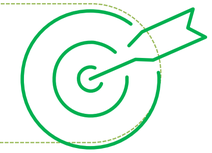
คณะกรรมการฯ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีอำนาจกำกับดูแลตามกฎหมาย

หมวด 4

การประมวลผลที่ถูกต้องตามกฎหมาย (Lawful Basis)

- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)
- เป็นการปฏิบัติหน้าที่ของหน่วยงานภาครัฐหรือเจ้าหน้าที่ (Official Authority)
- เพื่อปฏิบัติตามกฎหมาย (Legal Obligation)
- เพื่อปฏิบัติตามคำร้องขอหรือการให้ความยินยอมของเจ้าของข้อมูล (Consent)
- เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา (Contract)
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)



บทลงโทษ

บทลงโทษ

<u>แพ่ง</u>
ค่าสินไหมทดแทน

<u>อาญา</u>
จำคุกไม่เกิน 1 ปี / ปรับไม่เกิน 1 ล้านบาท

<u>ปกครอง</u>
ปรับไม่เกิน 5 ล้านบาท

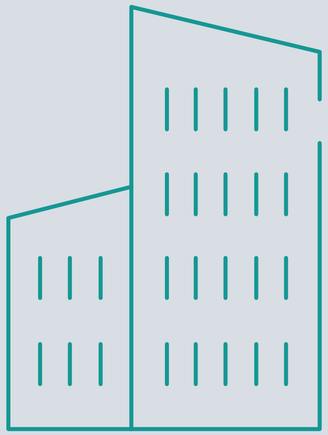
ผู้ละเมิด

อาจจะ CEO, DPO หรือผู้บริหารท่านอื่น

ที่ได้รับมอบหมายหน้าที่แต่ละเลย

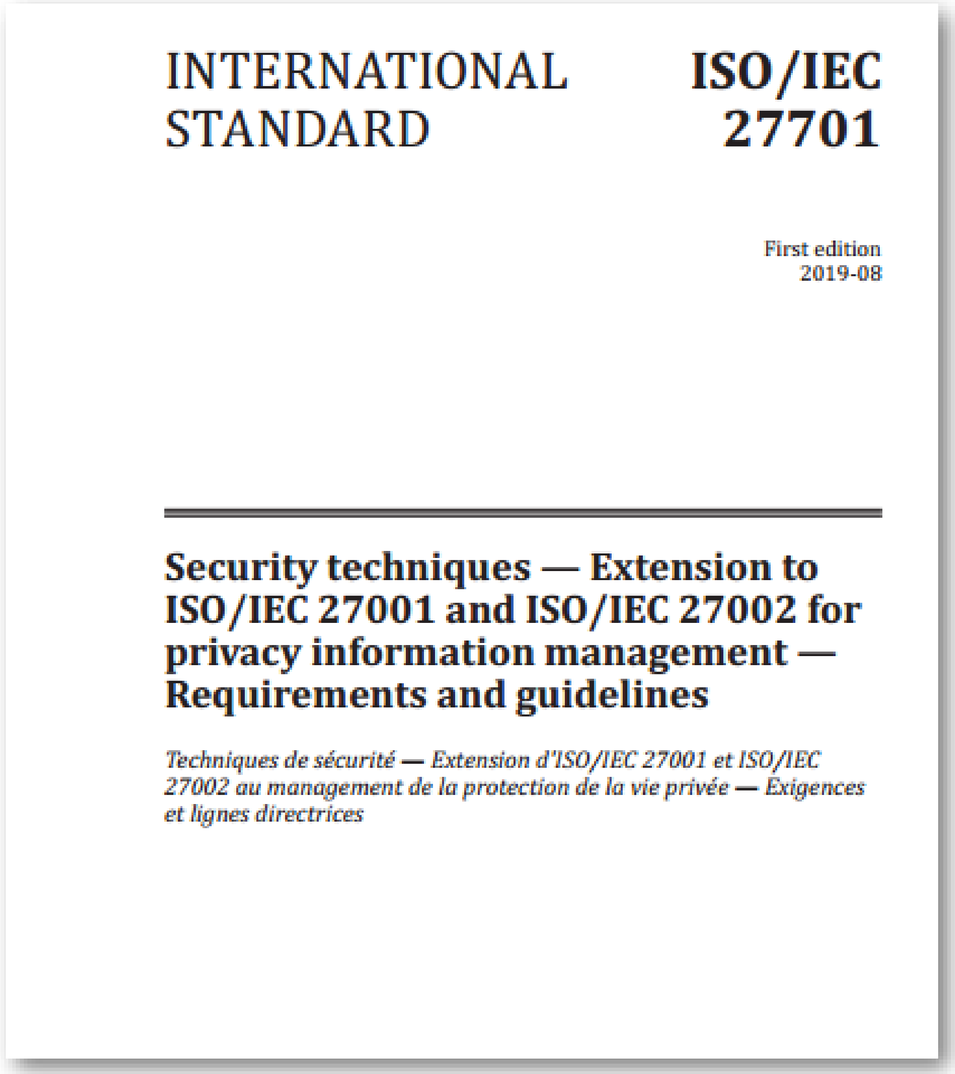
ผู้มีความผิดตามกฎหมาย

Data Controller เบื้องต้นต้องทำอะไรบ้าง (Overview)



1. **วิเคราะห์ข้อมูลส่วนบุคคล** ที่เก็บรวบรวมและใช้งานภายในองค์กร ข้อมูลเข้ามาจากทางไหน จัดเก็บที่ไหน ส่งต่อไปไหน
2. ตรวจสอบ **การจัดเก็บข้อมูลส่วนบุคคล** ว่าเกินความความจำเป็นหรือไม่ (ตามฐานกฎหมายที่เลือกใช้) ถ้าไม่จำเป็นแล้วต้องลบข้อมูล
3. **Inform/Notify** แจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล รวมถึงถึงสิทธิของเจ้าของข้อมูลและช่องทางติดต่อ (Special mailing, Privacy Policy webpage)
4. **เฝ้าระวัง** และจัดเก็บบันทึกผู้ที่เข้าถึงและใช้งานข้อมูลส่วนบุคคลทั้งในองค์กร และโดย Data Processor

Privacy information standard – ISO/IEC 27701:2019



INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

ISO/IEC 27701:2019 – Personal Information Management Role

PII Controller	PII Processor
Collects personal information and determines the purposes for which it is processed. More than one organisation can act as PII controller often known as co-controller, and this is where data-sharing agreements may be necessary.	Processes personal information on behalf of and only according to the instruction of the PII controller.
How ISO/IEC 27701 helps PII Controllers	**How ISO/IEC 27701 helps PII Processors**
• Provides best practice guidance • Gives transparency between PII controllers • Provides an effective way to manage PII processes	• Provides best practice guidance • Gives reassurance to customers that PII is effectively managed

ISO/IEC 27701:2019 Overview

Structure of ISO 27701

Much like other ISO standards, ISO 27701 divides its content by clause, of which Clauses 5–8 set out the additional requirements and amendments to be applied to ISO 27001, and warrant particular attention.

Clause 5: PIMS-specific requirements

This clause addresses every clause in ISO 27001 and identifies where additional content is necessary. The majority of the ISO 27001 clauses remain unchanged, with the caveat that ISO 27701 requires the organisation to recognise its need for data protection within its context, and this context informs all the other requirements.

Another notable addition affects the risk assessment, which will need to take into account the organisation's role in relation to PII – that is, whether it is a controller or a processor, and how that might affect the risks to the PII. Another entry recognises the existence of the new control sets and allows the organisation to reconcile its controls against a wider range of controls, including those from ISO 27701.

Clause 6: PIMS-specific guidance

This section provides additional content for the control guidance set out in ISO 27002. It establishes a top-level amendment that all references to 'information security' should be taken as including protection of privacy.

Controls with a potentially significant impact on privacy and data protection are given extensive extra guidance. This includes subjects such as removable media, cryptography and secure development.

Clause 7: Additional guidance for controllers

This clause provides guidance on ISO 27701's Annex A controls, which are specific to privacy for the purposes of PII controllers. These controls address many of the critical areas of data protection and privacy that are not accounted for by the controls provided in ISO 27001.

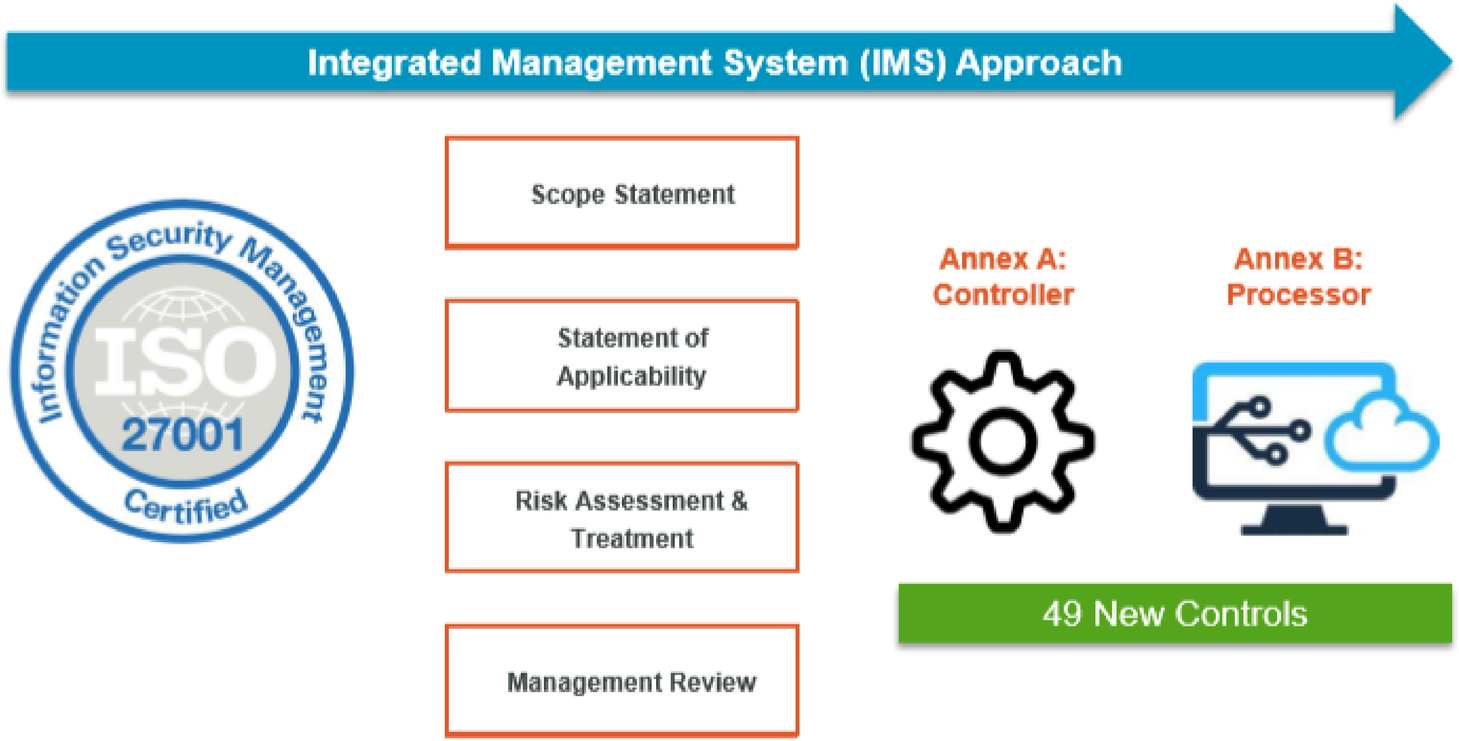
Clause 8: Additional guidance for processors

This clause provides guidance on ISO 27701's Annex B controls, which are specific to privacy for the purposes of PII processors. These controls address many of the critical areas of data protection and privacy that are not accounted for by the controls provided in ISO 27001.

Ref. IT GOVERNANCE GREEN PAPER | SEPTEMBER 2019

ISO/IEC 27701:2019 Controls

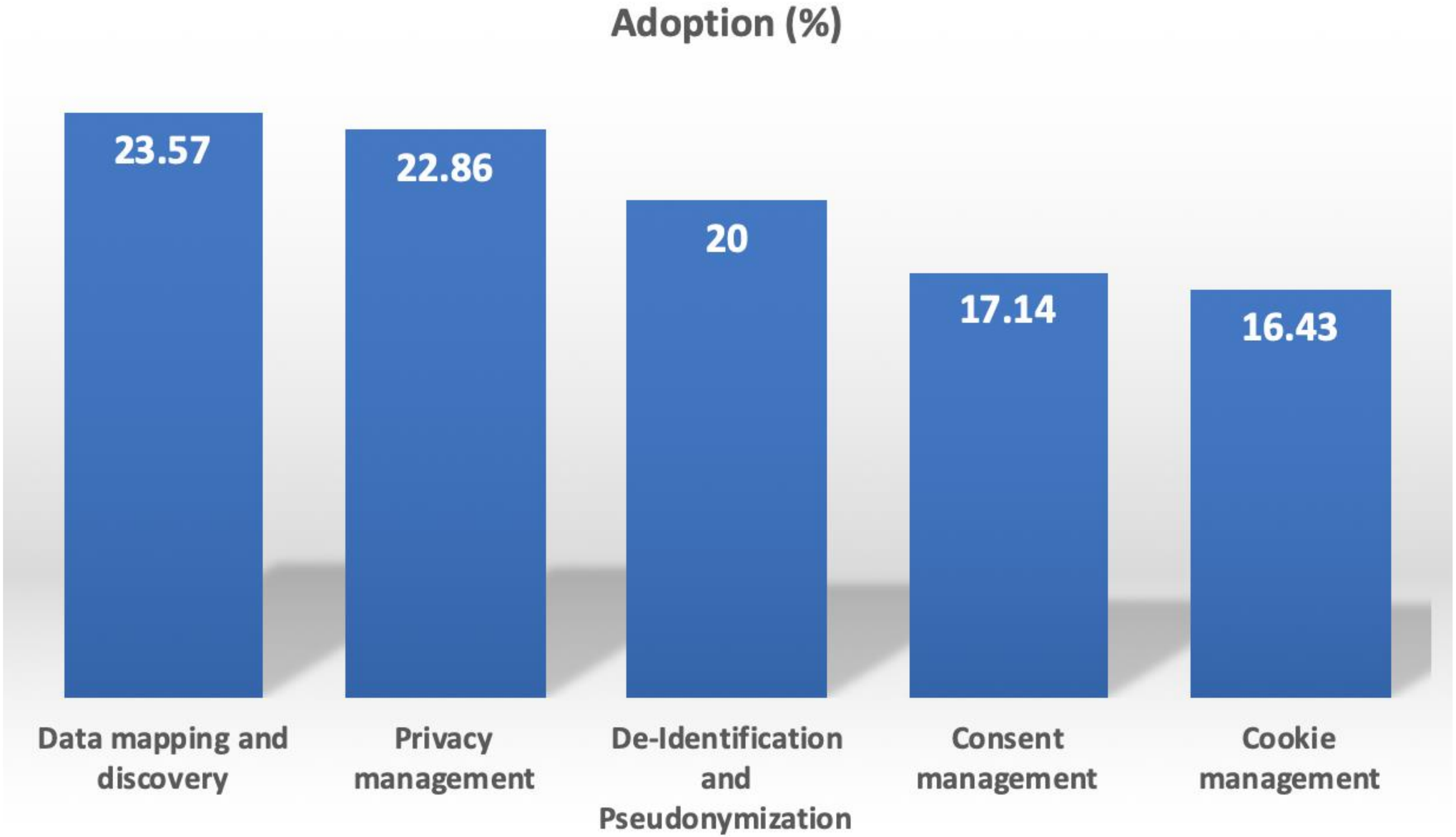
Implementing ISO 27701 with ISO 27001



Ref. ISO 27701: The New Global Data Privacy Certification

COALFIRE ISO – September 24, 2019

Privacy Enhanced Technology (PET)
What Privacy Technology should you Invest?



Source: Clarip


Q & A

การใช้มาตรฐาน ISO/IEC 20000:2018 เพื่อการบริหารจัดการบริการ IT อย่างมีประสิทธิผล

Agenda

- What is Service Management?
- Benefits of IT Service Management
- Using ISO/IEC 20000:2018 for managing your IT Services

What is Service Management?

- What is Service Management?

  ‘A set of *specialized* organizational *capabilities* that allows customers to derive value from the services they are provided’

- Capabilities…
  - Exist as processes & functions
  - Represent service provider capacity, competency, & confidence for action

- Capabilities permit the ‘shaping’ of resources

Why are high quality services needed?

- Why are high quality services needed?

  - Increasingly dependency on IT service provision
  - Increasing competitive pressures
  - More exacting user demands
  - Increased complexity of the infrastructure
  - Requirement to deliver value for money

Benefits of IT Service Management

- A continuous improvement in the quality of IT services
- Reduced long term costs in the development and delivery of IT services
- Reduced risk of not being able to meet business objectives
- Better communication between IT and the business
- Greater productivity and best use of skills and experience
- The ability to absorb a high rate of change
- IT staff are provided with best practice guidance
- Compliance to procedures can be audited

Service Management standard – ISO/IEC 20000:2018

INTERNATIONAL STANDARD

ISO/IEC 20000-1

Third edition
2018-09

Information technology — Service management —

Part 1: Service management system requirements

Technologies de l'information — Gestion des services —

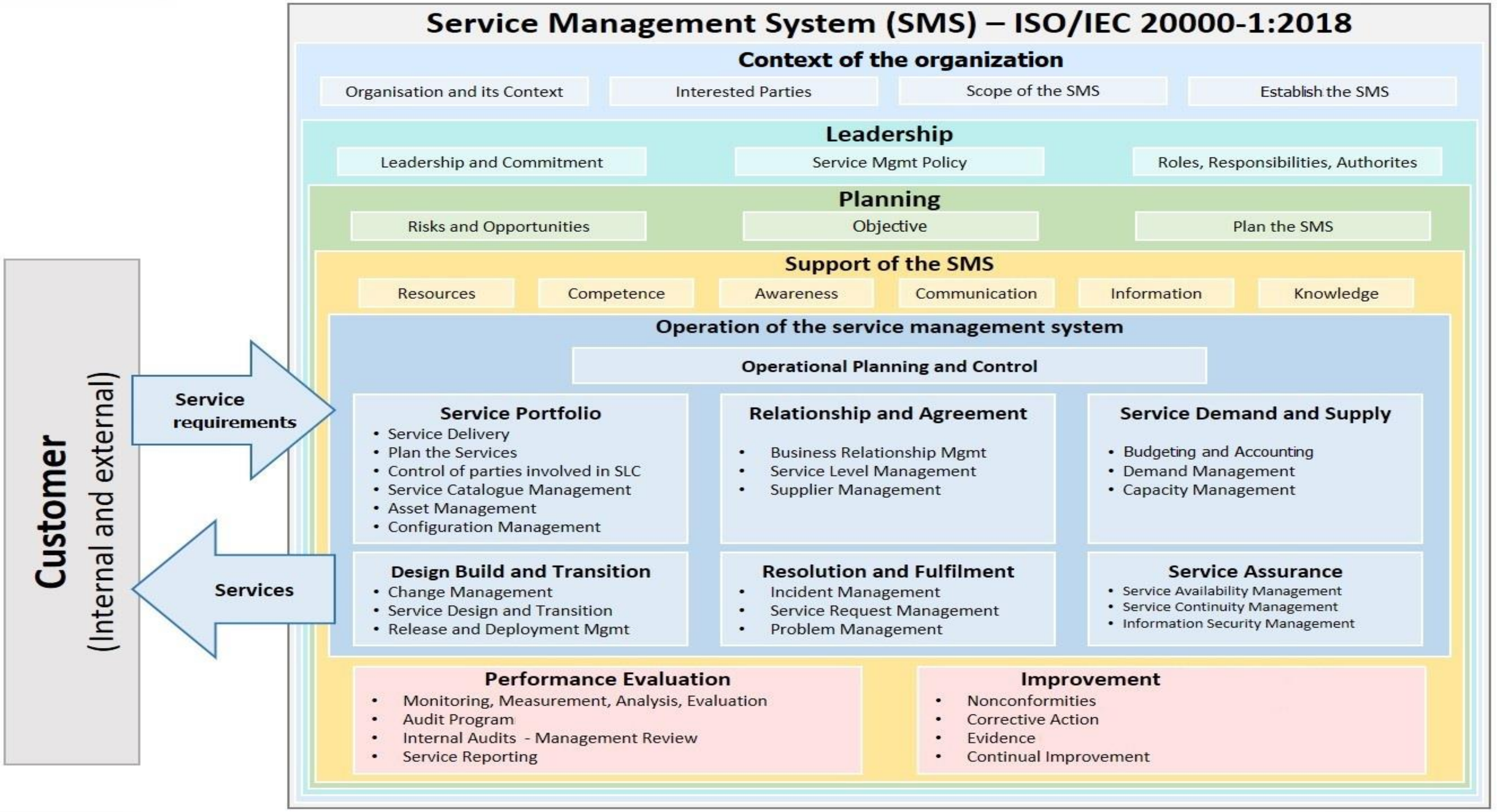
Partie 1: Exigences du système de management des services

ISO/IEC 20000:2018 can be summarized as:

- ***A standard*** to promote the adoption of an integrated process approach for the effective delivery of managed services to meet business and customer requirements

- ***A set of "controls"*** against which an organization can be assessed for effective IT Service Management processes

- The ISO 20000 standard defines the requirements for an organization to ***deliver managed services of an acceptable quality*** for its customers


Service Management System (SMS) – ISO/IEC 20000-1:2018
Context of the organization
Organisation and its Context
Interested Parties
Scope of the SMS
Establish the SMS
Leadership
Leadership and Commitment
Service Mgmt Policy
Roles, Responsibilities, Authorites
Planning
Risks and Opportunities
Objective
Plan the SMS
Support of the SMS
Resources
Competence
Awareness
Communication
Information
Knowledge
Operation of the service management system
Operational Planning and Control
Service Portfolio
Service Delivery
Plan the Services
Control of parties involved in SLC
Service Catalogue Management
Asset Management
Configuration Management
Relationship and Agreement
Business Relationship Mgmt
Service Level Management
Supplier Management
Service Demand and Supply
Budgeting and Accounting
Demand Management
Capacity Management
Design Build and Transition
Change Management
Service Design and Transition
Release and Deployment Mgmt
Resolution and Fulfilment
Incident Management
Service Request Management
Problem Management
Service Assurance
Service Availability Management
Service Continuity Management
Information Security Management
Performance Evaluation
Monitoring, Measurement, Analysis, Evaluation
Audit Program
Internal Audits - Management Review
Service Reporting
Improvement
Nonconformities
Corrective Action
Evidence
Continual Improvement
Customer
(Internal and external)
Service requirements
Services

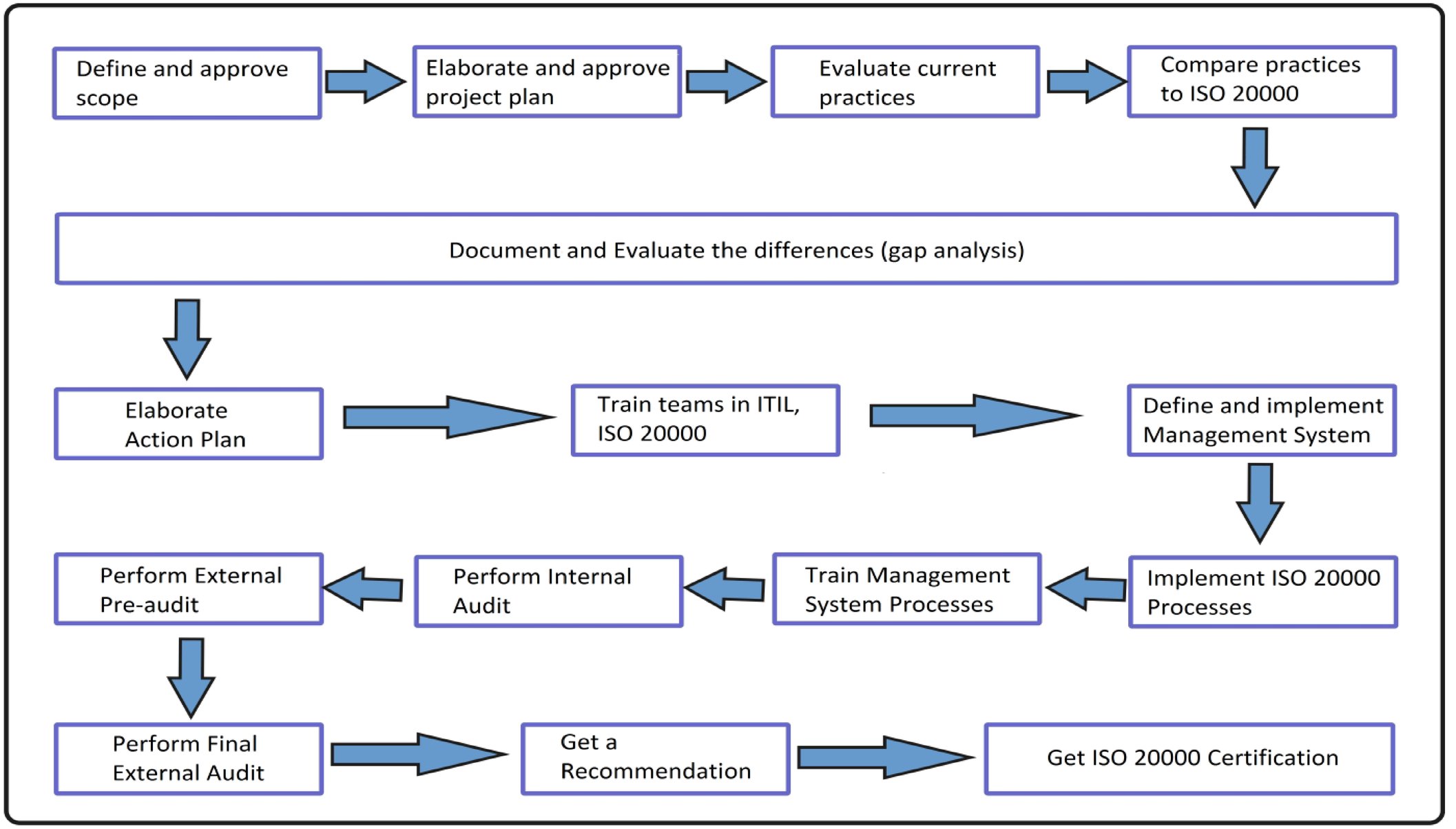
Using ISO/IEC 20000:2018 for managing your IT Services

- **Service Level Management**
  - ใช้กำหนดระดับของการให้บริการที่สอดคล้องตามข้อตกลงที่ทำไว้กับลูกค้า/ผู้ใช้งาน
- **Service Availability Management**
  - ใช้บริหารจัดการความพร้อมใช้งานของระบบงานต่าง ๆ อย่างมีประสิทธิภาพ
- **Service Continuity Management**
  - ใช้วางแผนรับมือกับเหตุการณ์ที่ไม่คาดหวังที่ทำให้เกิดการหยุดชะงักของ IT Services
- **Capacity Management**
  - ใช้บริหารจัดการขีดความสามารถของทรัพยากรต่าง ๆ ที่ใช้ในการให้บริการ อย่างมีประสิทธิภาพ
- **Information Security Management**
  - ใช้บริหารจัดการความมั่นคงปลอดภัยให้กับ IT Services รวมถึงสร้างความเชื่อมั่นให้กับลูกค้า/ผู้ใช้งาน

Using ISO/IEC 20000:2018 for managing your IT Services

- **Service Request Management**
  - ใช้ตอบสนองต่อคำร้องขอของลูกค้า/ผู้ใช้งาน อย่างมีประสิทธิภาพ
- **Incident Management**
  - ใช้บริหารจัดการเหตุการณ์ผิดปกติที่เกิดขึ้นกับ IT Services อย่างมีประสิทธิภาพ
- **Change Management**
  - ใช้บริหารจัดการความเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับ IT Services อย่างมีประสิทธิภาพ ทำให้เมื่อมีการเปลี่ยนแปลงเกิดขึ้นจะส่งผลกระทบต่อลูกค้า/ผู้ใช้งานน้อยที่สุด
- **Supplier Management**
  - ใช้บริหารจัดการซัพพลายเออร์ หรือ Vendor ให้ส่งมอบงานให้แก่เรา อย่างมีประสิทธิภาพ และถูกต้องตรงตามสัญญาหรือข้อตกลงที่ทำกันเอาไว้
- **Service Management Policy**
  - ใช้เป็นนโยบายเพื่อกำหนดทิศทางและกรอบการบริหารจัดการ IT Services ให้สอดคล้องตามความต้องการทางธุรกิจขององค์กร

ISO/IEC 20000:2018 Implementation



ISO/IEC 20000:2018 Implementation : Critical Success Factors

- **Team competence**:
  Service management employees need to have a deep understanding of service quality standards and the service management process.
- **Accountability**:
  Each process has to have an owner.
- **Documented policies and processes**:
  Documentation of all activities is absolutely essential.
- **Communications**:
  Communication between team members and the processes for communicating are of the utmost importance.
- **Audits**:
  Perform regular conformance audits and make improvements.


Q & A

THANK YOU

For more information, contact: **ACinfotec Consulting Services**

02-670-8980-3 | services@acinfotec.com | www.acinfotec.com


Consulting


Training


Assessment


Solutions

ACINFOTEC > DRIVING BUSINESS EXCELLENCE