อัพเดตมาตรฐานมาแรงปี 2563

มาตรฐานไหนที่องค์กรควรเลือกทำ

INFOTEC

15.03.2563

Speaker Profile

ชื่อวิทยากร : เกรียงไกร ชุ่มศักดิ์ตระกูล

ตำแหน่ง : Consulting Innovation Manager บริษัท ACinfotec

ประกาศนียบัตร :

- PECB Certified Trainer, PECB ISO27k Lead Implementer & Auditor
- PCI Professional, IRCA ISMS Lead Auditor
- CISSP, CEH, Security+

ประสบการณ์ :

- ที่ปรึกษามาตรฐาน ISO27001 ให้หน่วยงานภาครัฐ ภาคเอกชน หน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศ ธนาคารในประเทศและต่างประเทศ
- ที่ปรึกษามาตรฐาน PCI DSS ให้ธนาคารในประเทศ และธุรกิจชำระเงินออนไลน์
- ที่ปรึกษาด้านความปลอดภัยไซเบอร์ ให้บริษัทข้ามชาติในธุรกิจปิโตรเลียมและพลังงาน ธนาคารในประเทศ หน่วยงานกำกับ และหน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศ

Agenda

เวลา	หัวข้อ	วิทยากร
09.30 – 10:00	อัพเดตมาตรฐานมาแรงปี 2563 ... มาตรฐานไหนที่องค์กรควรเลือกทำ	เกรียงไกร ชุ่มศักดิ์ตระกูล
10:00 – 10.45	ISO27001:2013 ยังตอบโจทย์มาตรฐานด้านความปลอดภัยหรือไม่ ... เวอร์ชั่นใหม่ออกเมื่อไหร่ ?	เกรียงไกร ชุ่มศักดิ์ตระกูล
	PCI DSS v4.0 สถานการณ์ร่างมาตรฐาน และแนวทางที่จะเปลี่ยนไปในเวอร์ชั่นใหม่	เกรียงไกร ชุ่มศักดิ์ตระกูล
10.45 – 11.30	บริหารจัดการข้อมูลส่วนบุคคลด้วยมาตรฐาน ISO/IEC 27701:2019	สมบูรณ์ นิลฟุ้งขจร
	การใช้มาตรฐาน ISO/IEC 20000:2018 เพื่อการบริหารจัดการบริการ IT อย่างมีประสิทธิผล	สมบูรณ์ นิลฟุ้งขจร
11:30 – 12.00	มีอะไรใหม่ในมาตรฐาน ISO 22301:2019 ?	นิจิรา วัฒนพันธุ์

What are standards?

- A document, established by a consensus of subject matter experts and approved by a recognized body

- Provides guidance on the design, use or performance of materials, products, processes, services, systems or persons.

The benefits of using standards

01

Improving performance

Success is all about how you perform at every level of your organization. Standards promote a culture of continual improvement.

02

Reducing business risk

Businesses today simply can't afford to take an improvised, reactive approach to risk. Using standards can help you to identify your risks and minimize them

03

Becoming more sustainable

By helping you to take a close look at how you're using energy and resources, using standards can save you money and improve your image while benefiting the environment

04

Encouraging innovation

In a global economy of rapidly emerging new technologies and markets, standards help set the rules and establish the frameworks, making it easier to innovate successfully.

05

Standards for services

If you're operating in a service industry, you need to pay close attention to your processes to ensure quality doesn't slip. A whole range of standards can help you out.

DISRUPTIVE FORCES

More organizations are looking to upscale their business and benefit from the implementation of standards. To determine the factors that play an important role in the growth of an organization we must determine the disruptive forces that affect the organization's growth directly or indirectly. There are four major trends which ISO deemed crucial disruptive factors for organizations

INCREASING TRADE UNCERTAINTY

CHANGING SOCIETAL EXPECTATIONS

IMPACTS OF CLIMATE CHANGE

DIGITAL TRANSFORMATION

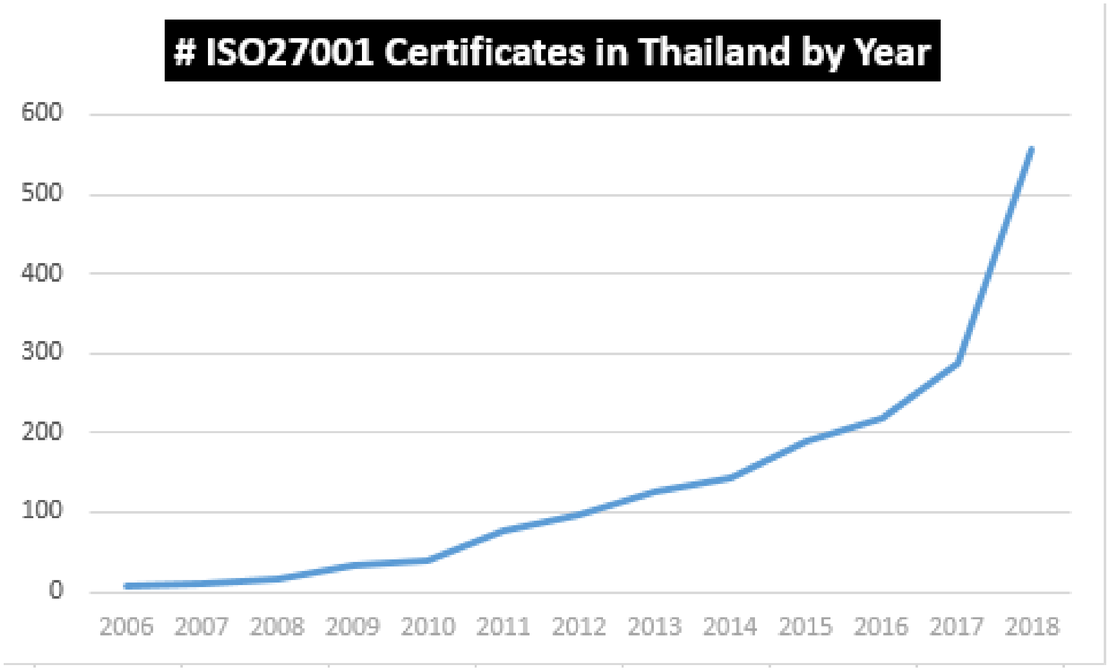
Which are Thailand top demanding standards for cyber security?

ISO 27001:2013

Industry's de facto Standard for Information Security

Number of certificates and sites in 2018 by country

Country	Site	Certificate
China	7,199	7,612
Japan	5,093	12,145
Taiwan, Province of China	827	1,410
Korea (Republic of)	353	530
Malaysia	276	470
Thailand	**239**	**557**
Indonesia	163	335
Viet Nam	113	241
Singapore	106	240
Philippines	94	331
Hong Kong	72	131
Worldwide	**31,910**	**59,934**



ISO 22301:2019

Crisis become closer than ever

ISO 27701:2019

Driven by Law and Regulation

PCI DSS v3.2.1

Driven by Business

PCI Non-Compliance : Negative consequences for businesses

1. Monthly penalties by the financial entities ranging from $5,000 to $100,000
2. Infringement consequences
3. Compensation costs PCI non-compliance
4. Legal Action
5. Damaged reputation for PCI non-compliance
6. Revenue loss

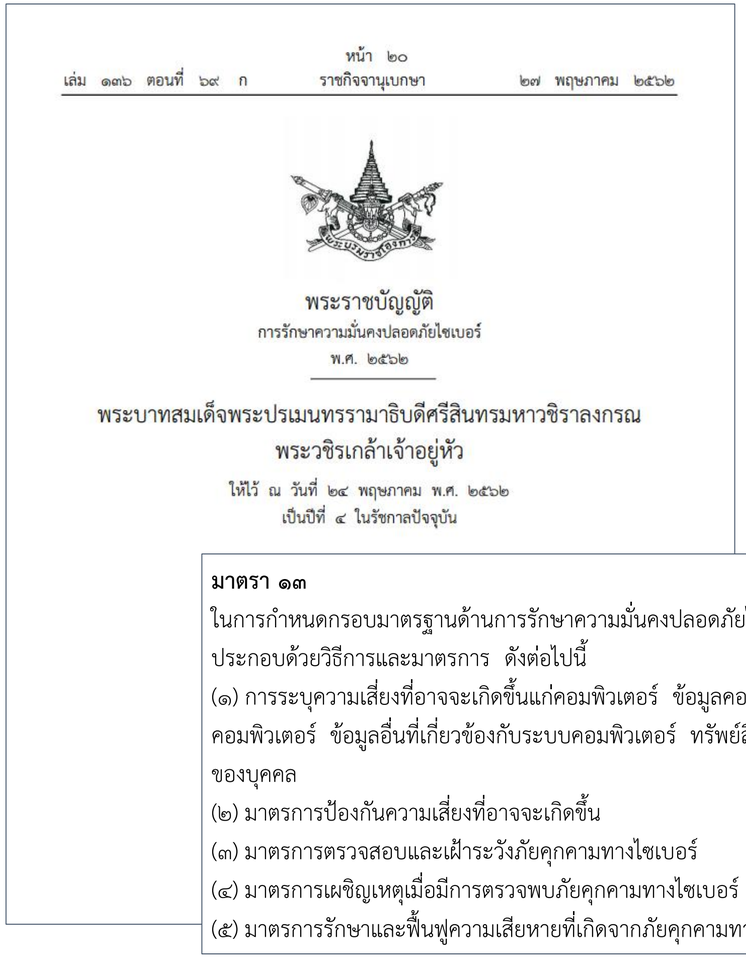
PCI DSS & Travel Agent Compliance Requirements

IATA

International Air Transport Association

NIST CSF v1.1

Driven by Law + Cybersecurity Protection Demand



หน้า ๒๐
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

มาตรา ๑๓
ในการกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้
(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล
(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น
(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

Function	Categories	Subcategories
Identify	Asset Management (ID.AM)	ID.AM-1 to ID.AM-6
	Business Environment (ID.BE)	ID.BE-1 to ID.BE-5
	Governance (ID.GV)	ID.GV-1 to ID.GV-4
	Risk Assessment (ID.RA)	ID.RA-1 to ID.RA-6
	Risk Management Strategy (ID.RM)	ID.RM-1 to ID.RM-3
	Supply Chain Risk Management (ID.SC)	ID.SC-1 to ID.SC-4
Protect	Access Control (PR.AC)	PR.AC-t to PR.AC-5
	Awareness Training (PR.AT)	PR.AT-1 to PR.AT-5
	Data Security (PR.DS)	PR.DS-1 to PR.DS-9
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1 to PR.IP-11
	Maintenance (PR.MA)	PR.MA-1 to PR.MA-2
	Protective Technology (PR.PT)	PR.PT-1 to PR.PT-5
Detect	Anomalies and Events (DE.AE)	DE.AE-1 to DE.AE-5
	Security Continuous Monitoring (DE.CM)	DE.CM-1 to DE.CM-8
	Detection Processes (DE.DP)	DE.DP-1 to DE.DP-5
Respond	Response Planning (RS.RP)	RS.RP-1
	Communications (RS.CO)	RS.CO-1 to RS.CO-5
	Analysis (RS.AN)	RS.AN-1 to RS.AN-4
	Mitigation (RS.MI)	RS.MI-1 to RS.MI-3
	Improvements (RS.IM)	RS.IM-1 to RS.IM-2
Recover	Recovery Planning (RC.RP)	RC.RP-1
	Improvements (RC.IM)	RC.IM-1 to RC.IM-2
	Communications (RC.CO)	RC.CO-1 to RC.CO-2

ISO27001:2013 ยังตอบโจทย์มาตรฐานด้านความปลอดภัยหรือไม่

History of ISO27001

BS 7799-2:1998
First Publication, mostly adopted in UK and some countries in Europe

ISO 27001:2005
Globally accepted as a standard for information security management with more than 8,000 certified organizations worldwide and more than 80 organizations in Thailand

ISO 27001:2013
Formal Publication

BS 7799-2:2002
Third revisions, became popular in Japan and was introduced to Thailand by ACinfotec with first certified organization

ISO FDIS 27001:2013
Final Draft International Standard

ISO 27001:2013

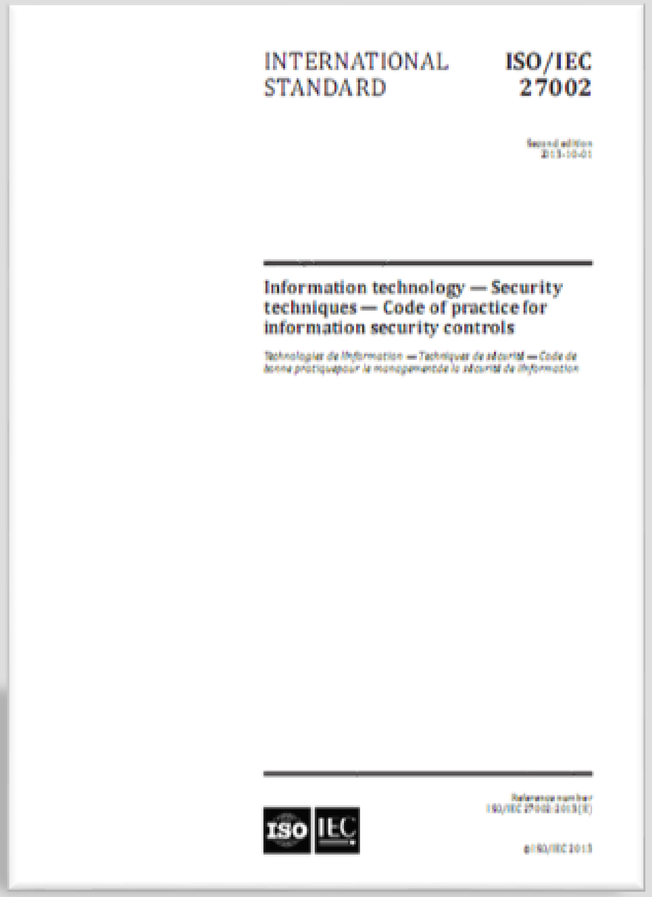
- The ISMS Requirements (for audit and certification)

- Published on 1 Oct 13
- Supersede ISO 27001:2005
- Certifiable and auditable
- Used 10 Clauses-structure (based on Annex SL) to align with modern management system standard
- Based on risk management approach and aims to achieve effective information security management through continual improvement process
- Included an Annex (Annex A) which lists the controls from ISO 27002 with the “should” replaced with “shall”

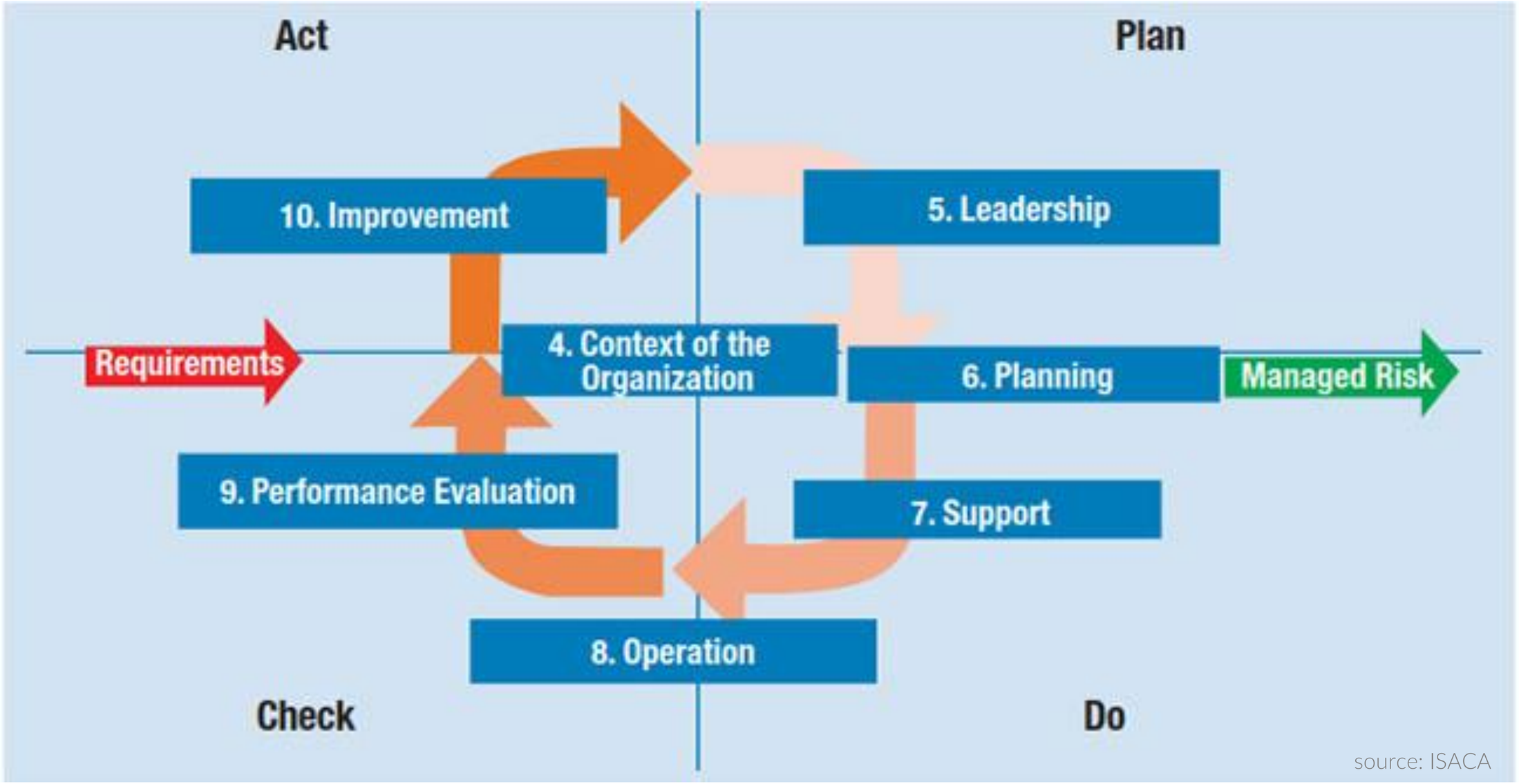
ISO 27002:2013

- The Guideline (for implementing security controls)

- Published on 1 Oct 13
- Supersede ISO 27002:2005
- NOT a certifiable or auditable standard – it is a code of best practice only
- It is intended to provide a catalogue of non-mandatory best practice with some implementation guidelines – the controls in ISO 27002 are contained in ISO/IEC 27001 Annex A as mandatory “shall” statements



Information Security Management System (ISMS)



source: ISACA

Controls in Annex A

Confidentiality, Integrity and Availability of Information

Ensuring that information is accessible only to those auth orized to have access

Safeguarding the accuracy and completeness of information a nd processing methods

Ensuring that authorized users have access to information and associated assets when required

ISO 27002:2013 Status

Status: Valid

New version being drafted targeted to be released at the end of 2021.

LATEST NEWS – ISO27002

- The standard is being revised to reflect changes in the field such as BYOD, cloud computing, virtualization, crypto-ransomware, social networking, pocket ICT and IoT
- The standard will be renamed “Information security controls”
- The standard will have a radically different structure:

The controls are being categorized into

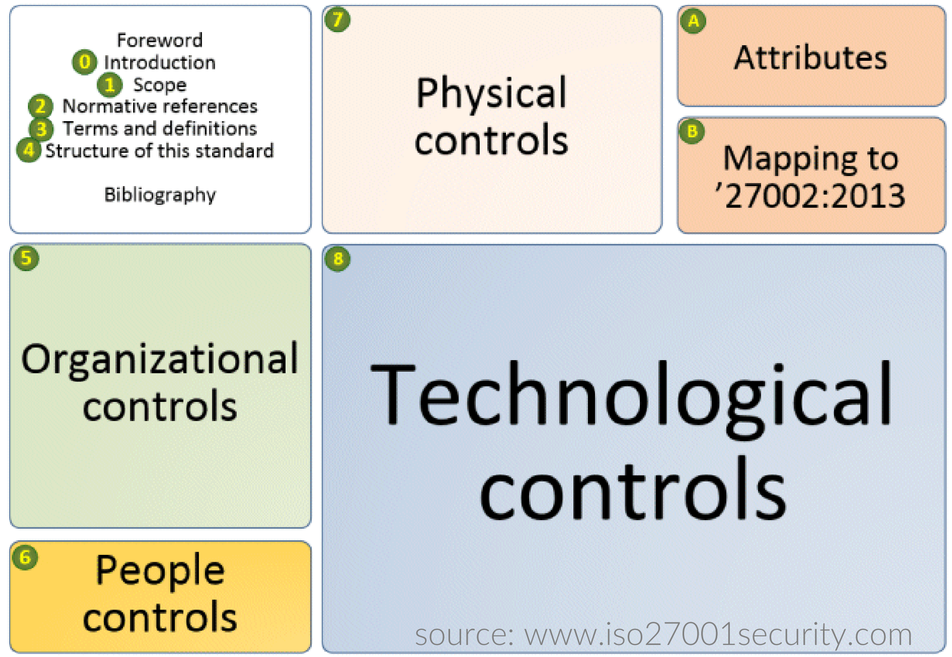
Organizational controls - controls involving management and the organization in general, other than those in ISO27001

Technical controls - controls involving or relating to technologies, IT in particular (implying “cybersecurity”, perhaps, if so defined);

People controls - controls involving or relating to behaviors, activities, roles and responsibilities etc.;

Physical controls - tangible controls such as locks, and other means of environmental protection and control such as fire and intruder alarms and uninterruptible power supplies;

External party controls - controls involving or relating to parties outside the scope of an ISMS (e.g. contracted cloud services, service level agreements, legal and regulatory obligations, privacy policies and other obligations to customers etc.)



ISO 27001:2013 Status

Status: Valid

LATEST NEWS – ISO27001

- ISO/IEC 27001 will be revised with the goal to have a new version in 2021, with a new list of controls (according to the future ISO/IEC 27002),
- Fundamental terms & definitions will be stated in the standard itself and not in a separate standard (such as ISO/IEC 27000)

Latest update of standards in ISO 27000 series

- ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems - Overview and vocabulary (fifth edition)
- ISO/IEC TS 27008:2019 — Information technology — Security techniques — Guidelines for the assessment of information security controls (second edition)
- ISO/IEC 27007:2020 — Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (third edition)
- ISO/IEC 27050-3:2020 Information technology — Security techniques — Electronic discovery — Code of practice for electronic discovery

Enforcement of ISO27001 in Thailand

ลำดับ	ชื่อประกาศ	หน่วยงานที่บังคับ	มาตรฐานที่อ้างอิง
1	หลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560	คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)	ISO27001:2005, เฉพาะ Annex A
2	หลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. 2560	คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)	ISO27001:2005, เฉพาะ Annex A
3	มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต (BAHTNET) (สรข. 4/2560)	ธนาคารแห่งประเทศไทย (ธปท.)	ISO27001 เวอร์ชั่นล่าสุด (2013)
4	มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ICAS) (สรข. 5/2560)	ธนาคารแห่งประเทศไทย (ธปท.)	ISO27001 เวอร์ชั่นล่าสุด (2013)

Payment Card Industry Data Security Standard (PCI DSS) v4.0

History of PCI DSS

DECEMBER 15, 2004
PCI DSS 1.0

PCI DSS Version 1.0 is released. This is the first time that all five major credit card brands have come together to create a comprehensive standard for all merchants in the payments cycle.

SEPTEMBER 2006
PCI DSS 1.1

PCI DSS Version 1.1 is released. Calls for the professional review of all web applications and the placing of virtual firewalls as a security measure.

OCTOBER 2010
PCI DSS 2.0

Reinforces the need for thorough scoping before an assessment and promotes more effective log management. It also broadens validation requirements for the assessment of vulnerabilities in a merchant environment.

NOVEMBER 2013
PCI DSS 3.0

Updates made as a result of shifting needs in the payments industry: Weak passwords and authentications by merchants and service providers;
Third-party security challenges;
Inconsistency in assessments

APRIL 2015
PCI DSS 3.1

Calls for merchants to deprecate the Secure Sockets Layer (SSL) and "early" Transport Security Layer (TSL) protocols immediately, as these encryption protocols put payment data at a high level of risk.

APRIL 2016
PCI DSS 3.2

Centered on a reformed change-management process, multi-factor authentication, service provider regulations and primary account number (PAN) masking.

FEB 2018
PCI DSS 3.2

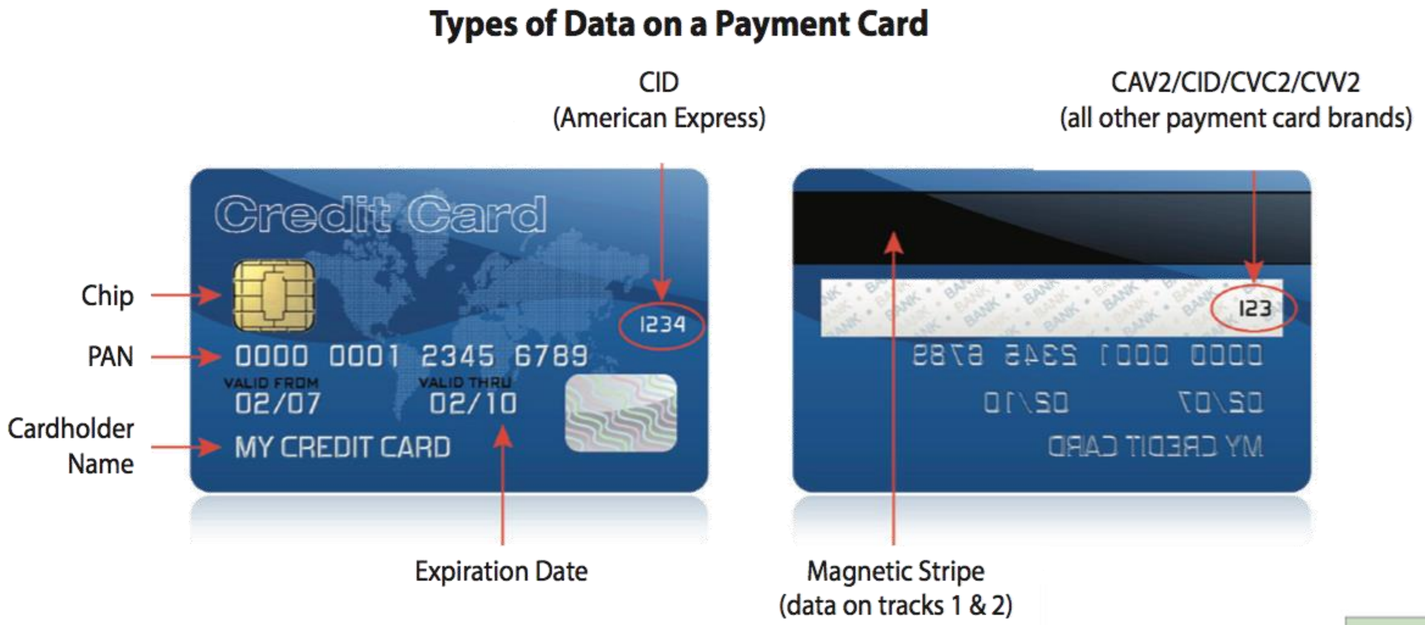
PCI 3.2 takes effect

- Eliminate use of SSL and early TLS version
- MFA will be required for ALL administrative access to cardholder data – not just consoles.
- Maintain detailed documentation of cryptographic architecture

PCI DSS - 12 Core Requirements

Build and Maintain a Secure Network and Systems	**1.**	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.**	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.**	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.**	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.**	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	**12.**	Maintain a policy that addresses information security for all personnel

PCI DSS – CHD & SAD



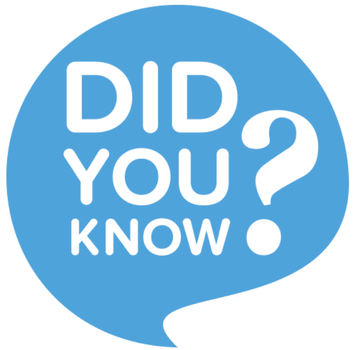
		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

Who need to comply with PCI DSS?

"Any organization that accepts payment cards or **stores, processes, or transmits** credit or debit card data must comply with the PCI DSS."

Goals for PCI DSS v4.0

- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility and support additional methodologies to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedure



The standard is still on RFC process and won't be published **until 2021** and won't be required for **2 years after the publication date**.

A first draft of PCI DSS v4.0

• The draft of PCI DSS v4.0 addresses feedback received during the 2017 RFC and **reflects changes in payments environments** and **security technologies**.

• The updates made to the standard focus on **strengthening security and adding flexibility**.

• While the 12 core PCI DSS requirements remain fundamentally the same, **several new requirements** are proposed to address evolving risks and threats to payment data and to reinforce security as a continuous process.

• **All requirements are redesigned to focus on security objectives**, and there is a **new validation option** that gives **more flexibility** to organizations **using different methodologies to meet the intent of PCI DSS** requirements.

Changes to PCI DSS's layout and descriptions

The overall structure of the PCI DSS is retained in version 4.0, and will keep the same 12 high level requirements.

Changes to PCI DSS's layout and descriptions v.4.0 will include:

1. More accurate requirement titles
2. Additional direction and guidance provided in the Overview section
3. Requirements organized into Security Objectives
4. Requirements refocused as objective or outcome-based statements focused on implementation of the security control as the end result.
5. Clear identification of Intent (Objective) for each requirement
6. Expanded Guidance

Examples of some of the proposed new requirements

1. Scoping – Increased testing and documentation will be required for confirmation of the accuracy and completeness of scope of the cardholder data environment (CDE) and periodic scope validation processes.
2. CHD Protection – Card encryption requirements will be expanded to include all transmissions of CHD instead of only those across public networks.
3. Security awareness training – Requirements for training of end users will be enhanced to include more information regarding current threats and phishing, social engineering, etc.
4. Risk assessment – The Council recognizes that the current PCI DSS requirement that a risk assessment be conducted is not always resulting in useful risk analysis and risk management outcomes. This requirement will be modified to ensure that the risk assessment is not being treated as a “checkbox exercise” by organizations.
5. Authentication – The new version of the DSS will provide more flexibility for the use of authentication techniques and solutions within the CDE to align them with industry best practices.
6. Cloud environments – Version 4.0 will evolve all requirements to be more accommodating for the use of technologies such as cloud hosting services.
7. Sampling – Additional direction for assessors on sampling guidance will be included to verify that controls are in place consistently across the entire population.

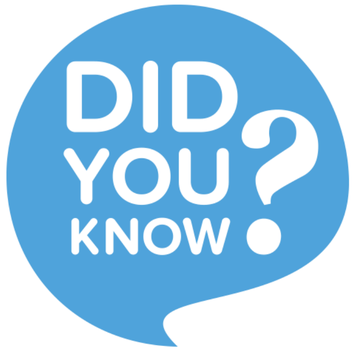
Two Implementation Options

Defined Implementation

- Follows current PCI DSS requirements and testing procedures
- Supports entities whose security implementations align with current requirements
- Provides direction on how to meet security objectives

Customized Implementation

- Focuses on the intent of each PCI DSS requirement
- Provides greater flexibility for entities to demonstrate how security controls meet common security objectives
- May suit risk-mature entities with a robust risk management approach
- Unlike compensating controls, customized validation will not require a business or technical justification for meeting the requirements using alternative methods, as the requirements will now be outcome-based. (Compensating controls will be removed)



Organizations can choose to report their compliance via one of these two options or choose a blended approach where some of the control requirements may be assessed under the defined implementation and others using the customized implementation approach.


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