\Orchestrating a brighter world NEC

ITU Cybersecurity Workshop
Cybersecurity and Risk Assessment in Practice

Role of standards and ISO/IEC 27000 series update

26 January 2017

Miho Naganuma
NEC Corporation

\Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create
the ICT-enabled society of tomorrow.
We collaborate closely with partners and customers around the world,
orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to
greater safety, security, efficiency and equality,
and enable people to live brighter lives.

Role of standards:
Risk management in international standards

\Orchestrating a brighter world NEC

Standardization : General

- Specifications
- Symbols & Marks
- Frameworks

- Scalability : Cost-down
- Compatibility & Inter operability
- Quality Assurance
- Uniformed service
- **Common concept with terms**

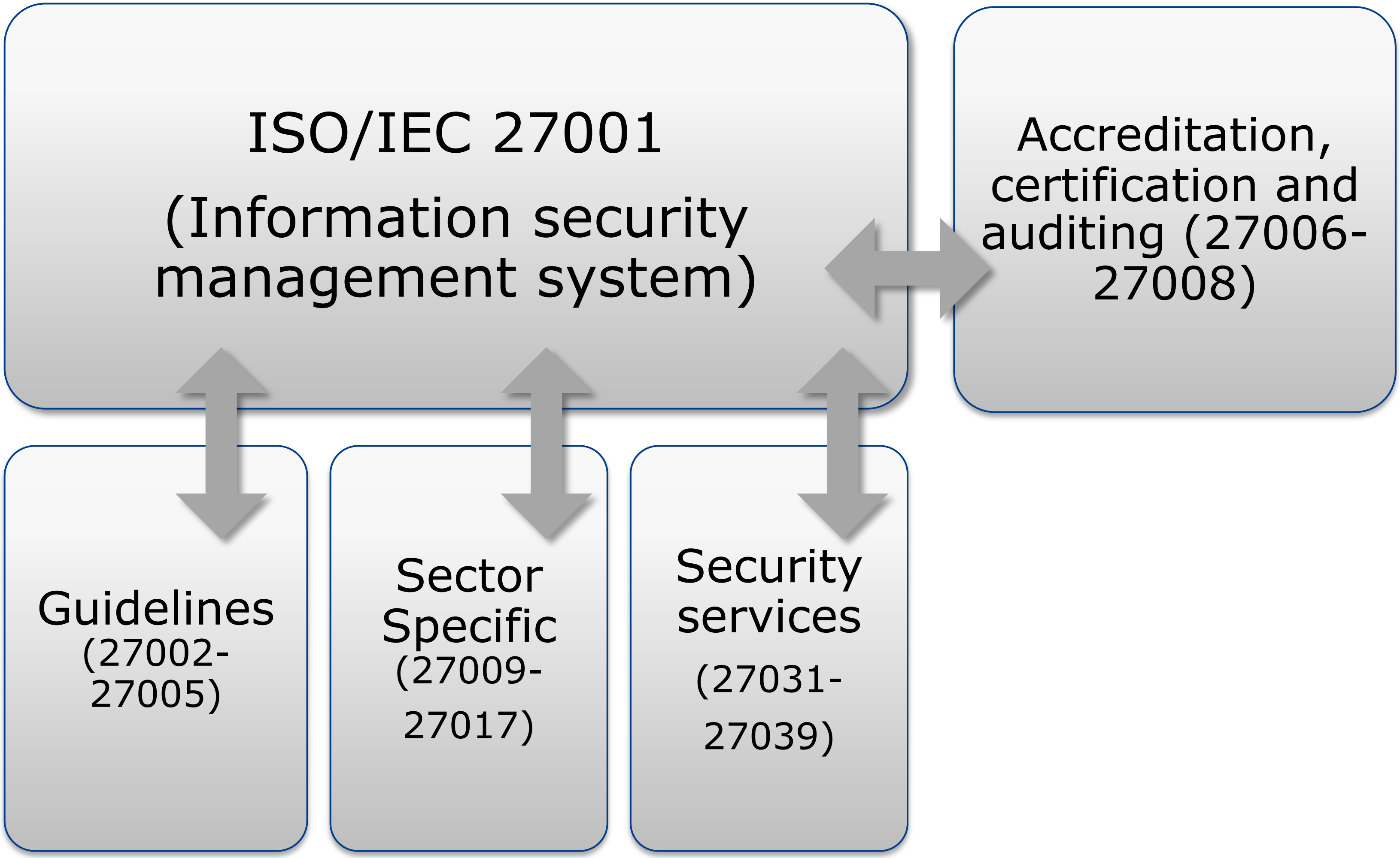
To provide things/frameworks that can be used by anyone and at anywhere

Information Security management with risk approach

ISO/IEC 27000 Series

- Requirements and guidelines on information security management within the context of an information security management system (ISMS).
- Risk based approach --Organizations' information security management should be based on risk management.
- Global common language -- Widely accepted concept around the world.

ISO/IEC 27000 series



ISO/IEC 27001

(Information security management system)

Accreditation, certification and auditing (27006-27008)

Guidelines (27002-27005)

Sector Specific (27009-27017)

Security services (27031-27039)

ISO/IEC 27005
Risk management

Telecom specific
ISO/IEC 270011 (ITU-T X.1051)

ISMS - Requirements

risk
effect of uncertainty on objectives

risk assessment
overall process of risk identification , risk analysis and risk evaluation

ISO/IEC 27001

Context of organisation
Leadership
Planning
Support
Operation
Performance Evaluation
Improvement

Actions to address risks and opportunities

risk management
coordinated activities to direct and control an organization with regard to risk

Information security requirements

ISO/IEC 27002 (Code of practice for IS controls)

0.2 Information security requirements

It is essential that an organization identifies its security requirements.

There are three main sources of security requirements:

a. assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b. legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

c. set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

27000 series update

Orchestrating a brighter world NEC

27000 series document update

ISO/IEC	Title	Status
27000	ISMS Overview and vocabrary	2014
27001	ISMS Requirements	2013
27002	ISMS Code of practice of information security controls	2013 Preparation for revision
27003	ISMS Guidance	2010 Planned in 2017
27004	ISMS monitor, measure, analysis and evaluation	2016
27005	Information security risk management	2011 Preparation for revision
27006	Requirements for bodies providing audit and certification of information security management systems	2015
27007	Guidelines for information security management systems auditing	2011 Planned in 2018
27008	Guidelines for auditors on ISMS controls	2011 Planned in 2017

27000 series document update

ISO/IEC	Title	Status
27009	Sector-specific application of ISO/IEC 27001 -- Requirements	2016
27010	Information security management for inter-sector and inter-organizational communications	2010
27011 (ITU-T X.1051)	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	2016
27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	2015
27014 (ITU-T X.1054)	Governance of information security	2014 Prepared for revision
27015	Information security management guidelines for financial services	2012
27016	Information security management -- Organizational economics	2014

27000 series document update

ISO/IEC	Title	Status
27017 (ITU-T X.1361)	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	2016
27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	2014
27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	2013 Planned in 2018
27021	Competence requirements for information security management systems professionals	Planned in 2018
27023	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	2015

27000 series document update

ISO/IEC	Title	Status
27031	Guidelines for information and communication technology readiness for business continuity	2011
27032	Cybersecurity	2012
27033 (Part 1-6)	Network security	2010-2014
27034 (Parts1-5)	Application security	2011- work ongoing
27035 (Part 3)	Information security incident management	2011- Work ongoing
27036 (Part 1-4)	Supplier relationship information security	2014-2016
27050 (Part 1-)	Electronic discovery	Work ongoing

New area and future work

New series for “Cyber”

- Cybersecurity standardisation framework
- Cyber insurance (New work item)
- Cyber resilience (Current Study Period)
- Cybersecurity (Current Study Period)

\Orchestrating a brighter world

NEC