Deloitte.

ILNAS
Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services

# Beyond the pure publication of ISO documents, what do we have ?

**Joint event**
**ILNAS and Luxembourg Chamber of Commerce**
**Friday, November 23rd 2012**

# Agenda

| | |
|---|---|
| 1 | Main types of published ISO documents |
| 2 | About ISO/IEC 27010:2012 and ISO/IEC TR 27015 project |
| 3 | Facts, figures and lessons learnt |

# 1. Main types of published ISO documents

# 1. Main types of published ISO documents 1/4

Be aware that the International Organization for Standardization (ISO) does not only publish standards.

Following types of ISO documents exist:

- **International Standard**

  Document established by consensus and approved by the ISO and/or the International Electrotechnical Commission (IEC).

  This document provides, for common and repeated use, rules, guidelines or characteristics for activities.

  Examples of ISO International Standards within information security domain:
  - ISO/IEC 27001:2005.
  - ISO/IEC 27002:2005.
  - ISO/IEC 27003:2010.
  - ISO/IEC 27013:2012 (guidelines on implementing both ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011 *service management system*).

# 1. Main types of published ISO documents 2/4

- **Technical Specification**

  Document published by the ISO and/or the IEC and for which there is the future possibility of agreement on an International Standard.

  Examples of ISO Technical Specifications within information security domain:
  - ISO/IEC WD TS 27017 (cloud computing).
  - ISO/IEC PDTS 30104 (physical security attacks and mitigation techniques).

  Note *These technical specifications are currently under development.*

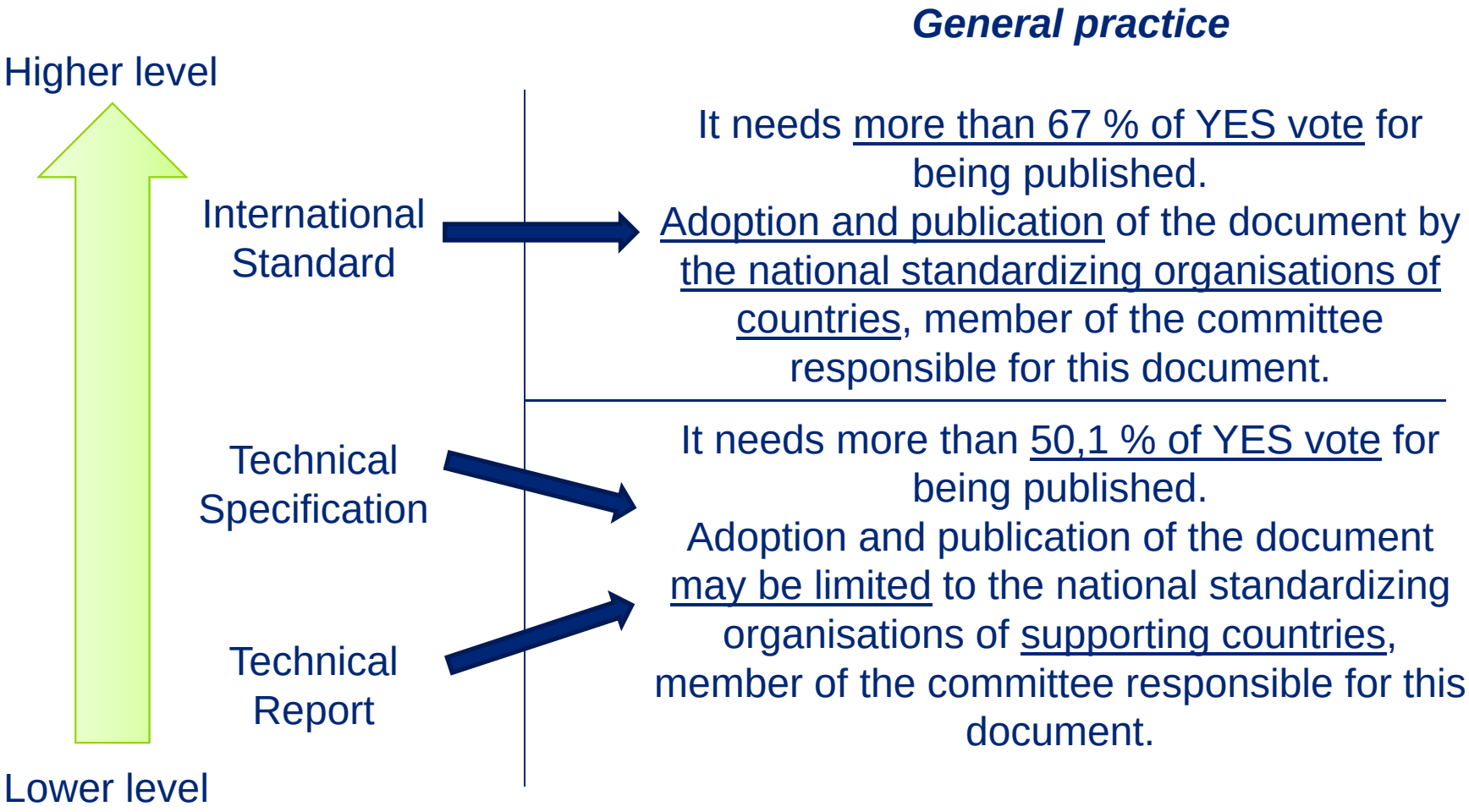
- **Technical Report**

  Document published by the ISO and/or the IEC and containing collected data of a different kind from which normally an International Standard or Technical Specification is published.

  Examples of ISO Technical Reports within information security domain:
  - ISO/IEC TR 27008:2011 (guidelines for auditors on assessing controls).
  - ISO/IEC TR 15446:2009 (common criteria).

# 1. Main types of published ISO documents 3/4

The main difference between these types of documents is in their recognition level from both international and national perspectives.



# 1. Main types of published ISO documents 4/4

How to recognize them ?

**ISO/IEC 27005:2011**

**Information technology -- Security techniques -- Information security risk management**

International Standard

**ISO/IEC WD TS 27017**

**Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002**

Technical Specification

**ISO/IEC TR 27008:2011**

**Information technology -- Security techniques -- Guidelines for auditors on information security controls**

Technical Report

# 2. About ISO/IEC 27010:2012 and ISO/IEC TR 27015 project

# 2.1 Introduction to ISO/IEC 27010:2012 & ISO/IEC TR 27015 pr.1/3

## ISO/IEC 27001:2005

- It defines requirements for establishing an Information Security Management System (ISMS).
- First published as BS 7799-2:1998 (British Standard).
- Now published as ISO/IEC 27001:2005.
  - Originally 8 pages.
  - Now 14 pages.

## ISO/IEC 27002:2005

- It defines a catalogue of information security controls.
- First published as BS 7799:1995.
- Then ISO/IEC 17799:2000.
- Now ISO/IEC 27002:2005.
  - Originally 50 pages.
  - Now 120 pages… and still growing.

# 2.1 Introduction to ISO/IEC 27010:2012 & ISO/IEC TR 27015 pr.2/3

## The controls problem

- ISO/IEC 27002:2005 is a universal cookbook with everybody having their own favourite recipes (i.e. information security controls) for complementing it.
- ISO/IEC 27002:2005 has become large and unwieldy.

# 2.1 Introduction to ISO/IEC 27010:2012 & ISO/IEC TR 27015 pr.3/3

## The solution

- Take out how to implement controls in details.
  *Move this content to technical standards (e.g. incidents management, network security, disaster recovery) in 2703x series.*
- Take out specific controls.
  *Move this content to specific standards (e.g. telecommunications, cloud) in 2701x series.*

ISO/IEC 27010:2012 is a specific standard for inter-organisational information sharing.

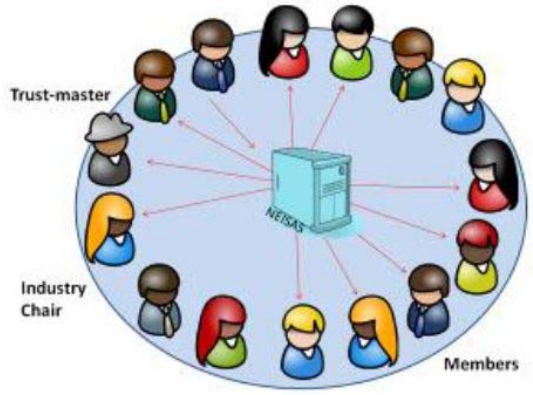
ISO/IEC TR 27015 project is a specific technical report for financial services.

# 2.2 About ISO/IEC 27010:2012 1/2

## Introduction

- Almost all organisations exchange information with known partners following information security controls from ISO/IEC 27002:2005.

- But communities of organisations are different...
  *Hence ISO/IEC 27010:2012.*




## ISO/IEC 27010:2012 applicability

- Is applicable to both public and private sectors.

- Contains models for information sharing:
  - Trusted Information Communication Entity (TICE) - Luxembourg contribution.
  - Warning, Advice and Reporting Point (WARP) - UK contribution.

*What is the main impact of having contributed to the design of information sharing models ?*

<u>It is a broader one</u> !
These models may be probably followed by a majority of communities of organisations throughout the world.

# 2.2 About ISO/IEC 27010:2012 2/2

## Description

- ISO/IEC 27010:2012 complements ISO/IEC 27001:2005 and ISO/IEC 27002:2005.
  - It has no additional ISMS requirements over ISO/IEC 27001:2005 but some warnings/observations.
    Example:
    - Ambiguity over “the organization” expression.
  - It adds 10 extra information security controls and augments 16 ones defined in ISO/IEC 27002:2005.
    - New information security controls are mainly located in a new control objective named *Information exchanges protection*.
      Examples:
      - Anonymous source protection.
      - Right to audit other members of information sharing community.
    - Augmentation of information security controls varies.
      Example:
      - Sharing information between community members about incidents that can have information security impacts.

# 2.2 About ISO/IEC TR 27015 project 1/2

## Introduction

- Almost all organisations providing financial services have established information security controls from ISO/IEC 27002:2005.

- But these organisations have specific information security needs and constraints while performing financial transactions...
  *Hence ISO/IEC TR 27015 project.*

## ISO/IEC TR 27015 project applicability

- Is applicable to organisations providing financial services, meaning anyone in the "business of money".

- The "financial services" term is defined as follows:
  *Services in the management, investment, transfer, or lending of money.*

# 2.2 About ISO/IEC TR 27015 project 2/2

## Description

- ISO/IEC TR 27015 project only complements ISO/IEC 27002:2005.
  - It has no additional ISMS requirements and warnings/observations over ISO/IEC 27001:2005.
  - It adds 2 extra information security controls and augments 26 ones defined in ISO/IEC 27002:2005.
    - New information security controls are:
      - Internet banking services.
      - Compliance monitoring.
    - Augmentation of information security controls varies.
      Examples:
      - Information security aspects to consider when establishing an on-line transactions system to customers.
      - Consideration of procured financial services in the business continuity risk assessment.

# 3. Facts, figures and lessons learnt

# 3.1 It is a long story

## ISO/IEC 27010:2012

- Potential needs identified October 2007.
- New Work Item proposed April 2008.
- Target Publication Date November 2012.
- Published April 2012.

**TOTAL : 4,5 years**

## ISO/IEC TR 27015 project

- Potential needs identified February 2008.
- New Work Item proposed October 2008.
- Target Publication Date November 2012 (this date should be met).

**TOTAL : 4,5 years**

**The time needed for an ISO document to be developed and published (starting the expression of its needs) is between 3 and 5 years.**

# 3.2 And a hard work

- The development of both documents has respectively required 8 editing sessions, with the participation of experts from various countries.

- ISO/IEC 27010:2012
  6 supporting countries:
  Korea – United Kingdom – South Africa
  Belgium – Japan – Luxembourg

- ISO/IEC TR 27015 project
  9 supporting countries:
  Russia – Italy – United States
  Brazil – Japan – Luxembourg
  Belgium – Ireland – Germany

- The total number of comments transmitted by countries prior to editing sessions varies from 2 up to more than 100 !

- This number of comments is not so important. Their content and impacts that they can have on the document are !

# 3.3 Why participating to the development of ISO documents ?

- To (at least) follow the evolution of standardizing activities that can impact your business and support activities.
  *Do you know ISO/IEC 27001:2005 and ISO/IEC 27002:2005 ?*
  *Do you also know that these standards will drastically change by the end of year 2013 ? Be prepared…*

- To intervene through contributions to the development of ISO documents if they may adversely impact you.

- To set up the tone by promoting your approach and methods linked to your business.

- To increase your expertise in the domains where you are involved.

- To expand your network by meeting experts from various organisations.
  It is the place where you can meet at the same time experts working at Boeing, EADS, Microsoft, Central Bank of Russia, US Department of Defense, NIST, Cisco, Fujitsu…

# Thank you for your attendance.

Deloitte.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

In Luxembourg, Deloitte consists of 58 partners and about 1,100 employees and is amongst the leading professional service providers on the market. For over 50 years, Deloitte has delivered high added-value services to national and international clients. Our multidisciplinary teams consist of specialists from different sectors and guarantee harmonised quality services to our clients in their field. Deloitte SA is a member of the Deloitte Touche Tohmatsu network, one of the world's leading professional services firms.