Standards and Standards Organizations

Deeth Williams Wall LLP

Presented by Thomas Wong and Richard Austin

September 21, 2016 (**revised**)

Content

1. Introduction
2. Why are Standards Important?
3. Using Standards to Manage Risk
4. Offensive Tactics: Making your Proprietary Technology the Standard

1. Introduction

- A "**Standards Organization**" is an organization whose primary activities are developing and issuing or otherwise producing technical standards that are intended to address the needs of relatively wide base of affected adopters.
  - Also referred to as Standard Setting Organizations (**SSO**) and Standard Developing Organizations (**SDO**)
- "**Technical standards**" are established norms or requirements about technical systems

Examples of Standards Setting Organizations

1. International Organization for Standardization (ISO)
2. International Electrotechnical Commission (IEC)
3. Internet Engineering Task Force (IETF)
4. EMVCo (Europay, MasterCard, and Visa)
5. Payment Card Industry Security Standards Council (PCI SSC)

Examples of Standards:

A. ISO/IEC 27000 Series

- Information security standards published jointly by ISO and IEC
- Best practice recommendations on information security management risks and controls within the context of an information security management system (ISMS)
- Broad, covers more than privacy, confidentiality, IT and technical security issues
- Applies to all sizes and shapes of organizations
- Includes 19 international standards under the general title of Information Technology – Security Techniques

ISO 27000 Family (revised 2020.02.06)

- **ISO 27000:2018** – Information security management (ISM) - Overview and vocabulary
- **ISO 27001:2013** – Information security management systems (ISMS) - Requirements
- **ISO 27002:2013** – Code of practice for information security controls
- **ISO 27003:2017** – ISMS - Implementation guidance
- **ISO 27004:2016** – Information security management - Measurement
- **ISO 27005:2018** – Information security risk management
- **ISO 27006:2015 –** Requirements for bodies providing audit and certification of the ISMS
- **ISO 27007:2017 –** Guidelines for ISMS auditing
- **ISO TR 27008:2019** – Guidelines for auditors on information security controls
- **ISO 27009:2016** – Sector-specific application of ISO/IEC 27001 - Requirements
- **ISO 27010:2015** – ISM for inter-sector and inter-organisational communications
- **ISO 27011:2016** – ISM Guidelines for telecommunications organizations based on ISO/IEC 27002
- **ISO 27013:2015 –** Guidance on integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- **ISO 27014:2013 –** Governance of information security
- ~~**ISO TR 27015:2012** – Information security management guidelines for financial services~~
- **ISO TR 27016:2014 –** ISM - Organizational economics
- **ISO 27017:2015 –** Code or practices for security controls based on ISO/IEC 27001 for cloud services
- **ISO 27018:2019 –** Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO TR 27019:2017 –** ISM Guidelines based on ISO/IEC 27002 for process control systems for the energy industry
- **ISO 27031:2011 –** Guidelines for ICT readiness for business continuity
- **ISO 27032:2012 –** Guidelines for cybersecurity

ISO Standard 27001: 2013

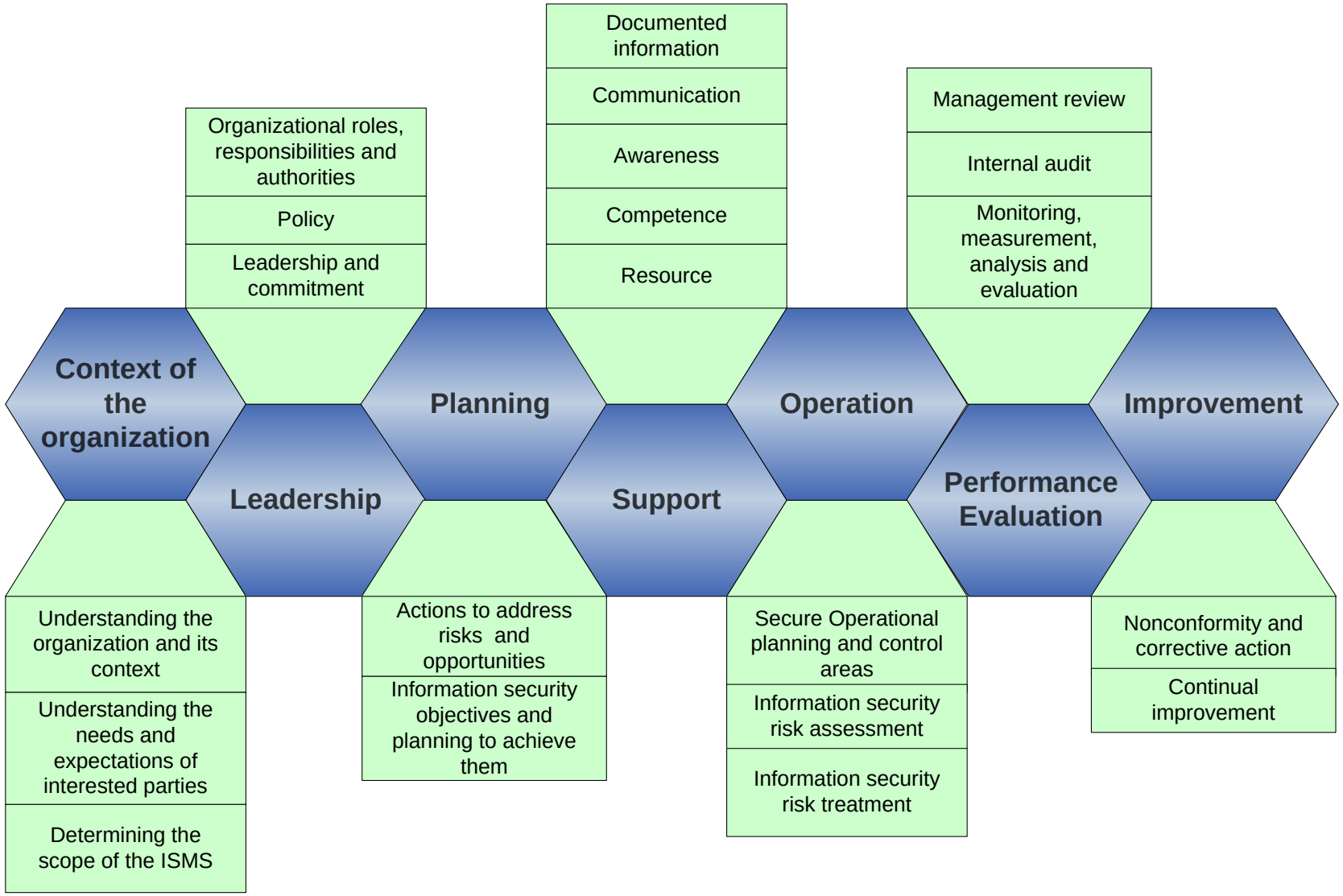
- The focus of ISO 27001 is to protect the confidentiality, integrity and availability of the information in a company.
- This is done by finding out what potential problems could happen to the information (i.e. a risk assessment), and then defining what needs to be done to prevent such problems from happening (i.e. risk mitigation or risk treatment). Therefore, the main philosophy of ISO 27001 is based on managing risks: find out where the risks are, and then systematically treating them.
- The safeguards (or controls) that are to be implemented are usually in the form of policies, procedures and technical implementation (e.g. software and equipment).

ISO Standard 27001: 2013

- Document requirements for establishing, implementing and documenting an ISMS or “Information Security Management System”
- Documents requirements for security controls to be implemented based on business requirements risk and legal/contractual obligations
- Two principal parts
  - Clauses 4-10
  - Annex A (Controls)

ISO Standard 27001: 2013

This image has been reproduced with permission from Glen Bruce, Director, Enterprise Risk Security & Privacy at Deloitte



ISO Standard 27001: 2013: Annex A

Annex A consists of 35 Control Objectives and 114 Controls

- Ex. A.7 Human resource security
  - **A.7.3 Termination and change of employment**

    Control Objective: To protect the organization's interests as part of the process of changing or terminating employment

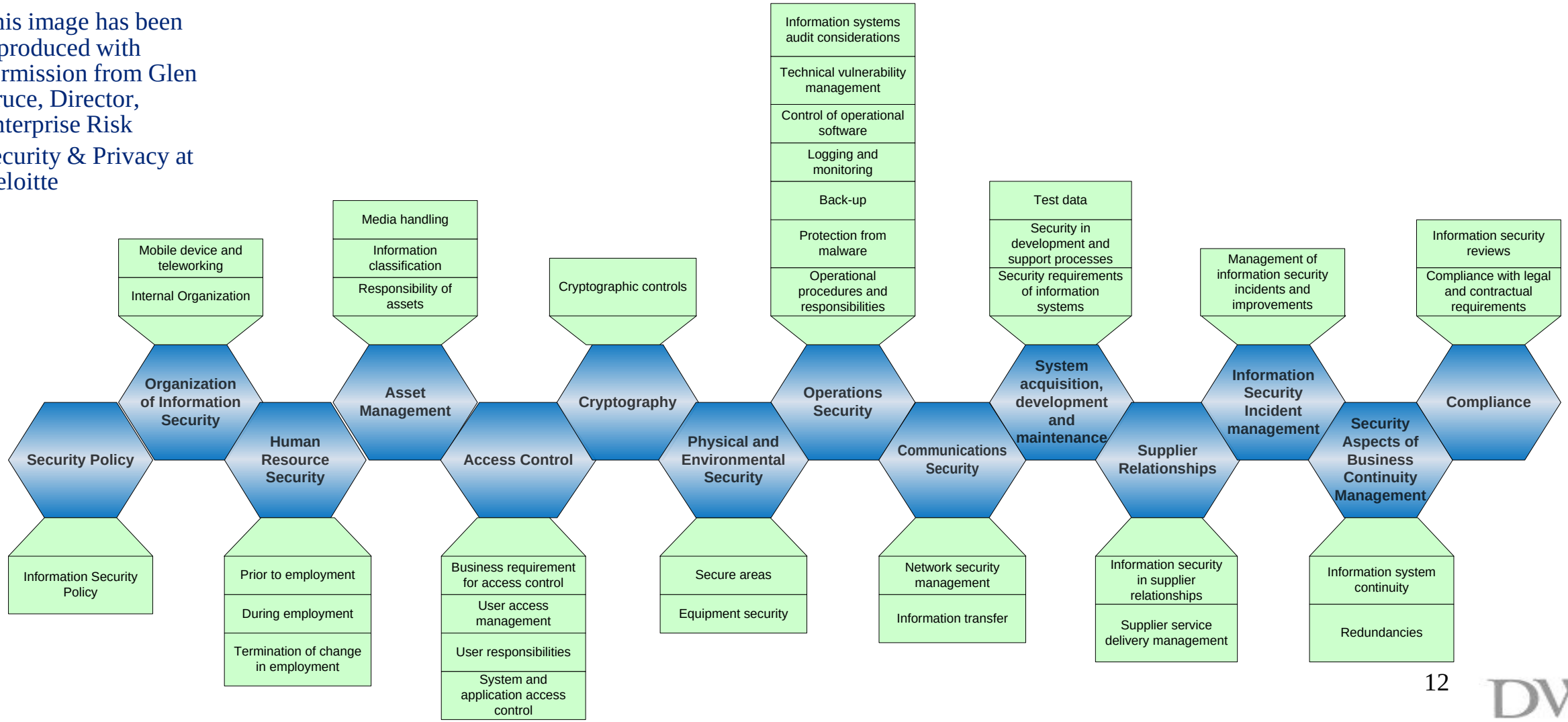
    Control (A.7.3.1): Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to employee or contractor and enforced.

ISO 27002:2013 – Code of practice for information security controls

- ISO 27002 has the same structure as Annex A of the ISO 27001
  - Each control from Annex A exists in ISO 27002, together with a more detailed explanation on how to implement it.

ISO 27002:2013 – Code of practice for information security controls

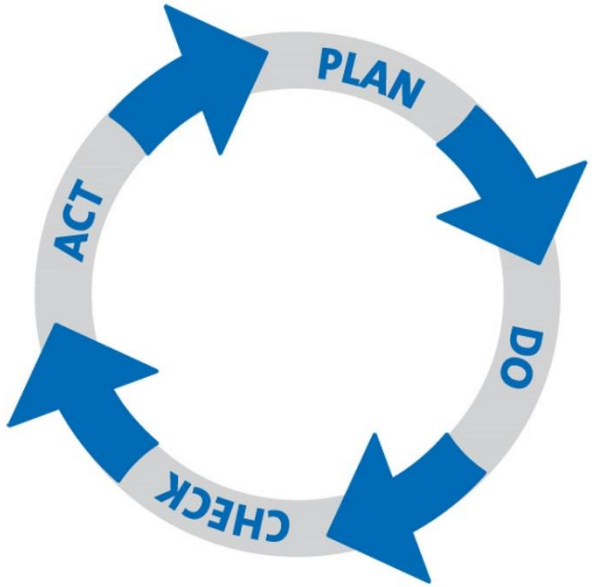
This image has been reproduced with permission from Glen Bruce, Director, Enterprise Risk Security & Privacy at Deloitte



ISO Standard 27001: 2013

Basic Principle of ISO quality management standards

- Continually improving performance



B. ISO Standard 37500: 2014 (Guidance Outsourcing):

- ISO 37500:2014 covers the main phases, processes and governance aspects of outsourcing, independent of size and sectors of industry.
- It is intended to provide a good foundation to enable organizations to enter into, and continue to sustain, successful outsourcing arrangements throughout the contractual period.

B. ISO Standard 37500: 2014 (Guidance Outsourcing):

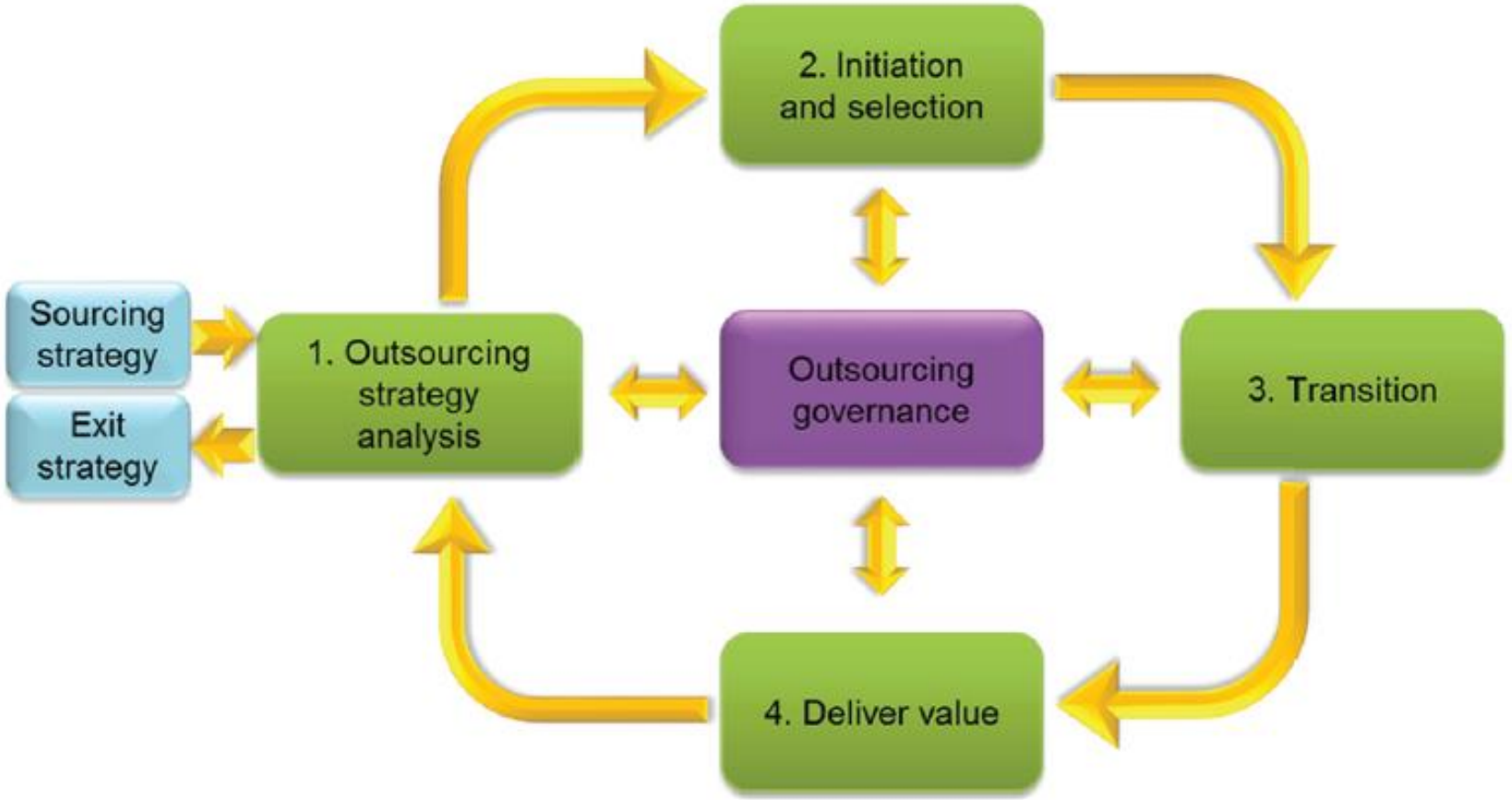


Figure 2 — Outsourcing life cycle model

This image from page 7 of ISO 37500:2014

B. ISO Standard 37500: 2014 (Guidance Outsourcing):

- The standard provides guidance on:
  - good outsourcing governance for the mutual benefit of client and provider
  - flexibility of outsourcing arrangements, accommodating changing business requirements
  - identifying risks involved with outsourcing
  - enabling mutually beneficial collaborative relationships

C. Payment Card Industry (PCI) Security Standards

- PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data
- The standards include:
  1. PCI Data Security Standard
  2. PIN Entry Device Security Requirements
  3. Payment Application Data Security Standard

D. EMV Standard

- EMV: an abbreviation for Europay, Mastercard and Visa, the three organizations that developed the initial specifications.
- Today, EMVCo manages, maintains and enhances the specifications. It is a six member organization — American Express, Discover, JCB, MasterCard, UnionPay, and Visa
- EMV is an open-standard set of specifications for smart card payments and acceptance devices.
- The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals.

2. Why Standards are Important

- There is an increasing reliance on standards because **life is getting harder**:
  - Complex systems blending technology, processes and people
  - Complicated technical issues, e.g. for the cloud, issues encompass interoperability, portability, reversibility, data security, data protection, service level standards
  - Technology systems now provide the central nervous system of business / deeper business penetration, frequently on a global basis
  - Ingenuity of cyber-criminals

Why Standards are Important (cont'd)

- Avoid ambiguities of commitments to:
  - ✓comply with industry practices / industry standards
  - ✓use "reasonable" / "commercially reasonable" / "all commercially reasonable" measures
- Trusted and reassure customers
- Provide ability to compare suppliers
- Regulatory and legal issues

Why Standards are Important (cont'd)

- Non-compliance with standards as a breach of a duty of care
  1. *Re Linked In Privacy Litigation* 5:12-CV-03088-EJD (2014) (use of hashed format of privacy protection when industry standard was to store passwords in a hashed and salted format)
  2. *Merrick Bank v Savvis Inc. & Savvis Communications Corp*., CIV 09-1088-PHX-CkJ
  3. *Ter Neuzen v Korn*,[1995] 3 SCR 674 (compliance with industry standards indicative of a lack of negligence)
  4. *R. v Placer Developments Ltd*., [1984] YJ No. 19
  5. *The TJ Hooper v Northern Barge Corporation* 1932 No. 430, 60 FD 2d 737
- Are a marketing tool

3. Using Standards to Manage Risk

- We often include standards in contracts to hold a party to a specific standard or deal with specific issues.
  - Example 1:

"At least once per calendar year Supplier will have a third party perform an internal control audit relating to the Services. The internal control audit will be at Supplier's cost, including any fees to be paid to the third party auditor. The control objectives for the audit shall be aligned with ISO27001:2013."

Example 2

Each Online Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes	Yes
Microsoft Dynamics Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Azure Core Services	Yes	Yes	Yes	Varies	Varies
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Power BI Services	Yes	Yes	Yes	No	No

Microsoft, Online Services Terms, May, 2016

Using standards in agreements requires recognition that:

1. Many standards do not require compliance with specific controls but require a risk assessment to identify what controls are required
   - ISO 27001: not all 114 controls are mandatory
   - ISO 27018: data controllers versus data processors
2. Compliance with standards is not compliance with the law
   - e.g. health or financial services sector (in the U.S. *Health Insurance Portability and Accountability* (HIPPA) and financial privacy provisions of *Gramm-Leach-Bliley Financial Modernization Act*
3. Compliance and certification are different things

Using standards in agreements requires recognition that:

4. Compliance with standards is no guarantee of protection or security:
   - Target data breach in November 2013
   - Heartland Payment Systems data breach in January 2009
   - Ford, Chrysler, and General Motors require their vendors to be ISO 9000 (Quality Management System) registered but General Motors has recalled 1.9 million vehicles in March of 2010 alone, and Chrysler had a double recall of its minivans in 2011.

Using standards in agreements requires recognition that:

5. Standards are not suited to non-standard requirements or unique requirements or customized offerings.
6. Can be difficult to get supplier commitments
   - Disclosure of non-compliance
   - Commitment to remain compliant
7. Cost of Standards and compliance/certification

4. Offensive Tactics

To be credible, standards must have certain attributes:

1. their development must be overseen by a recognized body
2. the development process must be open to input from all interested parties
3. the resulting standards must be documented and publicly available
4. there is usually a method for monitoring and verifying that organizations are complying with standards.

Standards setting process in Canada

- **Standards Council of Canada (SCC)**, a federal Crown corporation, that oversees the NSS and is responsible for accrediting organizations. SCC is a member of ISO.
- **National Standards System (NSS)** is the framework for developing, promoting and implementing national standards in Canada. Almost 15,000 people contribute to committees that develop national or international standards and more than 400 organizations are accredited by SCC.
- **SDO**: Once a standard is developed by a SDO (accredited by the SCC), the SDO may submit it to the SCC as a National Standard of Canada.
  - Requirements & Guidance – Approval of National Standards of Canada Designation: https://www.scc.ca/sites/default/files/publications/Approval_of_National_Standards_of_Canada_Designation_2015-10-01.pdf
- **International standards:** the SCC coordinates Canada's participation in the international standards system.

Implications of using proprietary technology in a standard

Implications of using proprietary technology in a standard

1. Issues relating to IP Rights:
    - **READ THE SDO'S POLICY!**
2. Anticompetitive risks: *Competition Act*

Issues relating to IP Rights

- **IP Rights and Open standards**: Typically, patents that are essential for the implementation of the standard will be licensed in accordance with the standard setting organization's IP policy

  Ex: IETF, ISO, and IEC permit their standards to contain specifications whose implementation will require payment of patent licensing fees.

- ***Qualcomm v. Broadcom* (Fed. Cir. 2008)**: a company can find itself barred from enforcing relevant patents against any firm practicing the standard if it fails to disclose relevant IP rights

Anticompetitive risks

- Antitrust authorities concentrate on standardisation agreements because they inherently involve competitors engaging in collective decision-making.
- There are provisions of the Competition Act that are potentially applicable and while there is no case law on these provisions regarding IP in standard setting context they are important to bear in mind
- *Competition Act* (R.S.C., 1985, c. C-34)
  - Section 32
  - Section 76
  - Section 79

Competition Act - Section 32(1) (Powers of Federal Court where certain rights used to restrain trade)

- **32 (1)** In any case where use has been made of the exclusive rights and privileges conferred by one or more patents for invention, by one or more trade-marks, by a copyright or by a registered integrated circuit topography, so as to

  (a) limit unduly the facilities for transporting, producing, manufacturing, supplying, storing or dealing in any article or commodity that may be a subject of trade or commerce,

  (b) restrain or injure, unduly, trade or commerce in relation to any such article or commodity,

  (c) prevent, limit or lessen, unduly, the manufacture or production of any such article or commodity or unreasonably enhance the price thereof, or

  (d) prevent or lessen, unduly, competition in the production, manufacture, purchase, barter, sale, transportation or supply of any such article or commodity,

Competition Act - Section 76 (Price Maintenance)

76 (1) On application by the Commissioner or a person granted leave …, the Tribunal may make an order … if the Tribunal finds that

(a) a person …[*with exclusive rights and privileges conferred by IP,*] directly or indirectly

(i) by agreement, threat, promise or any like means, has influenced upward, or has discouraged the reduction of, the price at which the person's customer or any other person to whom the product comes for resale [,] supplies or offers to supply or advertises a product within Canada, or

(ii) has refused to supply a product to or has otherwise discriminated against any person or class of persons engaged in business in Canada because of the low pricing policy of that other person or class of persons; and

(b) the conduct has had, is having or is likely to have an adverse effect on competition in a market.

Order (2) The Tribunal may make an order prohibiting the person…from continuing to engage in the conduct referred to in paragraph (1)(a) or requiring them to accept another person as a customer within a specified time on usual trade terms.

Competition Act - Section 79 (Abuse of Dominant Position)

- **79 (1)** Where, on application by the Commissioner, the Tribunal finds that

  (a) one or more persons substantially or completely control, throughout Canada or any area thereof, a class or species of business,

  (b) that person or those persons have engaged in or are engaging in a practice of anti-competitive acts, and

  (c) the practice has had, is having or is likely to have the effect of preventing or lessening competition substantially in a market,

- the Tribunal may make an order prohibiting all or any of those persons from engaging in that practice.

How to avoid competition issues

- Some general guidance in relation to the behaviour of members and participants in an SSO has been provided in the European Commission's guidelines:

> *Where participation in standard-setting is unrestricted and the procedure for adopting the standard in question is transparent, standardisation agreements which contain no obligation to comply with the standard and provide access to the standard on fair, reasonable and non-discriminatory terms will normally not restrict competition within the meaning of Article 101(1).*

Questions?