ISO/IEC JTC 1/SC 27 Work in Support of Legislation

Laura Lindsay

laurali@Microsoft.com

Cybersecurity related work

NIS Directive

CHAPTER V

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS

Article 16

Security requirements and incident notification

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

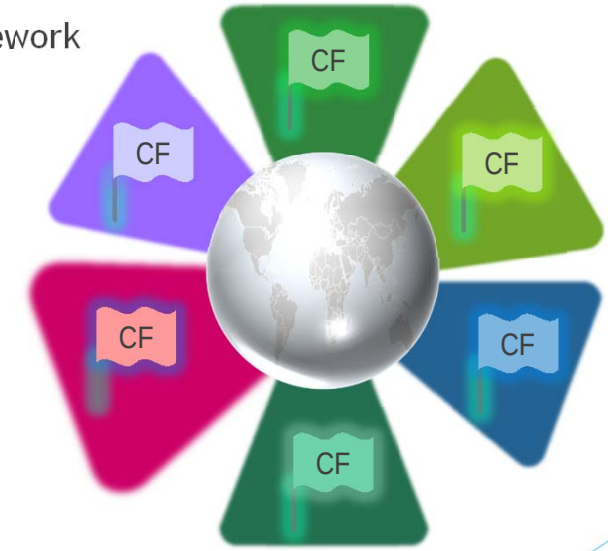
(e) compliance with international standards.

How ISO/IEC Standards support NIS Directive

NIS Directive	ISO/IEC Standards
Security of Systems and Facilities	27001 – Information Security Management Systems 27002 – Code of practice for Information Security Management 27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
Incident Handling	27035 series – Information Security Incident Management
Business Continuity Management	27031 - Guidelines for information and communication technology readiness for business continuity
Monitoring, auditing, testing	27000 family of standards

New and On-going work in ISO/IEC JTC 1/SC 27

- ISO/IEC TR 27103 – Cybersecurity and ISO and IEC Standards
- Ongoing investigation into needed Cybersecurity standards
  - What are the standards gaps in Cybersecurity
  - International Cybersecurity framework



ISO/IEC TR 27103

- Describes Risk-based approach
- Overview of Cybersecurity frameworks and programmes
- Cybersecurity Functions Defined
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Mapping of Categories to existing ISO and IEC Standards

Cybersecurity

Technical & Organizational Measures	• Information security through ISO/IEC 27000 Family of Standards • Risk Based approach through ISO/IEC 27001
Transparency	• Transparency through ISO/IEC 19086 series • Security Policy Guidance – Codes of Practice and implementation guidance (ISO/IEC 27002, ISO/IEC 27017) • Certification such as ISO/IEC 27001
Incident Management	• ISO/IEC 27035 series on Incident Management • ISO/IEC 29147 Vulnerability Disclosure • ISO/IEC 30111 Vulnerability Handling Process

GDPR related work

ISO/IEC 19944:
Cloud services and devices : data flow, data categories and data use

- Names and describes the flows of data between a device and a supporting cloud, and how to describe the use of different categories of data by the CSP
  - Detailed description of data flows
  - Taxonomy of data types
  - Definitions for use, scope, linkage to natural person
  - Formal structure for data use statements
- Goal: Improve transparency and guidance about data flows and data use
- Application: Easy-to-read statements about data use that represent unambiguous commitments

ISO/IEC 20889: Information technology — Security techniques — Privacy enhancing data de-identification techniques

- Classify known de-identification techniques using standardized terminology
  - Characteristics
  - Underlying technologies
  - Applicability of each technique to reducing the risk of re-identification
  - Utility of the resulting de-identified data
- Goal: Improve practice and transparency about de-identification
- Application: Provide clear descriptions and guidance about the goals and application of de-identification to enhance privacy

ISO/IEC 27552 Personal information Management System

- Introduced by French DPA (CNIL) = WP29 = EDPB (GDPR)
- Based on something organizations already know how to do
  - PIMS is a new management system extending 27001 with privacy requirements (new) as well as controls (ISO 27018 +)
  - Certification standard, like ISO 27001, with the same ecosystem of auditor, accreditation bodies and certificates

ISO/IEC 27552 organizes evidence

Technical & Organizational Measures	• De-identification and erasure to support data minimization • Receiving, documenting and modifying consent • Support data subject rights (access, portability, correct, erase) • Information security through ISO/IEC 27001
Record Keeping	• Purpose of processing • Lawful basis for processing • Disclosure and transfer to third parties • Geolocation • Record keeping for accountability
Demonstrate Adherence	• Processor obligations through ISO/IEC 27018 • Risk to data subject through Privacy Impact Assessment (ISO/IEC 29134) • Automated decision making (Pending)
Transparency to data subjects	• Transparency with data subject through ISO/IEC 19944 data use statements • Controller processor transparency through ISO/IEC 19086

Protection of PII: Key Standards