OFE Backgrounder
Standards for Cybersecurity in Europe

February 2018

ofe

Trust in ICT systems and services is a pillar of the Single Digital Market. Cybersecurity is critical for the private sector and the public sector alike. Cybersecurity and trust are key elements for the uptake of new technologies and enabling Europe's digital transformation.

High levels of security are achieved with robust security standards including effective risk-based management. Cybersecurity standards are available and constantly improved by security experts collaborating in international and European standards developing organisations. Typically standards do not tie themselves to particular categories of products and services allowing broad adoption in a variety of environments.

Cybersecurity Standards for Europe

Standards are developed in open standards developing organsisations. Europe has three European Standards Organisations formally recognised in Regulation 1025/2012: CEN, CENELEC and ETSI. These collaborate with the International Standards Organisations that operate under the WTO/TBT Agreement: ISO, IEC and ITU – this includes the Joint Technical Committee ISO/IEC JTC 1 for ICT standardisation.

In the area of Cybersecurity major international standardisation activities have taken place for many years already in ISO/IEC JTC 1 (in Subcommittee 27) and in IEC (standard series IEC 62443). Often these standards are accompanied by respective conformity assessment programmes.

Europe is well set up for a fast adoption of these international standards as European Standards. CEN/CENELEC have set up the joint TC 13 for cybersecurity. CEN and CENELEC have close relations with ISO and IEC via the Vienna and the Dresden/Frankfurt agreements. These facilitate rapid transposition of international standards into European ones. In addition, CEN/CENELEC JTC 13 has key experts from across Europe for developing further standards responding to European policy and market needs in the field of cybersecurity.

Moreover, ETSI has TC Cyber which develops standards for security and privacy for Europe with global impact.

Additionally, ICT technical specifications in the area of cybersecurity are developed in other global standards developing organization, often called fora and consortia: such as OASIS, IETF and W3C. Using the identification process of Regulation EU 1025/2012, these standards have the potential to be used for public procurement. If needed they can also be transposed into International or European Standards using well-established processes like PAS and FAST-TRACK.

Risk management approach

Strong risk management frameworks play a core part in mitigating cybersecurity threats. Indeed, related guidance is elaborated in a number of standards including the ones summarised in this background paper. Most importantly, risk management frameworks represent an effective tool to respond adequately to the fast changing nature of threats. Such framework are typically (1) based on a national strategy; (2) developed with wide stakeholder input through voluntary, open, transparent processes; (3) flexible and adaptable (so that it is capable not only of being used across sectors, but also of being impactful for specific threat profiles and for individual businesses); and (4) aligned with international standards and technical specifications.

Examples of available standards in the area of cybersecurity

The following examples illustrate which issues are addressed by available standards already:

Standard name	**Standard description**
ISO/IEC 27001:2013	Specifies the **requirements for establishing, implementing, maintaining and continually improving an information security management system** within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
ISO/IEC 27002:2013	Gives **guidelines for organizational information security standards and information security management practices** including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

Standard name	Standard description
ISO/IEC 27017:2014	Gives **guidelines for information security controls applicable to the provision and use of cloud services** by providing: - additional implementation guidance for relevant controls specified in ISO/IEC 27002; - additional controls with implementation guidance that specifically relate to cloud services.
ISO/IEC 27032:2012	Provides **guidance for improving the state of Cybersecurity**, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: - information security, - network security, - internet security, and - critical information infrastructure protection (CIIP).
ISO/IEC 27035-1:2016	Presents **basic concepts and phases of information security incident management** and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.
ISO/IEC 27035-2:2016	Provides the **guidelines to plan and prepare for incident response**. The guidelines are based on the "Plan and Prepare" phase and the "Lessons Learned" phase of the "Information security incident management phases" model presented in ISO/IEC 27035 1.
ISO/IEC 27031:2011	Describes the **concepts and principles of information and communication technology (ICT) readiness for business continuity**, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity.

Standard name	Standard description
IEC 62443-4:2017	Specifies process **requirements for secure development of products used in industrial automation and control systems**. This specification is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS). Also provides guidance on how to meet the requirements described for each element. The life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.
ETSI TR 103 456	**Implementation of the Network and Information Security (NIS) Directive**: Provides guidance on the available technical specifications and those in development by major cyber security communities worldwide designed to meet the **legal measures and technical requirements relating to implementation of the Network and Information Security (NIS) Directive**, including the sharing of information and network based risks and incidents and necessary defence measures. The guidance includes: considerations for incident notification and best practices in cyber security risk management. The document provides a broader cyber security context than the NIS Directive or the ENISA Standardization Gaps Report to facilitate evolution toward significant emerging open global platforms, and includes treatment of challenges associated with harmonizing the implementations across the diverse network and services sectors and Member State legal and operational environments.

The above table represents just some prominent examples. Where these standards are not yet European standards they can be transposed rapidly and provide a basis against which companies and public authorities can operate – including possible certification and self-certification of compliance to these standards.

Standardisation requests and planning for new standards

Europe has well functioning tools for planning the development of new standards. If the European Commission wishes to initiate a harmonised European Standard (usually to support legislation) or some other standardisation activity that is deemed critical for fulfilling European policy and market requirements in the area of cybersecurity and no international standard exists, a standardisation request can be given to the European Standardisation Organisations. This request is approved by the Committee on Standards (CoS – the Member States Committee overseeing the implementation of Regulation 1025/2012) and is listed in the EU Annual Union Work Programme for Standardisation. Regulation 1025/2012 also requires that the ICT Multi Stakeholder Platform (MSP) is consulted on any new ICT related standardization requests.

On a less formal level the European Commission may also use the ICT Standardisation Rolling Plan – maintained by the MSP - to list an action where a standard would be necessary and where the entire ICT standardisation community can react with respective development activities.

Standards, conformity and certification

Standards (European Norms – "EN") play a key role for complying with essential requirements laid down by regulators. The New Legislative Framework is the process that is applied in Europe in the areas of safety and health with high success for all market participants:

i. essential requirements are laid down in an Annex to the respective Regulation or Directive (e.g. General Product Safety Regulation, Low Voltage Directive, Machinery Directive);

ii. European Standards are developed that meet the requirements, are listed in the Official Journal of the EU and are implemented and followed by industry;

iii. assessment of compliance is done against the respective European Standards – self-assessment is possible and documented with a Supplier's Declaration of Conformity and market access is granted under the Presumption of Conformity; and,

iv. market surveillance authorities take a control function where certification is done against standards.

Standards are, therefore, at the core of responding to legal requirements and establishing the process or method how to comply with them. Assessment and certification are done against the processes and methods defined in standards.
International and European Standards are developed in a consensus process with the involvement of all relevant stakeholders. They are openly available – for free or for purchase. Thus they can be considered early on for product planning and design and effectively implemented in products and services.

Standards contribute to clarity of requirements and guide the way to be compliant. Strong cybersecurity standards as the ones listed above will lead to a high level of cybersecurity in Europe.

Closing remarks

Standards ensure high levels of cybersecurity. Standards are based on open, collaborative consensus building processes with involvement of key technical experts.

Standards are available for all market players – including public authorities – to implement and to follow. They are maintained and regularly updated for ensuring high-quality and transparency.

Standards should be the basis for assessing compliance. Often standards are accompanied by frameworks to assess compliance. These can be used for third party certification as well as for self-certification.

The cybersecurity requirement of a certification scheme should only be by reference to a single standard or a suite/family of standards designed to work together. Writing requirements directly into a scheme confuses the democratically enshrined principle of separation of powers – in this case the separation of standards from conformity assessment rules and ultimately risks creating market confusion undermining innovation/product design planning and potentially comprising security.

For more information, please contact OFE's CEO Sachiko Muto at sachiko@openforumeurope.org.

OpenForum Europe (OFE) is a not-for-profit, independent European based think tank which focuses on openness within the IT sector. We draw our support not only from some of the most influential global industry players, but most importantly from across European SMEs and consumer organisations and the open community. OFE also hosts a global network of OpenForum Academy Fellows, each contributing significant innovative thought leadership on core topics. Views expressed by OFE do not necessarily reflect those held by all its supporters.

OFE Limited, a private company
with liability limited by guarantee
Registered in England and Wales with
number 05493935

Registered office: Claremont House,
1 Blunt Road, South Croydon, Surrey
CR2 7PA, UK