Welcome

Bienvenue

Willkommen

European Multi-Stakeholder Platform (MSP) on ICT Standardisation

AGENDA

I European Multi-Stakeholder Platfom (MSP) on ICT Standardisation

II Rolling Plan for ICT Standardisation

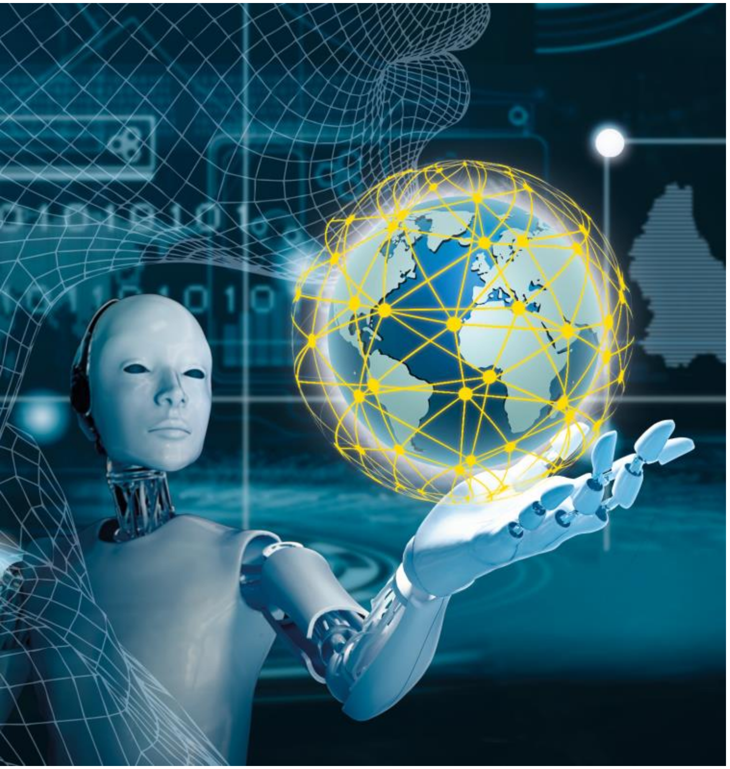
A – Key enablers and security

B – Societal challenges

C – Innovation for the Digital Single Market

D – Sustainable growth

OBJECTIVE OF THIS PRESENTATION



- Understand the role of the European MSP on ICT Standardisation
- Understand the objective of the Rolling Plan for ICT Standardisation
- Awareness of standard activities in different ICT fields
- Understand the benefits of using ICT standards
- Understand the European legislation and standardisation activities related to electronic identification and trust services including e-signatures
- Promote use and implementation of ICT standards in your company
- Encourage your participation in the standardisation process

EUROPEAN MSP ON ICT STANDARDISATION

A – OBJECTIVE

- Increase interoperability
- Promote the use of standards and specifications
- Industry preference/need for global standards
- Ensure availability of required standards and specifications for public authorities
- Provides public authorities with the certainty that with the use of the specs their “public interest” expectations are met
- Recognized specifications are not European Standards
- Specifications suitable for referencing, use remains voluntary, made available (recommended) for use in policies and legislation

EUROPEAN MSP ON ICT STANDARDISATION

B – ORGANISATION

- Expert Group created by Commission Decision of 28 November 2011 (OJ C349 of 30.11.2011)
- 3 - 4 meetings per year; first meeting March 2012
- Possibility to create sub-groups

Tasks

- Advise the European Commission on ICT standards work program
- Identify future ICT standardisation needs from policies and legislation
- Advise the European Commission on possible ICT standardisation mandates
- Inform Commission on progress in ICT standardisation activities
- Any other issue concerning support for ICT interoperability

EUROPEAN MSP ON ICT STANDARDISATION

C – STAKEHOLDERS

- European Institutions
- Administrations of Member States (~50% of the Platform members)
- European and international ICT standardisation bodies active in Europe: CEN, CENELEC, ETSI, ISO, IEC, ITU, …
- Citizens, experts
- Industry, businesses, SME
- Non-Governmental Organisations
- Persons or organisations with any legitimate interest
- Invitations to MS to nominate participants

EUROPEAN MSP ON ICT STANDARDISATION

D – STRATEGIC ROLE OF ICT STANDARDIDATION IN THE CONTEXT OF EU POLICY MAKING

- Identifies EU policy priorities where ICT standards should be considered as part of policy making (mostly from the EC)
- Rolling plan identifies areas for action at the standardisation landscape
- Make sure state-of-the-art technologies get implemented
- European standards developed by CEN, CENELEC and ETSI
- Standards developed by global industry-driven ICT fora and consortia
- Standards used in support of industrial or innovation policy
- Standards play a role in EU Research and Innovation
- Standards take an important role in government internal policies and public procurement

E – PROMOTING THE IMPLEMENTATION OF STANDARDS

- **The use of standardisation in support of policy making**
  - Create awareness of importance of standards
- **Public procurement**
  - Identifies available standards in areas with policy relevance
  - Diminish lock-in
- **Research and Innovation**
  - Source of new standards
  - Standardisation awareness in R&I
- **Testing and quality improvement in standards**
  - Ensure that there are products implementing the standards
  - To enable interoperability in a multi-vendor environment

EUROPEAN MSP ON ICT STANDARDISATION

F – ROLLING PLAN FOR ICT STANDARDISATION

- Current version of the Rolling Plan for ICT Standardisation from 2018
- To be updated at least once a year by the Commission, in collaboration with the MSP
- Defines the most important standardisation initiatives and actions supporting EU policies
- As the 2010-2013 ICT standardisation work program, its predecessor, the Rolling plan is a Commission document, written in collaboration with & advised by the MSP
- https://portail-qualite.public.lu/fr/confiance-numerique/normalisation-des-tic.html

A – KEY ENABLERS AND SECURITY

3.1.1 5G

3.1.2 Cloud computing

3.1.3. Public sector information, open data and big data

3.1.4 Electronic identification and trust services including e-signatures

3.1.5. Internet of Things

3.1.6. Cybersecurity / network and information security

3.1.7 ePrivacy

3.1.8 e-Infrastructures for research data and computing intensive science

3.1.9 Broadband infrastructure mapping

3.1.10 Accessibility of ICT products and services

Cloud computing

- Establish a coherent framework for Cloud Computing
- Related ongoing standardisation and research activities
  - ETSI Cloud Standards Coordination (see http://csc.etsi.org)
  - Cloud Standards Customer Council (see www.cloud-council.org)
  - ISO/IEC – JTC 1/SC 38
  - …

Electronic identification and trust services including e-signatures

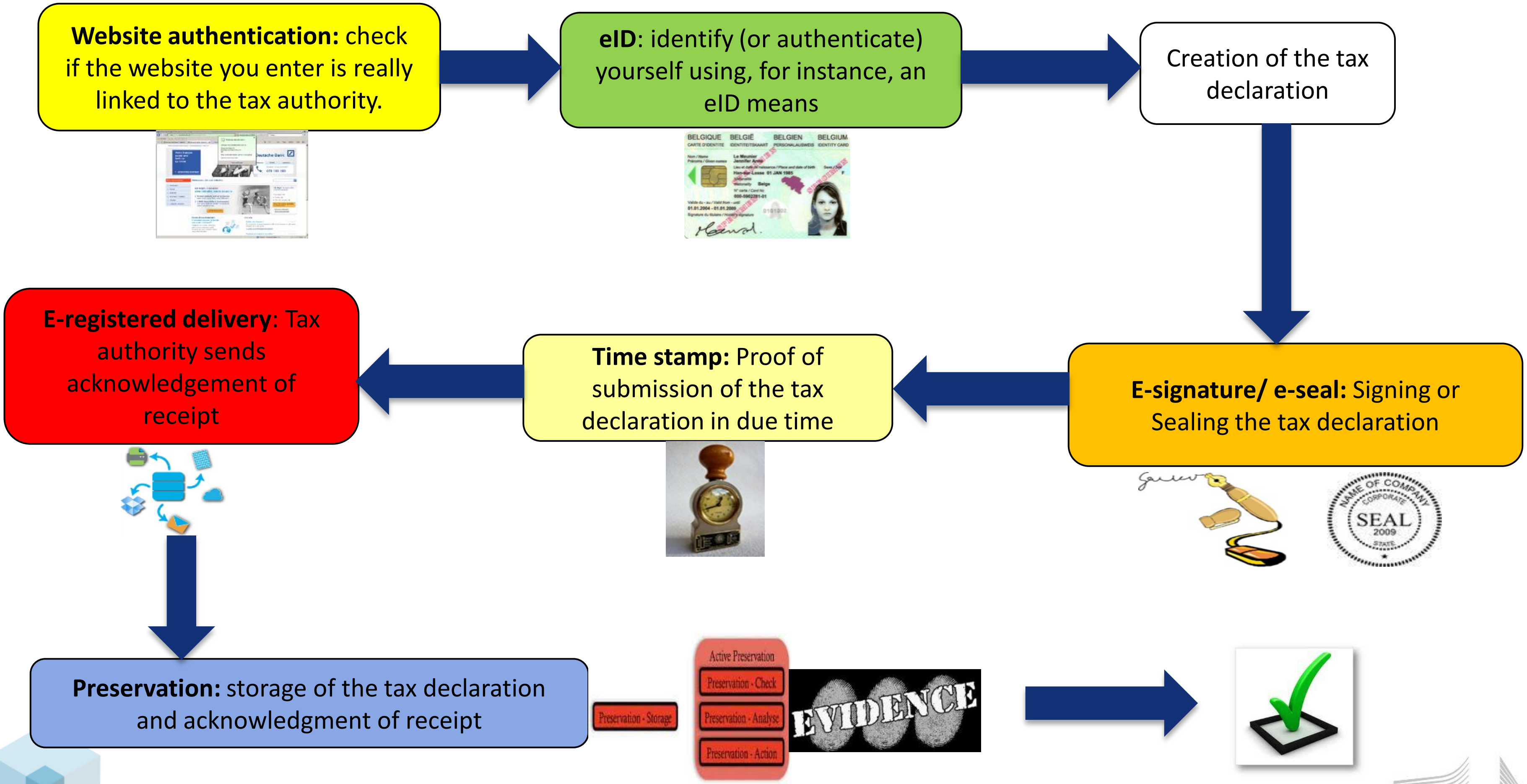
– Policy and objectives

- European legislation: Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation)

– Related ongoing standardisation and research activities

- CEN/TC 224 develops standards for strengthening the interoperability and security of personal identification (Trustworthy Systems, …)
- ETSI TC ESI: Trusted Lists (ETSI TS 119 612), signature formats (CAdES, XAdES, PAdES, ASiC), signature validation, …
- e-SENS (Electronic Simple European Networked Services): eID, eDocuments, eDelivery, and eSignature etc. for a pan-European digital platform for cross-sector, interoperable eGovernment services
- STORK: eID Interoperability Platform
- …

Electronic identification and trust services including e-signatures



Website authentication: check if the website you enter is really linked to the tax authority.

eID: identify (or authenticate) yourself using, for instance, an eID means

Creation of the tax declaration

E-signature/ e-seal: Signing or Sealing the tax declaration

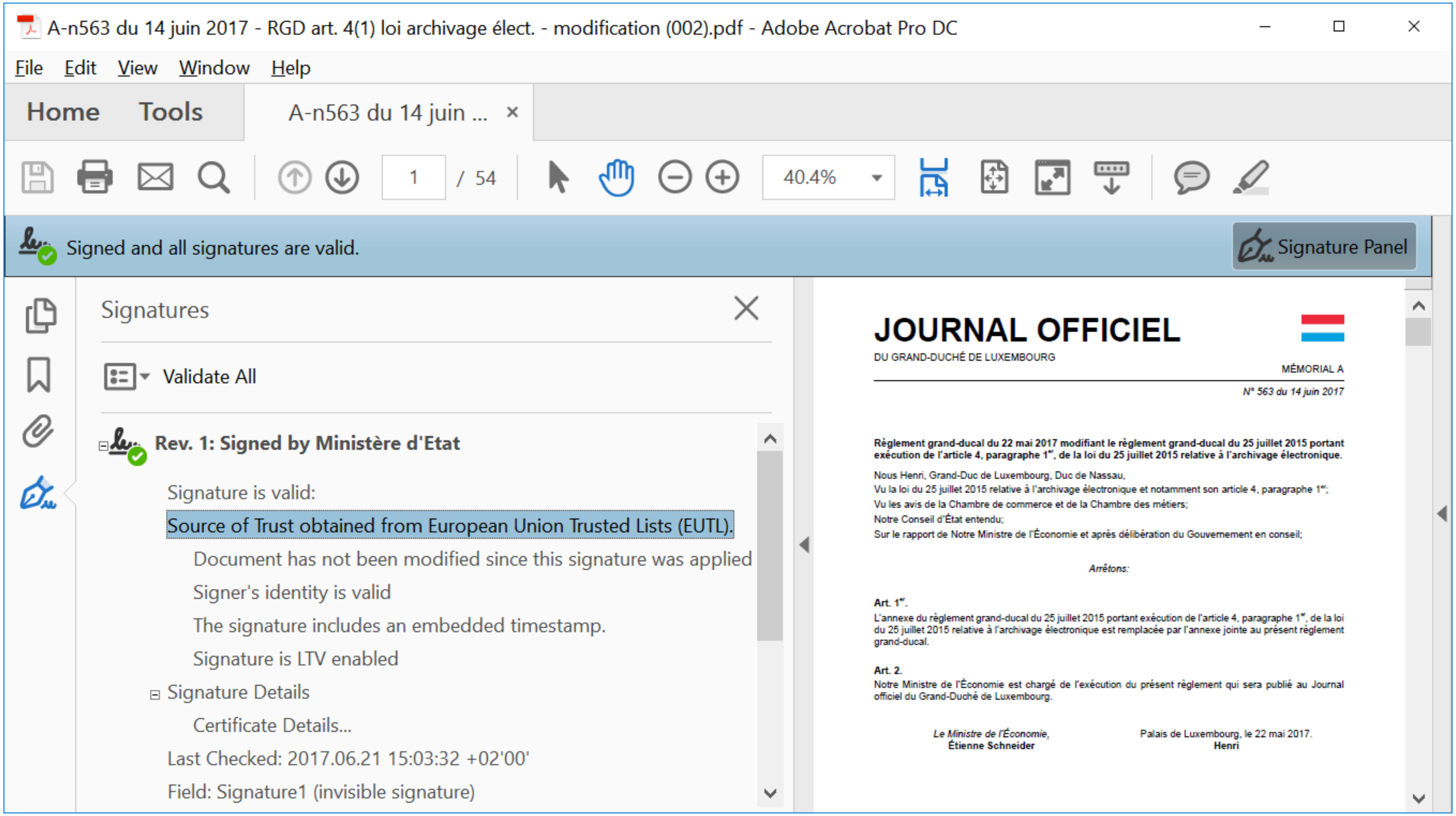
Time stamp: Proof of submission of the tax declaration in due time

E-registered delivery: Tax authority sends acknowledgement of receipt

Preservation: storage of the tax declaration and acknowledgment of receipt

Electronic identification and trust services including e-signatures

- Use Case: ETSI TS 119 621 – Electronic Signatures and Infrastructures (ESI); Trusted Lists


A-n563 du 14 juin 2017 - RGD art. 4(1) loi archivage élect. - modification (002).pdf - Adobe Acrobat Pro DC
File
Edit
View
Window
Help
Home
Tools
A-n563 du 14 juin ...
1
/ 54
40.4%
Signature Panel
Signatures
Validate All

Signed and all signatures are valid.

Rev. 1: Signed by Ministère d'Etat

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

Signature Details

Certificate Details...

Last Checked: 2017.06.21 15:03:32 +02'00'

Field: Signature1 (invisible signature)

JOURNAL OFFICIEL
DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 563 du 14 juin 2017

Règlement grand-ducal du 22 mai 2017 modifiant le règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,
Vu la loi du 25 juillet 2015 relative à l'archivage électronique et notamment son article 4, paragraphe 1er;
Vu les avis de la Chambre de commerce et de la Chambre des métiers;
Notre Conseil d'État entendu;
Sur le rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil;

Arrêtons:

Art. 1er.
L'annexe du règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique est remplacée par l'annexe jointe au présent règlement grand-ducal.

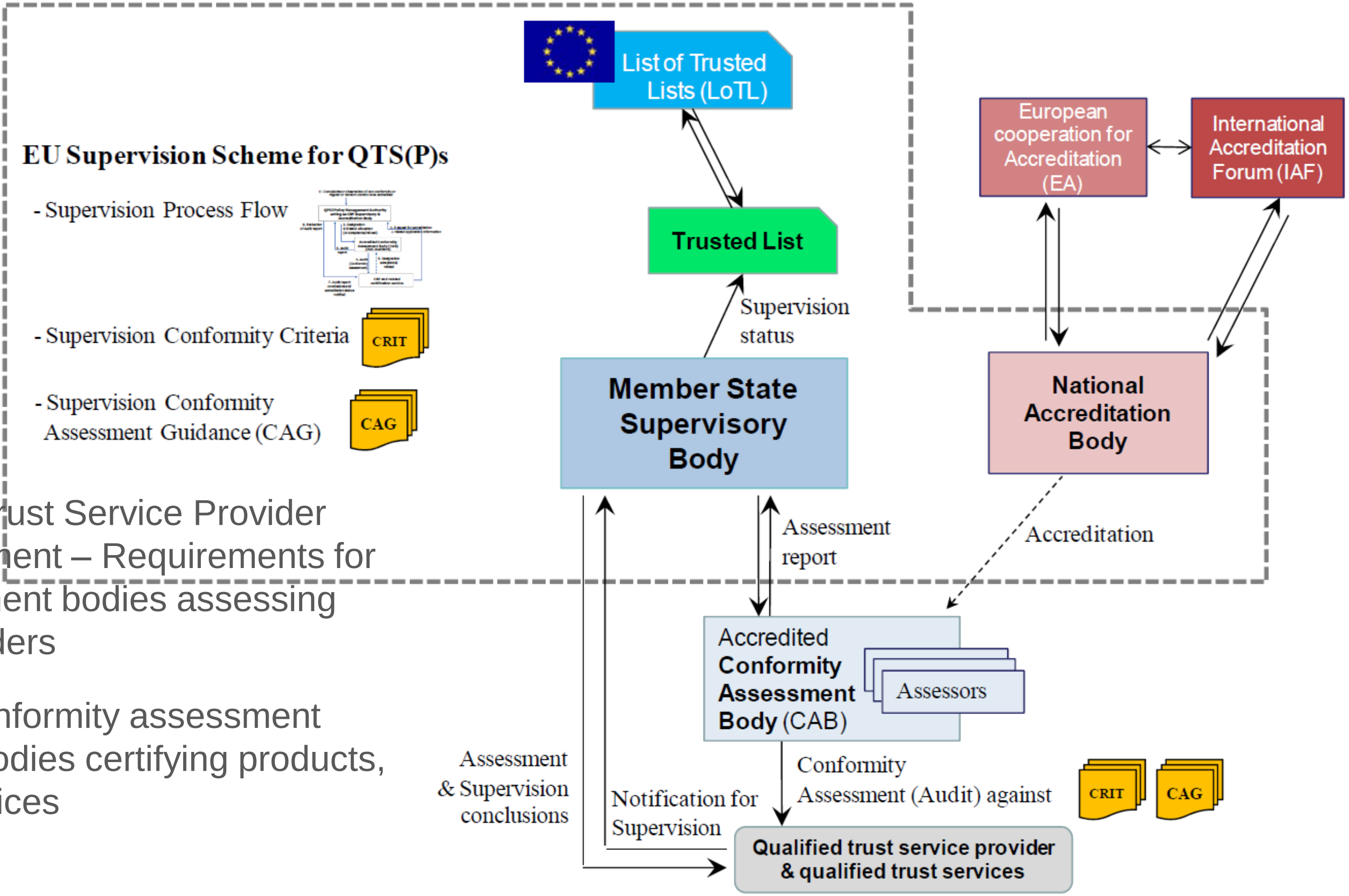
Art. 2.
Notre Ministre de l'Économie est chargé de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

Le Ministre de l'Économie,
Étienne Schneider

Palais de Luxembourg, le 22 mai 2017.
Henri

Electronic identification and trust services including e-signatures

- ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists


List of Trusted Lists (LoTL)
EU Supervision Scheme for QTS(P)s
- Supervision Process Flow
- Supervision Conformity Criteria
CRIT
- Supervision Conformity Assessment Guidance (CAG)
CAG
Trusted List
Supervision status
Member State Supervisory Body
European cooperation for Accreditation (EA)
International Accreditation Forum (IAF)
National Accreditation Body
Assessment report
Accreditation
Accredited Conformity Assessment Body (CAB)
Assessors
Assessment & Supervision conclusions
Notification for Supervision
Conformity Assessment (Audit) against
CRIT
CAG
Qualified trust service provider & qualified trust services

- ETSI EN 319 403 Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers
- ISO/IEC 17 065 Conformity assessment Requirements for bodies certifying products, processes and services

Electronic identification and trust services including e-signatures

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) - General policy requirements for trust service providers supporting electronic signatures;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Policy requirements for certification authorities issuing qualified certificates;
- ETSI EN 319 411-3 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 3: Policy requirements for Certification Authorities issuing public key certificates;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- CEN/TS 419 241 Security Requirements for Trustworthy Systems Supporting Server Signing;
- CEN/TS 419 261 Security requirements for Trustworthy Systems managing certificates and time-stamps

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Trust Service Practice (TSP) statement
  - Shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP policy
  - Shall identify the obligations of all external organisations supporting the TSP services
  - Shall make available to subscribers and relying parties its practice statement
  - Shall have a management body with overall responsibility for the TSP practices
  - Shall define a review process for the practices
  - Shall notify notice of practice changes
  - Shall state in its practices the provisions made for termination of service

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Information security policy
  - Documented, implemented and maintained
  - Shall retain overall responsibility for conformance with the procedures within its security policy
  - Shall be reviewed at planned intervals or if significant changes occur
  - A TSP's management security policy shall be documented, implemented and maintained including security controls and operating procedures for TSP facilities
    See ISO/IEC 27002:2013 clause 5.1.1 for guidance
- Segregation of duties
  - Duties and responsibilities shall be segregated to reduce misuse of the TSP assets

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Human resources
  - Necessary expertise, reliability, experience and qualifications
  - Should be able to fulfil the requirement of "expert knowledge, experience and qualifications"
  - Appropriate disciplinary sanctions shall be applied when violating TSP policies or procedures
  - Security roles and responsibilities shall be documented in job descriptions
  - TSP personnel shall have job descriptions defined from the roles they fulfil
  - Procedures in line with information security management procedures
  - Managerial personnel shall possess experience or training with the trust service that is provided
  - Shall be free from conflict of interest that might prejudice the impartiality of the TSP operations

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

Asset management

– General requirements
    - The TSP shall ensure an appropriate level of protection of its assets
    - The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment

– Media handling
    - All media shall be handled securely in accordance with the requirements of the information classification scheme

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Access control
  - Controls (e.g. firewalls) shall protect the TSP’s internal network domains from unauthorized access
  - The TSP shall administer user access of operators, administrators and system auditors
  - Access to information and application system functions shall be restricted in accordance with the access control policy
  - TSP personnel shall be identified and authenticated before using critical applications related to service
  - TSP personnel shall be accountable for their activities
  - Sensitive data shall be protected against being revealed through re-used storage objects being accessible to unauthorized users

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Cryptographic controls
  - Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle
- Physical and environmental security
  - Physical access to components of the TSP’s system whose security is critical to the provision of its trust services shall be limited to authorized individuals
  - Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities
  - Controls shall be implemented to avoid compromise or theft of information and information processing facilities
  - Critical components shall be located in a protected security perimeter

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

– Operation security

  - An analysis of security requirements shall be carried out at the design and requirements stage of any system development project
  - Change control procedures shall be applied for releases, modifications of any operational software
  - The integrity of TSP systems and information shall be securely handled to protect media from damage, theft, any unauthorized access and obsolescence
  - Media management procedures shall protect against obsolescence and deterioration of media
  - Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services
  - Shall specify and apply procedures for ensuring security patches are applied within a reasonable time after they come available

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Network security
  - Shall segment systems into networks or zones based on risk assessment
  - Restrict access and communications between zones to those necessary for the operation
  - Maintain any elements of their critical systems (e.g. Root CA systems) in a secured zone
  - Dedicated network for administration of IT systems that is separated from the operational network
  - Test platform and production platform shall be separated from other environments
  - Communication between trustworthy systems shall only be established through trusted channels
  - External network connection to the internet shall be redundant to ensure availability of services
  - Perform regular vulnerability scan on public and private IP addresses and a penetration test

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Incident management
  - Monitoring activities should take account of the sensitivity of information
  - Abnormal system activities that indicate a potential security violation, shall be reported
  - The TSP IT systems shall monitor events (Availability and utilization of needed services, …)
  - Respond quickly to incidents and to limit the impact of breaches of security
  - The TSP shall establish procedures to notify the appropriate parties
  - TSP shall also notify the natural or legal person of the breach of security or loss of integrity
  - Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity
  - The TSP shall remediate within a reasonable period after the discovery of a critical vulnerability

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

– Collection of evidence

  - Confidentiality and integrity of records shall be maintained
  - Records concerning the operation of services shall be completely and confidentially archived
  - Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings
  - The precise time of significant TSP environmental, key management and clock synchronization events shall be recorded
  - Records concerning services shall be held for a period of time after the expiration of the validity of the signing keys or any trust service token as appropriate for providing necessary legal evidence
  - Events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

– Business continuity management
  - In the event of a disaster, including compromise of the private signing key or trust service credentials, operations shall be restored as soon as possible
  - TSP shall define and maintain a continuity plan to enact in case of a disaster
  - Other disaster situations include failure of critical components of a TSP trustworthy system, including hardware and software
  - See clause 17 of ISO/IEC 27 002 for guidance

Electronic identification and trust services including e-signatures

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

- Compliance
  - Shall provide evidence on how it meets the applicable legal requirements
  - Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities. Applicable standards such as ETSI EN 301 549 should be taken into account
  - Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Internet of Things

- Dynamic global network infrastructure
- Key priority area of the digital single market
- Physical and virtual "things" have identities, physical attributes and virtual personalities
- Connect these "things" to data networks
- Related ongoing standardisation and research activities
  - Internet of Things Research in Europe Cluster (IERC) that are dealing with aspects of the standardisation in IoT
  - Future Internet PPP (FI-PPP) deals with some issues connected to the standardisation of the IoT
  - ISO/IEC JTC 1 WG 10 "Internet of Things"
  - …

Cybersecurity / network and information security

- Network and information security public-private platform (NIS Platform) has been set up by the Commission with representation from various stakeholders
- Policy and legislation
  - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – 2013
  - COM(2017) 477 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')
  - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the EU (NIS Directive)
  - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to personal data processing and on the free movement of such data (General Data Protection Regulation)

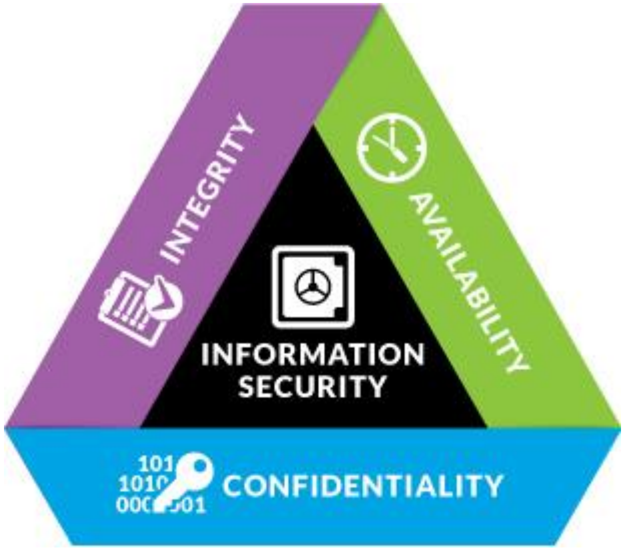
Cybersecurity / network and information security

– Related ongoing standardisation and research activities

- CEN and CENELEC have set up a Cyber Security Coordination Group. The CSCG and the NIS Public-Private Platform will regularly update the MSP on stakeholder requirements and advise the MSP
- ETSI TC CYBER
- OASIS hosts the PKCS 11 standardisation project for cryptographic tokens controlling authentication information (see www.oasis-open.org/committees/pkcs11) and the Key Management Interoperability Protocol (KMIP) (see www.oasis-open.org/committees/kmip)
- ISO/IEC JTC 1 SC 27
- IEEE has standardization activities in the network and information security space, including in the encryption, fixed and removable storage
- …

Cybersecurity / network and information security

ISO/IEC 27 000 – Information technology – Information security management systems



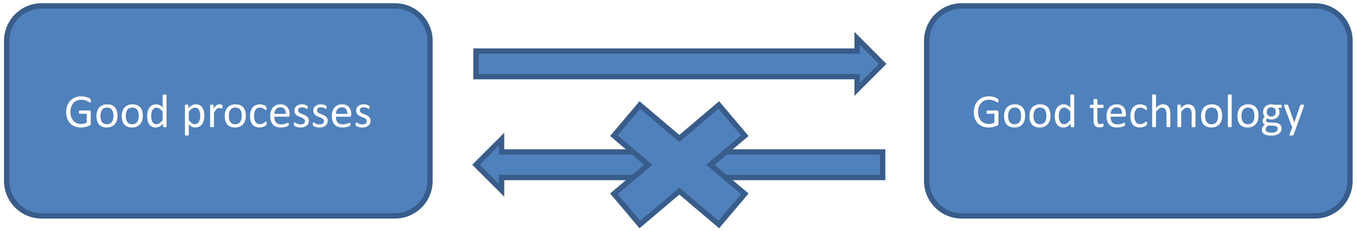
http://www.opentext.com/what-we-do/business-needs/information-governance/ensure-compliance/information-security-and-privacy

Preservation of confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability (ISO/IEC 27000:2016)

Cybersecurity / network and information security

ISO/IEC 27 001 – Information technology – Security techniques – Information security management systems – Requirements

- Information Security Management System (ISMS)
- Information security needs good management



Objectives

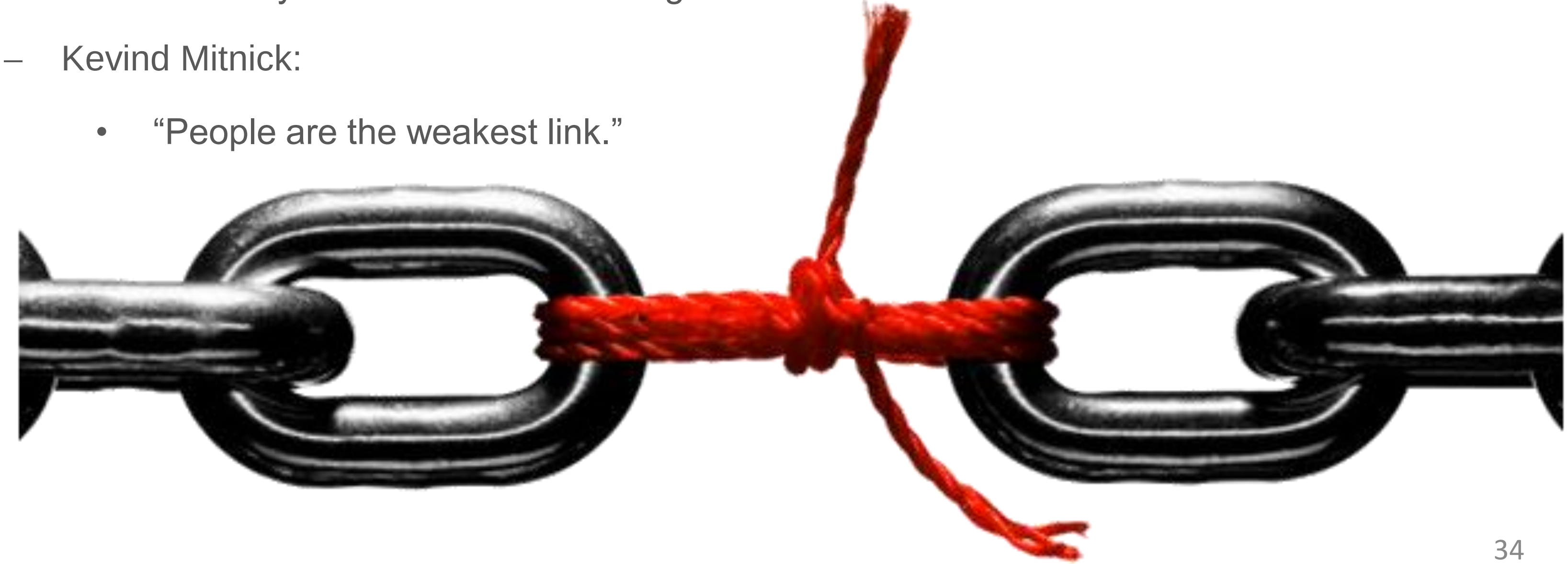
- Reduce the number of incidents
- Reduce the impact of incidents
- Learn from own and others' experience

Cybersecurity / network and information security

ISO/IEC 27 001 – Information technology – Information security management systems

Information Security Management System (ISMS)

- Bruce Schneier:
  - “Security is a chain: it is as strong as its weakest link”
- Kevind Mitnick:
  - “People are the weakest link.”



Cybersecurity / network and information security

ISO/IEC 27 001 – Information technology – Information security management systems

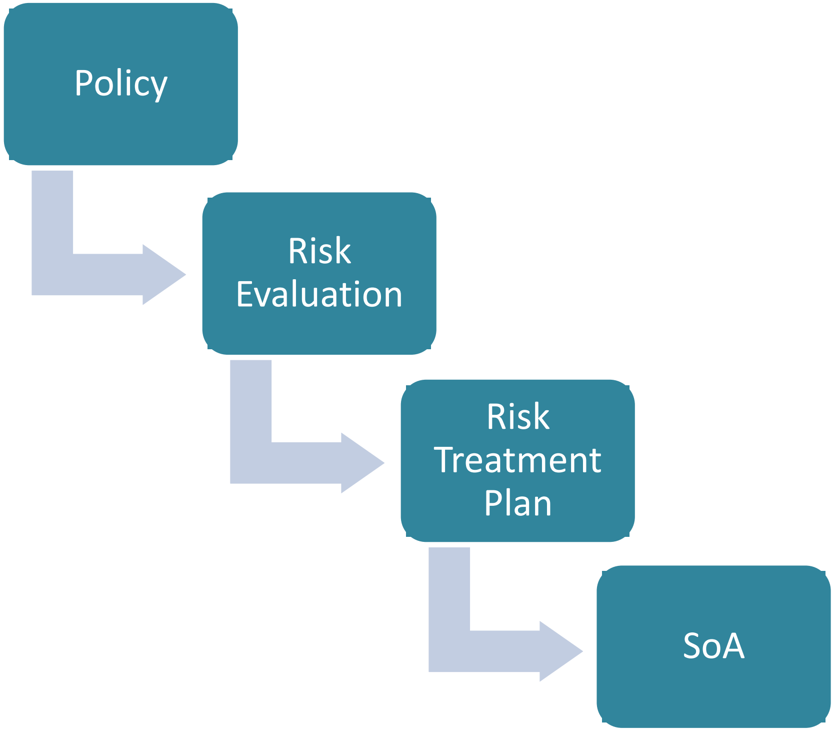
- Management system
  - Set of procedures an organisation shall apply in order to reach its objectives
  - Systemizing of the organisation in its way of operating
- Applicable to any organisation
  - Small or big, for any product or service, for any sector
  - Everyone is concerned within the scope of the standard
- Continual improvement
  - An organisation or a company evaluates its situation, determines objectives and creates a strategy, invests actions to achieve these objectives, then evaluates the results and adapts the processes to improve (PDCA)
- Assessable

Cybersecurity / network and information security

ISO/IEC 27 001 – Information technology – Information security management systems

Planning the ISMS

- The management shall establish a Security policy (objectives, commitment of the management, improvement)
- Risk evaluation
- Statement of Applicability (SoA) including controls of ISO/IEC 27002:2013
- Controls can only be excluded if no risks or below level of risk acceptance
- Any exclusion shall be documented and justified in SoA



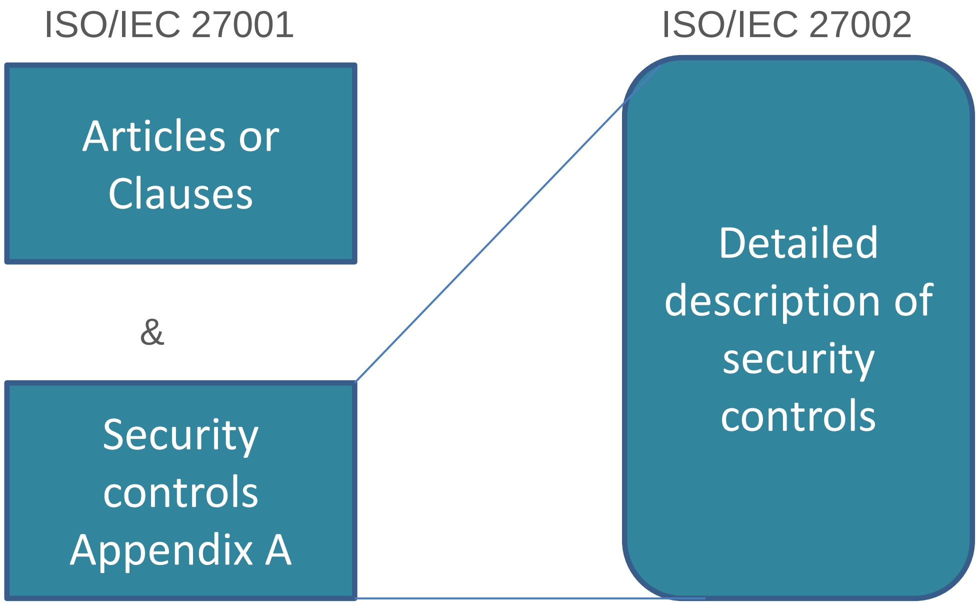
Cybersecurity / network and information security

ISO/IEC 27 002 – Information technology – Code of practice for information security controls

- Security recommendations or requirements
- Classical recommendations of security experts
    - Some controls are quite general, some precise
    - Some controls are applicable to all the organisation, some are applicable to specific areas
    - Provide recommendations which may be large and may include other security controls
- Selected to reduce risk to an acceptable level after their evaluation
- Policies (rules), documented procedures, guidelines, practices, organizational structures
    - Administrative
    - Technical
    - Legal

Cybersecurity / network and information security

ISO/IEC 27 002 – Information technology – Code of practice for information security controls


ISO/IEC 27001
Articles or Clauses
&
Security controls Appendix A
ISO/IEC 27002
Detailed description of security controls

Cybersecurity / network and information security

ISO/IEC 27 005 – Information technology – Information security risk management

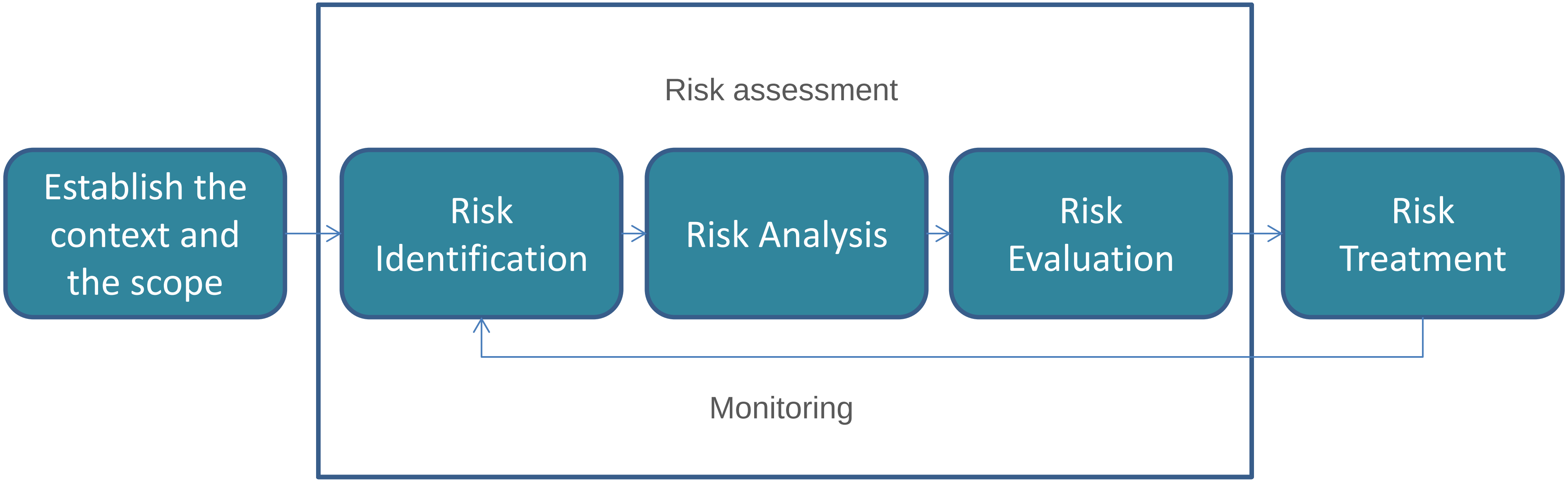
What is a risk?

- Effect of uncertainty on objectives
- An effect is a deviation from the expected – positive or negative (in information security we deal with negative effects)
- Risk is often characterized by reference to potential events and consequences, or a combination of these.
- Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Cybersecurity / network and information security

ISO/IEC 27 005 – Information technology – Information security risk management

– Information Security Risk Management



Cybersecurity / network and information security

ISO/IEC 27 005 – Information technology – Information security risk management

– Identify the risks: threats

  Examples:

  - Virus intrusion, Spying, Fire
  - Overload of information network
  - Corruption of the data, violation of user rights

– Vulnerabilities:

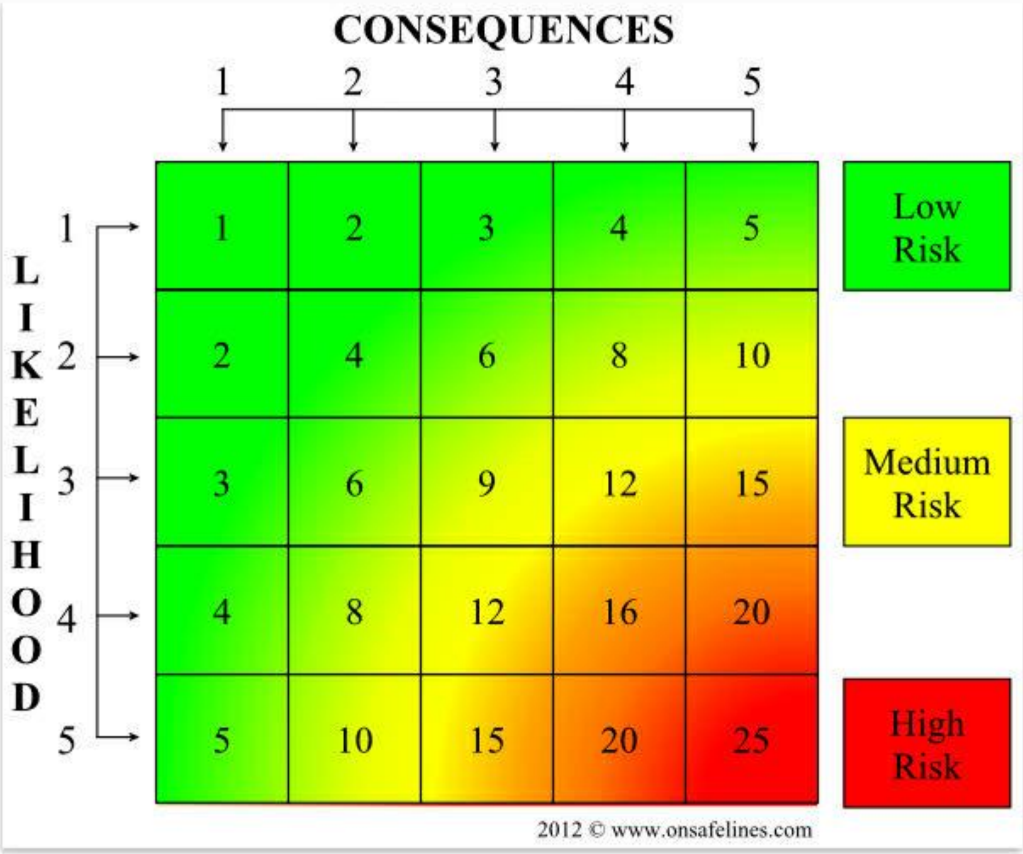
  Examples:

  - Missing of daily update
  - Portable database
  - Policy of easy password
  - Light internet network security

Cybersecurity / network and information security

ISO/IEC 27 005 – Information technology – Information security risk management

– R = L x C



CONSEQUENCES

LIKELIHOOD	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

🟩 Low Risk

🟨 Medium Risk

🟥 High Risk

2012 © www.onsafelines.com

Cybersecurity / network and information security

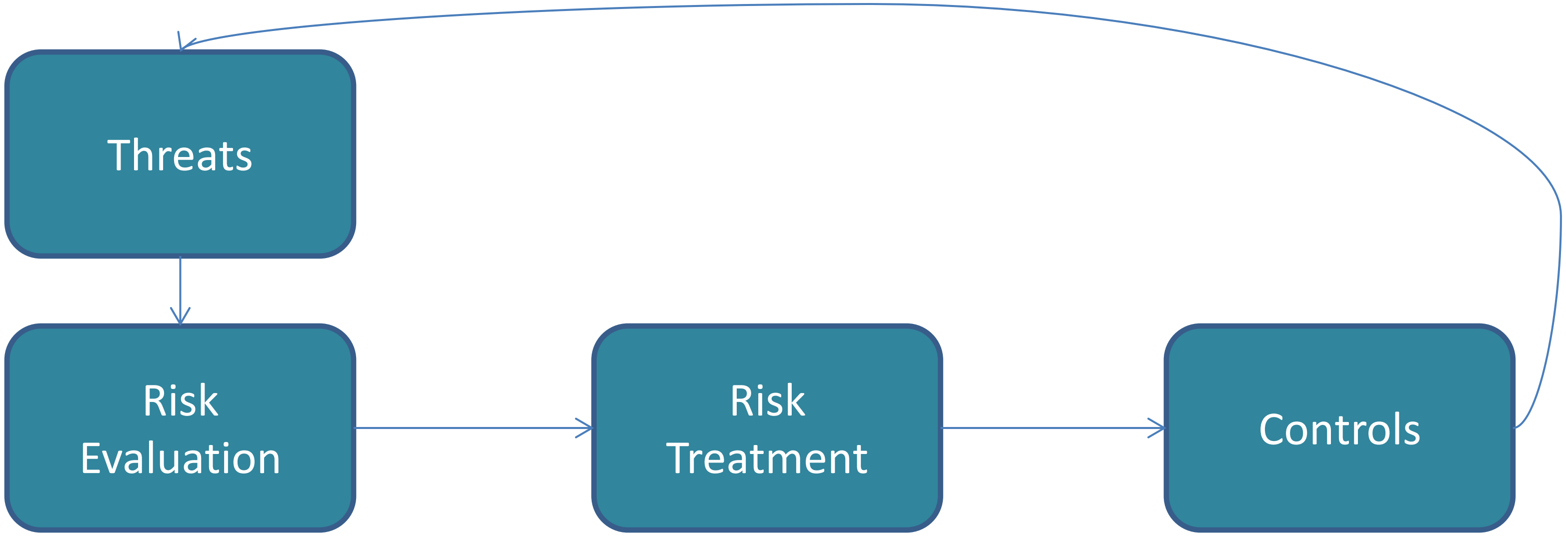
ISO/IEC 27 005 – Information technology – Information security risk management

Risk treatment

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing risk in order to pursue an opportunity
- Removing the risk source (i.e. the threat; not applicable to information security)
- Changing the likelihood (i.e. of the threat; to read as “changing the likelihood that and incident happens”)
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Accepting the risk by informed choice

Cybersecurity / network and information security

ISO/IEC 27 005 – Information technology – Information security risk management



ePrivacy

- Data protection by design
- Minimising the risk of
  - Divergent national approaches, with their related risks to freedom of movement of products and services
  - the development of several, potentially conflicting, private de-facto standards
- Related ongoing standardisation and research activities
  - ETSI TC CYBER: Privacy
  - CEN-CENELEC/TC 13 "Cybersecurity and Data protection" has been created in 2017, to develop standards for data protection, information protection and security techniques
  - …

3.2.1 eHealth, healthy living and ageing

3.2.4 e-Skills and e-Learning

3.2.5 Emergency communications

3.2.6 eGovernment

3.2.7 eCall

eHealth, healthy living and ageing

- ICT applied to health and healthcare systems can increase their efficiency
- Lack of interoperability between eHealth systems
- Related ongoing standardisation and research activities
  - CEN – Technical Committee 251 – Health Informatics: providing a focal point for standards in this domain, in close collaboration with ISO/TC 215
  - ETSI – develops DECT ULE, a low power wireless technology providing optimal radio coverage in indoor scenarios for reliable audio and data services suitable for many eHealth applications, e.g. health monitoring, emergency alarms for vulnerable people and remote medical monitoring
    ETSI Project (EP) eHealth provides a focus point in ETSI on issues such as mHealth and telemedicine. Development of standards to facilitate telemedicine and the "Internet Clinic"

3.3.1 e-Procurement – pre- and post award

3.3.2 e-Invoicing

3.3.3 Card, internet and mobile payments

3.3.5 Preservation of digital cinema

3.3.6 Fintech and Regtech Standardization

3.3.7 Blockchain and Distributed Digital Ledger Technologies

e-Invoicing

- Invoice, transmitted and received in a structured electronic data
- Automatic and electronic processing
- Increased efficiency, faster payments, reduced environmental impact
- New e-invoicing standards, based on different versions of XML
- Vast number of e-invoicing standards (many proprietary standards), data formats exist across EU
- Related ongoing standardisation and research activities
  - CEN
  - UN/CEFACT Cross-Industry Invoice
  - ISO

Card, internet and mobile payments

- Payments involving mobile phone, gain importance
- Mobile connected devices exceed the number of people on earth
- Based on card payments, credit transfer, direct debits or pre-funded cards and accounts
- Absence of common standards, standardisation gaps, lack of interoperability
- Near field communication (NFC): possible lead technologies for proximity mobile payments,
- Related ongoing standardisation and research activities
  - ETSI: Smart Secure Platform (SSP)
  - ITU-T:
  - W3C: Forum for Web Payments technical discussions
  - ISO TC68/SC7/WG10 - Mobile payments WG
  - ISO/IEC JTC1 SC 17- Cards and personal identification
  - NEXO and EPCNEXO: protocols for card payment in Eurozone

Blockchain and Distributed Digital Ledger Technologies

- Great potential in providing an infrastructure for trusted, decentralised and disintermediated services
- FinTech industry has been an early adopter because of its early awareness of bitcoin
- Promising technology to share data and manage transactions in a controlled manner
- Many possible applications to deliver social goods in the field of eHealth and eGovernment, health records, land registries or the security certification of links in an Internet of Things chain of devices, manage intellectual property rights and eID
- Related ongoing standardisation and research activities
  - ISO/TC 307: Blockchain and distributed ledger technologies
  - IEEE http://standards.ieee.org/develop/msp/blockchain.pdf
  - ITU-T
  - …

II ROLLING PLAN FOR ICT STANDARDISATION

D – SUSTAINABLE GROWTH

3.4.1 Smart grids and smart metering

3.4.2 Smart cities / technologies and services for smart and efficient energy use

3.4.3 ICT Environmental impact

3.4.4. European Electronic Toll Service (EETS)

3.4.5 Intelligent Transport Systems (ITS)

3.4.6. Advanced manufacturing

3.4.7 Robotics and autonomous systems

3.4.8. Construction - building information modelling

3.4.9 Common Information Sharing Environment (CISE) for the EU maritime domain

Smart grids and smart metering

- Energy system becomes consumer-centric
- Digital transformation of the energy sector
- Two-way digital communication between supplier and consumer
- Intelligent metering and monitoring systems, remote operation of meters
- Related ongoing standardisation and research activities
  - ESOs: EC mandate 490 (Smart grids technologies) completed in 2015
    Smart Meters Coordination Group (SM-CG)
    Electro-mobility work program, standards for the charging of electric vehicles
    Cyber Security and Privacy report
  - IEC: System committee on smart energy
  - ISO/IEC JTC1, IEEE, ITU-T, OASIS, IETF are also active in this field

Smart cities / technologies and services for smart and efficient energy use

- 75% of the EU population lives in urban areas
- Construction sector: highest energy consumer in the EU (~40%)
- Controlling the efficient consumption of energy at buildings
- Healthcare, education, emergency services
- Related ongoing standardisation and research activities
  - SEMANCO is developing a Semantic Energy Information Framework to model the energy-related knowledge planners
  - eeSemantics (stakeholders group launched by DG CONNECT): active in the area of energy efficient buildings data models
  - ISO, IEC: TC 268 “Sustainable development in communities”
    ISO-IEC/JTC1 WG11 “Smart cities”
  - …

Robotics and autonomous systems

- Strong economic contribution as an industrial and commercial activity
- Autonomous (or near-autonomous) vehicles
- High impact on everyday life
  - Healthcare, agriculture, civil, commercial or consumer sectors
  - logistics and transport
- Related ongoing standardisation and research activities
  - ISO/TC 299 — Robotics
    http://www.iso.org/iso/iso_technical_committee?commid=5915511
  - IEEE: navigation, applications for transportation and ethical considerations for the design of autonomous systems

Thank you

Merci

Danke

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10
E-mail : info@ilnas.etat.lu
www.portail-qualite.lu