Securing Critical Infrastructures In The Financial Sector

Standards and General Purpose Regulations: Impact on Financial Technologies

Objectives

Standards

Goal

- Learn about the ISO/IEC standards applicable to the financial sector
- Understand their impact for information technologies

General purpose regulations

- Explore general purpose regulations and their relevance to the financial sector
- Identify their impact on financial technologies


The Standards
Standards

List of standards and directives to be addressed

- ISO/IEC 27000 standards' family
- ISO/IEC 27015:2012
- Directive on security of network and information systems (NIS Directive)

ISO/IEC 27000 standards' family

⌘ Issued by	■ International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
⌘ Objective	■ Provide best practice recommendations on information security management: management of information risks through information security controls
⌘ Focus	■ Describes the fundamentals on information technology with respect to security techniques and information security management systems ■ Provides additional support to the financial industry to set up an appropriate information security management system for the provisioning of their financial services

**Note:* The adoption of the standard is not universal in the finance and banking sector, although the compliance of financial organisations is recommended

ISO/IEC 27000 standards' family

⌘ Value added	■ International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

⌘ ISO 27000 series	■ Sector-specific guidance for the financial sector:
	  ■ information security of assets
	  ■ information processing in order to support the information security of processed information

⌘ Impact on financial technologies	■ Requirements relevant to financial security

ISO/IEC 27000 standards' family

External parties

Secure areas

Exchange of information

Evaluate vulnerabilities

Reporting

ISO 27000 – Requirements (selected)

- specific requirements for maintaining the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties
- need to secure perimeters including walls, card controlled entry gates or manned reception desks
- maintain the security of information and software exchanged within an organization and with any external entity
- exposure to vulnerabilities is evaluated, and appropriate measures taken to address the associated risk
- information security events weaknesses associated with information systems are communicated such in a timely manner to allow for corrective action

ISO/IEC 27015:2012

⌘ Issued by	■ International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
⌘ Objective	■ ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services
	■ Technical report ■ Supplement of the ISO/IEC 27000 family of International Standards for organizations providing financial services ■ Guidance contained in this technical report extends information security controls defined in ISO/IEC 27002:2005 - Information security management and controls

Directive on security of network and information systems (NIS Directive)

⌘ Content	■ EU-wide legislation on cyber-security
⌘ Geographical area	■ EU-wide
⌘ Objective	■ Boost cyber-security in the EU
⌘ Focus	■ Legal measures to boost cyber-security in the EU ■ Requires Operators of Essential Services (OESs) to implement appropriate and proportionate security measures to achieve the outcomes set out by the NIS principles and notify the relevant national authorities of serious incidents and events

Directive on security of network and information systems (NIS Directive)

⌘ Scope

- Financial services and financial market infrastructure providers (including trading venues and central counterparties) are considered as “Operators of Essential Services” (OES)
- OES have to take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of their networks and information systems
- Prevent and minimize the impact of cyber incidents
- Serious incidents need to be notified to the relevant national authority (i.e. Computer Security Incident Response Teams) that each EU country will need to set up

*Note: Responsibility on the essential services providers: e.g., if a financial services company has outsourced the cloud computing services to a third party, the delegating entity still holds the main responsibility of any cyber attack data breach.

Directive on security of network and information systems (NIS Directive)

- Impact on banking and financial services

- Notification about incidents in the banking sector is indicated to be specified by member states:
  - Requirements for notification of incidents are part of normal supervisory practice in the financial sector

General purpose regulations

List of general purpose regulations and standards

- EU Privacy Rules – GDPR
- e-Privacy
- eIDAS

General Data Protection Regulation (GDPR)

Characteristics	*Details*
⌘ Content	▪ Designed in order to adapt the existing data protection legislation with respect to the way in which data is currently being used in the digital setting
⌘ Geographical area	▪ Europe-wide
⌘ Objective	▪ To empower EU citizens by making them aware of the kind of data held by institutions and the rights of the individual to protect their personal information
⌘ Focus	▪ Provides additional control to EU residents on over how their personal information is accessed, communicated and stored ▪ Failure to comply incurs significant penalties for institutions, this will be discretionary and, depending on the nature of the breach, ≈ 2% - 4% of worldwide revenue, max 20m

General Data Protection Regulation (GDPR)

Characteristics	*Details*
⌘ Scope	■ Standardises data privacy laws and mechanisms across industries, regardless of the nature or type of operations -> financial institutions are affected ■ Financial organizations collect large amounts of customer data which are used in a variety of processes and activities
⌘ Impact on banking and financial services	■ Institutions need to demonstrate the integrity and validity of their customer's consent with respect to how their data is shared and used ■ Processes involving customer data is exposed to different people, at different stages -> GDPR applied in any of the processes that requires the handling of any type of customer data ■ Inform customers on how they plan to process and use the data. Additionally, each institution needs to appoint a Data Protection Officer (DPO)

GDPR & relevance to financial services

Data subject consent	▪ Awareness of customers about personal data stored by financial institutions ▪ Any data that can be used to identify an individual (and any data related to pseudoanonymization)
Data portability	▪ Individuals can request access to, or the removal of, their own personal data from financial institutions
Minimizing chances of breach	▪ Financial institutions may keep some data to ensure compliance with other regulations, but in all other circumstances where there is no valid justification, the individual's right to be forgotten applies
Vendor management	▪ Wide deployment of outsourcing services -> firms need to ensure that personal client data is not accessible to external vendors, thus significantly increasing the data's net exposure
Reporting	▪ Non-EU organisations that collaborate with EU banks or serving EU citizens, to ensure vigilance while sharing data across borders

GDPR & relevance to financial services

Privacy by design

- Controllers should embed privacy features and functionalities into products, systems from the time that are first designed
- Appropriate measures can be appliedon collected data, pseudonymisation techniques and improved encryption

Pseudoanonymization

- Data must also be pseudonymised into artificial identifiers to ensure the data access stays within the realms of the 'need-to-know' obligations

Impact assessment

- Carry out an impact assessment (Privacy Impact Assessment - PIA) for organizations that perform data processing that may involve a high risk for the rights and freedoms of natural persons. The origin, nature, particularity and severity of such risk must be assessed

GDPR & relevance to financial services

Data Protection Officers (DPO)

- Responsible individual is identified as the Data Protection Officer within each organization (required for org. >250 empl.)
- Duties relevant to monitoring the implementation and application of internal policies, coordinating audits, supervising the execution of the impact evaluation, point of contact for the supervisory authority etc.

Biometrics

- Financial services may use of biometrics, such as for example fingerprints and eye scans to identify their customers
- Required to take the necessary technical and organisational measures to prevent this special data from being exposed, as a consequence their systems being poorly managed

e-Privacy

Characteristics	*Details*
⌘ Content	■ Particularise and complement the GDPR by identifying certain rules for the rights of natural and legal persons on electronic communication
⌘ Geographical area	■ Europe-wide
⌘ Objective	■ Respect for private life and protection of personal data in electronic communications
⌘ Focus	■ Protection of fundamental rights and freedoms of natural and legal persons with respect to the use of electronic communications services ■ Free movement of electronic communications data and electronic communications services within the EU Includes data to trace and identify the source and destination of a communication ■ Relevant to any metadata from electronic communications e.g., time/date of a call

e-Privacy

Characteristics	*Details*
⌘ Impact on financial technologies	■ All electronic communications exchanged in the financial sector are subject to stricter requirements, especially in the case that they contain personal or confidential data ■ Additional security requirements for the transmission of personal and confidential data through electronic means ■ Including email communication, fund transfers, information exchanges related to regulations such as AEI (Automatic Exchange of Information), FATCA (Foreign Account Tax Compliance Act) or MiFID (Markets in Financial Instruments Directive) ■ Enhanced requirements in applications developed (such as web-banking or mobile banking apps) where data such as transaction details are stored by the user ■ Internal screenings of e-mails and other electronic files will require the prior consent of the user

eIDAS

Characteristics	*Details*
⌘ Content	▪ EU regulation on a set of standards for electronic identification and trust services for electronic transactions in the European Single Market
⌘ Geographical area	▪ Europe-wide
⌘ Objective	▪ To provide certainty on the legal validity of all these services, businesses and citizens that will use the digital interactions as their natural way of interaction
⌘ Focus	▪ Ensure that individuals and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU member states ▪ Create a European internal market for eTS - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional means

eIDAS

Characteristics	*Details*
⌘ Impact on financial technologies	■ Legal effects for qualified electronic signatures, seals, certificates for electronic seals, timestamps and documents, as well as e-signature and e-seal creation devices ■ Legal framework for e-registered delivery services and website authentication services ■ Basis for eID schemes notified under the regulation in one member state to be recognised in one another ■ Security of personal data and breach notification requirements for all trust service providers ■ Supervision for Qualified Trust Service Providers (QTSPs), trusted lists and a trust mark for QTSPs to demonstrate compliance with the regulation