UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unIMC

Secure data lifecycle in banking industry

Nicola Fioranelli

Data & Application Protection

UniCredit Group S.p.A.

nicola.fioranelli@unicredit.eu

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Agenda

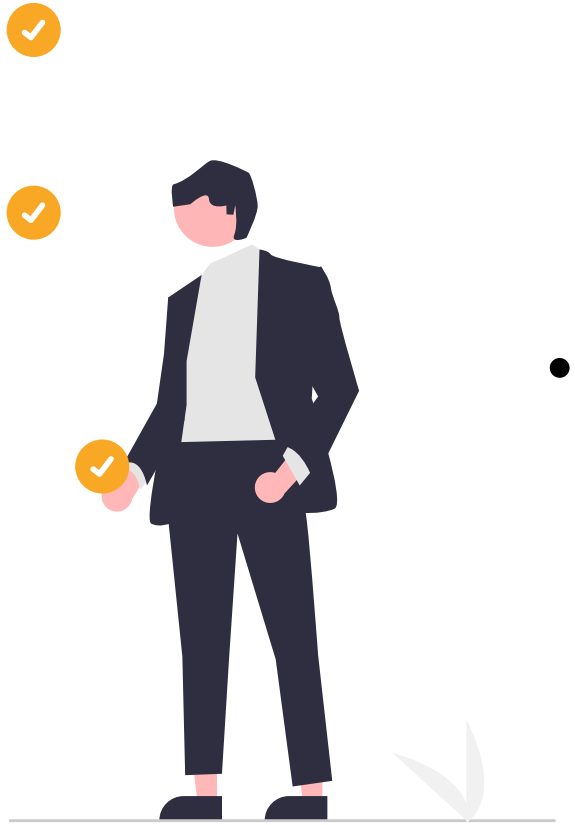
1. Objective
2. Legal context
3. Risks and reference guidelines
4. Data and lifecycle definition
5. Conclusion and future developments

1. Objective

Research origins

- Multiplicity of poorly integrated technological solutions for data protection
- Missing **reference framework** for the banking industry that takes care of data
- **Datification**
  - An increasingly widespread phenomenon but with unexpected repercussions
  - Huge amount of new data but that can’t be analyzed appropriately
  - «Myopia» of the data protection engineer

Objective



- Guarantee **security of data** at every stage of its **lifecycle**, in compliance with the **regulations and laws** in force
- Trace **data** and define its **flow** in order to be able to rebuild the **reason of its presence** in every instant

2. Legal context

European and local regulatory context

- **GDPR**
  - Article 4 – Definition of Controller
    - How this concept can be adapted in large enterprises
  - Article 5 – Principles
    - Accuracy
    - Storage limitation
    - Integrity and confidentiality
  - Article 17 – Right to erasure
    - Right to be forgotten
  - Article 25
    - Protection by design and by default

European and local regulatory context

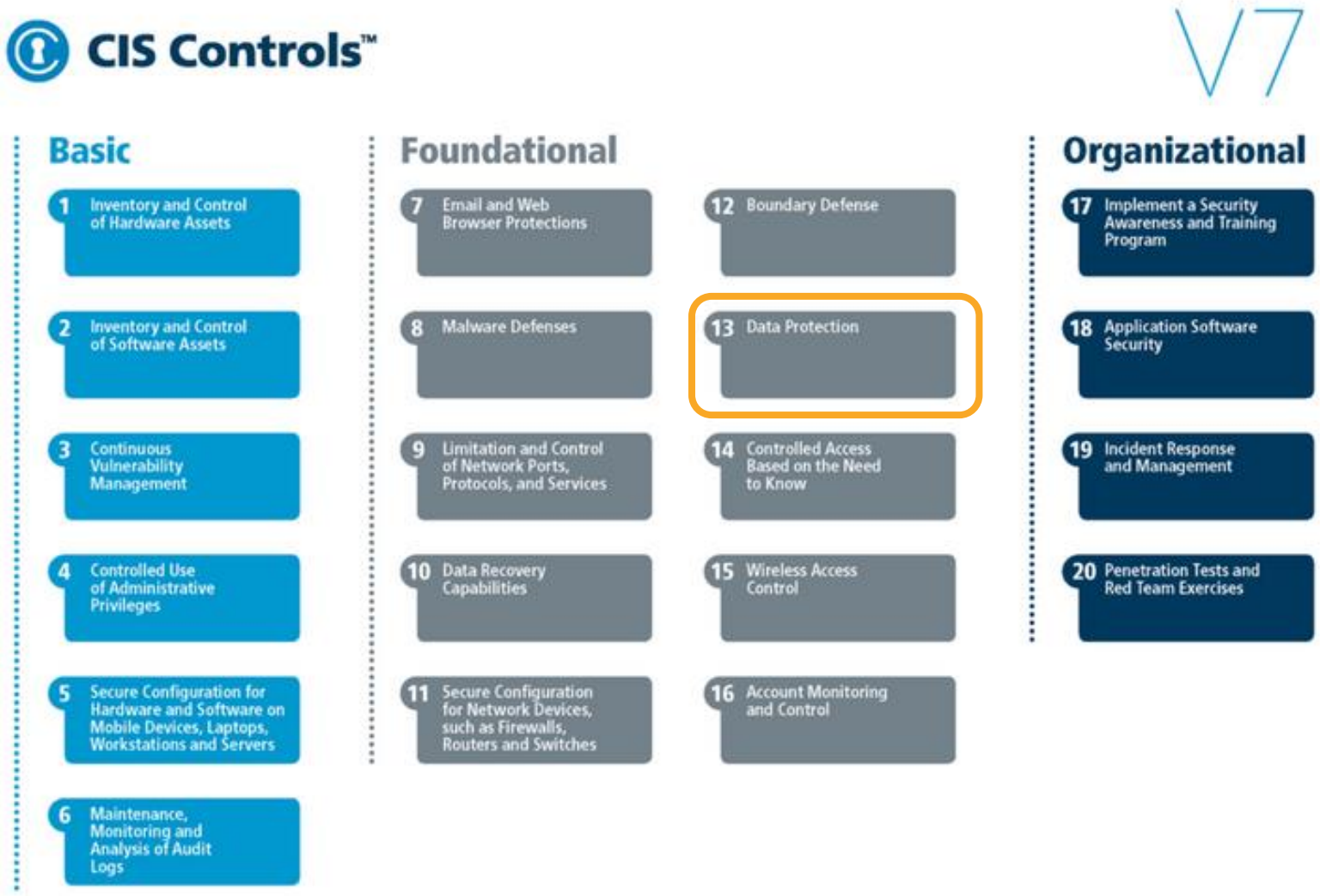
- **GDPR**
  - Article 32
    - Appropriate technical and organisational measures
- **Directive (EU) 2015/849** («Anti-Money Laundering Directive»)
  - Regarding document conservation
- **D.Lgs. 21 novembre 2007, n. 231** (also known as «Decreto Antiriciclaggio» from Banca d'Italia)
- **Data Retention Directive** (Directive 2006/24/EC)

3. Risks and reference guidelines

Risks linked to data usage

- **Features to be preserved**
  - Confidentiality, Integrity and Availability
- **Risks**
  - Destruction, Loss, Modification, Cancellation and Uncontrolled Access
- **Effects**
  - Discrimination, identity theft, loss of data control, financial losses, physical damage, psychological damage, economic disadvantages, reputational damage

Reference guidelines: CIS



CIS Center for Internet Security

Reference guidelines: ATT&CK

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Defence Evasion
- **Credential Access**
- Discovery
- Lateral Movement
- **Collection**
- **Command and Control**
- **Exfiltration**
- **Impact**

Reference guidelines: ENISA

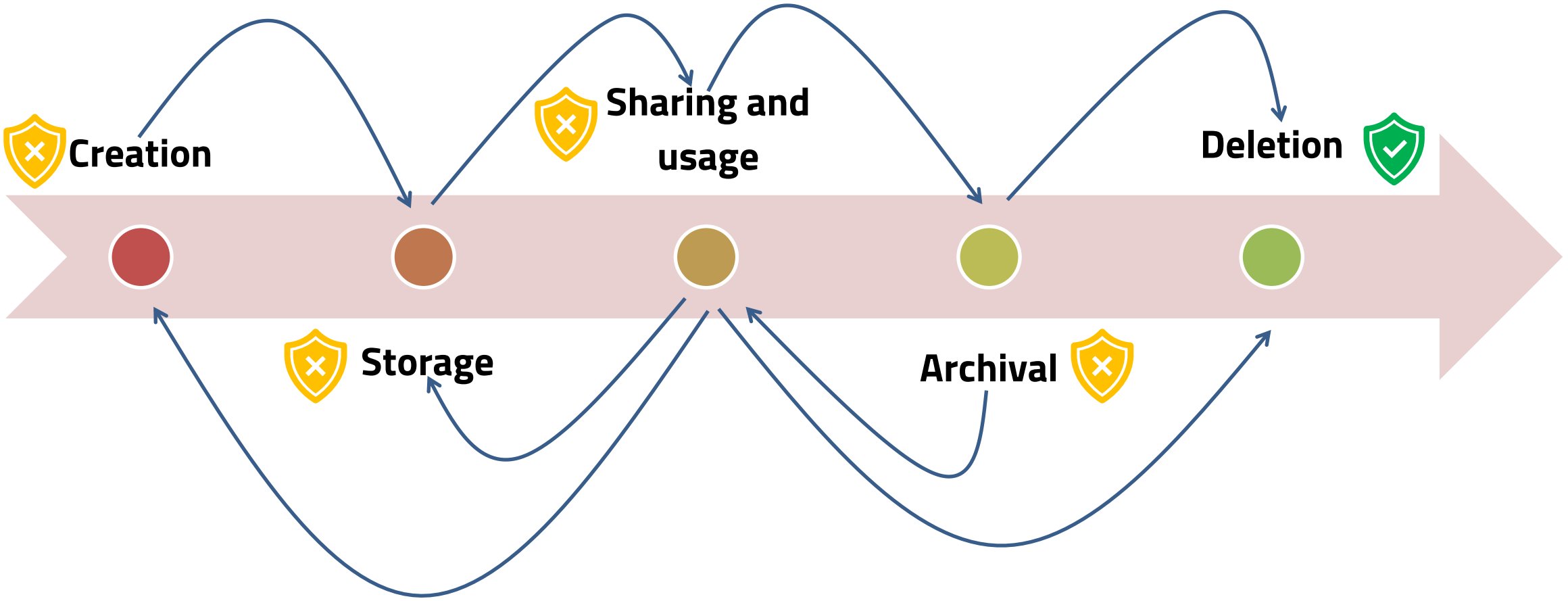
- Engineering data protection
- Anonymisation and pseudonymisation
- Data masking and privacy-preserving computations
- Access, communication and storage
- Transparency, intervenability and user control tools

4. Data and lifecycle definition

Data in the banking industry

- **Interested categories**
  - Employees
  - Clients
  - Vendors
  - Future employees
- **Type of data**
  - Application logic
  - Logs
  - Financial
  - Personal
  - Sensitive
  - Business critical
  - Credentials
- **Type of storage**
  - Structured
  - Unstructured

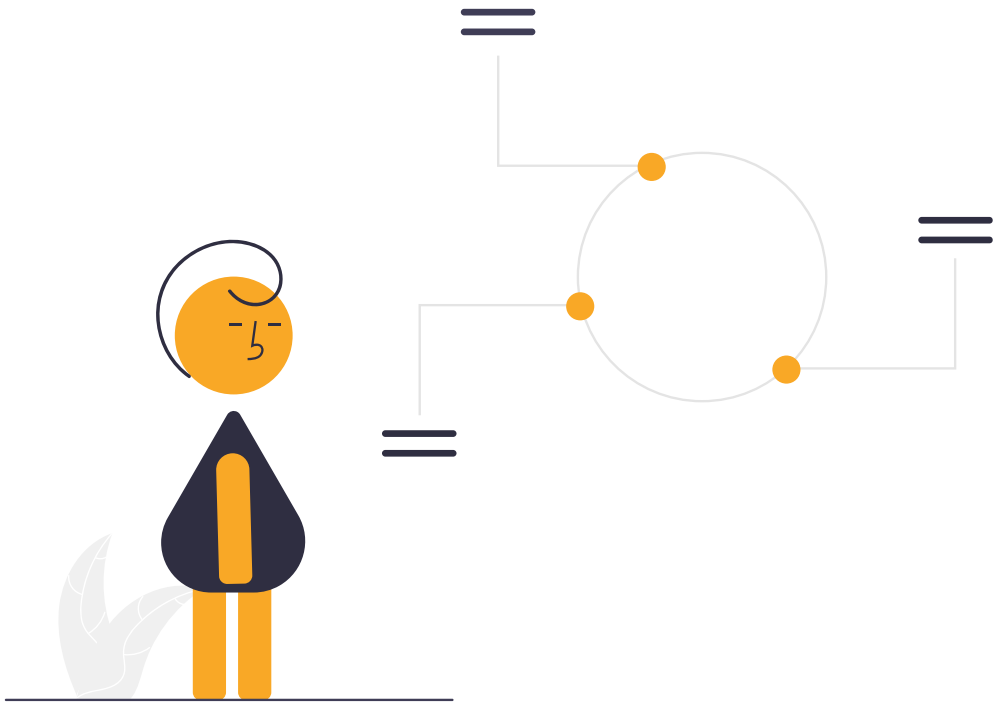
Data lifecycle definition



= compliance with GDPR

= potential threats

Usage matrix



	Creation	Storage	Sharing and usage	Archival	Deletion
Data at rest				X	
Data in use	X	X	X		X
Data in motion	X		X		

Threat matrix

	Creation	Storage	Sharing and usage	Archival	Deletion
Data at rest				• Data Exfiltration (C) • Data Destruction (I-A) • Data Manipulation (C-I-A) • Data Encrypted for Impact (A)	
Data in use	• Data Manipulation (I-A) • Adversary-in-the-Middle (C-I-A)	• Data Manipulation (C-I-A) • Data Exfiltration (C) • Data Encrypted for Impact (A) • Data Destruction (I-A)	• Information Gathering (C) • Data Encrypted for Impact (A) • Data Manipulation (C-I-A) • Malicious insiders (C) • Human error (C-I-A)		
Data in motion	• Adversary-in-the-Middle (C-I-A)		• Information Gathering (C) • Adversary-in-the-Middle (C-I-A) • Data Manipulation (C-I-A) • Human error (C-I-A)		

Supporting technologies

	Creation	Storage	Sharing and usage	Archival	Deletion
Data at rest		• Encryption ⌂ • Access control ⌂ • Privacy preserving storage		• Network segmentation ⌂ • Encryption ⌂ • Access control ⌂ • Activity control ⌂ • SOC alerts ⌂ • Anonymization ⌂ • Zero Knowledge Proof • Privacy preserving storage • Data Backup ⌂ • Data discovery ⌂	• Retention policy ⌂ • Data Owner Control
Data in use	• Data owner association • Users training • Classification ⌂	• Homomorphic encryption • Trusted Execution Environments ⌂	• Users training • Zero Knowledge Proof • Data Loss Prevention ⌂		
Data in motion	• Data owner association • End to End Encryption ⌂ • Network Intrusion Prevention ⌂		• Network Intrusion Prevention ⌂ • Data Loss Prevention ⌂		

⌂ = technology already diffused in the market

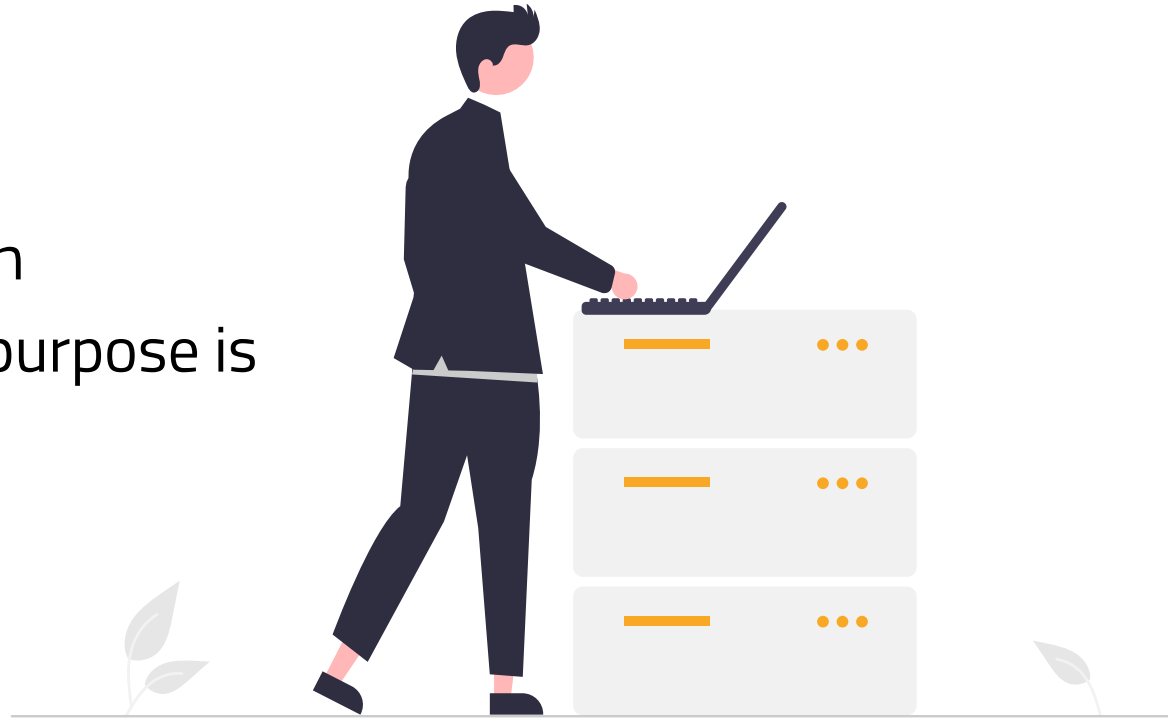
5. Conclusion and future developments

Data retention

- How is it possible to organize the deletion phase?
- Which thresholds can be adopted?
  - Financial data 10 years
  - Logs (min 6 – max 48 months)
  - What about company data?
- How should care about deletion? Lazy users or automatic algorithms?
  - Automatic removal with manual confirmation
  - Threshold based on statistical behavior

Data ownership

- How is it possible to associate data owners to data flows of applications that each day generate terabytes of data?
  - **Data owner bank**
    - Periodical maintenance
    - Updates needed
    - Allows to keep track of data in each instance and understand what its purpose is



The greatest challenge: awareness!

- Security tools should become less invasive and allow users to work without too many restrictions

- **Humans are still the week link in the chain**

Thanks for your attention!