Cyber Security for Europe

CyberSec4Europe: Incident Reporting Platform in the Financial Sector

Cyberwatching webinar, 2021-05-21

Susana González Zarzosa - ATOS

CyberSec4Europe: Incident Reporting in the Financial Sector Demonstrator

Cyber Security for Europe

Task 5.4 Goals

- Specification and design of demonstration case for Incident Reporting.
- Integration and deployment of the technologies and infrastructure required.
- Execution of the validation.

Research Challenges

- Lack of harmonization of procedures.
- Facilitate the collection and reporting of incident and/or data leaks.
- Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and overall cyber resilience.

Timeline

Phase 1 (January 2021):

- Basic incident reporting platform
- Regulations: PSD2 / ECB

Phase 2 (July 2022):

- Incident reporting platform enhancements
- Other regulations: eIDAS, NIS, TARGET2, GDPR
- Threat Intelligence Data Sharing

Constraints

- Limited Effort
- Integration of available technical assets (implemented in other WP)

Atos BBVA INTESA SANPAOLO

Why an Incident Reporting Platform in the Financial Sector?

- ✓ **Cybersecurity in the financial sector is crucial**, so it is strong the need to implement and leverage tools helpful to mitigate and tackle cyber threats and improving cyber resilience. In particular, to **facilitate the collection and reporting of security incidents and/or data leaks**.
- ✓ There is a need to **tackle the lack of harmonization in the EU mandatory incident reporting process**, which results from the different requirements defined by each supervisory authority at both, EU and national levels. The ambition is creating a demonstrator of a smart incident reporting platform to address the common need for standardized and coordinated cybersecurity notification in case of significant cyber and operative incidents.
- ✓ There is a need of developing a **platform that enables financial institutions to fulfil the mandatory incident reporting requirements** according to the different Supervisory Authorities rules.
- ✓ It would promote a **collaborative approach** to pave the way towards **public and private cooperation towards reaching the common goal of enhancing cyber resilience** not only across Europe but also beyond the EU borders.

Applicable regulations to financial institutions

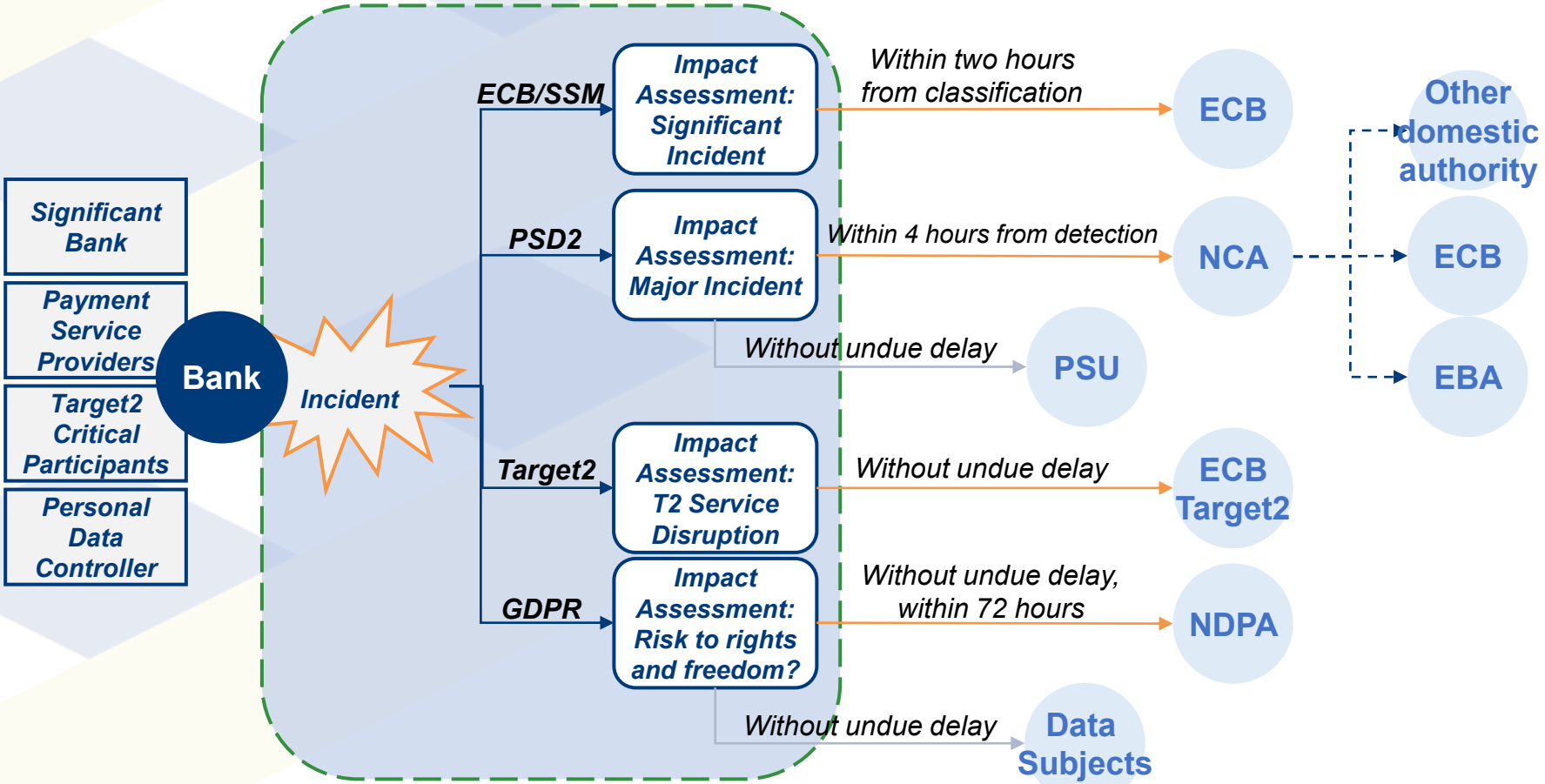
Cyber Security for Europe

FI

ECB Target2	***Target 2 Participants***	*A distinction is made between **critical participants** and **non-critical participants** depending on the market share in terms of value and/or the type of transactions processed.*
ECB SSM	***Significant Institutions***	*The ECB classify a bank as **Significant or Not Significant** based upon the criteria of Size, Economic Importance, Cross-Border Activities and Direct Public Financial Assistance.*
PSD2	***Payment Services Providers***	*Banks and financial institutions operating as **Payment Service Providers (PSPs).***
NIS	***Operator Essential Service***	*Banks and financial institutions are considered as **OES** because they (a) provide a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.*
GDPR	***Personal Data Processor / Controller***	*Banks and financial institutions operate both as **Processor**, which processes personal data on behalf of the controller, and **Controller** which determines the purposes and means of the processing of personal data.*
E-IDAS	***Trust Service Providers***	*Banks and financial institutions can operate with their trust services either as a **Qualified** or as a **Non-qualified trust service provider.***

Possible scenario for reporting

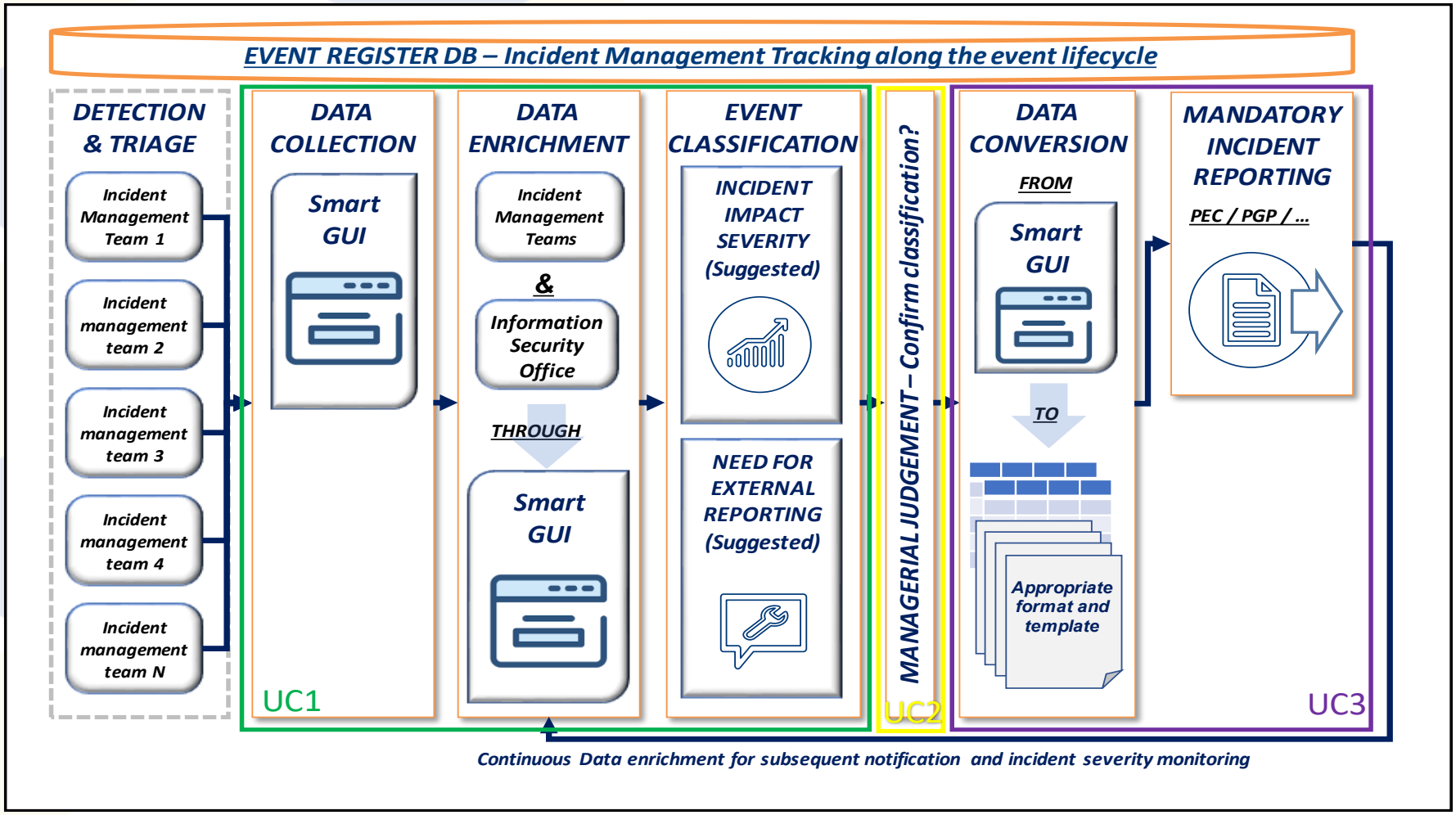
Cyber Security for Europe



There is a need for a common Taxonomy, Methodology and Data-set for an harmonised IR

Incident Reporting Workflow

Cyber Security for Europe



Demo: CyberSec4Europe Incident Reporting Platform Prototype

Cyber Security for Europe

Scenario

Show the functionalities of the CyberSec4Europe Incident Reporting Platform prototype in a hypothetical scenario in which a fictional financial institution undergo a security incident that might entail the legal obligation to send a report to the relevant Competent Authorities. In particular, we are considering the following mandatory Incident Reporting requirements for Significant Institutions and Payment Service Providers:

- ECB/SSM Cyber Incident Reporting Framework, as established by the ECB Banking Supervision
- Article 96(1) of Directive (EU) 2015/2366 (PSD2) and Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)

Actors

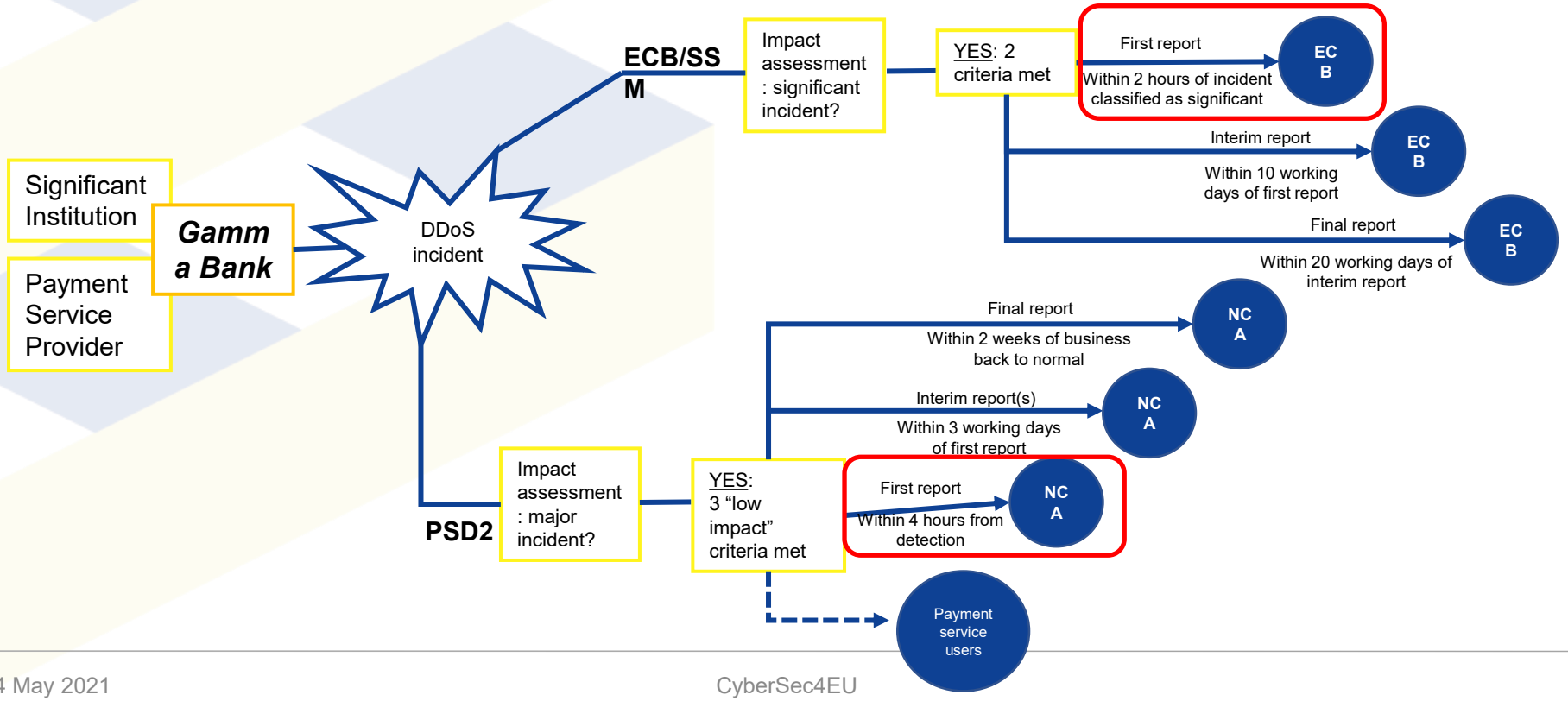
- The Incident Management Team (IMT)
- The Incident Classification Team (ICLT)
- The Controller
- The Incident Reporting Team (IRT)
- Administrator

Main Outcomes

- Incident reporting data collection.
- Incident reporting workflow enforcement with managerial judgement.
- Generation of incident reports following ECB and PSD2 Excel templates.

Demo: Attack Scenario

In December 2019, Gamma Bank, a large Italian financial institution, cut more than 500 jobs in its national offices and headquarter in an effort to reduce its expenditure. On December 23rd, a heavy DDoS attack simultaneously hit the web server hosting the home banking service and the mobile application server of the bank, making the bank's website and mobile app both unavailable for about 4 hours.
The incident sparked several complaints of the bank's customers on social media channels, who could not access their accounts and initiate any financial transaction from their computers or mobile devices. The bank's Incident Classification Team estimates that the incident affected more than 26.000 payment service users (more than 10% of the bank's payment users) and more than 10% of the bank's normal level of transactions, exceeding €100.000 in value. The row on social medias caught the attention of some major national news agencies and a few blogs and sectorial news websites also covered the incident, potentially damaging the bank's reputation.



Demo: CyberSec4Europe Incident Reporting Platform Prototype

Demo: CyberSec4Europe Incident Reporting Platform Prototype

Cyber Security for Europe

Next Steps

- Extend prototype to support complete incident reporting workflow
- Extend prototype to support other regulations (NIS, eIDAS, TARGET2, GDPR)
- Integrate prototype with MISP instance and Threat Intelligence Data sharing assets
- Connection with other projects (CONCORDIA, ECHO)

Cyber Security for Europe

Thank you

Susana González Zarzosa – Susana.gzarzosa@atos.net