

ECB's Confidentiality Regime and InfoSec Regulation impact

4 May 2023



[Redacted] Head of Section DG-SE/IGO
 [Redacted] Information Management Expert DG-SE/IGO

Background – intro to ECB, Eurosystem, ESCB & SSM

The main objective is to maintain **price stability**: safeguarding the value of the euro.



Monetary Policy

- The ECB and the national central banks **together** constitute the **Eurosystem** - the central banking system of the euro area.
- The ECB and all EU NCBs make up the **European System of Central Banks (ESCB)**.



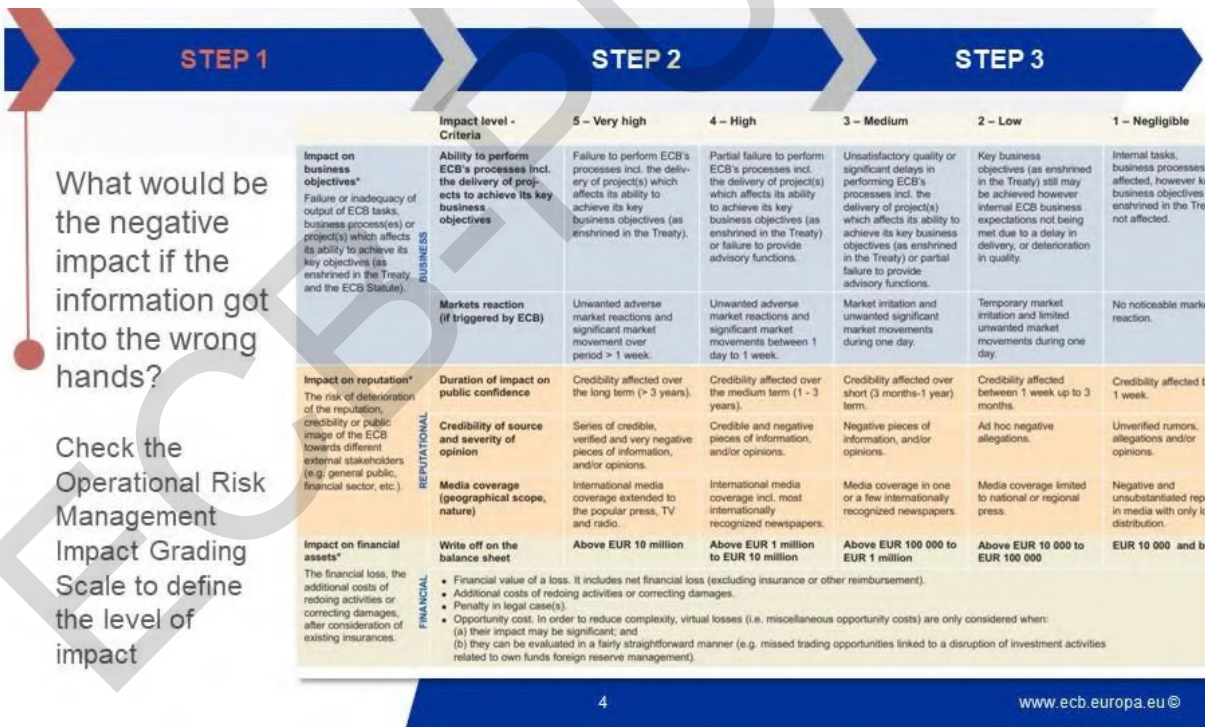
Banking Supervision

- The ECB is also responsible for the **prudential supervision of credit institutions** located in the euro area and participating non-euro area Member States.
- The ECB and all EA and non-EA participating countries NCAs work as part of the **Single Supervisory Mechanism (SSM)**.



ECB's Confidentiality Regime

- ✓ Approved by the Executive Board and binding on all ECB staff members
- ✓ All ECB information must be classified by its author or, in the case of an external document, its recipient





Choose a label based on the negative impact of misuse

Level of impact	ECB labels
Very high	ECB-SECRET
High	ECB-CONFIDENTIAL
Medium	ECB-RESTRICTED
Low or negligible	ECB-UNRESTRICTED
None	ECB-PUBLIC

✓ Classifying the document makes it clear who is allowed to access the information and how to protect it from misuse or unauthorised access.

5

www.ecb.europa.eu ©



CLASSIFICATION	DISTRIBUTION							STORAGE AND DISPOSAL		
	Internal			External				Electronic Storage	Physical Storage	Paper disposal
	Email	Post	Approval for internal distribution	Fax (recipient availability must be confirmed)	Email	Post	Approval for distribution outside ESCB/SSM			
ECB-SECRET	DARWIN links whenever possible	Not permitted, must be handed over personally	Senior manager of originating business area	Approved by EB member only in exceptional and urgent instances	Encryption mandatory DARWIN links whenever possible	Courier in double envelopes; receipt confirmation mandatory	Strict "need to know" approved by EB member	DARWIN, line-of-business application or encrypted storage device	Locked safe	Cross-cut shredding
ECB-CONFIDENTIAL	DARWIN links whenever possible	Sealed envelope	Manager of the information owner	Approved by senior manager only in exceptional and urgent instances	Encryption mandatory DARWIN links whenever possible	Registered mail or courier in double envelopes	"Need to know" approved by a manager of the information owner	DARWIN, line-of-business application or encrypted storage device	Locked cupboard	ECB locked waste container
ECB-RESTRICTED	DARWIN links whenever possible	Internal mail trailer	Yes approval required	Permitted	Encryption mandatory DARWIN links whenever possible	National post service or courier in sealed envelope	"Need to know" approved by manager of the information owner	DARWIN or line-of-business application	Locked cupboard or drawer	ECB locked waste container
ECB-UNRESTRICTED	No restrictions on distribution or removal from ECB if done for legitimate ECB/ESCB/SSM business purposes, no special rules on storage or disposal									
ECB-PUBLIC	No restrictions on distribution, storage or disposal									


Apply the rules to protect it

6

www.ecb.europa.eu ©

Common Rules and Minimum Standards

- ✓ Ensure consistent protection across ESCB
- ✓ Use DARWIN as platform to exchange sensitive information
- ✓ Ensure compliance with the ESCB/SSM information systems security
- ✓ Sensitive ESCB/SSM information not to be distributed outside the ESCB/SSM without explicit prior authorisation



Common Rules and Minimum Standards

How to classify sensitive ESCB and SSM sensitive information

ECB-UNRESTRICTED

1. Assess negative impact

Sound judgment of potential negative business / financial / reputational / individual impact of unauthorized access to, or disclosure of, sensitive ESCB and SSM information (according to the OIM Risk Impact Scale*)

2. Classify and label

Each document page should be numbered (page x of y) and labelled.

Avoid over-classification. Furthermore, the classification of sensitive information should be downgraded as soon as it does not require such high level of protection.

3. Who can be granted access

Access rights in DARWIN or local systems are to be granted in line with the rules below. A higher level of protection may be applied. A balance should be found to share where possible, protect where necessary.

Access rights should be verified regularly in DARWIN and local systems using pre-defined access groups. Responsibility for verification should be clearly assigned and communicated.

Very High	ECB-SECRET [NCB / NCA LABEL]	Persons who are directly involved in the matter and whose "need to know" access is explicitly authorised, to the extent possible in a traceable way, at the appropriate level within each ESCB central bank and SSM National Competent Authority.
High	ECB-CONFIDENTIAL [NCB / NCA LABEL]	Persons who "need to know", i.e. require the information for the proper performance of professional duties. "Need to know" should be interpreted broadly enough to enable staff to (a) access information relevant to their tasks; and (b) take over tasks from colleagues with minimal delay in the event of absences.
Medium	ECB-RESTRICTED [NCB / NCA LABEL]	Persons who are involved in the matter or could benefit from a general awareness of it in accordance with the respective roles of each ESCB central bank and SSM National Competent Authority.

To receive or grant access in DARWIN contact your [DARWIN helpdesk contact](#)

For general CRMS questions contact [CRMS helpdesk contact](#)

Please refer to the Common Rules and Minimum Standards for sensitive ESCB/SSM Information

* OIM Risk Impact Scale: <https://darwin.ecb.eu/livelink/livelink/overviews/00683289>

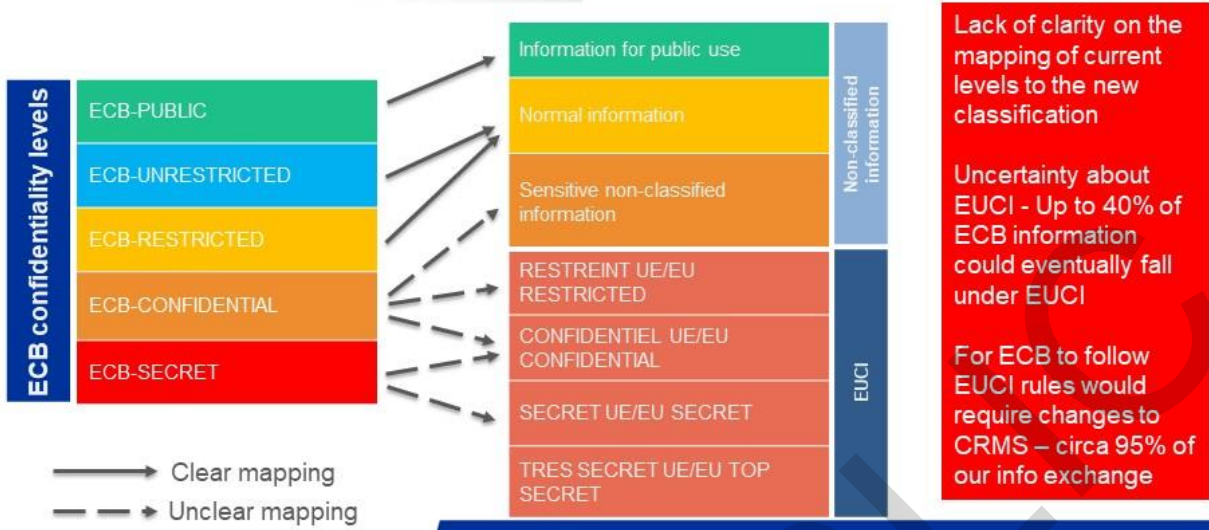
Desk aid provided by ESCB Task Force on Common Rules and Minimum Standards

ECB Information Security – EUCI regime

- The European Commission are proposing a new regulation on Information Security (led by DG Human Resources & Security)
- Will:
 - ✓ Establish uniform information that will align the handling of information within and across UIBAs
 - ✓ Directly applicable to all EU institutions, bodies and agencies (UIBAs)
- Being subject to the regulation will require us to follow the EUCI rules
- The ECB firmly supports the aims of this regulations but are very concerned about the concrete implementation and the effects each will have on the ECB's mission, the Eurosystem and SSM



ECB v. EC current info security regimes

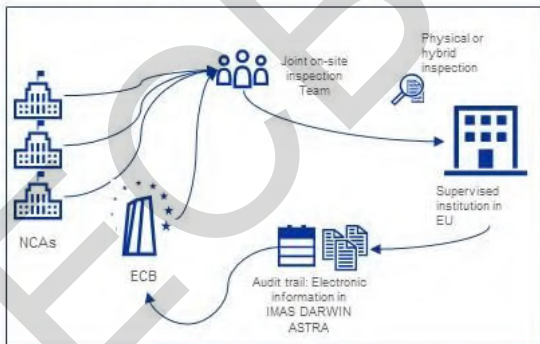


ECB – how we work ...

Business process 1:

On-site inspections by Joint Supervisory Teams

Council Regulation 1024/2013 of 15 October 2013 (the SSM Regulation) - the ECB supervises banks by performing off- and on-site inspections to ensure a detailed and thorough analysis of their business.



Examples of key documents: Loan tapes, financial statements, on-site inspection follow-up letters

Current ECB Handling

Sensitivity label: ECB-CONFIDENTIAL (as likely negative impact is high)
ORM impact definition: Partial failure to perform ECB's processes incl. the delivery of project(s) which affects its ability to achieve its key business objectives or failure to provide advisory functions. Unwanted adverse market reactions and significant market movements between 1 day to 1 week. Credibility affected over the medium term (1-3 years). Credible and negative pieces of information, and/or opinions. International media coverage incl. most internationally recognized newspapers.
Financial impact: Above EUR 1 million to EUR 10 million

Provisional Assessment under EC Rules

EU-CONFIDENTIAL as the misuse or leakage of this information could harm the essential interests of the Union

EC protective measures would not allow current business process:

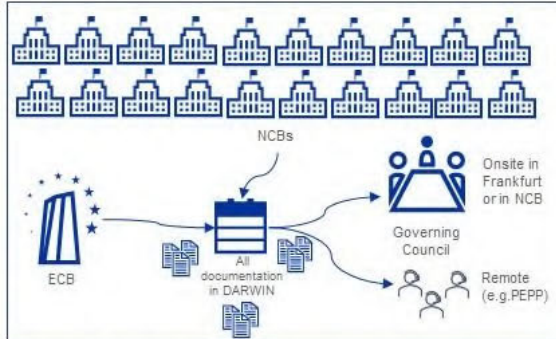
- Information only accessible on premise
- Information handled in separate secure areas
- Security clearance (of both ECB and NCA staff)
- Separation of Communication and Information Systems

ECB – how we work ...

Business process 2:

Governing Council MonPol meeting

The Governing Council is the main decision-making body of the ECB. It consists of the six members of the Executive Board, plus the governors of the national central banks of the 19 euro area countries.



Examples of key documents: Macroeconomic Projection Exercise (MPE) / Forecast related documents during embargo period

Current ECB Handling
Sensitivity label: ECB-SECRET (as likely negative impact is very high)
ORM impact definition: Failure to perform ECB's processes incl. the delivery of project(s) which affects its ability to achieve its key business objectives (as enshrined in the Treaty). Unwanted adverse market reactions and significant market movement over period > 1 week. Credibility affected over the long term (> 3 years). Series of credible, verified and very negative pieces of information, and/or opinions. International media coverage extended to the popular press, TV and radio.
Financial impact: Above EUR 10 million

Provisional Assessment under EC Rules
EU-SECRET as the misuse or leakage of this information could seriously harm the essential interests of the Union
EC protective measures would not allow current business process:
 - Information only accessible on premise
 - Information handled in separate secure areas
 - Security clearance (of both ECB and NCA staff)
 - Separation of Communication and Information Systems

ECB conditions

- At the ECB:
 - we work in virtual teams as part of a system (Eurosystem, ESCB, SSM) with NCAs and NCBs;
 - mobile and remote work is a must;
 - our ability to respond effectively and exercise our basic tasks would be considerably affected by having to follow the current EUCI rules (within the ECB and across these systems).
- We, therefore, request to be excluded from the regulation in whole (our preference) or in part (i.e. for ESCB/SSM activities).

InfoSec - classifications, markings and definitions

Non-classified information	Information for public use	PUBLIC USE	Information intended for <u>public use or official publication or already disclosed</u> , which can be shared without restrictions inside or outside the Union institutions and bodies.
	Normal information	EU NORMAL	Information intended for use by a Union institution or body in the execution of its functions which is neither sensitive non-classified nor for public use. This category covers all <u>normal working level information</u> processed in the Union institution or body concerned.
	Sensitive non-classified information	SENSITIVE	Union institutions and bodies shall categorise, handle and store as sensitive non-classified all information that is not classified but which they must <u>protect due to legal obligations or because of the harm that may be caused to the legitimate private and public interests</u> , including those of the Union institutions and bodies, Member States or individuals by its unauthorised disclosure.
EUCI	RESTREINT UE/EU RESTRICTED	R-UE/EU-R	Information and material the unauthorised disclosure of which could be <u>disadvantageous to the interests</u> of the Union or of one or more of the Member States.
	CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C	Information and material the unauthorised disclosure of which could <u>harm the essential interests</u> of the Union or of one or more of the Member States
	SECRET UE/EU SECRET	S-UE/EU-S	Information and material the unauthorised disclosure of which could <u>seriously harm the essential interests</u> of the Union or of one or more of the Member States
	TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS	Information and material the unauthorised disclosure of which could cause an <u>exceptionally serious prejudice</u> to the essential interests of the Union or of one or more of the Member States

13

www.ecb.europa.eu ©

ECB IT & Cyber Security Standards Safeguards



14

www.ecb.europa.eu ©

ECB information safeguards – concrete examples

- Security assessment determines the level of information that can be handled
- Audit trails ensure traceability of actions
- Security clearance controls in EDRMS to manage the need to know
- Four eyes principle for managing groups and permissions
- Content is encrypted at rest and in transit
- Coming soon - Data Loss Protection to ensure persistent classification and control data exfiltration



Example: Permission layers in the EDRMS

Amended text option 1 (and our preference): a total exclusion of the ECB from the scope

New recital (7a):

In order to preserve the specific nature of the European Central Bank's (ECB) and its tasks and activities as part of the European System of Central Banks (ESCB) and the Single Supervisory Mechanism (SSM), which are performed in cooperation with the national central banks and national competent authorities, this Regulation should not apply to ECB, ESCB and SSM Information.

Article 2 revised:

This Regulation shall apply to all information handled and stored by the Union institutions and bodies, including information related to activities of the European Atomic Energy Community, other than Euratom Classified Information, **and excluding information related to the ECB and its tasks and activities within the ESCB and the SSM.**

Amended text option 2: exclusion of the ECB's ESCB and SSM activities

Recital (5) revised:

By creating a minimum common level of protection for EUCI and non-classified information, this Regulation contributes to ensuring that the Union institutions and bodies have the support of an efficient and independent administration in carrying out their missions. At the same time, each Union institution and body retains its autonomy in determining how to implement the rules laid down in this Regulation, in line with its own security needs. This Regulation shall in no case prevent Union institutions and bodies to fulfil their mission, as entrusted by the EU legislation, or encroach on their institutional autonomy. **Due account should also be taken that the measures do not negatively affect the Union entities' efficient information exchange and operations with other Union entities and national competent authorities.**

New recital (7a):

In order to preserve the specific nature of the European Central Bank's (ECB) tasks and activities as part of the European System of Central Banks (ESCB) and the Single Supervisory Mechanism (SSM), which are performed in cooperation with the national central banks and national competent authorities, this Regulation should not apply to ESCB and SSM Information.

Article 2 revised:

This Regulation shall apply to all information handled and stored by the Union institutions and bodies, including information related to activities of the European Atomic Energy Community, other than Euratom Classified Information, **and excluding information related to the ECB's tasks and activities within the ESCB and the SSM.**