EUROPEAN CENTRAL BANK
EUROSYSTEM

EU Information- and Cyber-Security Regulations

Impact on ECB

14 February 2023

[redacted]

Background

- The European Commission are proposing two regulations on:
  - Information Security *(led by DG Human Resources & Security)*
  - Cyber Security *(led by DG DIGIT)*

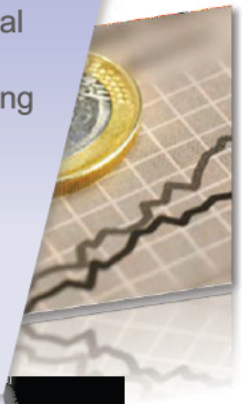
- Both:
  - ✓ Establish uniform information and cybersecurity rules that will align the handling of information within and across UIBAs
  - ✓ Directly applicable to all EU institutions, bodies and agencies (UIBAs)

- The ECB firmly supports the aims of both regulations but are very concerned about the concrete implementation and the effects each will have on the ECB's mission, the Eurosystem and SSM

Background – intro to ECB, Eurosystem, ESCB & SSM

Monetary Policy

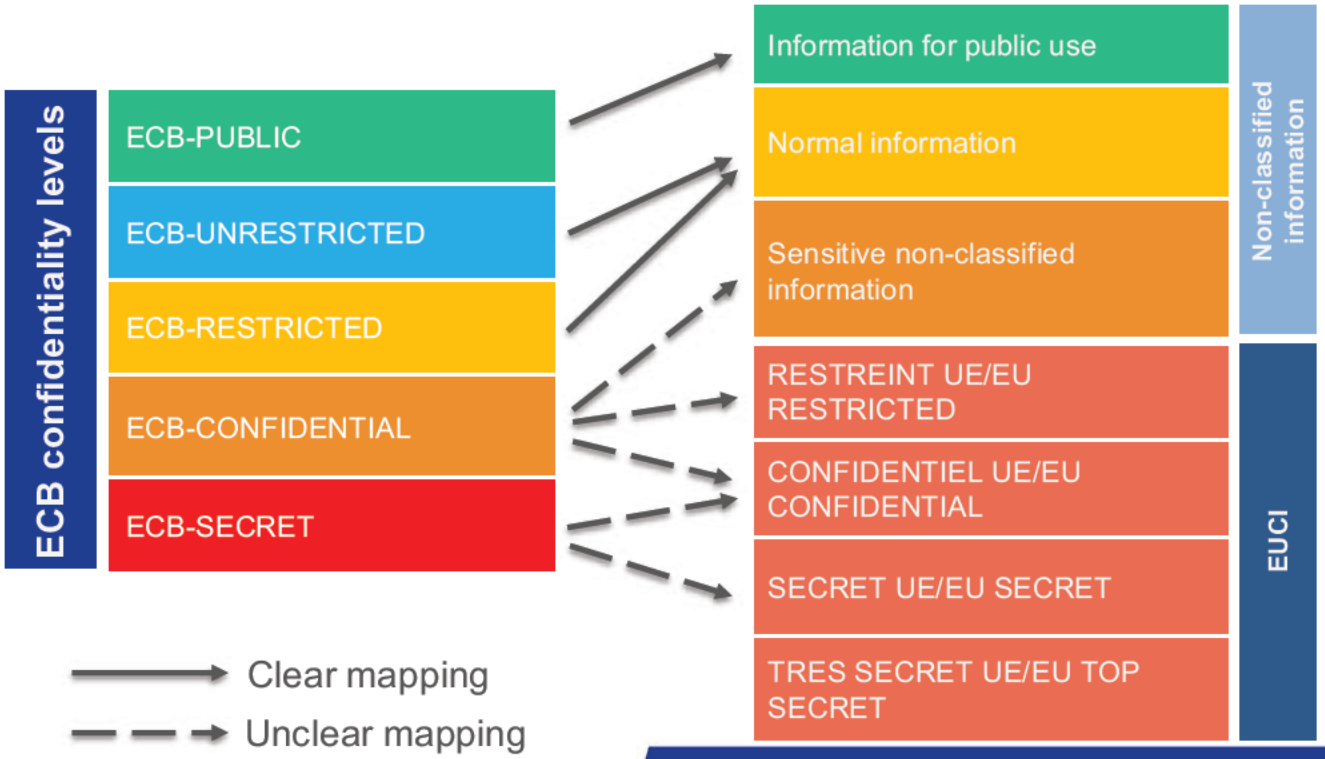
- The ECB and the national central banks **together** constitute the **Eurosystem** - the central banking system of the euro area.
- The main objective is to **maintain price stability:** safeguarding the value of the euro.
- The ECB and all EU NCBs make up the **ESCB**



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.
- We do this as part of the **Single Supervisory Mechanism** which also comprises the national competent authorities.

ECB v. EC current info security regimes



Lack of clarity on the mapping of current levels to the new classification

Uncertainty about EUCI - Up to 40% of ECB information could eventually fall under EUCI

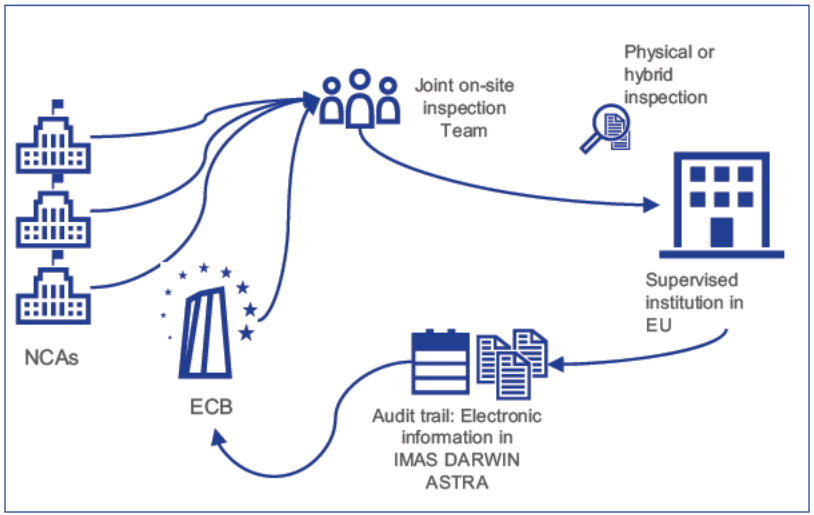
Adoption of new classification implies changes to CRMS

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

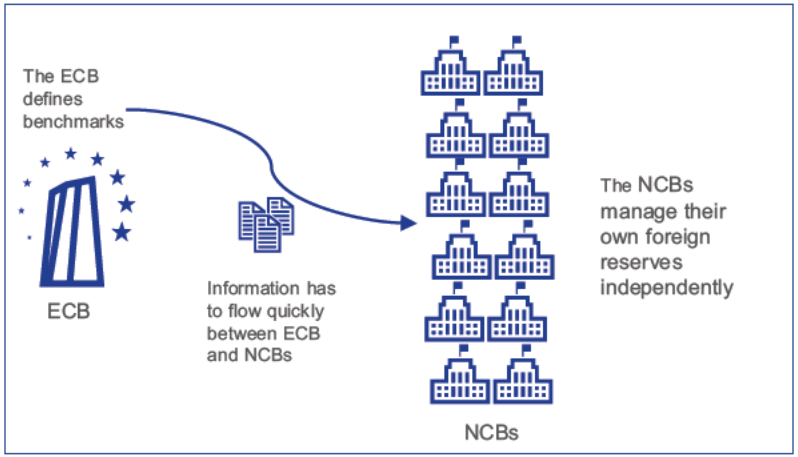
EC protective measures would not allow current business process:
- Information only accessible on premise
- Information handled in separate secure areas
- Security clearance (of both ECB and NCA staff)
- Separation of Communication and Information Systems

ECB – how we work …

Business process 2a:

Foreign exchange operations

The Eurosystem conducts foreign exchange operations in accordance with Articles 127 and 219 of TFEU. ECB's rationale for holding foreign currency reserves is to be able to intervene in the foreign exchange market whenever needed, to prevent disorderly market conditions that could have an adverse impact on price stability in the euro area and at the global level.



Examples of key documents: Annual re-distribution of the ECB's foreign reserves, Gold sales related documentation

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

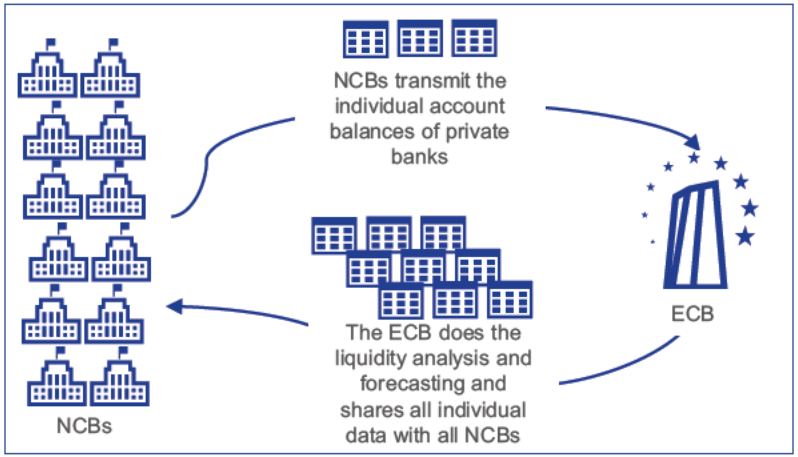
EC protective measures would not allow current business process:
- Information only accessible on premise
- Information handled in separate secure areas
- Security clearance ((of both ECB and NCA staff)
- Separation of Communication and Information Systems

ECB – how we work …

Business process 2b:

Daily Liquidity Operations

Central bank liquidity management means supplying to the market the amount of liquidity consistent with a desired level of short-term interest rates. This is achieved through open market operations and requires analysis and forecasting of the liquidity situation in the euro area.



Examples of key documents: Individual bank account balances

Current ECB Handling

Sensitivity label: ECB-CONFIDENTIAL *(as likely negative impact is high)* and *Market sensitive*

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:

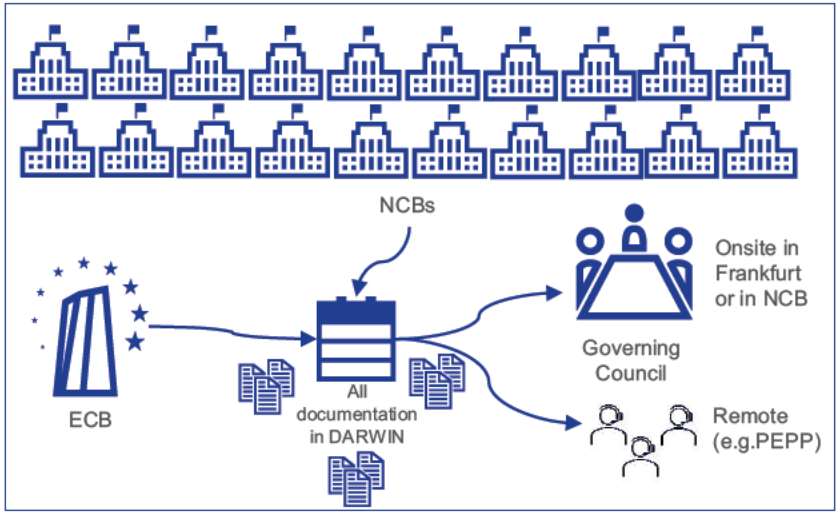
- Information only accessible on premise
- Information handled in separate secure areas
- Security clearance (of both ECB and NCA staff)
- Separation of Communication and Information Systems

ECB – how we work …

Business process 3:

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

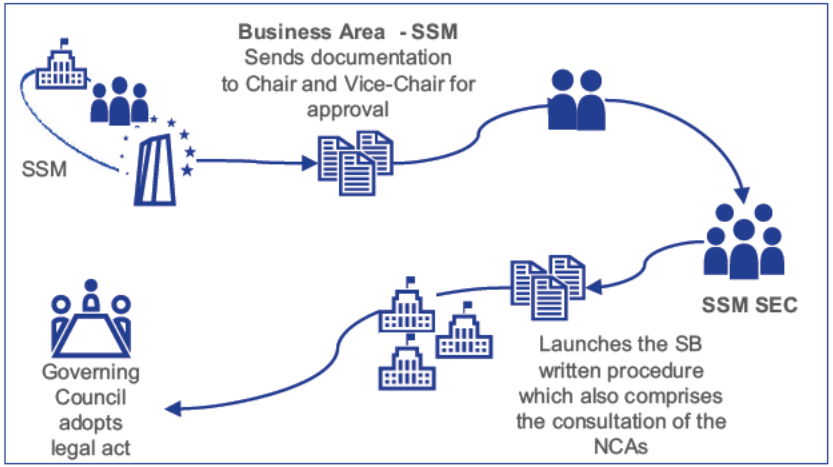
ECB – how we work …

Business process 4:

Legal acts/policies concerning operation in the SSM

(e.g. failing or likely to fail decision, withdraw of banking license or other emergency measures to stabilize a bank)

The ECB shall carry out its tasks within a single supervisory mechanism composed of the ECB and national competent authorities. The ECB shall be responsible for the effective and consistent functioning of the SSM.



Examples of key documents: SSM legal acts

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

Sensitive non-classified information as must be protected due to legal obligations or because of the harm that may be caused to the legitimate private and public interests, including those of the Union institutions and bodies.
EC protective measures would hinder from using existing rules and systems:

- Strong authentication and encryption in transmission and storage
- Encryption keys under UIBA responsibility
- Only stored and processed in EU
- Interoperable metadata to automate security measures
- Data leak protection measures
- Need to know and zero-based trust for service providers and contractors

ECB – our request

- The ECB supports both regulations, however:
  - we work as part of a system (Eurosystem, ESCB, SSM) with NCAs and NCBs;
  - our ability to respond effectively and exercise our basic tasks will be considerably affected (within the ECB and across these systems);
  - under the principle of proportionality we request that:
    - **Option 1:** the ECB's, Eurosystem, ESCB and SSM activities are excluded from the scope of the proposed EU regulations *(similar to NIS2 that expressly excluded NCBs from its scope precisely for these reasons)*
    - **Option 2:** the special needs of the ECB, Eurosystem, ESCB and SSM are recognised e.g. via recital or other legal text

For the Cyber Security Regulation: *The European Commission has already accepted a modification of Recital (7). The amended text emphasises that the measures to be put in place by the Union entities to implement the draft Regulation "**should not include any obligations directly interfering with the exercise of the missions of Union entities or encroaching on their institutional autonomy**". The recital also states that "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**".*

ORM Impact Grading Scales

	Impact level - Criteria	5 – Very high	4 – High	3 – Medium	2 – Low	1 – Negligible
Impact on business objectives* Failure or inadequacy of output of ECB tasks, business process(es) or project(s) which affects its ability to achieve its key objectives (as enshrined in the Treaty and the ECB Statute). BUSINESS	**Ability to perform ECB's processes incl. the delivery of projects to achieve its key business objectives**	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).	Partial 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) or failure to provide advisory functions.	Unsatisfactory quality or significant delays in performing ECB's processes incl. the delivery of project(s) which affects its ability to achieve its key business objectives (as enshrined in the Treaty) or partial failure to provide advisory functions.	Key business objectives (as enshrined in the Treaty) still may be achieved however internal ECB business expectations not being met due to a delay in delivery, or deterioration in quality.	Internal tasks, business processes affected, however key business objectives (as enshrined in the Treaty) not affected.
	Markets reaction (if triggered by ECB)	Unwanted adverse market reactions and significant market movement over period > 1 week.	Unwanted adverse market reactions and significant market movements between 1 day to 1 week.	Market irritation and unwanted significant market movements during one day.	Temporary market irritation and limited unwanted market movements during one day.	No noticeable market reaction.
Impact on reputation* The risk of deterioration of the reputation, credibility or public image of the ECB towards different external stakeholders (e.g. general public, financial sector, etc.). REPUTATIONAL	**Duration of impact on public confidence**	Credibility affected over the long term (> 3 years).	Credibility affected over the medium term (1 - 3 years).	Credibility affected over short (3 months-1 year) term.	Credibility affected between 1 week up to 3 months.	Credibility affected below 1 week.
	Credibility of source and severity of opinion	Series of credible, verified and very negative pieces of information, and/or opinions.	Credible and negative pieces of information, and/or opinions.	Negative pieces of information, and/or opinions.	Ad hoc negative allegations.	Unverified rumors, allegations and/or opinions.
	Media coverage (geographical scope, nature)	International media coverage extended to the popular press, TV and radio.	International media coverage incl. most internationally recognized newspapers.	Media coverage in one or a few internationally recognized newspapers.	Media coverage limited to national or regional press.	Negative and unsubstantiated report in media with only local distribution.
Impact on financial assets* The financial loss, the additional costs of redoing activities or correcting damages, after consideration of existing insurances. FINANCIAL	**Write off on the balance sheet**	**Above EUR 10 million**	**Above EUR 1 million to EUR 10 million**	**Above EUR 100 000 to EUR 1 million**	**Above EUR 10 000 to EUR 100 000**	**EUR 10 000 and below**
	• Financial value of a loss. It includes net financial loss (excluding insurance or other reimbursement). • Additional costs of redoing activities or correcting damages. • Penalty in legal case(s). • Opportunity cost. In order to reduce complexity, virtual losses (i.e. miscellaneous opportunity costs) are only considered when: (a) their impact may be significant; and (b) they can be evaluated in a fairly straightforward manner (e.g. missed trading opportunities linked to a disruption of investment activities related to own funds foreign reserve management).					

InfoSec - Confidentiality levels

These levels are based on the damage that unauthorised disclosure may cause to the legitimate private and public interests, including those of the Union, Union institutions and bodies and Member States or other stakeholders, so that the appropriate protective measures can be applied (art. 2.3)

Non-classified information	Publicly available information	PUBLIC USE
	Normal information	EU NORMAL
	Sensitive non-classified (e.g. contract related)	SENSITIVE
EUCI	RESTREINT UE/EU RESTRICTED	R-UE/EU-R
	CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
	SECRET UE/EU SECRET	S-UE/EU-S
	TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS

Impact analysis non-classified	
Number of changes required	69
Compliance status	Non-compliant
Level of impact	Medium/High
Type of changes required	Policy changes, IT changes

Impact analysis EUCI	
Number of changes required	194
Compliance status	Non-compliant
Level of impact	Low/Medium/High
Type of changes required	Policy changes, new procedures

InfoSec - classifications, markings and definitions

Non-classified information	Information for public use	PUBLIC USE	Information intended for public use or official publication or already disclosed, 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 normal working level information processed in the Union institution or body concerned.
	Sensitive non-classified information	SENSITIVE	Union institutions and bodies shall categorise, handle and stored as sensitive non classified all information that is not classified but which they must protect due to legal obligations or because of the harm that may be caused to the legitimate private and public interests, 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 disadvantageous to the interests 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 harm the essential interests 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 seriously harm the essential interests 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 exceptionally serious prejudice to the essential interests of the Union or of one or more of the Member States

InfoSec – non-classified information

Non-classified information			
	Information for public use	PUBLIC USE	Information intended for public use or official publication or already disclosed, 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 normal working level information processed in the Union institution or body concerned.
	Sensitive non-classified information	SENSITIVE	Union institutions and bodies shall categorise, handle and stored as sensitive non classified all information that is not classified but which they must protect due to legal obligations or because of the harm that may be caused to the legitimate private and public interests, including those of the Union institutions and bodies, Member States or individuals by its unauthorised disclosure.

- Labels only needed for Sensitive non-classified
- CIS requirements for sensitive non-classified
  - Strong authentication and encryption in transmission and storage
  - Encryption keys under UIBA responsibility
  - Only stored and processed in EU
  - Interoperable metadata to automate security measures
  - Data leak protection measures
  - Need to know and zero-based trust for service providers and contractors
- Exchange of normal and sensitive info outside EUIBAs requires need to know

Impact analysis non-classified information	
Number of changes required	26
Compliance status	Partially compliant / Non-compliant
Level of impact	Medium
Type of changes required	Policy changes, IT changes

Information shared with NCBs/NCAs from EU NORMAL will require a need-to-know

InfoSec – EUCI (1)

EUCI	RESTREINT UE/EU RESTRICTED	R-UE/EU-R	Information and material the unauthorised disclosure of which could be disadvantageous to the interests 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 harm the essential interests 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 seriously harm the essential interests 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 exceptionally serious prejudice to the essential interests of the Union or of one or more of the Member States

- **Suitability to handle and store EUCI**
  - Institutions need to be eligible to handle EUCI through an assessment and accreditation process
- **Risk assessment process to define protection measuress**
  - Contingency and business continuity plans
- **Personnel security**
  - Personal need-to-know
  - Briefing on protection obligations (every 5 years)
  - Security clearance for EU CONFIDENTIAL and above (granted by National Security Authority) (valid for max. 5 years)
  - Authorisation procedure to grant access to EUCI

Impact analysis EUCI	
Number of changes required	155
Compliance status	Partially compliant / Non-compliant
Level of impact	Medium/High
Type of changes required	Policy changes, new procedures

No objective definition of harm differentiating the levels, e.g. the difference between harm and serious harm is a subjective assessment