FIN-FSA
FINANSSIVALVONTA

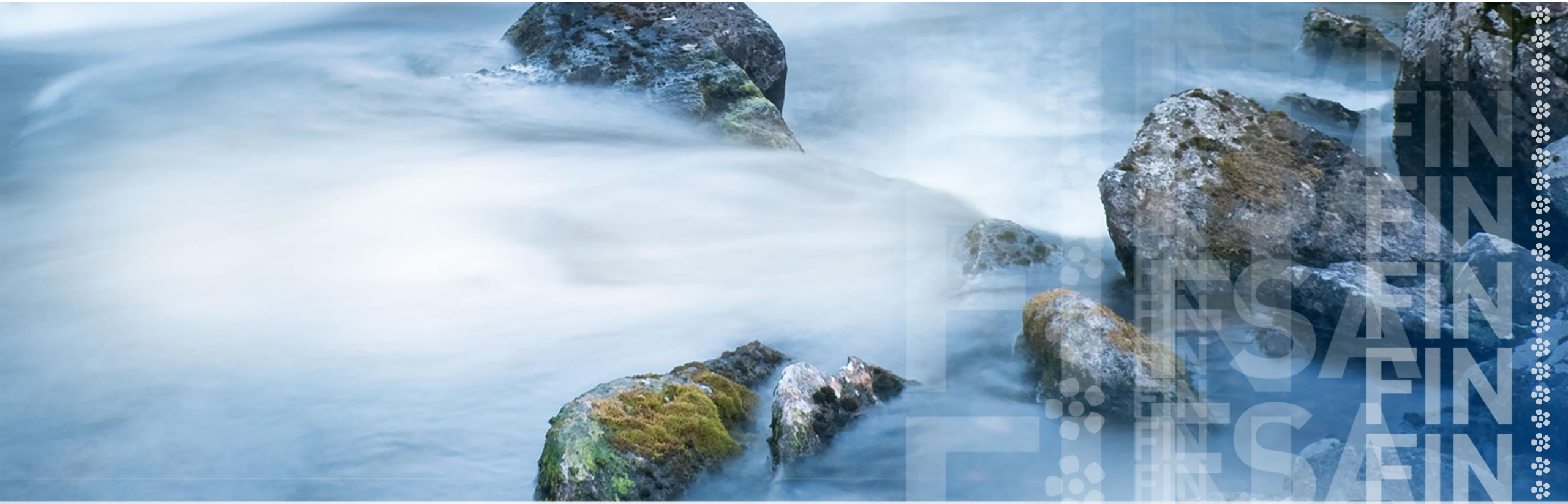
Presentation to supervised entities of the Reporting System for supervised entities' financial standing and risks

Webinar 16 January 2025

Event programme

- Opening of the event
- Update on the reform of the Reporting System
- Presentation of the Suomi.fi service
- Upcoming changes to credit institutions’ reporting
- Reporting of default risks (MK)
- Digital operational resilience reporting (DORA)
- Presentation of the Reporting System
- Questions

Update on the reform of the Reporting System



Reform of the Reporting System

- The reform of the Reporting System concerns electronic, standardised and regular reporting of financial standing and risks to the FIN-FSA
  - EBA ITS data collections (22)
  - EIOPA ITS data collections (10)
  - ESMA data collections (4)
  - National data collections (33)
- Identification and authorisation of Finnish and foreign reporters takes place via the Suomi.fi service
- Reporters have access to the Reporter Portal
  - Information on applicable reporting obligations can be viewed in an up-to-date way
  - Report submission
  - Reporting-related communication

Report submission and feedback

- Reports can be submitted in three different ways
  - Uploading the report file (XBRL/XML/CSV) into the system
  - Submitting the report file directly from your own system over an STP connection (Application to Application, A2A)
  - Completing the web templates (only recommended for a small number of templates)
    - No web templates are being planned for the CSDR7, CSDR9 and MMF data collections

- In the Reporter Portal, the reporter can view
  - Status of the processing of the report
  - Feedback on the report
    - Feedback on a report submitted over an SFTP connection is also submitted directly back the reporter's own reporting system

- Reporters may send reports for validation in the Validation Service (test environment) before submitting an official report to the FIN-FSA
  - The reports are not used for supervisory purposes

National data collections

In the Reporter Portal	Reporting period	Reporting set
3 January 2025	31 December 2024	National data collections KA, KB, JM, MA, MV, VA, VB, VE, VK, VL, VM, VN, VO, VP, VQ and VT

When reporting for the first time in the new reporting system, the reporter should start well in advance in order to ensure, for example, that Suomi.fi mandates function and that the FIN-FSA has time to respond to any reporting-related questions.

Supervision release 13 January 2025: Financial Supervisory Authority reminds supervised entities of their obligation to submit correct and checked supervisory data

- Repeated qualitative shortcomings have been identified in a number of different sectors and reporting forms.
- Incorrect data negatively impacts the FIN-FSA's fulfilment of its statutory tasks
- Information based on reporting is widely shared with stakeholders, for example through statistics
- Automated validation of reporting reception does not catch all errors
- Inaccuracy of supervisory data can lead to extensive retrospective corrections and supervisory sanctions
  - Developing the reporter's own quality assurance is important
- The supervised entity must update the declaration of the accuracy of reported data whenever changes take place in the reporting process it describes.
  - Verification of reported data form

https://www.finanssivalvonta.fi/en/publications-and-press-releases/supervision-releases/2025/financial-supervisory-authority-reminds-supervised-entities-of-their-obligation-to-submit-correct-and-checked-supervisory-data/

Jakelu Distribution Service was retired at end of 2024

- The remaining national Virati surveys migrated to the Reporter Portal as at 31 December 2024, after which the reporting of financial standing and risks takes place entirely in the new system.
- Only revision reports will be reported in the outgoing reporting system.

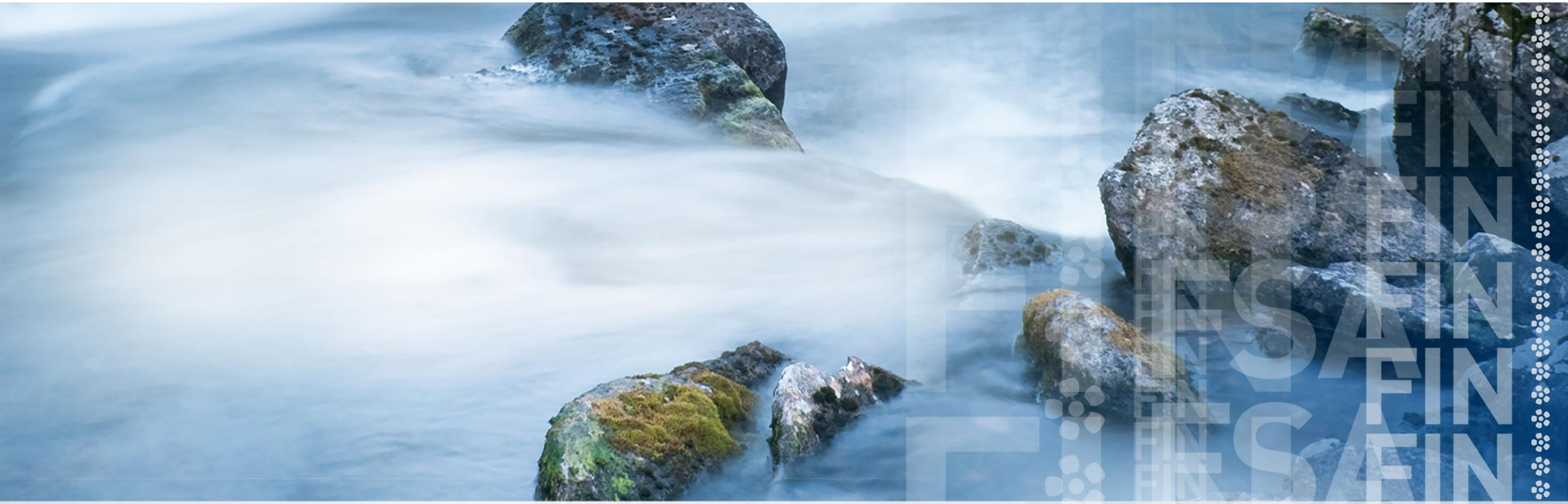
- Any workbooks required by reporters for revision reports in the outgoing reporting system will be supplied by the FIN-FSA to reporters in the Reporter Portal or by secure email.

Update on the reporting system reform

- Information on the reform of the Reporting System can be found on the FIN-FSA's website
- Reporting obligations by data collection – reporting maps for the financial sector and insurance sector
- Contacts primarily through the FIN-FSA's Reporter Portal

- Questions and feedback: NewReportingSystem@finanssivalvonta.fi

Presentation of the Suomi.fi service



Suomi.fi authentication

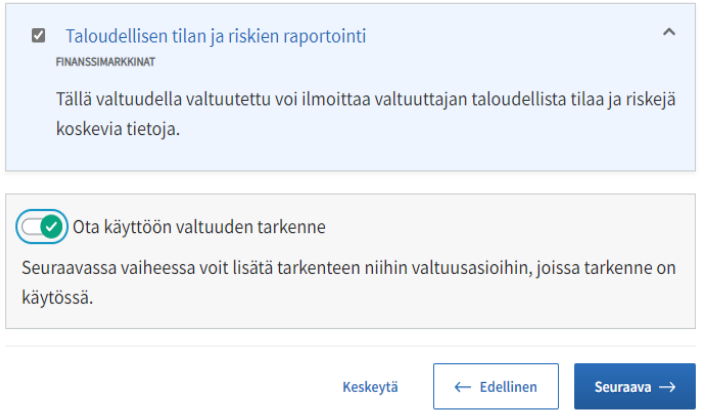
- Logging in the Reporter Portal and Validation Service requires strong authentication through the Suomi.fi identification service
  - Login requires: personal identification tool, mandate, and reporting obligation in the portal for the entity on behalf of which the person reports
- Reporters log in with a personal identification tool
  - When the reporter has a Finnish personal ID: banking IDs, mobile certificate or certificate card
- UID and Finnish Authenticator Identification Service: If the person responsible for reporting does not have a Finnish personal ID, they must register a foreign individual's unique identifier (UID) for themselves
  - The granting of a mandate also requires that the recipient has a Finnish personal ID or a UID
  - The Reporter Portal only accepts authentication of foreign individuals via the Finnish Authenticator application (country-specific eIDAS authentication is not supported)

Suomi.fi eAuthorizations service

- Via the Suomi.fi eAuthorizations service, the reporter is granted mandates to represent an entity
  - The reporter must have a mandate for reporting granted by an entity under the reporting obligation
- Mandates for the reporter can be granted by a person authorised to represent the entity according to a basic register or the register of mandate
  - Basic registers: Trade Register, Business information system and the register of association
  - Example: the managing director of an entity under the reporting obligation grants mandates for an employee responsible for reporting
- Authorisation with an application: If an entity's basic register information does not allow granting mandates, the entity may apply for the right to grant mandates by submitting an application to the register of mandates
  - Examples: The entity does not have representatives entered in the Trade Register, all representatives are foreign persons; a foreign company (no Business ID)

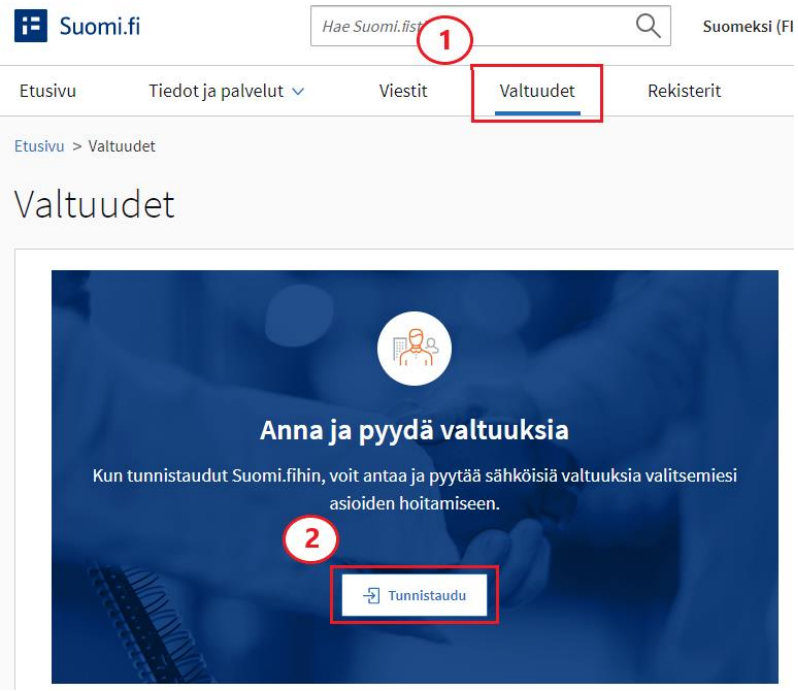
Mandate specifier

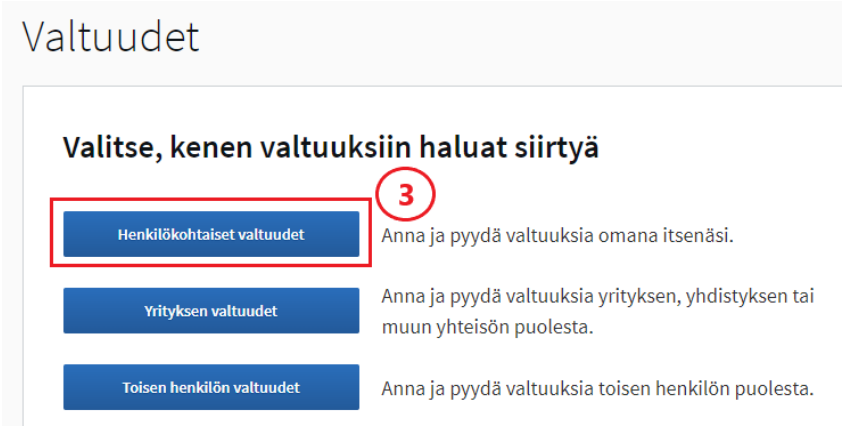
- Mandate theme: Reporting of financial standing and risks
- Mandate specifier
  - The specifier ALL enables the mandate holder to report to all data collections applicable to the entity
  - A survey-specific mandate can be used to grant a mandate for a specific data collection
    - Based on data collection codes, such as KA, VA
    - A list of the data collection codes is found in the reporting map for the financial sector and the insurance sector
    - For every mandate theme, one needs to specify the data collection to which the mandate applies. A mandate without a specifier cannot be used in the Reporter Portal

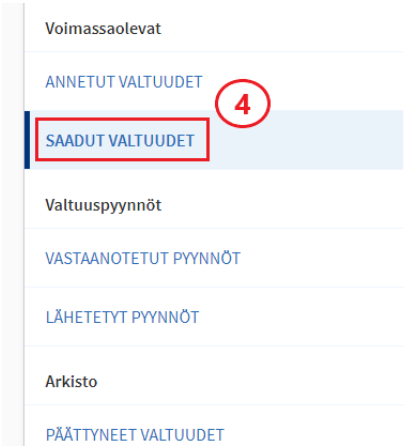


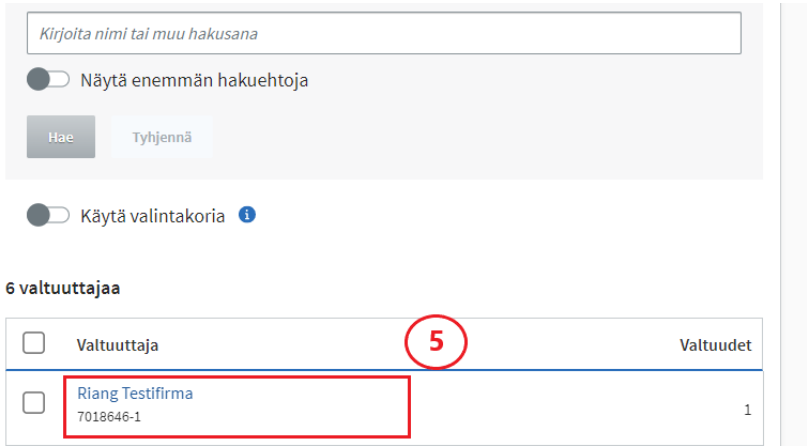
Practical instructions: Checking a mandate

1. Log into the Suomi.fi eAuthorizations service: https://www.suomi.fi/e-authorizations
2. Log in using a personal identification tool
3. Select Personal mandates
4. On the Personal mandates page, select “Received mandates”
5. Select the entity whose mandates you want to view



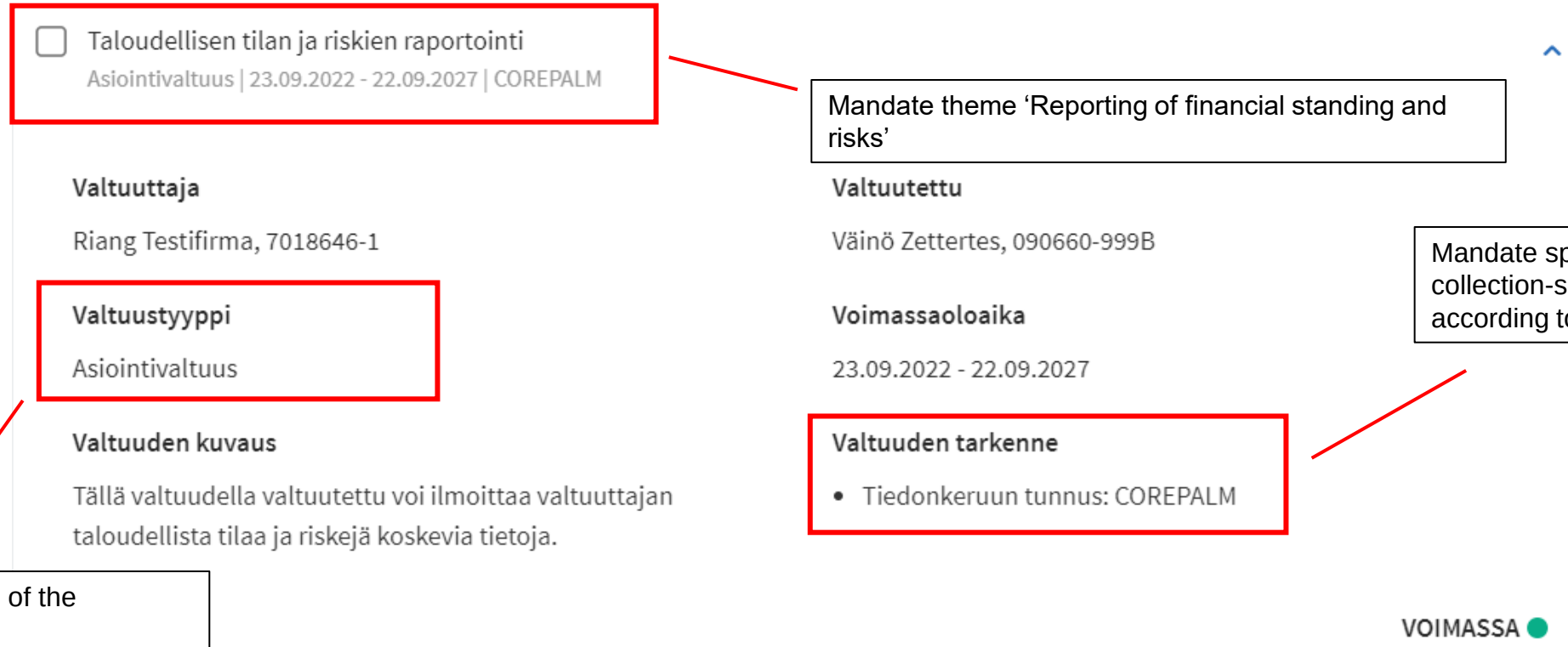






Practical instructions: Mandate checking

6. Check that the content of mandates meets the requirements of the Reporter Portal



Mandate theme ‘Reporting of financial standing and risks’

Mandate specifier ALL or data collection-specific specifier according to data collection maps

Mandate type is one of the following:
- Mandate for transactions
- Mandate to represent

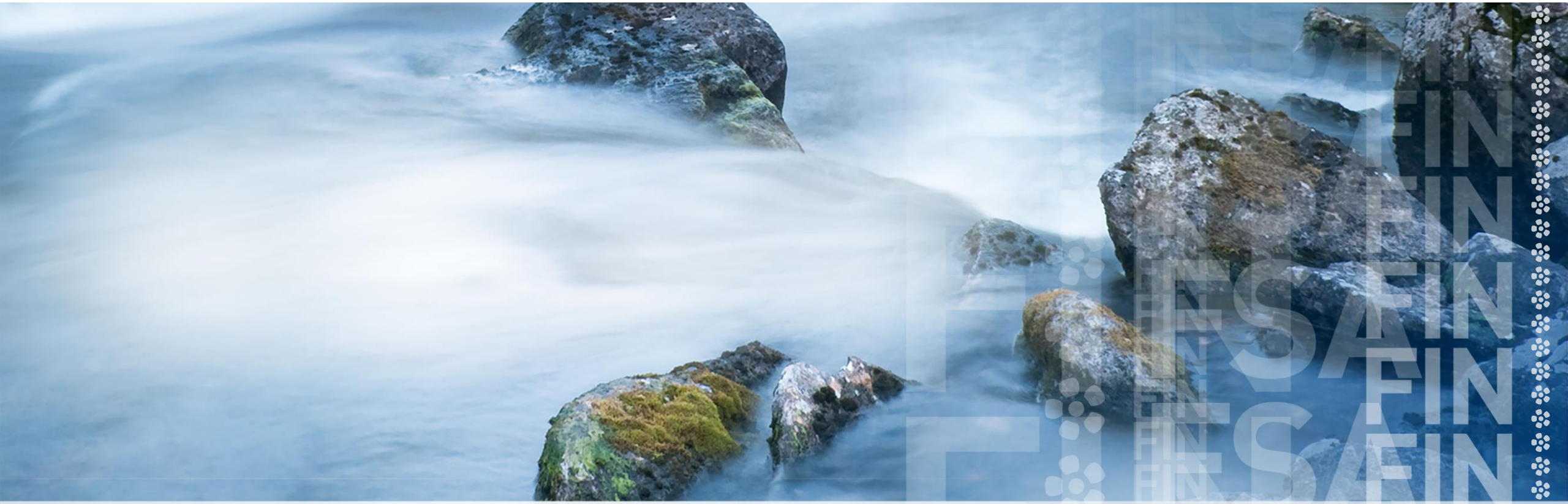
Managing mandates

- Entities must check their granted mandates twice a year in the Suomi.fi eAuthorizations service to ensure that they are consistent with the mandate holders' duties
  - When the duties change, the mandates must also be checked
- Users are recommended to log in concurrently for all entities that have granted them rights for the Reporter Portal
  - This ensures that the user receives email messages on behalf of all entities that have granted them a mandate
- When one's employment contract ends, it is the employer's duty to ensure that mandates for the FIN-FSA's reporting system are terminated via Suomi.fi mandate management
  - The user must ensure that email notifications of new messages in the reporter portal have been deactivated before a mandate is terminated
  - If email notifications have not been deactivated and the mandate has already been terminated, please contact NewReportingSystem@fiva.fi.

Further information on Suomi.fi services in the Reporter Portal

- • Instructions provided by FIN-FSA for reporters
  - Instructions on Suomi.fi eservices for reporters
  - General description of the Suomi.fi service for users of the Reportal Portal
  - Webinar 31.5.2022 demo on mandate (from 20:35 onwards)
- Instructions provided by Suomi.fi
  - Information on e-Authorisations service
  - Information on authorisation with application
  - Information on the identification service
  - Information on UID
- Questions
  - General questions concerning Suomi.fi services: organisaatiopalvelut@dvv.fi
  - Questions concerning mandates in the reporter's portal: NewReportingSystem@fiva.fi

Upcoming changes to credit institutions' reporting



Upcoming changes to credit institutions' reporting

- Version 4.0 will enter into force in the first half of 2025 and include several new and updated reporting requirements.
  - Reporting release 2/2025
- New ITS amending the supervisory reporting framework (COREP templates) to implement the most immediate changes driven by the EU Banking Package (CRR3 and CRD6).
    - Significant changes to COREP reporting starting from Q1 2025 reporting
- Minor technical amendments to reporting obligations by class 2 investment firms (COREP templates) in alignment with the CRR3/CRD6 changes.
- Reporting requirements under the Digital Operational Resilience Act (DORA) (ICT contract register)
    - More on DORA later in this presentation
- Reporting of asset-referenced tokens (ARTs) and electronic money tokens (EMTs): implementation of the new reporting requirements for these issuers under the MiCA Regulation

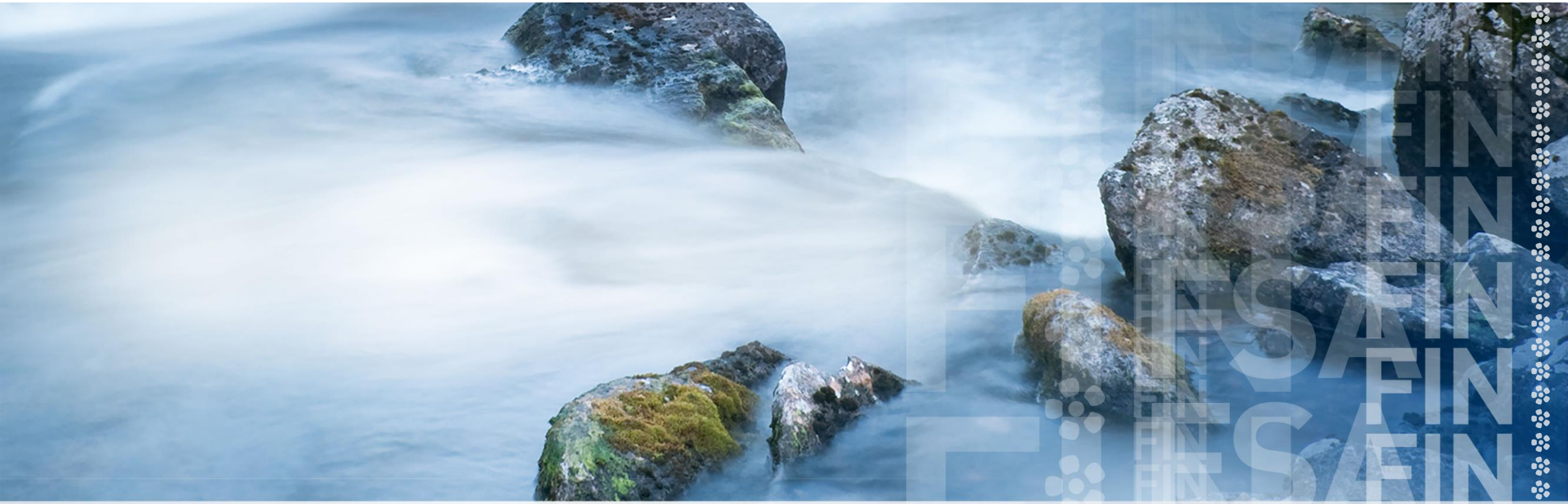
Upcoming changes to credit institutions' reporting

- EBA reporting framework 4.1 is expected to apply from 4/2025. Changes include
  - Internal approaches used for calculation of own funds requirements (supervisory benchmarking)
  - MiCAR additional reporting
  - Pillar 3 templates (reported directly to EBA)
- EBA reporting framework 4.2 is expected to apply from 9/2025
  - Additional reporting requirements regarding operational risk
  - Changes to reporting on resolution planning and MREL decisions
- Other reporting changes brought about by CRR3 and CRD VI will be implemented later and separate consultation papers will be prepared in line the roadmap published by the EBA
  - CRR3/Step 2.1 Coming for consultation soon, first reporting reference date provisionally 30 June 2026
  - CRR3/Step 2.2 Coming for consultation during 2025 (includes ESG reporting module)

XBRL-CSV to be adopted in EBA ITS reporting

- XBRL-CSV will replace XBRL xml format in EBA ITS reporting
- Technical change, affecting reporters who produce EBA ITS report files themselves
  - Reporter Portal's form templates will work as before
- FIN-FSA will adopt XBRL-CSV in EBA ITS reporting for 30 September 2025 data
  - An exception is EBA ITS DORA (ICT contract register, CTPP Critical Third-Party Provider), which will be reported for 31 March 2025 data as XBRL-CSV. Further information on this will be published later in a reporting release
- EBA technical documentation for version 4.0 includes specifications for producing XBRL-CSV reports

Reporting of default risks (MK)



Reporting of default risks – background

- Legislation on the management of default risks in the granting of consumer credit (Credit Institutions Act, chapter 15, section 11b and Act on the Registration of Certain Creditor Providers and Credit Intermediaries, section 13) entered into force on 1 July 2023. In the same context, supervision of certain credit providers and credit intermediaries was transferred to the FIN-FSA.
- The FIN-FSA is preparing regulations and guidelines aimed at guiding supervised entities on the management of default risks in the granting of consumer credit.
  - Management of default risks in the granting of consumer credit is monitored using default risk reporting data (MK report)
- The regulations and guidelines are currently being circulated for comment.

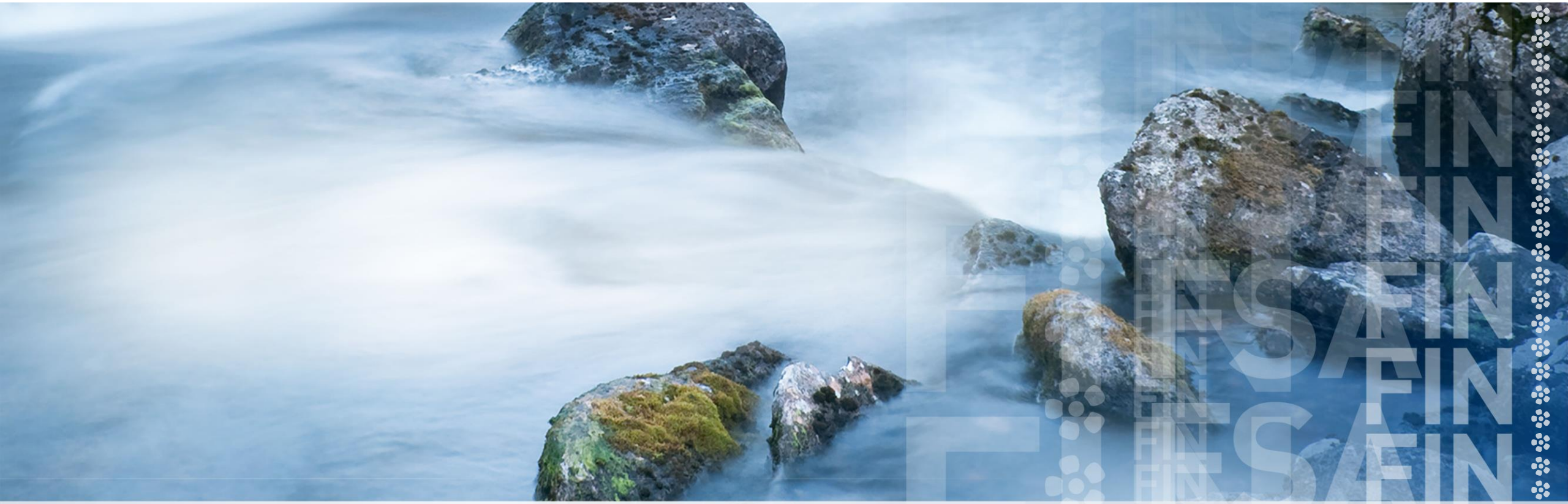
Reporting of default risks – objectives

- The objective of the regulations and guidelines is to determine
  - **how the supervised entity shall assess the reasonableness of the risk of default in connection with the granting of credit when granting credit to a consumer. Reasonableness is measured by the payment behaviour of the 5% highest risk class.** In this class are approved loans for which the highest risk score has been calculated using a credit risk model at the time of the loan application.
  - **how the supervised entity shall measure the reliability of the risk classifications system model in the risk of default at the time the loan is granted. Reliability is measured by the Gini coefficient of the credit risk model, which measures the ability of the credit risk model to distinguish good payers from problem payers at the time of the credit decision**
  - **The data to be submitted to the FIN-FSA in the Default Risk Management (MK) report. The report data is used to monitor the above-described**
    - payment behaviour of the 5% highest risk class
    - value of the Gini coefficient of the credit risk model
- The regulations and guidelines do not yet specify thresholds for the reasonableness of default risk and the reliability of the risk class system model. They may be specified at a later stage, once data received from repeated reporting have been analysed.

Reporting of default risks – report content

- **Annual reporting of default risks (MK reporting) will begin at the start of 2026 and will apply to all entities that grant unsecured consumer credit in Finland.** (Finnish and foreign banks (with or without a branch) and other companies granting consumer credit)
- The reference date for the default risk report (MK report) is 31 December. The reference period used is a one-year period 1–2 years before the reference date.
  - In other words, in the first reporting round, all new credit granted between 1 January and 31 December 2024 will be reported for reference date 31 December 2025.
- The loans to be reported will be divided into 20 as equal as possible classes in the rows of the default risk report. Each class will contain around 5% of the total number of granted loans.
  - For example, if the rejection limit of the credit risk model is 100 and the risk score model's risk score range 100–120 is 5% of all approved loans in the sample (number of loans), the reference set for the first 5% highest risk class is the loans that have been risk-scored and that received 100–120 points at the time of loan approval.
  - Similarly, if the risk score range 121–135 would have 5% of all approved applicants in the sample, the reference set for the second 5% highest risk would be the loans that have been risk-scored and that received a score of 121–135 at the time of loan approval.
- The data to be reported by product in the columns of the default risk report are
  - Due or overdue loans, number and euros (<30 days, 30-90 days and >90 days)
  - Number of repaid loans
  - Realised credit losses, number and euros. Realised credit losses also include data on any loan portfolios that have been sold, insofar as they have been subject to write-downs.
- In addition, the default risk report provides some additional individual information, including the name of the product, the Gini coefficient and the share of the 5% highest bad loans of all loans in the class.
- A default risk report (MK report) template can be found in the consultation material

Digital operational resilience reporting (DORA)



DORA reporting

- About DORA

- ICT incident reports
- ICT contract register
- Annual reporting of ICT incidents

ICT = Information and communication technology)

About DORA

Cyber Resilience

The ability of an organisation to continue to carry out its mission by anticipating and adapting to *cyber threats* and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incidents*.

Source: Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO and NIST (definition of "Resilience")

Source: Cyber Lexicon 2023 edition

The Digital Operational Resilience Act (DORA) (EU) 2022/2554 entered into force on 17 January 2023 and applies from 17 January 2025

- Chapter I – General provisions
- Chapter II – ICT risk management
- Chapter III – ICT-related incident management, classification and reporting
- Chapter IV – Digital operational resilience testing
- Chapter V – Managing of ICT third-party risk
- Chapter VI – Information-sharing arrangements
- Chapter VII - Competent authorities

ICT = Information and communication technology

DORA reporting to the FIN-FSA

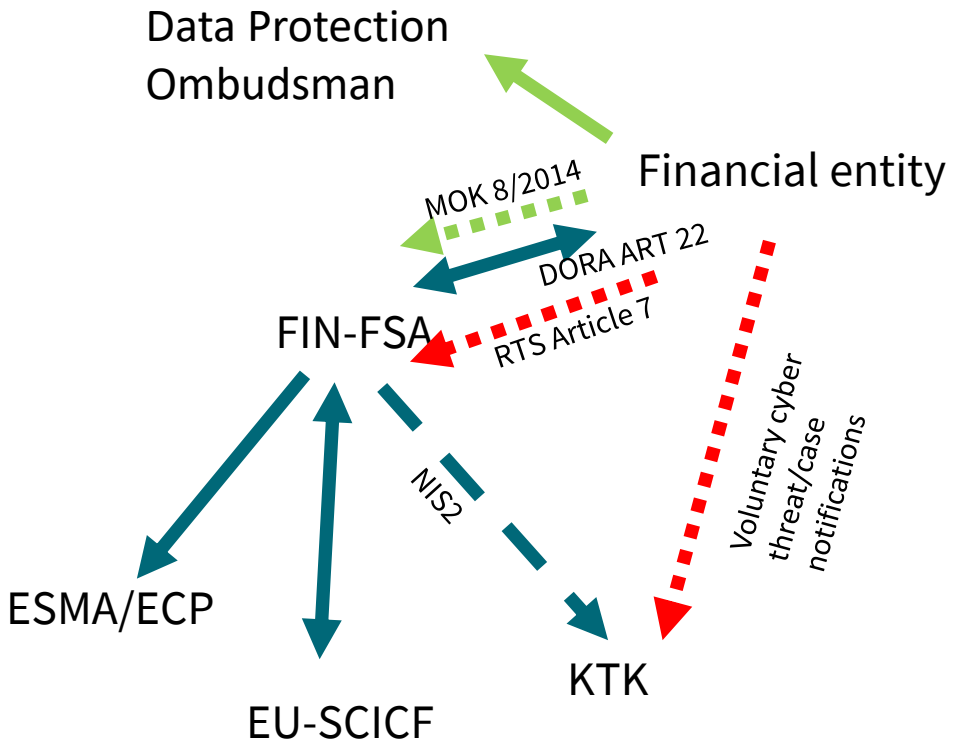
- Much of the old topic-related reporting continues as it is
  - Annual report on losses due to operational risks
  - Notification of outsourcing
- Incident reports (Articles 17 – 23)
  - Content changes slightly
  - Thresholds are also changing
- Voluntary cyber-threat notifications
- Annual reporting of ICT incidents
- Register of information on ICT service providers (contract register)
  - Article 28
- Report on the review of the ICT risk management framework (on request, Article 6 (5))

Incident report

About incident reporting

- Incident management process (Article 17)
- Reporting and voluntary notification (Article 19)
- Reporting content (Article 20), see ITS and RTS.

- Joint draft ITS on major incident reporting
- RTS on criteria for the classification of ICT-related incidents
- Delegated regulation - EU - 2024/1772 - EN - EUR-Lex (classification criteria, materiality thresholds)



Outsourcing of incident reporting

- JC 2024-33 - Final report on the draft RTS and ITS on incident reporting, Article 6.
- Outsourcing of incident reporting is possible
  - Must be part of a general and/or long-term arrangement
  - Prior to first reporting, the FIN-FSA must be informed of the arrangement
    - Name, contact details and the identification code of the third party to which incident reporting has been outsourced
  - The FIN-FSA must also be informed when the said arrangement ends.
- This also applies to intra-group outsourcings
- In principle, outsourcing already in use does not need to be separately notified to the FIN-FSA when DORA begins to be applied in January 2025.
- The FIN-FSA will contact directly those supervised entities where outsourcing cannot be carried out with regard to restrictions and exemptions related to this authorisation.

About aggregated incident reports

- JC 2024-33 - Final report on the draft RTS and ITS on incident reporting, Article 7.
- Aggregation is possible, i.e. a third party to whom reporting is outsourced (Article 7 (1)) may report data for multiple financial entities in a single report if the following conditions are met
  - The incident originates from or is caused by, for example, a third-party ICT provider.
  - This provider provides the ICT service to more than one supervised financial entity, or to a group, in the Member State
  - Each reporting supervised entity classifies the incident as major
  - The incident affects supervised entities within a single Member State and the aggregated report relates to entities supervised by the FIN-FSA
  - The supervised entities have outsourced incident reporting to a third party (see previous slide)
  - The FIN-FSA has explicitly permitted aggregated reporting
- This does not apply to significant credit institutions and trading venues.
- In principle, those companies that have already aggregated their incident reports will be able to continue aggregation and will not need to seek separate authorisation from the FIN-FSA to aggregate data when DORA begins to be applied in January 2025.
- The FIN-FSA will contact directly those supervised entities where outsourcing cannot be carried out with regard to restrictions and exemptions related to this authorisation.

About classification and criteria

Classification

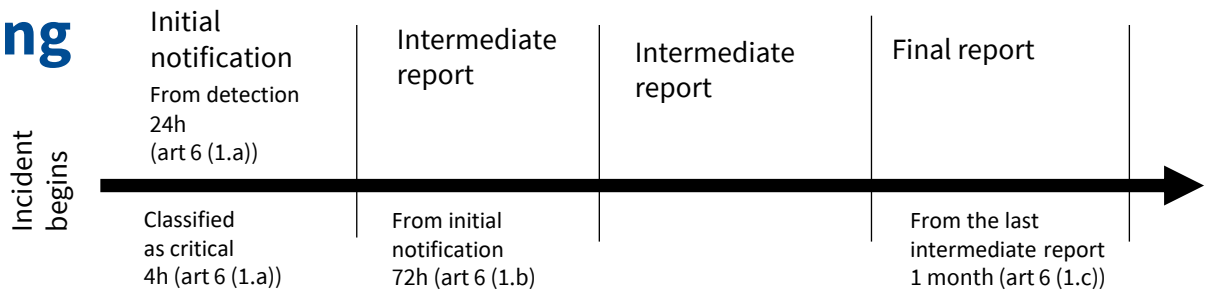
- See RTS on criteria for the classification of ICT-related incidents page 7.
- Commission Delegated Regulation – EU – 2024/1772
- An incident is considered major if
  - it impacts a critical service
  - and 2 or more criteria are met
- Also, any successful unauthorised access to a network or system is a major incident.

Criteria

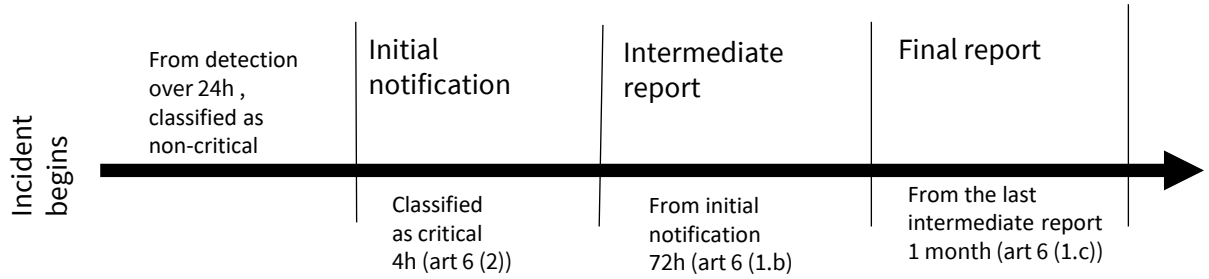
- See RTS on criteria for the classification of ICT-related incidents page 8.
- Commission Delegated Regulation – EU – 2024/1772
  - Clients, financial counterparts and transactions (Article 1)
  - Reputational impacts (Article 2)
  - Duration and service downtime (Article 3)
  - Geographical spread (Article 4)
  - Data losses (Article 5)
  - Criticality of services affected (Article 6)
  - Economic impact (Article 7)

About time limits for incident reporting

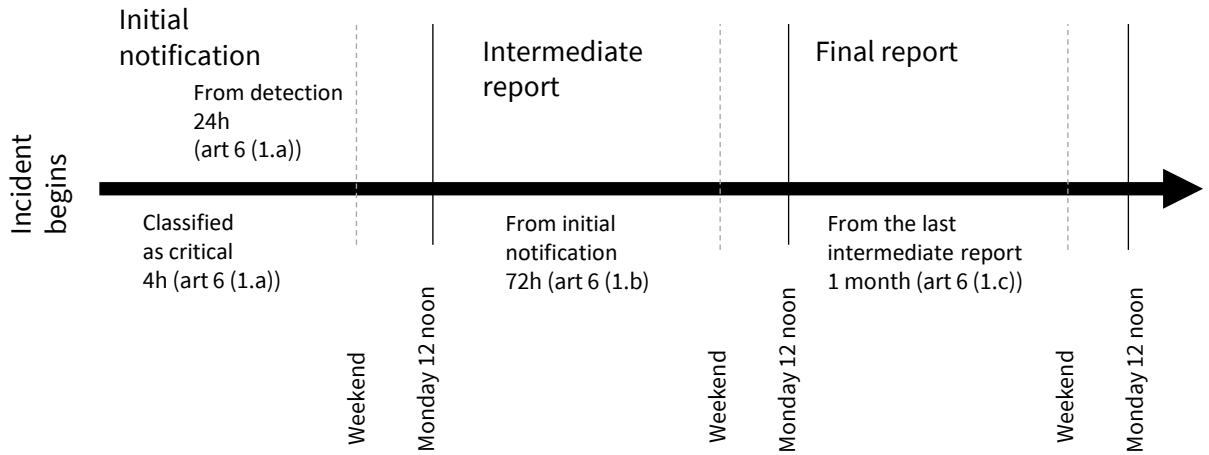
RTS Article 6
Initial notification, intermediate and final reports



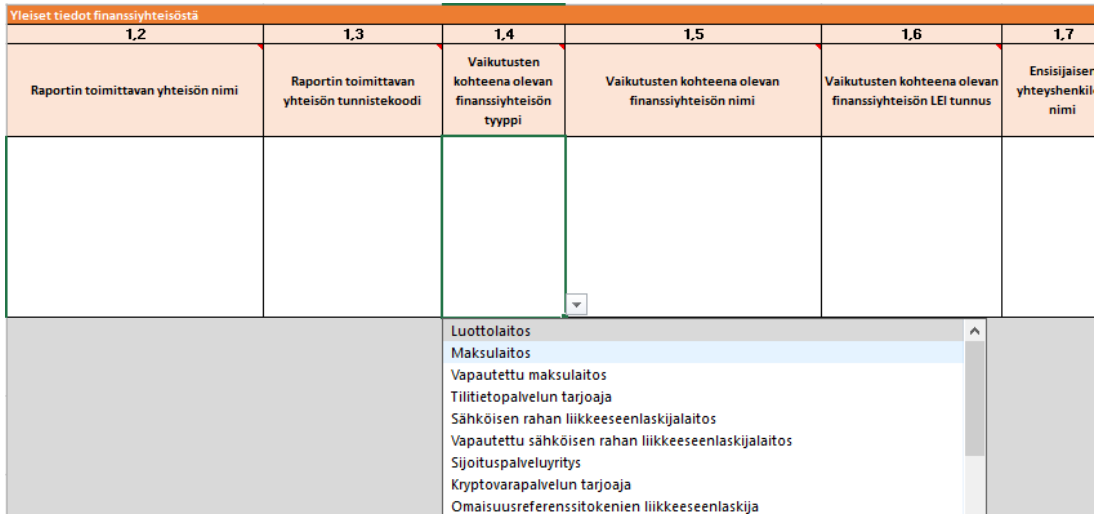
RTS Article 6 (2)
Initial notification and reclassification of severity

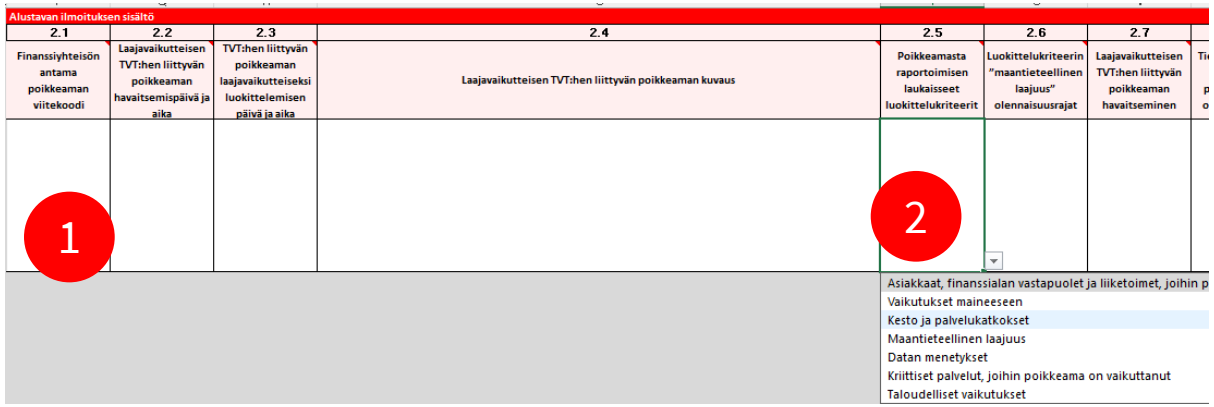


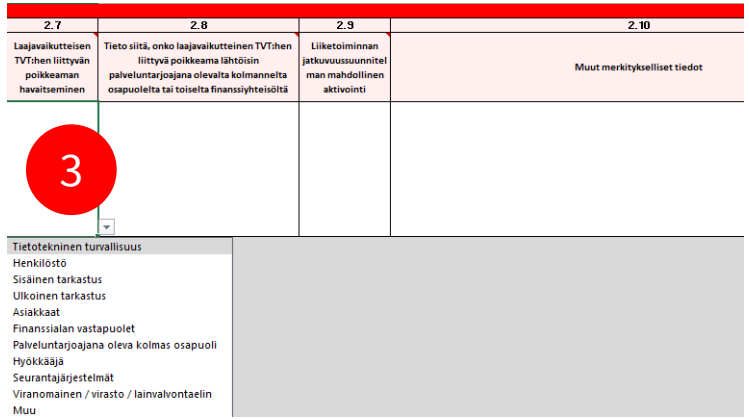
RTS Article 6 (4), weekends and bank holidays
The incident report can be submitted by 12 noon of the next working day.
Not applicable to : credit institutions, central counterparties, operators of trading venues, and other financial entities identified as essential or important entities pursuant to national rules



Initial notification







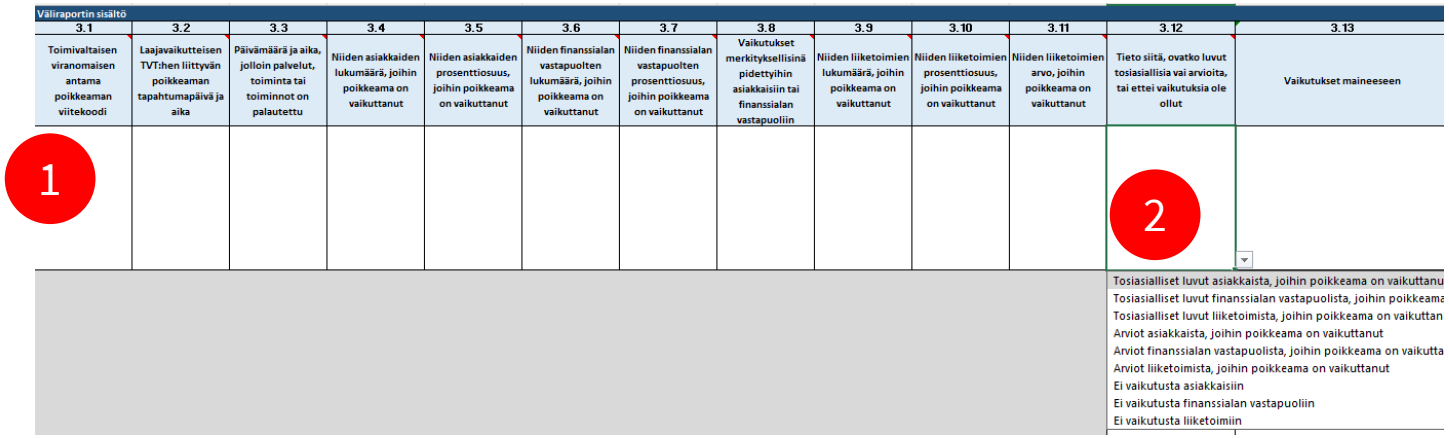
General information, 15 fields

- Information about the reporting entity
- An incident affecting multiple entities can be reported in a single report (with a few exceptions)

Initial notification, 10 fields

- Description of the incident
- 1 – Incident reference code provided by the reporting entity
- 2 - which thresholds were exceeded; there may be several
- 3 - how the incident was detected

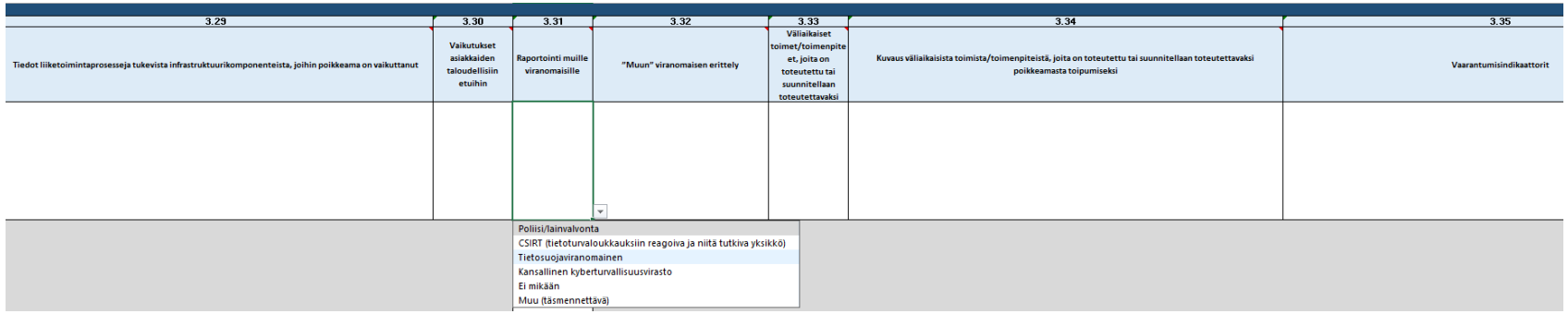
Intermediate report



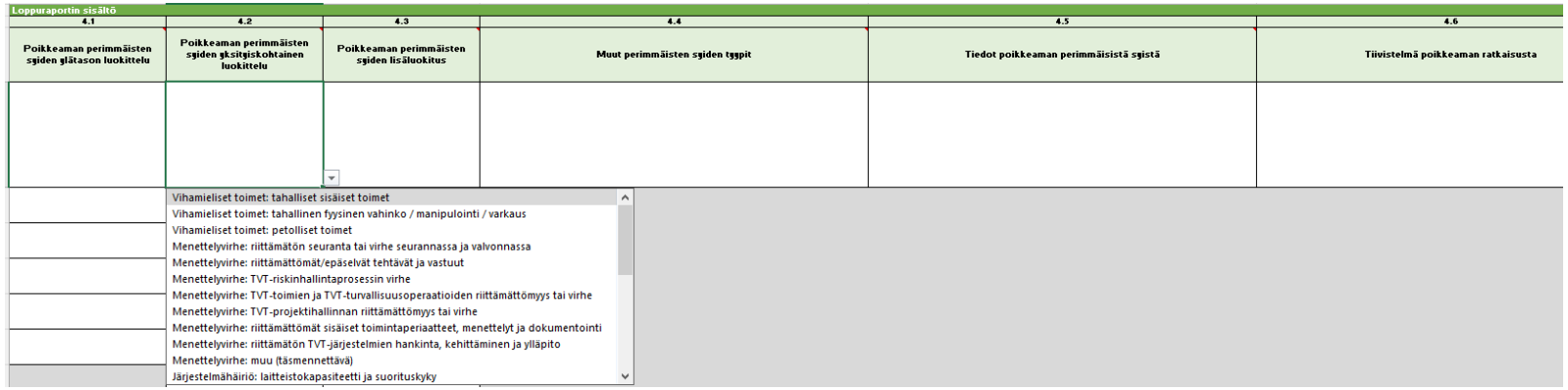
35 fields

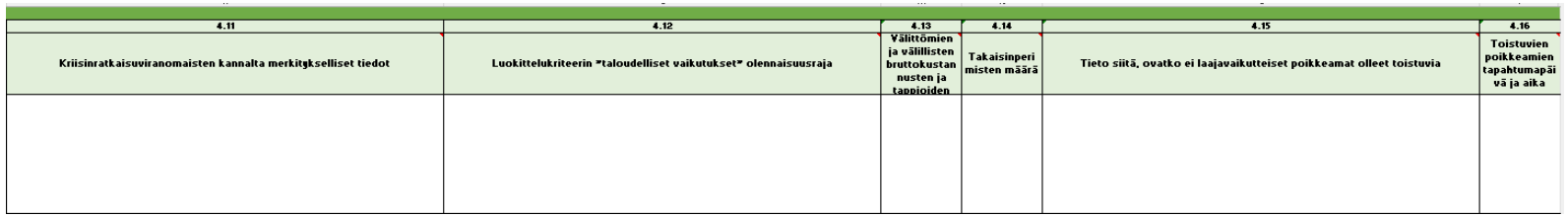
- A wide range of assessments and information on impacts
- Information on duration and downtime
- Information on measures taken

- 1 - Incident reference code received from FISA
- 2 – assessments or information; several may be selected



Final report





16 fields

- Root causes
- Incident resolution summary
- More detailed information about the incident

How to submit incident reports

- Through the current (FISA) channel
- In spring 2025 with Excel
- Later, this will be replaced by a www form.
- This concerns
  - Incident reports (initial, intermediate and final)
- Voluntary cyber threat notifications with Excel through the same FISA channel
- See FIN-FSA's E-services (identification) on how identification and authorisation take place
- See E-services (incident report) for instructions on
  - how apply for reporting mandates
  - how to send incident reports

Voluntary notification of cyber threats

Notification of cyber threats

- Digital Operational Resilience Act (DORA) (EU) 2022/2554 Article 19 (2).
- Delegated Regulation – EU – 2024/1772, Article 10 contains materiality thresholds, i.e. what cyber threats are considered to be significant
- JC 2024-33 - Final report on the draft RTS and ITS on incident reporting, RTS Article 7, and ITS Annex III contains information on the contents of the fields.
- Reporting via FISA (same channel as incident reports).

Content of voluntary notification of cyber threats

Significant Cyber Threats

1	2	3	4	5	6	7	8	9	
Name of the entity submitting the notification	Identification code of the entity submitting the notification	Type of financial entity submitting the report	Name of the financial entity	LEI code of the financial entity	Primary contact person name	Primary contact person email	Primary contact person telephone	Second contact person name	Second c

13	14	15	16	17
Description of the significant cyber threat	Information about potential impact	Potential incident classification criteria	Status of the cyber threat	Actions taken to prevent materialisation

18	19	20
Notification to other stakeholders	Indicators of compromise	Other relevant information

20 fields

- Information about the reporting entity
- Information about the threat
- Information on measures taken

Annual report of ICT incidents

Annual report of ICT incidents

- DORA Article 19(4.c)
- See Joint Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents
- Starts in spring 2026 and covers ICT incidents in 2025
- More detailed guidelines will follow later.

JOINT COMMITTEE GUIDELINES ON AGGREGATED ANNUAL COSTS AND LOSSES OF MAJOR ICT-RELATED INCIDENTS

eba European Banking Authority · eiopa European Insurance and Occupational Pensions Authority · ESMA European Securities and Markets Authority · JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Annex: Reporting template for gross costs and losses and financial recoveries in a reference year

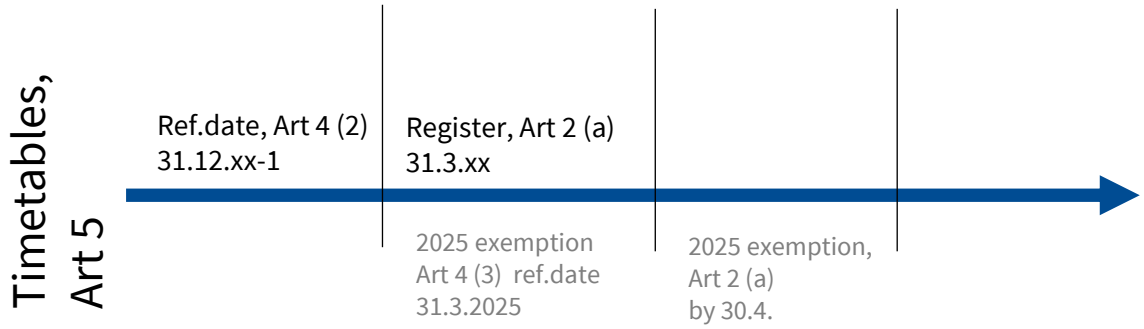
Name of the financial entity	
Legal Entity Identifier	
Start and end date of the reference year of the financial entity	
Currency	

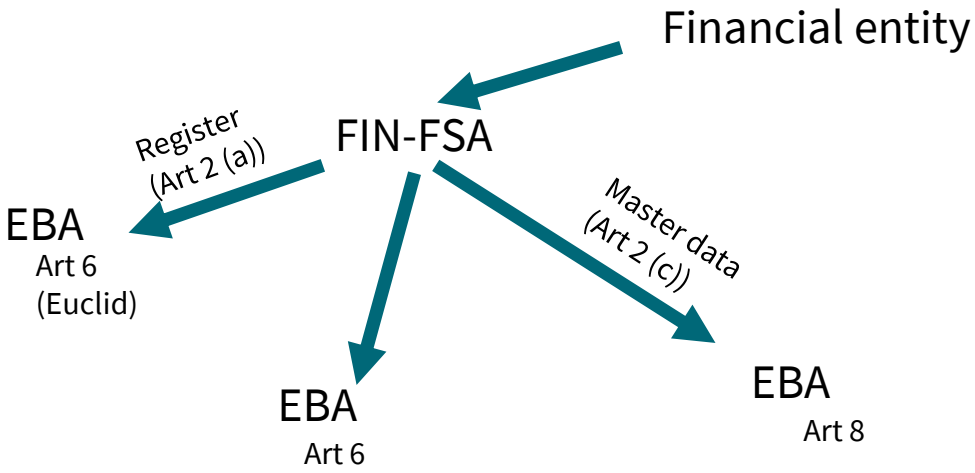
Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the reference year (1000s of units)	Recoveries of the incident in the reference year (1000s of units)
1				
2				
...				
Total for reference year	----------	----------		

ICT contract register

ICT contract register

- DORA Article 28(3).
- The data will be used at EU level to identify critical ICT actors and initiate oversight
- Reporting for the first time by 30 April 2025.
- ESAs decision: timelines in contract register reporting and in ESA 2024 22 Decision on reporting of information for CTPP designation.pdf
- There is also an Excel describing validations and a description of the data model.
- To the FIN-FSA through the same reporting channel as other reports, i.e. the Reporter Portal (via the RAPU channel).





SI banks and reporting of registers of information

- SI banks report directly to the ECB.
- Those financial institutions that are part of an SI group, but whose reporting is not covered by an SI bank, will report their registers of information to the FIN-FSA in the same way as other financial institutions.

About registers of information

- Implementing Technical Standards to establish the templates for the register of information has draft ITS and Excel templates – soon to be outdated.
- Implementing Regulation - EU - 2024/2956 describes the content of the registers of information
  - Reporting entities are identified by LEI. See B_01.01.0010.
  - ICT contractual partners are identified by either LEI or EUID. See B_05.01.0010 and B_05.01.0020.
- The register shall report
  - At the level of the individual financial entity, when the financial entity is not part of a group of financial entities
  - At the level of the individual financial entity, when it is part of a group of financial entities, but where the parent company is outside the EU and has no parent company operating in the EU.
  - At the highest level of consolidation for groups of financial entities within the EU, where the financial entity reporting the register is subject to DORA supervision.

Register templates

- B_01.01 – financial entity maintaining the register
- B_01.02 – financial entities with scope of consolidation
- B_01.03 – list of branches
- B_02.01 – general information on contractual arrangements
- B_02.02 – specific information on contractual arrangements
- B_02.03 – list of intra-group contractual arrangements
- B_03.0X – multiple signatories
- B_04.01 – Financial entities making use of the ICT services
- B_05.01 – ICT third-party service providers
  - direct
  - intra-group
  - subcontractors included in supply chains
  - ultimate parent undertakings of the above
- B_05.02 – supply chains
  - Implementing Regulation example
- B_06.01 – function identification
- B_07.01 – assessments of the ICT services
  - risk assessments: substitutability, date of last audit, etc.
- B_99.01 - definitions from entities making use of the ICT services

Attachments and links

DORA

- DORA Act eur-lex 2022/2554
- RTS Delegated Regulation 2024/1774 (eur-lex 2024/1532)

- Websites
  - Digital Operational Resilience Act | European Banking Authority
  - ESAs published second batch of policy products under DORA | European Banking Authority
  - DORA EBA Roadmap

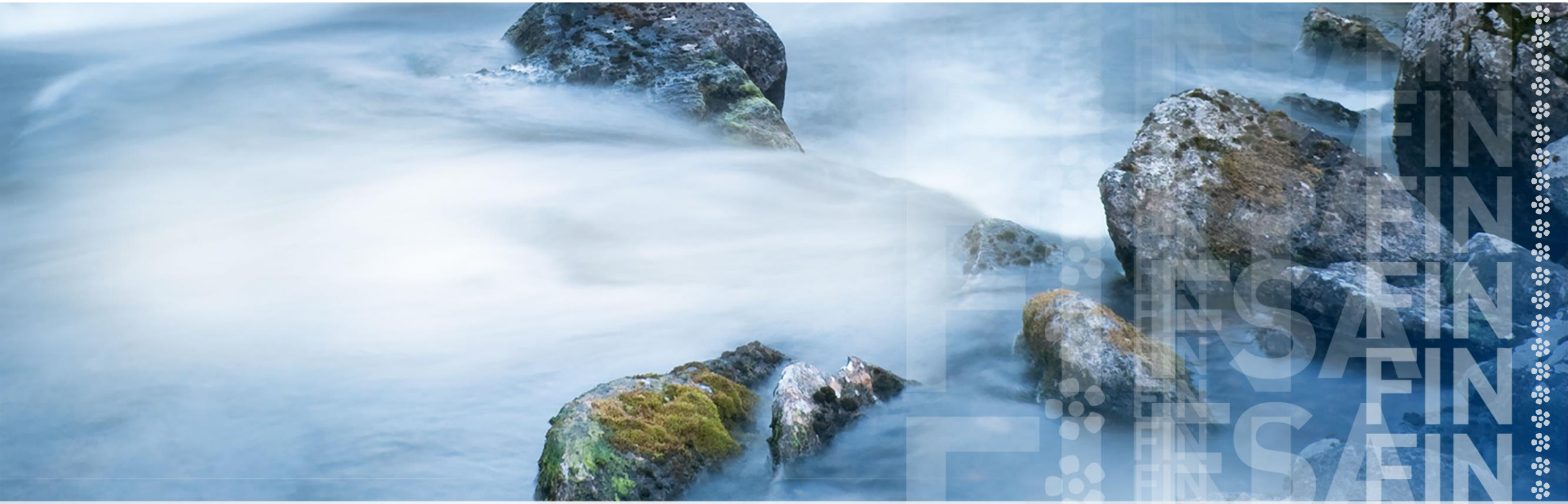
- Possibility to request interpretation assistance:
  - Q&A on regulation – EIOPA
  - Q&A form
  - Search Q&As – EIOPA; can filter DORA-related questions
  - Joint Q&As – EIOPA; this is also relevant for DORA
- You can also find there links to the EBA and ESMA Q&A pages: some of the questions are such that the answers are valid across all sectors.

RTS and ITS links

- RTS Delegated Regulation 2024/1774 (eur-lex 2024/1532) complement DORA with regulatory technical standards
- Contracting
  - About policy content: Regulatory Technical Standards on the policy on ICT services supporting critical or important functions provided by ICT third-party service providers
  - Important functions, risk management: Joint Regulatory Technical Standards on subcontracting ICT services supporting critical or important functions
  - Delegated Regulation 2024/1773 content of the policy regarding contractual arrangements
  - Register of information: Implementing Technical Standards to establish the templates for the register of information
  - Implementing Regulation - EU - 2024/2956
- Threat-Led Penetration Test (TLTP) JC 2024-29 - Final report_DORA RTS on TLPT.pdf

- ICT incidents:
  - Delegated Regulation – EU – 2024/1772 classification criteria for ICT-related incidents, materiality thresholds, details of reports
  - Joint draft ITS on major incident reporting
  - RTS on criteria for the classification of ICT-related incidents
- Annual report of ICT incidents:
  - Joint Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents

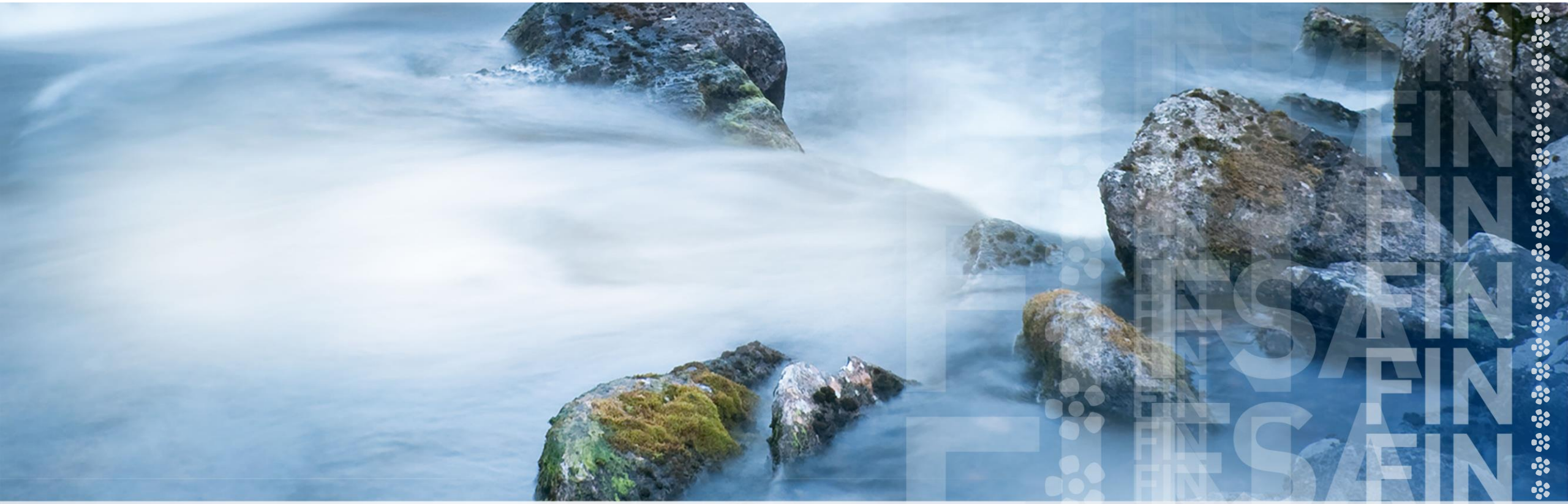
Presentation of the Reporting System



Presentation of the reporting system

- Suomi.fi login
- General use of the Reporter Portal
- Submissions of reports dashboard (Reporting obligations and report submission on web templates)
- Load files dashboard (uploading a CSV file)
- Discussions

Questions



Contacts/further information

- More information on the reform of the Reporting System is available on the FIN-FSA website
- Contacts primarily through the FIN-FSA Reporter's Portal
- Questions and feedback: NewReportingSystem@finanssivalvonta.fi

FIN-FSA
FINANSSIVALVONTA

Thanks!