REPORT ON THE WORK OF THE ECSDA TASK FORCE ON SYSTEMIC RISK INDICATORS

January 2024

European Central Securities Depositories Association, aisbl
Rue Royale 75, 1000 Brussels, Belgium - ecsda.eu – info@ecsda.eu - +32 2 230 99 01
RPM/VAT : BE0464619112 – Tribunal de l'entreprise francophone de Bruxelles
ING – BE30 3630 9647 3311 – Transparency Register : 92773882668-44

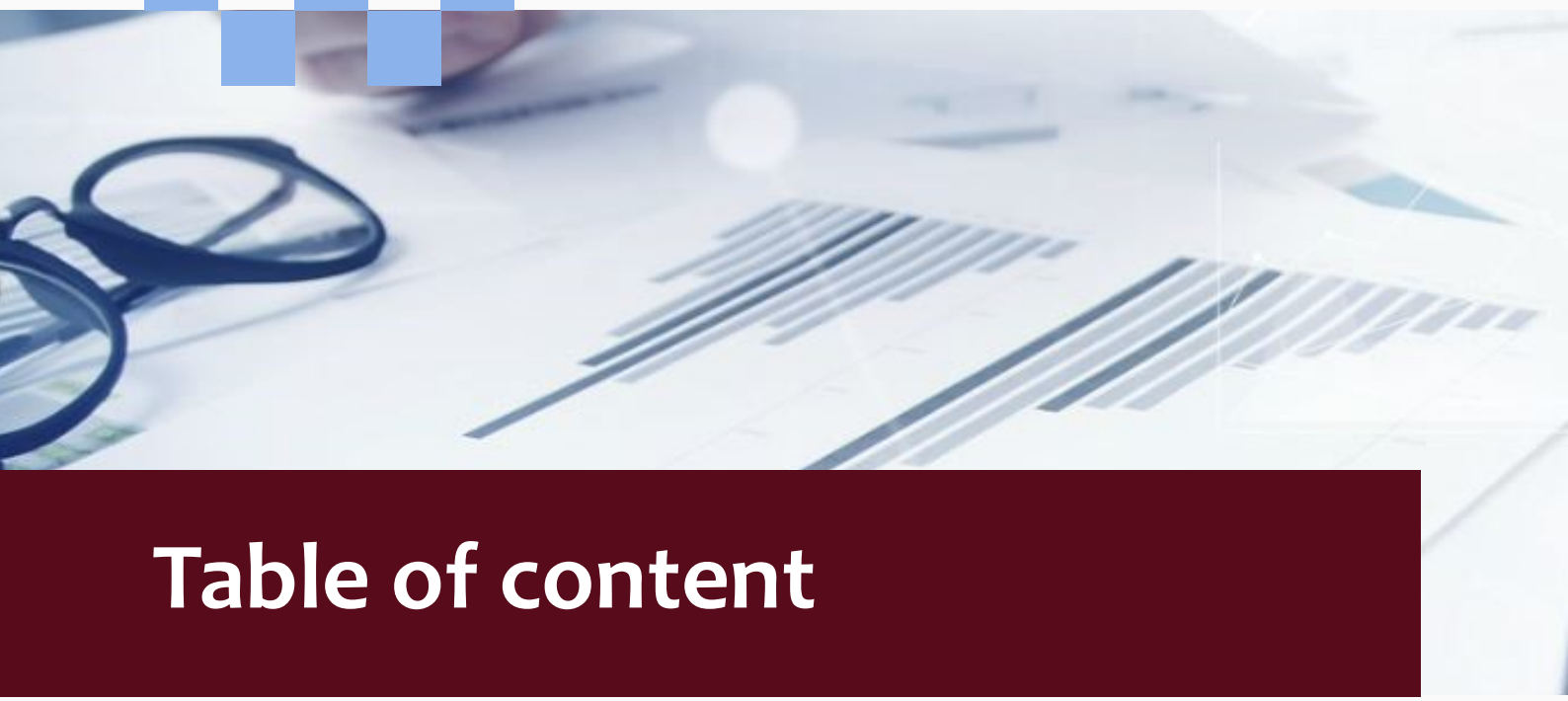
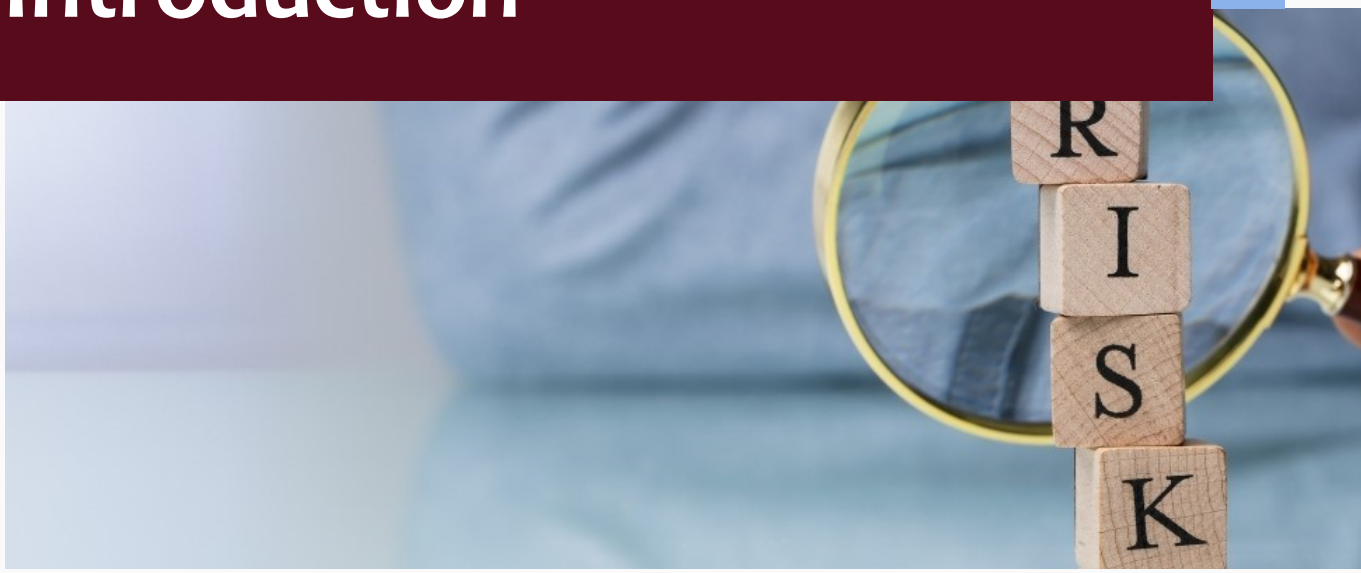


Table of content

Introduction



In the course of 2022, the ECSDA Risk Management Working Group set up a Task Force on systemic risk indicators. The objective was to define indicators allowing CSDs to identify, assess, measure, respond to and report on systemic risk. From the outset, the Task Force focused on the potential exposures to macroeconomic stress for CSDs and the systemic risk implications of the interaction between CSDs and market participants for the financial ecosystem.

The Task Force met on a regular basis between October 2022 and May 2023. The discussions leveraged existing publications on systemic risk (e.g., the quarterly - European Systemic Risk Board (ESRB) risk dashboard) and the experience of the Task Force members in the field. Several surveys were conducted among the Task Force members and the broader ECSDA Risk Management Working Group to collect input in a structured way.

The discussions revealed that systemic risk touches upon various other domains that deal with significant stress, disruption or financial shocks, such as business continuity, disaster recovery and recovery planning. It was, therefore, a challenge to approach some of these domains from a systemic risk perspective and leverage existing insights, while avoiding unnecessary overlap.

The Task Force concluded on a proposed set of indicators, structured in the form of a high-level systemic risk dashboard that is presented in the following pages. It is expected to evolve and mature over time.

1. Background

The 2007-2008 crisis revealed how interconnected banks were, and made authorities realize the need for macro-prudential policies to ensure that aggregate risks at the level of the entire financial system remained acceptable.

This fostered extensive research on systemic risk and put the spotlight on systemic institutions, the so-called Systemically Important Financial Institutions (SIFIs). The Financial Stability Board (FSB) defines a SIFI as a *financial institution whose distress or disorderly failure, because of their size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity*. More generally, the International Monetary Fund (IMF), the FSB, and the Bank for International Settlement (BIS) formally defined *systemic risk* as *the risk of widespread disruption to the provision of financial services that is caused by an impairment of all or parts of the financial system, and which can cause serious negative consequences for the real economy*.

In practice, there are two ways of measuring the systemic importance of a financial institution in the system. The first approach relies on information on positions and risk exposures, which is typically confidential and only shared externally with regulators. The second approach relies on public market data, such as stock returns, option prices, or credit default swaps, as they are believed to reflect all information about publicly traded firms.

While several prominent examples of such measures have been proposed over time (the Marginal Expected Shortfall, the Systemic Expected Shortfall, the Systemic Risk Measure, and the Delta Conditional Value-at-Risk), they can be categorised into two different types:

- on the one hand, there are those measuring the expected capital shortfall of an institution conditional on a financial crisis occurring;
- on the other hand, there are those measuring the Value-at-Risk of the financial system conditionally on a specific event affecting a given firm.

In other words, so far, the formal measurement of systemic risk has mostly:

- been structured around the interactions between a firm and the system it is a part of;
- distinguished between the impact of the firm (in distress) on the system and the impact of the system (in distress) on the firm.

2. The case of CSDs

The elements above have influenced the work of the ECSDA Task Force on systemic risk indicators for Central Securities Depositories (CSDs). This said, we decided to adopt a more qualitative approach as CSDs' systemic risk profile is relatively low, especially when compared with SIFIs or some other types of Financial Market Infrastructure (FMI). This said, FMIs are at the heart of the financial system and have a major role to play in ensuring its stability, which explains why FMIs, including CSDs, are de facto regulated as systemic entities.

In the FMI space, the key reference of regulations is the CPMI-IOSCO Principles for Financial Market Infrastructures (or PFMI). Published in early 2012, the PFMI clarified regulatory expectations when it comes to the risk management of FMIs. These principles largely underpin the European Market Infrastructure Regulation (EMIR), applicable to Central Counterparties (CCPs), and the Central Securities Depository Regulation (CSDR), applicable to European CSDs.

Systemic risk considerations are pervasive in the PFMI and the regulations based on them, which are all premised upon a number of observations:

- **FMIs play a critical role in the financial system and the broader economy. While safe and efficient FMIs contribute to maintaining and promoting financial stability and economic growth, FMIs also concentrate risk. If not properly managed, FMIs can thus be sources of financial shocks or a major channel through which these shocks are transmitted across domestic and international financial markets.** In line with the PFMI, *"an FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs."* (Principle 17 Operation Risk)

- **Market forces alone will not necessarily achieve fully the public policy objectives of safety and efficiency because FMIs do not necessarily bear all the risks and costs associated with their activities.** Moreover, the institutional structure of an FMI may not provide strong incentives or mechanisms for safe and efficient design and operation, fair and open access, or the protection of participant and customer assets. **Overall, FMIs may thus generate significant negative externalities for the entire financial system and real economy if they do not adequately manage their risks.**

- **FMIs should be not only safe but also efficient.** Efficient FMIs contribute to well-functioning financial markets. **An FMI that operates inefficiently may distort financial activity and the market structure, affecting not only its participants but also its participants' customers.** These distortions may lead to lower aggregate levels of efficiency and safety, as well as increased risks within the broader financial system. In making choices about design and operation to enhance efficiency, FMIs should ensure risk primacy and not let other considerations take precedence over the establishment of prudent risk-management practices.

3. Key concepts

At this stage, we would like to introduce a number of key concepts often used in systemic risk discussions.

3.1. Inbound and outbound systemic risk

This notion of directionality is important. Indeed, as an entity belonging to the very system whose risk is being assessed, we wanted to be able to distinguish between the risk the system poses to an entity (inbound) and the risk an entity poses to the system (outbound). This distinction between **the risks taken** (and thus the resilience to systemic stress) and **the risks posed** (and thus the contribution to systemic stress) is fundamental. This is also why we distinguish between "stress" and "vulnerability". When systemic risk materializes, the entity at the origin of the problem is deemed to be **releasing *stress* (outbound)** that other entities need **to absorb (inbound)**, which they will do if they do not suffer from material *vulnerabilities*.

3.2. Contagion and amplification

Mechanisms at work during events with a systemic impact include contagion and amplification. Contagion can turn an isolated incident into a widespread incident and amplification can turn a minor incident into a severe incident. Both mechanisms are typically at work in systemic events, which impact a significant number of market players in a material way. Contagion can take several forms. It can be direct (e.g. bilateral exposures) or indirect (e.g. information spill-overs). Amplification can also take several forms, such as negative feedback loops or pro-cyclicality.

3.3. Concentration and interconnectedness

By playing a central role in the financial plumbing system, CSDs spare market participants the need to establish a lot more bilateral relationships than they already have. Concretely, by using CSDs to access one or several markets, participants avoid the need to set up multiple other bilateral arrangements with other participants in the different markets. So, while CSDs concentrate the risk of participants (who become more dependent on CSDs), CSDs simultaneously reduce the level of interconnectedness in the market. There is thus a trade-off between concentration and interconnectedness. Note that this reasoning also applies to Central Counterparties (CCPs).

4. Towards a systemic risk dashboard for CSDs

In our work, we explored how CSDs can monitor and manage systemic risk and we ended up articulating our conclusions along three axes:

- First, CSDs should monitor external factors that may produce systemic shocks and thus release stress that the CSDs need to be able to manage;
- Then, CSDs should manage their own risk profile so as to (i) minimise vulnerability to external stress and (ii) avoid releasing stress itself, towards its ecosystem;
- Finally, CSDs should monitor the level of vulnerability of the ecosystem to remain fully aware of the ecosystem's ability to cope with stresses that CSDs may release.

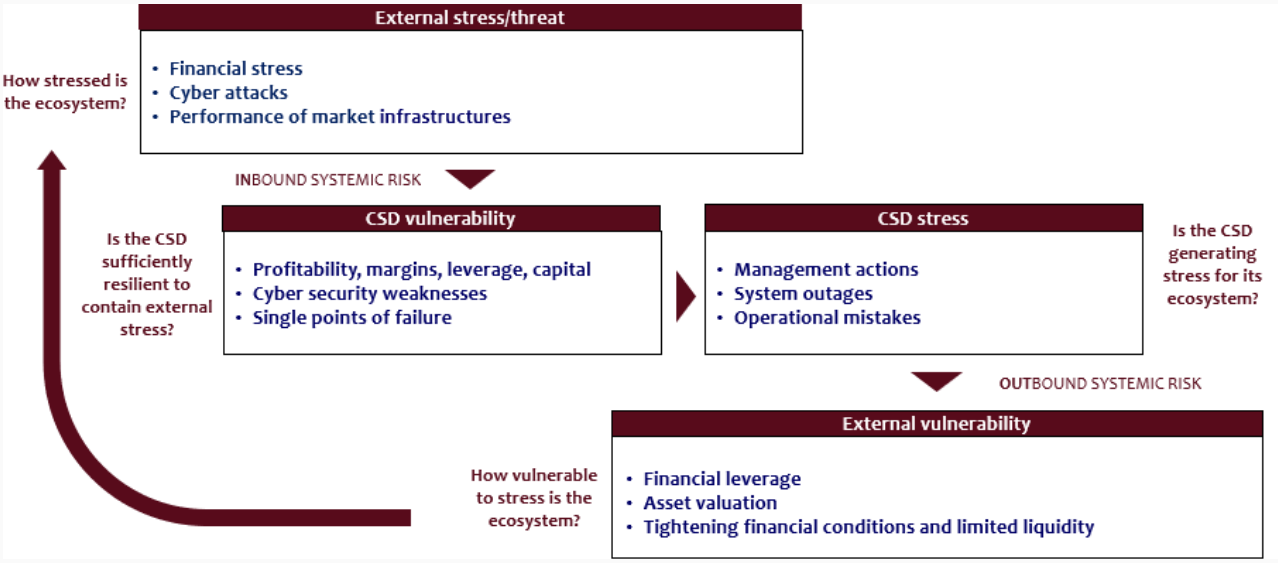
Leveraging the concepts and the conclusions introduced above, we produced a systemic risk dashboard, which supports the CSDs' ambition *not to create stress when the ecosystem is vulnerable and not to be vulnerable when the ecosystem is stressed*.

In order to achieve this, CSDs need to monitor:

- the stress level in the ecosystem (1) and in CSDs (2), and
- vulnerabilities in the ecosystem (3) and in CSDs (4).

For each of those four areas of monitoring, it was decided to limit the number of indicators to three. The measurement of these indicators can be translated in a Red-Amber-Green (RAG) coding, or in a Stable, Upward or Downward trend.

Whilst systemic risk events typically occur on short notice, the indicators are measuring longer-term evolutions that may lead to the accumulation of stress and/or the widening of vulnerabilities in the system or in CSDs.



4.1. External stress

In order to comment on the **external stress level**, a number of metrics were considered and discussed, which resulted in three metrics being **selected**:

1. Financial stress: the volatility in the market, the difficulty to transact, increasing spreads, are all indicators of stress that should trigger alerts at CSDs as they mean CSDs need to verify their resilience level.
2. Cyber-attacks (such as DDoS, ransomware, cyber data breaches). Possible source of metrics: the FS-ISAC (Financial Services Information Sharing and Analysis Center) Global Cyber Threat Level.
3. Performance of market infrastructures (such as SWIFT, T2/T2S outages/delays).

- The macroeconomic situation (growth, interest rates, inflation): the metric was rejected as it is a metric that CSDs should monitor in the context of business risk management but not necessarily a metric that contains a lot of information about the level of stress in the market (which is the object of this exercise).
- (Geo)political instability (such as demonstrations, sanctions, supply chain disruptions): this metric was rejected as this indicator seems more "indirect" from a CSD perspective. The consensus was to drop it and focus on the financial stress indicator instead.
- Service provider (Critical Utilities, IT providers) distress: this metric was rejected partly because it was deemed too specific to give a good idea of the general level of stress in the financial ecosystem and partly because of potential duplication with other metrics such as cyber-attacks and performance of market infrastructures.

4.2. Internal vulnerability

In order to assess the **internal (CSD) vulnerability level**, several metrics were considered and discussed with the ESCDA Risk Management Working Group, which resulted in three metrics being **selected**. These metrics are internal CSD metrics that are not expected to be shared with the outside world (other than with regulators where relevant). Each CSD may therefore select the most relevant metrics for its risk profile. Three areas are to be considered in most cases:

1. Profitability, margins, leverage, capital: CSD vulnerability is deemed to arise from financial resilience gaps and/or operational resilience gaps. This metric is supposed to capture financial resilience gaps.
2. Cyber security weaknesses (e.g. non-deployed vulnerability patches)
3. Single points of failure (e.g. services without back-up solution)

A number of other metrics were considered but eventually **not withheld** for several reasons: concentration/dependency on a limited number of clients: this metric was considered as a duplication in the sense that having a limited number of clients means financial performance could be quickly destabilized (the financial equilibrium of the CSD is fragile) and financial performance is already tracked with the first indicator. Moreover, the consensus was that it is better to monitor this metric in the context of business risk management as this is also driven by market trends (e.g., the consolidation of custodians).

4.3. Internal stress

In order to comment on the **internal (CSD) stress level**, a number of metrics were considered and discussed with the ESCDA Risk Working Group, which resulted in three metrics being **selected**. Note that these metrics are internal CSD metrics that will not be shared with the outside world. It is up to each CSD to select the most relevant metrics for its risk profile. Below is a list of suggestions:

1. Management actions: management actions are actions taken by management, either to manage a stress situation or in the day-to-day management of the CSD. Such actions could include procyclical actions (actions that amplify stress in the market) or actions aiming at externalizing stress (e.g., usage of loss-sharing mechanisms).
2. System outages
3. Operational mistakes

A number of metrics were also considered but eventually **not withheld** for a number of reasons: in particular, settlement efficiency: while a sudden decrease in settlement efficiency is a source of stress for the ecosystem, sudden drops are unlikely to come out of nowhere and the main sources (system outages and non-performance of market infrastructures) are already included in other views, i.e. external stress and CSD vulnerability. Moreover, work is currently on-going at ECSDA level on this metric as figures vary wildly across CSDs. As a consequence, there was a consensus to drop it.

4.4. External vulnerability

In order to assess on the **external vulnerability level**, (i.e., meaning that the ecosystem is vulnerable and may not be in a good position to absorb stress as the potential for a severe market correction and/or liquidity and insolvency issues is high), a number of metrics were considered and discussed with the ESCDA Risk Management Working Group, which resulted in three potential metrics being **selected**:

1. Financial leverage: vulnerability may be increased in case of high levels of leverage in the market (i.e. the fact that companies and financial institutions have issued a lot of debt and/or obtained a lot of loans)
2. Asset valuation: rich valuations across asset classes (i.e. the fact that asset prices are high in the market and are thus exposed to negative news) may indicate the market is vulnerable to excessive corrections – amplifying volatility.
3. Tightening financial conditions and limited liquidity are also signs of fragility.

5. Additonal remarks

The Task Force also discussed global themes and impacts, such as *climate change*, and decided not to have it appear explicitly in the dashboard. Indeed, such global themes are often integrated in/covered by other metrics, in a way that reflect whether the CSD is directly or indirectly exposed to it. For instance, in case of direct exposure to climate change, we would expect a metric in the CSD vulnerability box to reflect that. In case of indirect exposure to climate change, we would expect a metric in the external stress box to reflect that.

Interdependencies between CSDs, for instance through market links or through a common participant base, do not appear directly in the dashboard either. This is because interdependencies are integrated in the other metrics. Having a large number of links, for instance, increases the vulnerability of the CSD to external stress (performance of market infrastructures) as it increases the likelihood that an issue occurs on one of the links. A large number of links also increases the vulnerability of the ecosystem to the CSD (limited manual processing capacity, absence of back-up solutions, single points of failure) as it means that an issue at the CSD will impact more markets.

There is also the risk of *unintended consequences of regulation*, which may not be designed to adequately take into account the specific risk profile of CSDs. Abiding by certain regulatory requirements too strictly may therefore in some instances prove to be counter-productive. An example is the two-hour recovery time objective set in regulation, which may not be realistic in all situations of system disruption; in some cases, if CSDs are pressured to recover faster or more aggressively, they may be forced to externalise the shock (e.g. by cancelling transactions). Doing so may create further systemic risk. CSD management and regulators should be conscious of such consequences.

CONCLUSION

The analysis has shown that there are relevant external stress factors that CSDs could monitor to anticipate on potential shocks that could impact them. The likelihood and severity of such impacts may depend on the CSDs' own vulnerabilities that it could therefore monitor as well, together with the stress that they could reflect or generate by themselves to the broader ecosystem, which in turn may be more or less sensitive to such stress in function of its own vulnerabilities.

The scope and calibration of the indicators to be monitored will vary depending on the risk profile of each CSD, the market(s) in which it operates and its risk appetite and strategy towards systemic risk – considering the risk/reward trade-off of addressing vulnerabilities to, or absorbing the impact of, systemic stress. As for any type of risk, the risk response for systemic risk will be to mitigate, accept, transfer or avoid the risk – by acting on either the likelihood or severity of the potential systemic impact.

The Task Force believes that the four selected sets of indicators are defined in a sufficiently generic way to allow for such tailoring while maintaining a certain level of consistency. Each CSD can of course determine additional indicators or be more granular in the measuring of the indicators proposed in this dashboard.

It is proposed that the ECSDA Risk Management Working Group review the Systemic Risk Dashboard and the selected indicators by 2025, in order to integrate lessons learned from its practical implementation across ECSDA members.

Contributors

Members of the ECSDA Systemic Risks Task Force

- Pierre Paul Stacanov, Euroclear Belgium, France & Nederland, Chair
- Kristina Akerberg, Euroclear Sweden
- Fernando Centelles, Iberclear
- Ebru Cicekdagi, Clearstream Banking SA
- Christophe Diederen, Euroclear Bank
- Lavinia Gheorghe, Depozitarul Central
- Hubertus Hecht, OeKB CSD
- Flemming Larsen, Euronext Securities | Copenhagen

ABOUT ECSDA

The European Central Securities Depositories Association (ECSDA) represents 40 Central Securities Depositories (CSDs) across 36 European countries. As regulated financial market infrastructures, CSDs play a vital role in supporting safe and efficient securities transactions, both domestic and crossborder.

40
Members

36
Countries

1.8
Quadrillion €
Worth instructions annualy

71
Trillion €
Worth assets

CONTACT US

+32 230 99 01

Info@ecsda.eu

www.ecsda.eu