esma European Securities and Markets Authority

TRV Risk Analysis

A framework to assess operational resilience

ESMA document number: 50-165-2165
Publication date: 19 December 2022

ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis

Legal reference for this Report: Regulation (EU) No. 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, Article 32 'Assessment of market developments, including stress tests', '1. The Authority shall monitor and assess market developments in the area of its competence and, where necessary, inform the European Supervisory Authority (European Banking Authority), and the European Supervisory Authority (European Insurance and Occupational Pensions Authority), the European Systemic Risk Board, and the European Parliament, the Council and the Commission about the relevant micro-prudential trends, potential risks and vulnerabilities. The Authority shall include in its assessments an analysis of the markets in which financial market participants operate and an assessment of the impact of potential market developments on such financial market participants.' The information contained in this publication, including text, charts and data, exclusively serves analytical purposes. It does not provide forecasts or investment advice, nor does it prejudice, preclude or influence in any way past, existing or future regulatory or supervisory obligations by market participants.

The charts and analyses in this article are, fully or in part, based on data not proprietary to ESMA, including from commercial data providers and public authorities. ESMA uses these data in good faith and does not take responsibility for their accuracy or completeness. ESMA is committed to constantly improving its data sources and reserves the right to alter data sources at any time. The third-party data used in this publication may be subject to provider-specific disclaimers, especially regarding their ownership, their reuse by non-customers and, in particular, their accuracy, completeness or timeliness, and the provider's liability related thereto. For more details on these disclaimers, please consult the websites of the individual data providers whose names are given throughout this report. Where third-party data are used to create a chart or table or to undertake an analysis, the third party is identified and credited as the source. In each case, ESMA is cited by default as a source, reflecting any data management or cleaning, processing, matching, analytical, editorial or other adjustments to raw data undertaken.

ISBN 978-92-95202-66-5, doi 10.2856/700003, ISSN 2599-8749, EK-09-22-557-EN-N
European Securities and Markets Authority (ESMA)
Risk Analysis and Economics Department
201–203 Rue de Bercy
75012 Paris
FRANCE
risk.analysis@esma.europa.eu

A framework to assess operational resilience

Contacts: antoine.bouveret@esma.europa.eu; victor.herraez@esma.europa.eu [1]

Summary

The operational resilience of financial entities that play a critical role in the financial system is key to financial stability. In this article, we present a novel approach to assess operational resilience for financial entities providing time-critical services. These tools provide the means for supervisors to measure and test different aspects of financial entities' operational resilience in a standardised and comparable manner and can be adapted to different types of financial institutions for which continuous operations is expected. We present an application of those tools in the context of the fourth ESMA CCP stress test.

Introduction

The recent rise in cyber-attacks on financial institutions, together with outages experienced by market participants such as trading venues, have emphasized the need to identify, measure and mitigate operational risks, in order to ensure a robust financial system.

Traditionally, in the area of banking institutions, the focus of operational risk has been on the financial consequences of events, with operational risk being defined as "*the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events*" (BCBS, 2021a); The term operational resilience was introduced more recently, it is defined as "*the ability to deliver critical operations through disruption*" (BCBS, 2021b), putting the focus on entities' ability to continue to operate or recover their critical operations in the face of disruptive operational risk events.

Whereas the Principles for Financial Market Infrastructures (PFMI) define operational risk as: "*The risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by an FMI.*" (CPMI-IOSCO, 2012). This definition focuses on maintaining the service availability of FMIs, given that these entities perform a critical intermediary role in the financial system, since their lack of operational resilience could have systemic implications.

ESMA (2018) provide a framework for the assessment – i.e. the identification, monitoring and analysis – of operational risk from a regulatory and supervisory perspective for institutions and markets under ESMA's remit. In particular, three priority areas are identified: market misconduct, infrastructure disruptions and cyber-attacks. Those last two areas have a direct impact on operational resilience.

In that context, policymakers worldwide have been working towards strengthening the operational resilience of their financial systems. In the EU, the Digital Operational Resilience Act (DORA) details new requirements for managing IT risks, sharing threat intelligence, reporting IT incidents and managing and overseeing IT third parties.

In line with these efforts, in its fourth CCP Stress Test[2], ESMA introduced a new set of quantitative tools to assess and compare the operational resilience of CCPs (ESMA, 2022).

[1] This article was written by Antoine Bouveret and Victor Herraez, with contributions from Jakub Schrimpel.

[2] ESMA, "4th ESMA Stress Test Exercise for Central Counterparties", 5 July 2022.

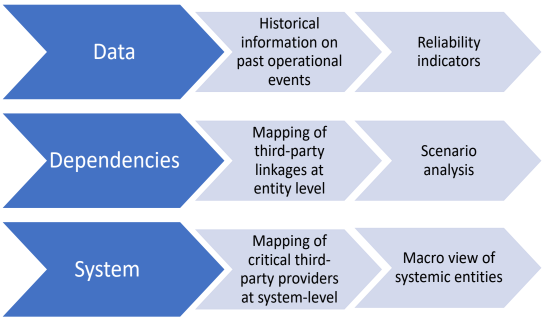
These three tools provide novel approaches which allow of different operational resilience aspects to be better understood and can also be adapted for their use on other types of financial entities.

The tools developed in this article are particularly relevant for financial institutions providing time-critical services such as CCPs, trading venues or payment and settlement systems.

This paper aims to provide an overview of the three new tools (Chart 1), their methodology and an application to assess operational resilience in the financial sector, using insights from their use in the context of the fourth CCP stress test performed by ESMA.

The first tool uses historical data on operational incidents in order to compute reliability indicators that provide information about the overall level of operational resilience. The second tool uses scenario analysis techniques to assess the risks from outages of critical third-party providers. Finally, the third tool is a mapping of interconnections and risks that allows systemic critical third-party providers to be monitored and concentration risks at system level to be assessed.

Chart 1
Operational resilience
Several tools to assess resilience


Data
Historical information on past operational events
Reliability indicators
Dependencies
Mapping of third-party linkages at entity level
Scenario analysis
System
Mapping of critical third-party providers at system-level
Macro view of systemic entities

Source: ESMA.

Tool 1: Reliability indicators

Introduction

Reliability indicators aim to provide information about the level of operational resilience for each entity in scope.

When assessing the operational resilience of financial entities, it would be ideal to understand the level of resilience of all the different components of the organisation with respect to the universe of possible operational risks that could affect it, which is a significant methodological challenge.

Alternatively, one can look at past data of incidents and outages and calculate reliability[3] metrics related to the frequency and severity of past operational events. These indicators can be used to assess the operational resilience of each entity over the sample period. This approach allows a baseline understanding of each entity's general level of operational resilience to be formed, with the advantage that it is based on data from real events and with the limitation that past data may not reflect changes adopted by the entity or the scale and nature of future incidents.

Methodology

To construct reliability indicators the first step is to define

- the scope of business functions,
- types of incidents, and
- quantitative variables (time duration, financial loss) that are of interest.

In the fourth ESMA CCP stress test, the emphasis was on events affecting the most critical functions of CCPs (such as clearing and settlement of transactions). Quantitative variables were defined based on the duration of operational events.

Once this is defined, it may also be necessary to create some "buckets" in order to aggregate heterogeneous information or create specific variables to better adapt to the characteristics of the entity in scope. Two examples from the

[3] Reliability is defined as the probability that a component (or an entire system) will perform its function for a specified period of time,

fourth ESMA CCP stress test can help illustrate this process:

1. Given our choice of outage time duration as our quantitative variable, it was necessary to separate events that had different levels of severity. This was important to avoid aggregating the duration time of incidents that may have a different impact on the financial system (this issue does not occur when aggregating monetary quantities). For this purpose, three severity buckets were created, based on the criticality of CCP activities affected by the event (critical function, critical supporting function, etc.). This allows the incidents to be aggregated and different metrics to be computed based on the severity of the impact to the financial system and the associated regulatory requirements.
2. A variable quantifying the scope of the incident was also introduced, as CCPs provide services to multiple products and markets. This variable helps differentiate between outages that only affected individual products or clients, from those that affected complete markets or the whole CCP.

After defining the data model, the subsequent step is to request data from the entities in scope and aggregate them through indicators that help establish an understanding and facilitate comparison across entities.

For the development of indicators, due to the novelty of the exercise, we chose to pursue two different approaches. The first approach is a simple set of indicators based on literature from the discipline of reliability engineering (Modarres et al., 2016), which mainly describes the average recurrence and duration of events and expected operational availability.

The metrics used are the following:

- Mean time between failures (MTBF): The average time (in days) between the breakdowns of services
- Mean time to repair (MTTR): The average time (in hours) taken to recover from a failure
- Expected one-year unavailability: The expected downtime in a one-year period using the two previous measures[4]. It is computed as the ratio of MTTR to MTBF (divided by 250 trading days):

$$EXP_{1Y} = \frac{MTTR}{MTBF/250}$$

The second set of indicators follows a model-based approach that uses past data and numerical simulations to estimate the frequency and duration of operational risk events (Table 2). This approach focuses more on the tail risk and complements the first set of indicators, which is focused on average values.

Table 2

CCP availability

Simulation using the loss distribution approach

In operational risk analysis, monetary losses or unavailability of core functions of an entity can be estimated using the loss distribution approach (Shevchenko, 2010). The frequency and severity of operational risk events are modelled using parametric distributions and the distribution of aggregated losses (or time unavailability) is estimated using numerical simulations (Monte Carlo methods). This type of approach is common used to measure operational risk for banks and has also been used to estimate aggregate losses due to cyber risks for the financial sector (Bouveret, 2019).

Using collected data on past operational risks events for CCPs in our sample, we apply the loss distribution approach to (i) the risks of unavailability of clearing or settlement and (ii) the risk of unavailability of critical functions.

The frequency of operational risk events is modelled using a Poisson distribution. The probability that k operational risk events occur over a year is given by:

$$p_k = \frac{\lambda^k}{k!}e^{-\lambda}$$

The average number of events per year λ is equal to the average number of events that occurred for each CCP from 2016 to 2021.

The severity of operational risk events, i.e. the duration of outages, is modelled using a lognormal distribution, which has a fatter tail than the normal distribution, implying that long outage events are more likely. The probability density function f is given by:

$$f(x) = \frac{1}{x\sqrt{2\pi\sigma^2}}exp^{\left(-\frac{(ln(x)-\mu)^2}{2\sigma^2}\right)}$$

Since the dataset is small, for each type of operational risk event, CCPs have been grouped in four categories (lowest severity, low severity, high severity and highest severity) based on the average duration of events. Each CCP within a group is assumed to have the same severity distributions, i.e. the parameters of the lognormal distribution are equal for each CCP within a group but different across groups. The parameters are estimated based on all the risks events within a group using the maximum likelihood.

Chart 2 compares the distributions obtained for the events related to the unavailability of clearing or settlement: CCPs in Group 1 (green curve) experienced events of short duration, with a peak in frequency of around 1 hour; whereas for CCPs in Group 4 (purple curve) experienced

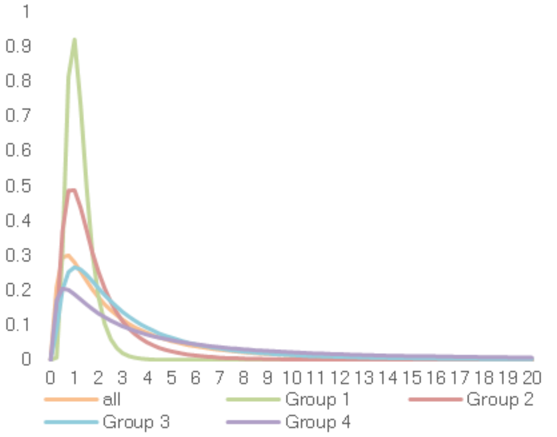
[4] Asensio et al. (2022) use a similar approach to model systemic risk related to the use of Cloud Service Providers and assess options to mitigate those risks.

events lasting more than 4 hours which account for around 10% of the events in the sample.

Chart 2

Distribution of disruption time

Heterogeneity across groups of CCPs



Note: Distribution of disruption time for clearing or settlement unavailable by group.
Sources: CCPS, ESMA.

Finally, the distribution of (i) the unavailaility of clearing or settlement functions and (ii) the unavailability of critical functions are calculated using 100,000 simulations for each CCP.

Once the distribution is known, we calculate risk metrics such as the one-year 95% Value-at-Risk (VaR) — the cumulated duration time of operational risk events that a CCP would experience on average in 95% of the cases — and the 95% Expected Shortfall (ES) — the average cumulated duration time in the worst 5% of cases — to obtain risk measures for each CCP and type of events.

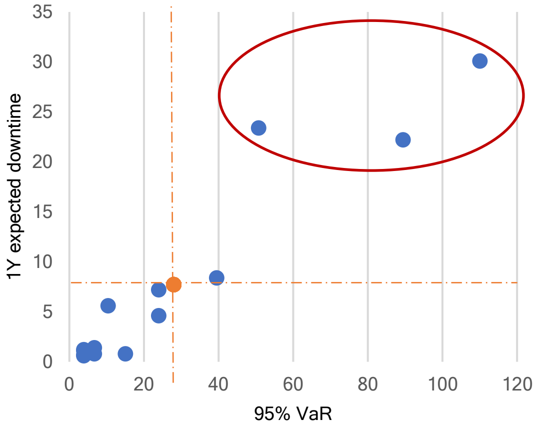
Use

The different indicators can be assessed individually against a desired benchmark, or they can be compared across entities. For example, in the CCP Stress Test, we compared entities using a scatterplot with a chosen metric (here one year expected downtime) for both methodologies (average values and model-based tail estimates) in order to visualise the entities that were performing worse than their peer group (Chart 3). In this chart, each blue point represents a different CCP, while the red point indicates the average for all entities in scope. Such a visualisation allows entities with high-risk indicators to be identified (red oval).

Chart 3

Operational risk metrics

Clearing or settlement unavailable



Note: 95% VaR and 1Y expected downtime by CCP in hours for clearing or settlement unavailable.
Sources: CCPs, ESMA.

This methodology can, thus, be used to develop a baseline understanding of the general level of operational resilience across entities based on historical data of past events. While the reduced amount of data limits the accuracy of the modelling, this flexible approach can be used to benchmark operational risk across entities and inform supervisory priorities.

Tool 2: Scenario analysis of third-party dependencies

Introduction

The second tool focuses on a more specific risk through the use of scenario analysis techniques: the outage of a critical third-party service provider.

Through the scenario analysis, we assume that each critical third-party service provider connected to a financial entity faces an outage sequentially. We then analyse the impact of the outage on each entity, taking into account the available operational risk management tools in place. This analysis yields a measurement of the amount of exposure of each entity to single points of failure linked to third-party entities[5].

[5] The analysis has similarities with Englund and Sosa (2022) who use US banks regulatory reports to identify critical financial market utilities (including the US real-time gross settlement system Fedwire and the clearing house for large value transactions CHIPS) and then estimates the impact of a disruption of the payment system on the bank network. While Englund and Sosa (2022) focuses on the impact of an outage of a payment system on bank networks, our analysis focuses on the impact of an outage of a third-party provider on a CCP or the network of CCPs.

The scope of third-party entities included comprises all providers that are needed for the entities in scope to operationally deliver their critical functions. Such providers include utilities, technology providers[6], financial services, intragroup services and FMIs.

It must be noted, that, in the scenario analysis, the outage of each third party is assumed, irrespective of the likelihood of an outage to happen.

Methodology

The analysis is based on five steps: (i) the mapping of dependencies, (ii) the risk assessment of each third-party provider, (iii) the mapping of operational risk management tools, (iv) the assessment of any residual impact after taking into account operational risk management tools and (v) the measurement of exposure to single points of failure.

(i) Mapping of dependencies

Entities included in the analysis are asked to identify the critical third-party service providers that are needed for different critical functions to operate. Intragroup service providers were also reported for entities belonging to groups[7].

(ii) Risk assessment of third-party providers

In a second step, entities are asked to assess for each identified critical third-party service provider the consequences of an outage in line with the scenario description. For this risk assessment, entities have to consider the hypothetical situation where no operational risk management tools would work / exist to be able to separately evaluate the reported tools.

(iii) Mapping of operational risk management tools

In the third step, entities provide information about the operational risk management tools they have in place to mitigate the effects of critical third-party service provider outages. These tools are broadly categorised into two types: (a) redundancy, where different third-party service providers are operationally set-up as substitutes, and (b) internal tools, which includes any kind of internal capabilities for impact mitigation (such as alternative communication tools, manual computations).

(iv) Assessment of residual impact

In the fourth step, entities are asked to assess the residual impact that would remain after applying the reported operational risk management tools. Residual impact uses the same type of metrics than those of step (ii).

(v) Measuring exposure to single points of failure

Using the information collected in the four previous steps, we develop a measure of exposure (“weighted exposure") to third-party risk. This indicator provides information about the amount of exposure to critical third-party service providers for each entity in scope. This measure takes into account the residual risk after applying operational risk management tools and the percentage of activity of the entity that would be affected in the event of an outage.

These indicators are an increasing function of the number of critical third-party service providers to which each entity is passively exposed. The exposure to each third-party entity is weighted using a value ranging between 0% and 100%, depending on the share of the activity that would be affected by the outage of that specific third-party. This weighting is used to allow for comparability between different peers irrespective of their operational structure.

The specific failure probabilities of each third-party entity are not calculated due to the absence of data. Instead, they are characterized with information about the risk profile of the entities. For the CCP Stress Test, this was done by differentiating the exposures depending on whether the critical third-party service providers were FMIs, Intragroup companies, other financial entities or non-financial entities.

Use

The scenario analysis allows the overall operational structure and risk management

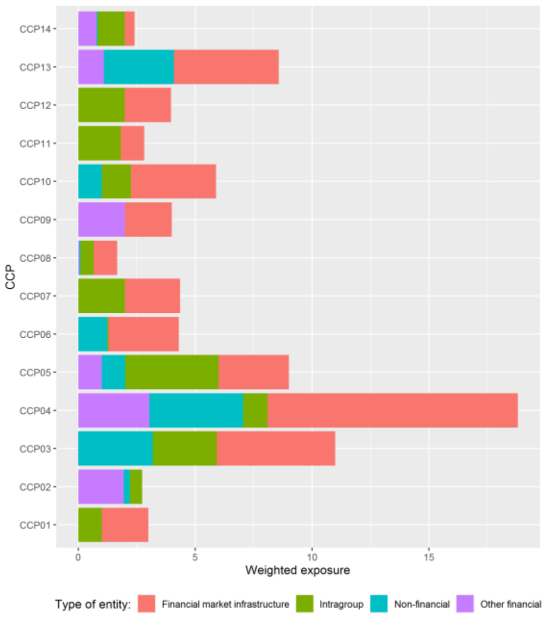
[6] Systems can be considered a key area of potential operational weakness given the high degree of digitisation of financial services providers and the central role played by IT systems for FMIs (ESMA, 2018).

[7] Intragroup entities can be considered part of an internal organisation that is a potential operational risk source (ESMA, 2018).

strategy to be evaluated, with the main output being a measure of exposure to critical third-party service providers that are single points of failure. This measure allows entities to be compared to their peers and identifies those that are most exposed to this type of risk, as along with the composition of their surface exposure. Chart 4 shows as an example the exposure indicator for each CCP included in the fourth ESMA Stress test for critical clearing or settlement functions.

Chart 4 indicates that CCPs have different risk profiles with respect to their exposure to third-party critical service providers that represent single points of failure, with weighted exposure ranging from less than 5% up to almost 20% for one CCP.

Chart 4
CCP weighted operational risk exposure
Heterogeneity across CCPs



Note: Exposure of CCPs to third parties, weighted by the clearing activity impacted by a third-party outage.
Source: ESMA fourth CCP Stress Test

Overall, the methodology of this third-party dependency analysis provides a framework to map and measure the risk exposure of entities due to outages affecting critical third-party service providers. Authorities can then monitor the level of exposure and channels of operational risk transmission of individual entities.

Tool 3: System-wide analysis of critical third-party providers

Introduction

The third tool leverages the results from the scenario analysis to build a mapping of dependencies between the entities in scope and the universe of critical third-party providers , thus moving from an entity to a system-wide perspective. This mapping provides information about the interconnections within the sector and the types of risks of the interconnections after taking into account the entities' risk management tools. The objective of this tool is to identify risks at a system-level, including the identification of systemic entities, the level of concentration, and potential channels of operational risk contagion. For entities providing time-critical services, the outage of a third-party critical provider could impede the continuous provision of services.

Methodology overview

For the system-wide analysis, the information collected in the analysis of third-party dependencies (tool 2) is leveraged to assess concentration and systemic risks using a system-wide perspective. It is built taking into account three elements:

- The mapping of operational interconnections between entities in scope and critical third-party service providers.
- The risk of each interconnection, defined by the type of impact (described as risk levels in the charts presented in the subsequent usage section) that each entity would experience if the critical third-party provider suffered an outage.
- The operational risk management tools that the CCPs have in place.

These components are used to derive network graphs and interconnectedness measurements that allow systemic entities and degrees of concentration to be identified. The results can be computed taking into consideration all entities together but also looking at specific categories in a separated manner.

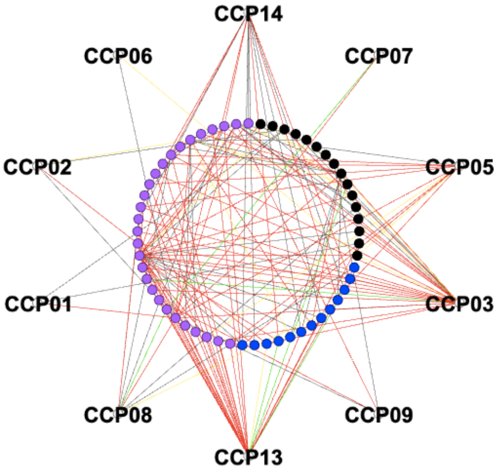
In that setting, only significant connections are used (i.e. when more than 10% of the clearing activity — measured by margins — would be impacted by an outage) to help focus the analysis on the most important nodes.

Use

The outputs of this tool are (i) network graphs that depict the connections between critical third-party service providers and entities in scope and (ii) measures of interconnectedness.

Charts 5 and 6 describe the overall network of critical service providers connected to multiple entities and highlight the ten most interconnected entities and their associated risks from the fourth ESMA CCP Stress Test.

Chart 5
Network analysis of third-party dependencies
Relationship between third-party providers connected to multiple CCPs (inner ring) and the respective CCPs (outer ring)



Note: Each node (circle) in the inner circle shows a third-party entity that is connected to more than one CCP. Colours of each node indicate the type of entity; Colours of the edges connecting with CCPs indicate the type of risk of the interconnection. More information about the methodology below. Only interconnections whose weight is higher than 10% of clearing activity (measured by margins) are displayed.

Source: ESMA fourth ESMA CCP Stress Test

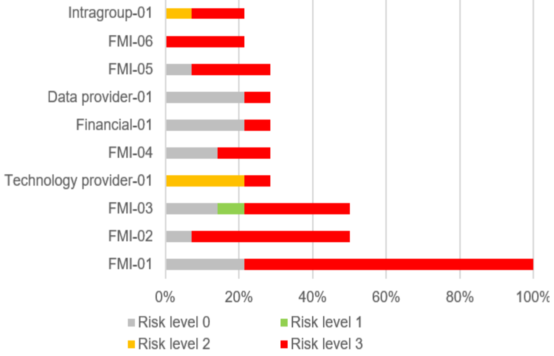
The critical third-party service providers are characterized with three colours:

- FMI group entities (purple colour node): FMIs, payment systems, settlement systems, central banks.
- Other financial entities (blue colour node): Regulated financial institutions excluding those in the first group (such as credit institutions, insurance undertakings or investment firms).
- Non-financial entities (black colour node): Entities outside the financial regulatory perimeter (such as providers of cloud and data services or utilities).

The risk arising from the interconnections is described using colours similar to a “traffic light” approach:

- Risk level 0 (grey colour): The CCP has a preventive/protective tool in place to prevent any risk in the event of a third-party outage.
- Risk level 1 (green colour): In the event of a third-party outage, the CCP would experience an impact leading to a deterioration of its ability to achieve a specific Service Level Agreement (Type of impact: Other Service Level Agreement breach).
- Risk level 2 (orange colour): In the event of a third-party outage, the CCP would experience an impact of the following type: critical supporting function non available.
- Risk level 3 (red colour): In the event of a third-party outage, the CCP would experience an impact of the following type: clearing or settlement function unavailable.

Chart 6
Third-party entity interconnectedness
Top-10 critical third-party providers based on the number of CCPs to which they provide services and the associated risk of the interconnections



Note: The length of the bar indicates the percentage of total CCPs connected to the critical third-party provider and the colours indicate the risk for different parts of the exposure surface. More information about the methodology below.

Source: ESMA fourth CCP Stress Test

For the interconnectedness indicators we use bar charts where:

- The indicated percentage of interconnectedness is calculated as: [number of connected CCPs / Total number of CCPs 8].
- The size of each colour part of the interconnectedness bar is calculated as: [number of connected CCPs to Risk level X / Total number of CCPs].

The colours that illustrate the risk follow the same "traffic lights" approach that the interconnectedness graphs described before.

Overall, the methodology of this system-wide analysis of critical third-party service providers allows risks from interconnected critical third-party service providers to be monitored, taking into account the dependencies across entities, the operational risk management tools available and the impact from outages in nodes of the network. This tool has applications from an entity and system-wide supervisory perspective.

Conclusion

In this paper we provide an overview of a quantitative approach to measuring the operational resilience of financial entities and provide examples of its usage based on its implementation in the context of the fourth ESMA CCP Stress Test.

We develop novel tools that can be applied to financial entities providing time-critical services and allow:

- Comparable operational risk indicators to be computed using reliability measurements of past incidents data in order to inform supervisory priorities.
- The exposure of different entities to risk from outages affecting critical third-party service providers to be mapped and measured.
- The network of critical third-party providers to be mapped in order to monitor risks from systemic entities or monitor concentration issues.

Overall, the tools presented in this framework contribute to a better understanding of operational resilience and the risks from critical third-party service providers to financial entities for both authorities and market participants, allowing the quantitative measurement of risks to be carried out in a comparable manner across entities. These tools can also expand the range of quantitative indicators available to ESMA and Authorities to monitor operational risk, as advocated by ESMA (2018).

This framework has been applied to CCPs in the context of the fourth ESMA CCP Stress Test but can also be adapted to other types of financial entities.

[8] 14 CCPs were included in the fourth ESMA CCP Stress Test

References

Asensio, C., Bouveret, A. and A. Harris (2022), "Financial stability risks from cloud outsourcing", ESMA Working Paper No.2.

Basel Committee on Banking Supervision (BCBS) (2021a), "Revisions to the Principles for the Sound Management of Operational Risk".

Basel Committee on Banking Supervision (BCBS) (2021b), "Principles for Operational Resilience".

Bouveret, A. (2019), "Estimation of losses due to cyber risk for financial institutions", Journal of Operational Risk, Vol. 14(2). DOI: 10.21314/JOP.2019.224.

Committee on Payment and Market Infrastructure (CPMI) and International Organization of Securities Commissions (IOSCO) (2012), "Principles for Financial Market Infrastructures".

Committee on Payment and Market Infrastructure (CPMI) and International Organization of Securities Commissions (IOSCO) (2015), "Public quantitative disclosure standards for central counterparties".

Curti, F., Migueis, M. and R. Stewart (2020), "Benchmarking operational risk stress testing models", Journal of Operational Risk, Vol. 15(2). DOI: 10.21314/JOP.2020.239.

Englund, C. (2022), "An Approach to Quantifying Operational Resilience Concepts", FEDS Notes, July.

ESMA (2018), "Operational risk assessment – the ESMA approach", ESMA Report on Trends, Risks and Vulnerabilities No.1.

ESMA (2022), "4th ESMA Stress Test Exercise for Central Counterparties", Report.

International Organization of Securities Commissions (IOSCO) (2022), "Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic", Consultation report, January.

Modarres, M., Kaminskiy, M.P., and Krivtsov, V. (2016). Reliability Engineering and Risk Analysis: A Practical Guide (3rd ed.). CRC Press. https://doi.org/10.1201/9781315382425.

Shevchenko, P. (2010), "Calculation of aggregate loss distributions", Journal of Operational Risk, Vol. 5(2). DOI: 10.21314/JOP.2010.077.

esma European Securities and Markets Authority