Ebook

# Unlocking the value of your counterparties' CSP attestation data

## Leading financial institutions share their key success factors

1.0 Overview →

2.0 Combatting the cyber threat with CSP attestation data →

3.0 Collecting and assessing attestation data →

4.0 Handling non-compliance →

5.0 Success factors →

5.1 Methodology →

5.2 Resources →

5.3 Communication →

5.4 Tools and processes →

5.5 Community →

6.0 Best practices: A planning and execution checklist →

7.0 Conclusion →

# 1

# Overview

**With increasing digitisation, the cyber threat facing financial institutions has never been greater.**

**In this environment, financial institutions need to have the right controls in place to protect their own organisations — and they also need to understand the risks associated with their counterparties.**

**SWIFT's Customer Security Programme (CSP) helps you cover both bases.** As well as attesting to your own security controls, you can also access your counterparties' attestation data – and thereby tap into another data point to help you manage counterparty risk.

In this ebook, financial institutions that are leading the way in this field share the insights they have learned along the way, and some key success factors that can help you and your organisation get additional value from counterparty attestation data.

**"Counterparties that generally have weaker CSP controls may run greater cyber risks, which increases the likelihood and potential severity of an unexpected outcome."**

**Victor Abiola —** Global Head, Operational Risk, Corporate and Investment Bank at Standard Bank

# 2

# Combating the cyber threat with CSP attestation data

**Cybercrime continues to present a major challenge for financial institutions. In today's environment, you need to have robust defences in place to protect yourself from attacks.**

**And, as attacks such as the 2020 SolarWinds hack and the Accellion FTA breach have highlighted, an important part of these defences is understanding the risk associated with your counterparties and suppliers.**

## 93-99%
## average compliance rate for individual mandatory controls in 2020.

**Introduced in 2016, SWIFT's Customer Security Programme (CSP) aims to support our community in combating cyber threats.** As part of the programme, financial institutions are required to assess their compliance with a list of mandatory and advisory security controls, and to attest compliance with the mandatory controls (advisory controls are recommended) on an annual basis. This attestation is done via the KYC Security Attestation (KYC-SA) application on swift.com.

In 2020, the overall attestation rate was 89%, while the average compliance rate for individual mandatory controls ranged from 93% to 99% – a particularly impressive achievement against the backdrop of the pandemic. This demonstrates the community's commitment to cyber hygiene, and shows how far entities in the SWIFT community have come in establishing cyber risk management frameworks and adopting cybersecurity risk countermeasures.

## Requesting counterparty data

As well as submitting your own attestations, you can also request attestation data from counterparties in order to find out whether those counterparties are compliant with CSP controls.

The work of the Counterparty Cyber Risk Management Forum (CCRM) has been key to developments in this area. Comprising entities in the SWIFT community, it was formed in early 2019. A CCRM guide was also published, focused on the sharing and integration of counterparties' cyber risk data into institutions' existing risk management processes.

**This practice benefits the financial community in several ways.**

| | |
|---|---|
| **1. Counterparties** | Counterparties that allow attestation data to be used in this way can raise their profile and engender trust with other entities by demonstrating a 'clean bill of health.' Without this, financial institutions could find they are subject to additional security measures when doing business. |
| **2. Supervisors** | Supervisors benefit from a stronger ecosystem if their supervised entities allow their attestation data to be used. |
| **3. Financial Institutions** | Financial institutions can use their counterparties' attestation data to identify counterparties that are not yet compliant with key controls, and integrate that data into their risk frameworks. |

## Learn from the early adopters

Many institutions may wish to use their counterparties' attestation data to better manage risks, but don't always know where to start. Now there is an opportunity to learn from leading financial institutions that have taken the initiative and are already using CSP attestation data to gain more insights into their counterparties.

Following on from our previous publication, Assessing Cybersecurity Counterparty Risk – A Getting Started Guide, and building on the information and good practices shared by the CCRM forum, this ebook explores how you can use counterparty attestation data to measure risk more effectively. In the following pages, leading institutions share the insights they have gained as early adopters. They also identify some key success factors that can help others make the most of counterparty attestation data – from the methodology and processes needed, to the importance of communicating effectively with internal and external stakeholders.

# 3

# Collecting and assessing attestation data

**There is a clear opportunity for financial institutions to use counterparty attestation data to help them assess the way they interact and do business with those counterparties.**

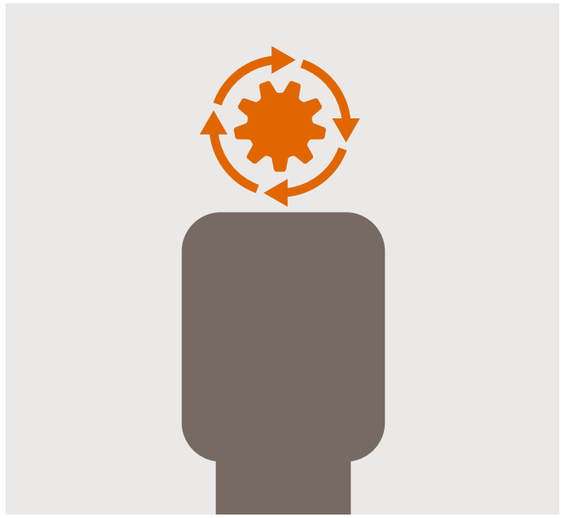
**First you need to have processes in place to collect and assess CSP data.**

At the simplest level, attestation data can be collected using SWIFT's KYC-SA application. Beyond that, different financial institutions may approach the task in different ways. Some request attestation data from all their counterparties, whereas others focus on specific groups such as high-risk countries.

**"We've got a number of different data sets that help us get comfortable with the counterparties we deal with. And CSP data is one of those critical data points."**

**Brad Lustig —** Global Transaction Banking – Risk Executive at Bank of America

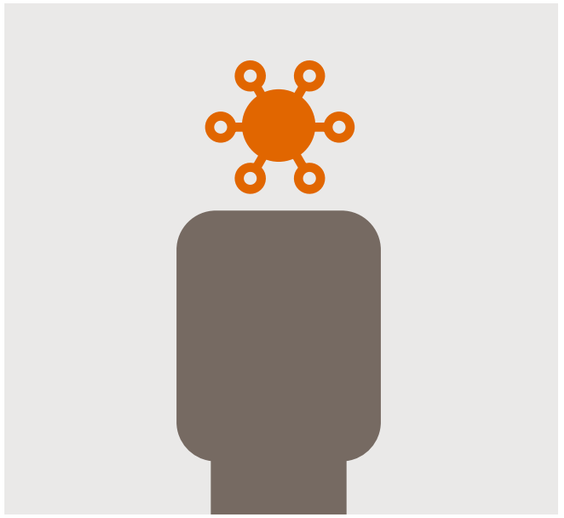
## Managing the data that has been gathered



### Manual or automated?

While some opt for spreadsheets, others have built in-house tools to consume their attestation data. For example, Kamal Mohanty, SVP Cyber Risk, Global Payments & Receivables at Citi's Treasury and Trade Solutions group, explains that the bank's internally developed application ingests SWIFT's KYC-SA report for analysis. The application reduces manual touchpoints and also builds the foundation for SWIFT's CSP API integration, when launched.

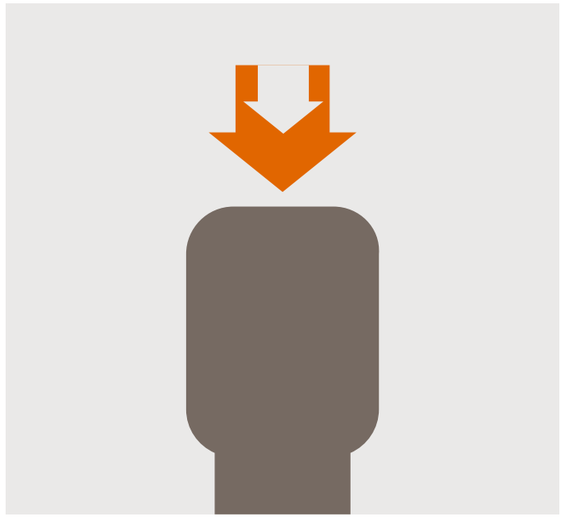
BNY Mellon, meanwhile, is currently exploring the possibility of incorporating a real-time data feed using APIs that could help them aggregate data and track metrics over time.



### Holistic view

As well as addressing compliance gaps, financial institutions are also incorporating CSP data into their existing risk frameworks and reviews. "Citi continually enhances its comprehensive multi-faceted risk reviews, designed around holistic data elements including relevant counterparty CSP data," says Mohanty.

"The advent of the CSP tool has been a huge help for us," adds Bank of America's Lustig. "We do very thorough annual portfolio reviews and client reviews for clients that fit into that high-risk spectrum, and those routines incorporate a lot of our risk partners across the bank. We have now embedded a review of CSP scores into that process."



### Negative news

Leading financial institutions are also increasingly referring back to their counterparties' attestation data in response to external events. For example, if the bank hears negative news about a particular region or type of entity that is currently being targeted by cyber criminals, there is the option of drilling down into relevant entities' CSP scores to check for any weaknesses.

"If a counterparty were to disclose an event to us, we could then track this back to their CSP attestation data and ask, 'How did this bank fail in terms of those controls, versus what's actually happened?'" explains Andrew Pamphilon, Network Manager at Standard Bank.

# 4

# Handling non-compliance

## While financial institutions report that most of their counterparties are fully compliant with CSP controls, a minority may fall short of full compliance in the following ways:

1

**Counterparties do not comply with all CSP controls.** If counterparties do not meet all the controls, financial institutions need to decide how to proceed. One consideration is that some CSP controls are mandatory, whereas others are advisory. Some institutions may carry out a ranking exercise to identify which of the CSP controls are the most critical.

2

**Attestation has expired.** A recently expired attestation may not be a major concern. However, an attestation that expired six months ago could indicate a lack of stringent cybersecurity management that institutions may decide to investigate.

You'll need to decide for yourself how to handle each of these scenarios. In some cases, this may mean initiating a one-to-one communication process with counterparties that fall short of full compliance, and/or tracking their progress in adopting any missing controls.

On occasion, counterparties may fail to submit attestation data. This can be due to a number of reasons, including lack of resources.

In some cases, missing data may simply be an oversight. "We have had cases where the counterparty came back and said they had saved the attestation as a draft," says Alexander Reinecke, Senior Product Manager Industry Engagement and Transaction Surveillance at Deutsche Bank.

Some institutions may decide not to share attestation data with their counterparties based on internal policies or other reasons. In these situations, financial institutions may be concerned about the possible reasons why, such as a weakness in their controls.

**Enhancing CSP processes**

Several financial institutions initially found that some counterparties did not respond to their requests for attestation data. However, this issue was largely addressed with the introduction of the 'Grant All' feature in November 2020.

For counterparties that have opted in, Grant All automatically grants all requests for attestation data from existing correspondents – considerably reducing the number of data requests that go unanswered.

In another development, SWIFT has introduced an additional layer of assurance for attestations. As of 2021, all attestations must be supported by an independent assessment, including a review of existing controls and their efficiency, and confirmation that they support compliance with the relevant CSP controls. The independent assessment can be performed by internal and/or external resources, and a directory of CSP assessment providers is available on swift.com.

### Taking action

If counterparties refuse to share attestation data, or fall short of compliance with key controls, this may affect the decisions financial institutions make about those relationships. As Bank of America's Lustig observes: "If we're expanding business with a client that refuses to share that information, it's absolutely going to be a factor in our decision-making as to whether we want to proceed or not."

In some cases, the actions financial institutions take to address non-compliance may vary depending on whether the counterparty in question is a new or existing relationship.

"We've drawn a line in the sand, which basically says that if a counterparty does not comply with all mandatory controls, we will not onboard them – we're quite upfront about that," says Tony Valente, Senior Manager, Economic Crime Prevention, Commercial Banking, Lloyds Bank. "I think there's a bit more complexity with existing relationships. That's where we really have to understand the other factors, and see if there's anything else we can draw comfort from."

Leif Simon, Director, Transactions Surveillance Solutions, Deutsche Bank, adds: "Ultimately the intention is to continue doing business with our counterparties. We want to avoid a situation where we have to pull the plug."

### Context matters

Financial institutions should also look at attestation data in the context of other information about those relationships. For example, counterparties may be able to demonstrate that they address a particular CSP control using an alternative approach.

### Market considerations

In some markets, there may be few alternative providers available, meaning it is not necessarily feasible to draw a line in the sand. "If you're a global bank, you have the power of choice and the CSP information is a bit more actionable," comments Victor Abiola – Global Head, Operational Risk, Corporate and Investment Bank at Standard Bank.

However, as Abiola notes, there are still options available when it comes to addressing a shortfall in controls. "If you don't have those choices, and the only partner you depend on in a particular country doesn't have those strong controls, how do you make a decision about that? It might be that you focus on working it out with that bank, or improving the dialogue," he explains.

# 5

# Success factors

# So what are the factors that you need to consider when getting the most out of your counterparties' attestation data? Leading banks have identified the following areas as key to success:


5.1 Methodology →

5.2 Resources →

5.3 Communication →

5.4 Tools and processes →

5.5 Community →

# 5.1 Methodology

It is essential to define what you plan to do with counterparty attestation data once it has been gathered. “In our case, because there are not many examples of non-compliance, we felt the most logical thing was to approach any counterparties that are not meeting a control, and have direct bilateral contact with them to find out what happened,” says Deutsche Bank’s Simon.

In addition, some users might consider some CSP controls to be particularly crucial, and focus on those accordingly. “We have come up with a handful of core controls that we believe are critically important,” says Raghu Srinivasan, Managing Director, Treasury Product Executive, Bank of America. “Whether counterparties are compliant with those specific controls factors heavily into our understanding of the risk that the counterparty brings to the portfolio.”

### Centralised approach

BNY Mellon has opted to centralise the management of counterparty attestation data through a central control team. “That is important because it ensures that we have a consistent approach to the framework, how we’re looking at the data, and how we’re measuring it across our lines of business,” explains Joanne Cash, Head of Operations Control Management, BNY Mellon. “Then we bring relevant experts to the table to look at what we’re pulling together on their behalf.”

She adds that this has enabled the bank to develop expertise not only on the completion of its own attestations, but on the consumption of counterparty attestations, and managing any questions that arise.

Standard Bank, has also centralised the management of counterparty attestation data within a central team based in South Africa. “The nature of the issues is quite multi-departmental,” comments Abiola. “So it was quite important, especially at the beginning, to have different perspectives in the room on how we were going to use the data.”

### Finding a home for the project

For Lloyds Bank, one initial challenge was the lack of a ‘natural home’ for the project, particularly because – unlike KYC – it is not a regulatory requirement. “It didn’t fit neatly into the KYC process, because assessing CSP compliance for a new relationship comes before KYC has even started,” says Valente. “Nor did it fit into our financial crime risk framework, which is very specific.” Ultimately, the team opted to build attestation data into the bank’s payment services policy – “and from that, we were able to build the necessary risk management approach and get the accountabilities assigned.”

### Risk-based approach

Another key decision is how many counterparties you should target in the first instance. While some financial institutions may aim to request attestation data from all their counterparties, others may prefer a more iterative approach, focusing on the biggest-risk counterparties first.

**Tips for your institution**

“If you can’t do everything in one go, I would recommend that you do as we did – define a risk-based approach that helps you to prioritise the counterparties you want to request, and then work through them in order.”

**Leif Simon —** Director, Transactions Surveillance Solutions, Deutsche Bank

# 5.2 Resources

As with any project, it's essential to have the right resources in place. An important step is getting engagement from all relevant stakeholders and gaining senior sponsorship.

"We set up a small team covering our internal efforts to work with the CSP programme, both in terms of our own self-attestation, and also in terms of consuming and making sense of counterparty data," says Deutsche Bank's Simon. "The important thing was to involve a number of stakeholders right from the beginning – the earlier you get everyone on board, the easier it is to work as a team."

In practice, there are a number of stakeholders to consider, from key subject matter experts for the lines of business to risk, compliance and legal teams, as well as internal and external auditors.

"We have operationalised our CSP Consultation and Consumption efforts for new and existing clients. This approach has helped streamline and progress the CSP programme, and in sharing ongoing information with relevant stakeholders, including client oversight and relationship divisions," comments Citi's Mohanty. "As an organisation, this contributes to the ongoing conversation on the risk(s) when making decisions about a relationship."

### Bringing in resources

In some cases, the project may call for additional resources. Lloyds Bank, for example, opted to bring in an external contractor to help develop the process.

"He wasn't from a financial crime or cybersecurity background, but he did understand how things work in large financial institutions in terms of management information and reporting," says John Baggott, Senior Manager, Payments, Industry & Development, Lloyds Bank.

"He established a process to consistently interpret the information received from counterparties, where they fell short of compliance and where they had plans to remediate; and he was able to present that information in an easily digestible way."

With the process developed, the contractor was able to hand the resulting model over to a business as usual team. Key to this approach, notes Baggott, was being able to explain the importance of cyber controls to senior management in order to secure the necessary budget.

**Tips for your institution**

"Aligning teams and deciding who should be involved – both on your side and on your counterparty's side – will be more and more important as you get more into using CSP data to form appetite, make decisions or conduct follow-up due diligence with counterparties."

**Victor Abiola —** Global Head, Operational Risk, Corporate and Investment Bank, Standard Bank

# 5.3 Communication

Another important success factor is the ability to communicate effectively about the CSP programme, both within the organisation and with external stakeholders.

### From general updates to targeted discussions

Deutsche Bank's Simon explains that communication efforts include providing general information about the CSP programme widely within the bank.

"Then, of course, we had more focused communications for target groups such as sales and client managers so they understood what they needed to do with counterparties flagged as non-compliant."

BNY Mellon, likewise, provides talking points to relevant front-office staff to help them answer questions from counterparties or clients. Other initiatives include an intranet site that provides links to resources on the SWIFT website, as well as an FAQ document to ensure questions are responded to with a consistent message.

### Set a drumbeat for your activity

Other communication measures may include monthly working groups to review counterparty attestation data and updates from internal and external audit teams. Oonagh McGrane, Director, FI Commercialisation, Client Products at Lloyds Bank, says that a monthly forum enables the bank to review progress and exceptions in a structured way. "That provides an effective drumbeat to the activity," she adds.

### Communicating with clients

And, of course, a key part of managing attestation data is communicating with counterparties to understand any issues or queries that may arise in relation to controls and compliance.

"It's about reaching out to those clients and understanding any mitigations before any decision is made against appetite," says Baggott from Lloyds Bank. "It's also about understanding what the client intends to do to close those gaps – so it's quite an open dialogue."

**Tips for your institution**

"Invest upfront in creating documents and putting information in one place so you can direct people to it, instead of having to answer the same questions every time they come in. Otherwise you're going to end up buried in requests."

**Joanne Cash —** Head of Operations Control Management, BNY Mellon

"Socialising the Customer Security Programme initiative at various internal forums will help increase organisational awareness and the cyber resilience value one can get from CSP consultation and consumption."

**Kamal Mohanty –** SVP Cyber Risk, Global Payments & Receivables, Citi

"Keep those channels of communication open with the different business lines, because they're the ones that are working with the counterparties."

**Kevin Domaratius —** Senior Associate, Operations, BNY Mellon

# 5.4 Tools and processes

When it comes to tools and processes, there is more than one way to approach the management and analysis of attestation data.

For financial institutions that have a sizeable number of counterparties, the first step is to download the counterparty attestation report available on the KYC-SA tool. The data can then be reviewed, with different criteria applied to identify counterparties that fall short of full compliance with the controls.

### Getting started

As Deutsche Bank's Reinecke explains, the "bare minimum" needed to get started is having the core roles in place to operate the KYC-SA portal, both for counterparty attestation consumption and to manage your own CSP attestation.

"We take a report from the KYC-SA tool," Reinecke comments. "It is possible to download a number of reports, including one that lists all the controls, mandatory and advisory, along with the controls status and some other base data of the counterparty."

From there, the bank applies logic to interpret the data. "We read out which control is compliant, which is not compliant, which is compliant by a given date and whether the attestation is expired or valid. This flows into reporting that we regularly do internally, and map against those parties we have requested access to."

### In-house tools vs spreadsheets

Some institutions opt to build internal tools in order to handle their counterparty attestation data. As mentioned earlier, Citi, for example, downloads data from KYC-SA and uploads it to an application for data interpretation. BNY Mellon, likewise, has built a process and a tool structure that incorporates a lot of the detail provided by SWIFT's report.

Other approaches can also work very effectively. "As far as the process goes internally, it doesn't need to be anything complicated," says Lloyds Bank's Baggott. "A simple spreadsheet and PowerPoint deck is all we required. The portal provides all the data you need to consume – you can then just leverage existing ways of working."

**Tips for your institution**

"The number of counterparties we interact with is significant and we are able to manage CSP consultation and consumption at scale by focusing on automation. Institutions with fewer counterparties can also start their CSP journey by manually managing their data."

**Kamal Mohanty —** SVP Cyber Risk, Global Payments & Receivables, Citi

# 5.5 Community

Last but not least, community has an important role to play for financial institutions looking to make the most of their attestation data. In a post-pandemic world, you should take any opportunity to meet with your peers and share experiences.

One important resource has been SWIFT's group of peer global transaction banks. Communicating with them has enabled information sharing about how best to handle attestation data, as well as providing an opportunity to discuss potential operational enhancements.

"The community element has definitely helped by providing us a common platform for bi-lateral conversation regarding cyber resilience," says Citi's Mohanty.

"By working together, we can strengthen the community, and also share lessons learned and best practices. For example, during a counterparty CSP conversation, we discussed the topic of staying resilient while evolving with virtualisation, and both parties walked away with innovative industry approaches."

Beyond the CSP, financial institutions can tap into further opportunities for information sharing. "We don't just receive information from SWIFT and from the CSP – there are also other information-sharing activities that go on at a senior level within the IT intelligence community," says BNY Mellon's Cash. "That information, handled on a need-to-know basis, can provide insights that you can use to research a particular CSP control."

**Tips for your institution**

"This isn't competitive – it's in the interest of the whole community. So let's keep talking and helping each other reach a fully compliant position."

**John Baggott —** Senior Manager, Payments, Industry & Development, Lloyds Bank

6

# Best practices: A planning and execution checklist

# Here are some key actions you can take to start using your counterparties' CSP attestation data to enhance risk management within your organisation:

- ☑ Gain senior sponsorship and engage all relevant stakeholders.
- ☑ Make sure the necessary resources are in place – consider bringing in external resources if necessary.
- ☑ Decide which counterparties you will ask for data. This could be every counterparty – or it may be preferable to focus on high-risk counterparties in the first instance.
- ☑ Communicate internally and with external stakeholders – intranets, FAQs and monthly forums can help to drive knowledge and consistency.
- ☑ Depending on your business, prioritise which CSP controls are the most critical for your firm. This might mean differentiating between mandatory and advisory controls, or even ranking mandatory controls to identify the most important to you.
- ☑ Building an automated tool can be advantageous for large institutions with high numbers of counterparties, but plenty can be achieved using spreadsheets and manual processes.
- ☑ Take advantage of opportunities to meet with peers and share experiences.

7

# Conclusion

**CSP attestation data may not be a silver bullet. But when it comes to assessing counterparty risk, it is a valuable addition in the toolbox that you can use very effectively alongside other available data points.**

**While some financial institutions may face challenges in terms of securing the resources needed to get value from counterparty data, the insights shared by early adopters make it clear that there are plenty of ways for financial institutions of all sizes to benefit.**

For example, while some financial institutions may ask all counterparties for attestation data, others may benefit from focusing on high-risk counterparties in the first instance. Another consideration is that automated tools can be a valuable approach if you have a high number of counterparties – but there is still much that can be achieved using readily available tools such as Excel.

Counterparties' CSP attestation data can help you improve cybersecurity in a way that is both affordable and accessible. And as Deutsche Bank's Simon notes, "The single most important piece of advice I could give anyone is to just get going and start requesting the data."

# More information

To discuss how you can use CSP counterparty attestation data to enhance your cyber risk management, contact: csp.communications.generic@swift.com

For more information about the SWIFT Customer Security Programme, visit www.swift.com/csp.

For more information about our Financial Crime Compliance solutions, including Payment Controls for enhanced fraud detection and prevention, visit www.swift.com/fcc.

Thank you to all the contributors to this ebook from participating financial institutions: Bank of America, BNY Mellon, Citi, Deutsche Bank, Lloyds Bank and Standard Bank.

We would also like to thank CLS for the insights they contributed to the Assessing Cybersecurity Counterparty Risk– A Getting Started Guide, which this ebook builds upon.

**Building a stronger community**

As part of SWIFT's continuing commitment to sharing data and strengthening the financial services ecosystem, we take part in a number of initiatives to help organisations improve cybersecurity. These include:

- Partnering with the Carnegie Endowment for International Peace and the World Economic Forum (WEF) to provide a toolkit to help financial institutions enhance their cybersecurity.
- Providing CSP data to the world's leading anti-virus providers, thereby promoting collaboration and data sharing while strengthening cybersecurity efforts across industries.
- Sharing data with central banks via the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB).