



EUROPEAN CENTRAL BANK

EUROSYSTEM

# Cyber Information and Intelligence Sharing Initiative (CIISI-EU)

*Cyber information and intelligence  
sharing: a practical example*

Euro Cyber Resilience Board Secretariat

September 2020



# Contents

<b>1</b>	<b>Foreword by the ECRB Chair</b>	<b>2</b>
<b>2</b>	<b>Executive Summary</b>	<b>3</b>
<b>3</b>	<b>Introduction, ECRB Context and Objectives of CIISI-EU</b>	<b>5</b>
<b>4</b>	<b>Members of the CIISI-EU Community</b>	<b>8</b>
<b>5</b>	<b>CIISI-EU Overarching Design Principles</b>	<b>10</b>
<b>6</b>	<b>CIISI-EU Buildings Blocks for the Target Operating Model</b>	<b>11</b>
<b>7</b>	<b>Protocols for Sharing Intelligence</b>	<b>13</b>
<b>8</b>	<b>Organisation and Roles</b>	<b>19</b>
<b>9</b>	<b>Managing the Risks</b>	<b>23</b>
<b>10</b>	<b>Key Success Factors</b>	<b>25</b>
<b>11</b>	<b>Guidance on Design, Implementation and Operationalisation Phasing</b>	<b>27</b>
<b>12</b>	<b>Getting Further Information</b>	<b>33</b>

# 1 Foreword by the ECRB Chair

*“Financial market infrastructures are crucial for intermediation between market participants and end users. They are essential for the everyday livelihood of European citizens, for instance by transmitting salary and pension payments. They are vital for the functioning of the financial system and the financing of the real economy, as they settle market transactions through a web of settlement banks, clearing houses, settlement systems and custodians.*

*Protecting the integrity of market infrastructures is critical for the functioning of the financial system. Cyberattacks are already used to harm companies and to interfere with national and international interests. Cyberattacks against financial market infrastructures would undermine confidence in the financial system, with repercussions on the economy as a whole. Fending off these attacks is therefore a matter of European security.*

*Exchanging cyber information and intelligence among peers within a trusted community including major financial infrastructures allows members of that community to leverage their collective knowledge, experience and capabilities to address the threats they may face. It enables them to make informed decisions about their defensive capabilities, threat detection techniques and mitigation strategies. By sharing cyber information and intelligence, financial infrastructures act in the public interest to support the safe and sound operation of the entire financial system.*

*To facilitate this, in February 2020 the members of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)<sup>1</sup>, established the Cyber Information and Intelligence Sharing Initiative (CIISI-EU)<sup>2</sup>, which is currently being implemented.*

*We should not underestimate the significance of this step. Never before have pan-European financial infrastructures and related central banks, in close liaison with Europol and the European Union Agency for Cyber Security (ENISA), come together and agreed to share information and intelligence. For years, the industry has talked about sharing information and intelligence, but few and insufficient initiatives have been taken in that direction.*

*While the ECRB and - with it - CIISI-EU are “closed” initiatives, aiming at a specific group of financial infrastructures and authorities, the philosophy and design of CIISI-EU can be a source of inspiration for other communities and stakeholders, within and outside the financial sector, within and outside Europe. Therefore, this ECRB Secretariat paper provides a practical example on how to share cyber information and intelligence. I hope that other communities will take inspiration, so we can continue to strengthen cyber resilience at national, European and even global level.”*

**Fabio Panetta, Member of the Executive Board, European Central Bank**

---

<sup>1</sup> [ECRB web page](#)

<sup>2</sup> [CIISI-EU press release](#)

## 2 Executive Summary

Cyber threats pose a serious risk to the stability of the European and global financial system. Cyber threats are borderless and the capabilities of the attackers are constantly evolving, threatening to disrupt the interconnected global financial systems. To successfully combat cyber risk, entities<sup>3</sup> need to actively participate in information and intelligence sharing arrangements and collaborate with trusted stakeholders within the industry as a whole.

The Cyber Information and Intelligence Sharing Initiative (CIISI-EU) is a multilateral cyber information and intelligence sharing initiative, which brings together a community of public and private entities, to facilitate the systematic and structured sharing of vital strategic, operational and tactical cyber information and intelligence as well as best practices among themselves.

The CIISI-EU members act as a self-selecting, like-minded community that seeks to drive cyber information and intelligence sharing.

The core objectives of CIISI-EU are to protect the financial system by preventing, detecting and responding to cyberattacks; to facilitate the sharing of information, intelligence and best practices between financial infrastructures; and to raise awareness of cybersecurity threats.

The CIISI-EU Community is comprised of pan-European financial infrastructures, central banks (in their operational capacity), critical service providers, ENISA and EUROPOL, as represented in the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB).

The CIISI-EU Community shares vital strategic, operational and tactical information and intelligence among themselves using an automated platform; and creates a trusted community where they will meet to discuss cybersecurity threats and share related information, intelligence and best practices.

By exchanging cyber information and intelligence within the CIISI-EU Community, members can leverage the collective knowledge, experience and capabilities of the sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-based decisions regarding defensive capabilities, threat detection techniques and mitigation strategies.

---

<sup>3</sup> The term will be broadly used herein to include central banks, payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector.

CIISI-EU is a market-driven initiative, for the market, by the market, with the ECB contributing in its catalyst function. Authorities in their capacity as regulators, overseers and/or supervisors are not part of the CIISI-EU Community and regulatory reporting on cyber incidents and data breaches are outside the scope of the information and intelligence sharing within the CIISI-EU Community.

## 2.1 Purpose of This Document

This document provides an overview of CIISI-EU and the building blocks of the initiative. This document is not a detailed, prescriptive method, but a summary of the approach taken by the members of the ECRB. It provides overarching guidance, structure and inspiration to other entities, communities, sectors and jurisdictions, who may consider building their own cyber information and intelligence sharing initiative, in a flexible manner that suits their own specificities. CIISI-EU is an evolving initiative, and will be enhanced over time as the members foster trust and collaboration, and share common experiences.

This document is aimed at:

- Central banks, payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector
- National cybersecurity and law enforcement agencies
- Public authorities at national and European levels
- Organisations interested in providing cyber threat intelligence services, platforms and other technical services

Although CIISI-EU is aimed at financial infrastructures, it can be applied by other communities within and outside the financial sector, at national, European or even at global level.

Any further enquiries about CIISI-EU should be directed to [ECRB@ecb.europa.eu](mailto:ECRB@ecb.europa.eu)

## 3 Introduction, ECRB Context and Objectives of CIISI-EU

### 3.1 Introduction

The cyber threat is borderless and the capabilities of the adversaries are constantly evolving, readily scalable and increasingly sophisticated, threatening to disrupt the interconnected global financial systems. Threat actors are highly motivated and can be persistent, agile, and use a variety of tactics, techniques and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. To counter the threat and address the risk, entities are required to also be dynamic and agile. Amongst other things, entities should have effective cyber threat intelligence processes and actively participate in information and intelligence sharing arrangements and collaborate with trusted stakeholders within the industry.

Cyber information and intelligence is any information that can help an entity identify, assess, monitor, defend against and respond to cyber threats. Examples of cyber information and intelligence include indicators of compromise (IOCs), such as system artefacts or observables associated with an attack; motives of threat actors; TTPs; security alerts; threat intelligence reports; and recommended security tool configurations.

By exchanging cyber information and intelligence within a sharing community, entities can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-informed decisions regarding defensive capabilities, threat detection techniques and mitigation strategies. By correlating and analysing cyber information and intelligence from multiple sources, an entity can also enrich existing information and make it more actionable (e.g. by sharing effective practical mitigations). This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information. Entities that receive and use this information and intelligence impede the threat's ability to spread and subsequently raise their individual level of protection. Moreover, by impeding the potential contagion of such threats, the community acts in the public interest by supporting the safe and sound operation of the financial system as a whole.

In light of the above, on 27 February 2020, the ECRB members agreed to establish and join the Cyber Information and Intelligence Sharing Initiative (CIISI-EU).<sup>4</sup>

---

<sup>4</sup> [CIISI-EU press release](#)

## 3.2 The Context for Developing CIISI-EU

At the December 2018 ECRB meeting, it was agreed that given the interconnectedness of the European financial sector, meaningful information and intelligence sharing among pan-European financial infrastructures was a key requisite for a resilient European financial system. The ECRB agreed to establish a working group to develop the building blocks for a trusted network for information and intelligence sharing among the members of the ECRB.

The working group noted that the EU landscape on cyber information and intelligence sharing is fragmented from three different perspectives: geography, sector and content. It appeared that EU countries were at different levels of maturity with regard to establishing meaningful information and intelligence sharing arrangements, while it was not clear to what extent entities and related relevant authorities were connected to such arrangements at national level. Next to that, there appeared to be no EU-wide information and intelligence sharing arrangement specifically for financial infrastructures active at pan-European level. Finally, although the concept of information and intelligence sharing was widely supported by market participants and authorities alike, there was no clear common understanding what “information and intelligence” was in the context of cyber security and cyber resilience and how to share this information and intelligence.

In 2019-20, the working group defined the core objectives of information and intelligence sharing amongst the ECRB participants. In order to fulfil the objectives, and develop a structured approach to information and intelligence sharing, the working group thereafter set out: what levels, types and attributes of information and intelligence should be shared (within a common taxonomy); who such information and intelligence should be shared with; when (in terms of frequency) such information and intelligence should be shared; the format for sharing such information and intelligence; and how such information and intelligence should be shared.

In the context of how to share information and intelligence, the working group also explored a number of possible market solutions, which could be used to optimally share information and intelligence between ECRB members, taking account of the effectiveness, usability, security and cost of such solutions.

Based on this structured approach, analysis and the possible solutions, the working group developed a target operating model for information and intelligence sharing. On the basis of the work done, on 27 February 2020, all ECRB members agreed to establish and join the Cyber Information and Intelligence Sharing Initiative (CIISI-EU).

CIISI-EU is a multilateral cyber information and intelligence sharing initiative, which brings together a community of public and private entities, to facilitate the systematic and structured sharing of vital strategic, operational and tactical cyber information and intelligence as well as best practices among themselves, via technical platforms, calls and in-person meetings, based on commonly agreed taxonomies and sharing conventions. CIISI-EU is comprised of a number of core integrated building blocks, which are bound together by a common CIISI-EU Terms of Reference and Community Rulebook, to ensure that members can collaborate in a coherent and effective manner.

### 3.3 Core Objectives of CIISI-EU

The core objectives of CIISI-EU are to:

- Prevent, detect, respond and raise awareness of cybersecurity threats to the CIISI-EU Community members, thereby discharging a public interest responsibility;
- Enable relevant and actionable intelligence sharing within the CIISI-EU Community, with Law Enforcement and potentially to the wider ecosystem to better protect the European financial sector against cybersecurity threats;
- Encourage active contribution and active participation within a 'trusted circle', rather than passive consumption or weak usage;
- Synthesize and actively propagate the sharing of strategic intelligence in addition to operational TTPs and tactical IOCs; and
- Continuously learn and evolve, as a collective, with regard to the process of analysing, developing and sharing cyber information and intelligence.



## 4 Members of the CIISI-EU Community

The CIISI-EU community is comprised of pan-European financial infrastructures, central banks (in their operational capacity), critical service providers, ENISA and EUROPOL, as represented in the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB).

The key stakeholders in the overall implementation of CIISI-EU are: the CIISI-EU Secretariat, the CIISI-EU Community members (see below); the third-party cyber threat intelligence provider<sup>5</sup> and the third-party platform provider CIRCL (MISP).

- Banca d'Italia
- Banco de Espana
- Banque Centrale du Luxembourg
- Banque de France
- BME
- CLS Bank International
- Danmarks Nationalbank
- De Nederlandsche Bank
- Deutsche Börse Group
- Deutsche Bundesbank
- EBA Clearing
- European Central Bank
- ENISA
- equensWorldline
- European Central Counterparty N.V.
- Euroclear
- Europol
- Iberpay
- Krajowy Depozyt Papierów Wartościowych

<sup>5</sup> The CIISI-EU third-party cyber threat intelligence provider has been selected on the basis of a thorough procurement process. If other prospective sharing communities consider setting up a similar initiative, they would need to conduct their own procurement process for the third-party cyber threat intelligence provider and the third-party platform provider.

- London Stock Exchange Group (on behalf of LCH SA and Monte Titoli)
- Mastercard Europe SA
- Nasdaq Nordic (on behalf of Nasdaq Clearing and Nordic Exchanges)
- Nationale Bank van België/Banque nationale de Belgique
- SIA
- STET
- SWIFT
- TARGET Services
- Visa Europe

## 5 CIISI-EU Overarching Design Principles

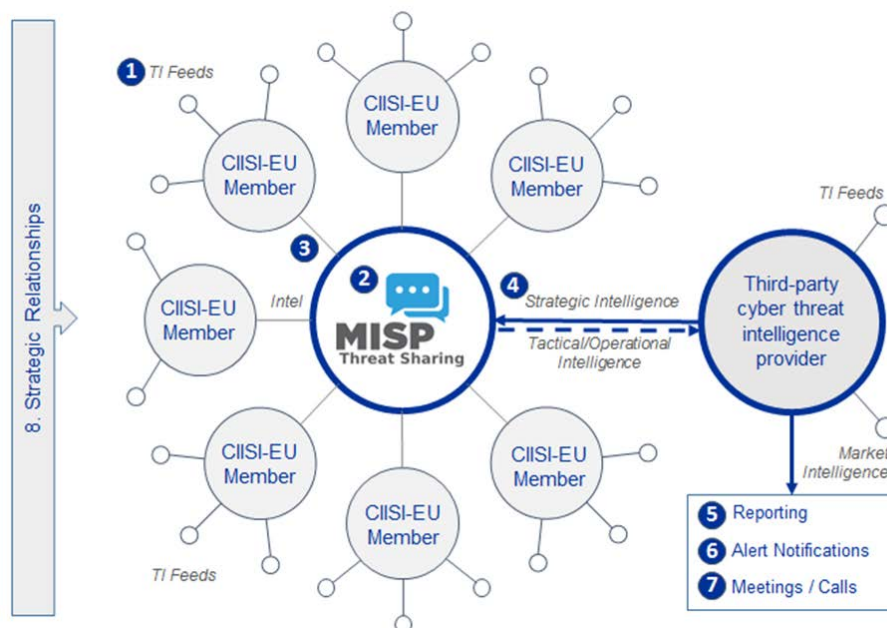
The development and operationalisation of the initiative has been a complex endeavour given the size and complexity of the different entities involved, and the need to ensure that any model can cater for all entities and satisfy all specificities and nuances.

The overarching criteria for any multilateral initiative to be successful from the development phase to final operation is that there must be strong stakeholder management; close collaboration and cooperation; a clear collective vision and commonly agreed principles; and a strong control environment and culture, that considers all the risks and can adequately mitigate them.

From the very inception, the working group designed the model based on a number of design principles. It was commonly agreed that CIISI-EU should:

- Not 'reinvent the wheel' but should re-use proven components (commercial / open source) and use best practices
- Go beyond just recirculating known tactical / operational Indicators of Compromise (IOCs) and add value through dissemination of strategic information
- Be practical and (relatively) easy to implement
- Have strong usability to encourage strong uptake and usage across all members
- Be ambitious but start small and only scale when it works
- Be cost-efficient and allow any costs to be aggregated and shared across all members
- Allow members to implement at their own pace
- Focus on sharing between members and should exclude regulatory / supervisory reporting
- Create a culture of openness, cooperation and collaboration, not competitiveness nor fear of regulatory judgement.

## 6 CIISI-EU Buildings Blocks for the Target Operating Model



At the highest level, the CIISI-EU Community members defined a target operating model which comprised of a number of core building blocks:

1. **Threat Intelligence Feeds:** CIISI-EU Community members already have existing commercial and open source feeds, which provide them with cyber threat information and intelligence. CIISI-EU Community members can keep their existing threat intelligence feeds. If information from these sources are relevant for the CIISI-EU Community, members can share them voluntarily and on a best efforts basis to the extent legally and contractually possible
2. **Central Shared Platform / MISP:** MISP is an open-source threat intelligence platform for sharing cyber security information and is funded by the Computer Incident Response Centre Luxembourg (CIRCL) and the European Union. As the core central platform, MISP was selected for its vendor neutrality which prevents longer-term 'lock-in'. CIRCL is responsible for hosting the CIISI-EU MISP platform and each CIISI-EU member will connect to the CIRCL's hosted central MISP platform in one of three ways. Each CIISI-EU Member: i) can host its own MISP instance at its own premises, which can connect to the central MISP platform, ii) can connect directly to the central MISP platform using secure web browser, or iii) can interface its existing, in-house technical platform to the central

MISP platform. In all cases, the network of MISP connections will synchronise with each other and the collective will operate as a closed and trusted group

3. **Information and Intelligence Sharing:** CIISI-EU Community members will elect what information or intelligence is important enough to warrant disseminating onto the shared platform via their MISP instance – the principles, conventions and taxonomies for such sharing are outlined in a later section
4. **Strategic Analysis:** The third-party cyber threat intelligence provider will have access to the centralised MISP platform and will add value through the synthesis of strategic analysis based on the collective tactical and operational intelligence being shared on MISP and based on their own knowledge of the cybersecurity threat landscape
5. **Reporting:** The third-party cyber threat intelligence provider will produce strategic intelligence, monthly dashboards and bi-annual reports, the latter focussed at Board level and written in business language, as well as other more bespoke reports (when required). The analysis will be presented at the bi-annual in-person ECRB meetings and will be available on the provider's intelligence portal. The strategic reports will typically cover monthly threat assessments, strategic intelligence update by threat actor and significant global cyber events of relevance to the financial system.
6. **Alert Notifications:** An alerting mechanism to the CIISI-EU Community will be provisioned via SMS text, e-mail distribution, or by using other collaborative tools ensuring appropriate security and confidentiality requirements are met. The notifications will alert CIISI-EU Community members of new information and intelligence placed on the platform, which may be critical to their operations
7. **Trusted group Calls / Meetings:** A core tenet of CIISI-EU are the trusted group calls and in-person meetings. The calls and meetings are held on a regular basis with the CIISI-EU Community members and the third-party cyber threat intelligence provider, to share intelligence and foster trust within the CIISI-EU Community. The trusted group calls are held on a regular basis, typically every month, and trusted group in-person meetings are held twice per year. In both cases the third-party cyber threat intelligence provider will take the lead in analysis, organisation and direction. The discussions will be confidential without meeting minutes. At least one staff member from each CIISI-EU Community member is expected to attend the calls and meetings and openly share information and intelligence with each other
8. **Strategic Relationships:** The CIISI-EU Community is a so-called “closed” community, but intend to build strategic relationships with other information sharing communities to enrich the information and intelligence and to bridge communities

# 7 Protocols for Sharing Intelligence

## 7.1 Categories of Information and Intelligence to be Shared

The CIISI-EU Community shares Strategic, Operational and Tactical information and intelligence:

- **Strategic** - Strategic information/intelligence refers to the contextual framework which shapes an adversary's operating environment and intended course of action. It is designed to explore the 'Who and Why' of an entity's threat landscape. The sharing of strategic information and intelligence drives decision makers and planning in the mid to long term, typically at senior level. In this instance, strategic information and intelligence supports the CIISI-EU Community on setting strategy and objectives based on the changing landscape and future considerations.
- **Operational** - Operational information/intelligence involves trend analysis of adversary capabilities and attack methodologies. It is concerned with the 'When, Where and How' of an attack campaign and implies an understanding of adversarial skillset. Analysing an adversary's campaign history allows the analyst to identify characteristic attack vectors and patterns of behaviour that can be used to proactively identify the likely precursors of an impending attack and defend against it (e.g. group X previously targeted my network before event Y; my entity should prepare for a similar campaign when event Y reoccurs). Sharing of operational information and intelligence drives intelligence and security operations in order to support 'Business as usual' security objectives and decision making.
- **Tactical** - Tactical information/intelligence refers to the visibility of the tools and hacking methodologies used by cyber adversaries to breach victim networks. High quality, actionable tactical information/intelligence gives a unique insight into hackers' methods/capabilities and forms the basis for understanding intent at an operator level. It is concerned with the 'How and What' of an attack and can include detection indicators, such as: MD5 hashes, IP addresses and malicious domains.

As a combination, these three categories of information and intelligence enable the different stakeholders at the entity (e.g. Board, CISO, operators, etc) to make the appropriate business and operational decisions.

## 7.2 Principles for Intelligence Sharing

Each member of the CIISI-EU Community is responsible for contributing the information and intelligence and insights they gain within their own organisation to the CIISI-EU Community. Every member is expected to be an active participant, i.e. not only benefiting by consuming but also by actively contributing.

The overarching principle for the sharing of information and intelligence within the CIISI-EU Community is **to deliver information to the community as quickly and accurately as possible in a format that is accessible by all in order to allow members to better protect themselves**, and in so doing, 'achieve immunity' against current and likely future threats whilst remaining in line with data privacy restrictions.

The CIISI-EU Community adheres to the following intelligence sharing principles:

- **Actionable and Relevant.** The information and intelligence needs to be actionable and relevant to the end-user
- **Common taxonomy.** The nature of information and intelligence being shared must be commonly agreed by the CIISI-EU Community. This will avoid unnecessary duplication of effort and ensure efficient and economical use of resources
- **Centralised Control.** The CIISI-EU Secretariat will operate as the central function providing direction to the third-party providers and support in ensuring the centralized and easy flow of information
- **Responsiveness.** The CIISI-EU Community members must be responsive to the needs of other members to support their needs in a timely manner
- **Objectivity.** When creating and sharing intelligence and assessments, effort must be made to remove any potential bias and to present objectively
- **Systematic Exploitation.** CIISI-EU Community members and the third-party cyber threat intelligence provider must actively and continuously exploit the information and intelligence shared in the platforms in order to provide additional insights
- **Source Protection.** The Traffic Light Protocol (TLP) must always be used and followed
- **Continuous Review.** CIISI-EU Community members, the CIISI-EU Secretariat and the third-party providers will continually review both the intelligence they share and the processes by which they share it, in order to continuously enhance their value to the community
- **Format and accessibility.** CIISI-EU Community members must use the prescribed formats, protocols and taxonomies prescribed in the CIISI-EU Community Rulebook to allow the information and intelligence to be fully utilised, exploited and easily consumed

- **Timeliness.** Timeliness is a crucial feature of information and intelligence sharing for it to be effective at mitigating potential cyber threats and as an input into response and recovery. Information and intelligence must be disseminated to the CIISI-EU Community in an accurate and timely manner
- **Compliant.** The information and intelligence shared must comply with applicable Laws and Regulations (e.g. GDPR, copyright, other legal/contractual obligations, etc)
- **MoSCoW Trigger** CIISI-EU Community members follow specific conditions to determine when to share. See below

### 7.3 MoSCoW Framework to Determine What to Share

CIISI-EU Community has adopted the MoSCoW (Must, Should, Could, Won't) Framework to help organisations understand what they should share:

- **Must Share.** Intelligence must be shared if a fellow CIISI-EU member will benefit from the information, e.g. cyber security incidents related to the operation of financial infrastructures and involving an adversary either against the organisation, another participant, another financial organisation or an organisation within the supply chain; and/or knowledge of an adversary including details of their infrastructure, TTPs, Modus Operandi, Malware, Operations, campaigns, intent, or any information and intelligence that will better allow its profiling, thus supporting prediction, detection, response and remediation efforts
- **Should Share.** Intelligence should be shared if it would support a CIISI-EU member's better understanding, e.g. how they are detecting and responding to particular techniques or malware families using the MITRE ATT&CK technique or YARA rules for the detection of malware
- **Could Share.** Intelligence could be shared if it supports the operational effectiveness of a Security Operations team, e.g. share the methodologies that the member believes would be of value to the community such as internal intelligence reports, success metrics, target operating models or policies and procedures
- **Won't Share.** Intelligence cannot be shared if it breaches legal restrictions, e.g. personal data that is contrary to data privacy legislation in their own countries, details that could be seen as 'targeting of an individual', derogatory or inflammatory material, or information or intelligence where the quality of the original source cannot be measured or that could support any false information campaigns



## 7.4 Types of Information and Intelligence to be Shared

In general, the types of information exchange are expected to encompass:

- **Indicators of Compromise (IOCs)** – these are technical artefacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message
- **Tactics, Techniques, and Procedures (TTPs)** – these describe the behaviour of a threat actor. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit. The CIISI-EU Community uses the MITRE ATT&CK Framework when describing the TTPs of an adversary
- **Security Alerts** - also known as advisories, bulletins, and vulnerability notes - are brief, usually human readable, technical notifications regarding current vulnerabilities, exploits and other security issues
- **Threat Intelligence Reports** – these are generally prose documents that describe TTPs, threat actors, campaigns, types of systems or information being targeted that provide greater situational awareness. Threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes
- **Tool Configurations** – these are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files
- **Motives and Goals of Threat Actors** – these allow one to better understand the motives behind attacks. To predict potential future attacks, it is essential that entities understand the motives, goals and campaigns being undertaken by a threat group, especially state actors or ideologically motivated groups

By default, it is always assumed that information exchanged without classification is for use only by members at level TLP:AMBER.

## 7.5 Data Privacy

One prime concern raised with sharing of intelligence between entities is privacy. This is a valid concern that must be clarified prior to the launch of such an initiative but should not be viewed as insurmountable.

### 7.5.1 Where is the Personal Data?

From the types of information and intelligence detailed above, it is unlikely that strategic and operational types of information and intelligence will contain personal data, as this information is related to the nature of attack, how these attacks technically work, the relevant threat actor groups and how the trends of the attacks seem to be evolving. Usually such information is not connected to an individual and their actions.

For tactical intelligence, however, which includes IOCs and data types such as IPs, email addresses and attachment names, email subject names etc. one can clearly deduce that personal data may exist.

Although email addresses, IP addresses and related fields may be personal, it is unlikely that participating entities will be able to determine if there is a natural person behind these email or IP addresses or email attachments/subjects; consequently, identifying personal data related to any natural person is unlikely.

### 7.5.2 Why Share Data which could Potentially be Personal?

Tactical information and intelligence (such as IPs addresses, email addresses etc.) are critical in preventing cyberattacks. In an operational capacity, the exchange of these types of tactical information and intelligence is necessary as they are often automatically integrated into the monitoring and threat hunting activities to identify possible compromise. Most significant cyberattacks are initiated from unsolicited email messages with links or attachments and therefore these types of tactical information and intelligence are crucial for identifying and stopping attacks in a timely manner.

By sharing the tactical information and intelligence outlined above, the initiative is in fact helping the participating entities to become more secure and protect themselves better (which also includes protecting the personal data they have as part of their normal business processes) and thereby strengthen the broader financial system as a whole.

It is important to note that entities must take personal responsibility in vetting the information and intelligence, before sharing it with others. The CIISI-EU Community Rulebook sets out the key principles and criteria that participating members must take on board prior to sharing such tactical information and intelligence.

As mentioned above each participating entity should deduce what they can share based on the MoSCoW Framework. And based on the criteria set out in the CIISI-EU Community Rulebook, members can opt to not share information which they deem to be too sensitive, irrelevant, legally prohibited etc.

### 7.5.3 Safeguarding

The sharing community must ensure that the infrastructure, which is used to host and share all this data, some of which could be personal, is robustly developed and maintained with the proper access control, encryption, data retention controls to safeguard this information and ensure its anonymity wherever possible.

## 8 Organisation and Roles

The CIISI-EU Community made various decisions around the structure and organisation of the initiative:

- Membership Restrictions
- Organisational Structure
- Secretariat Role
- Member Obligations
- Third-Party Providers

The decisions made around structure and organisation apply to the CIISI-EU Community, but other prospective communities could adapt and take alternative routes, based on their own unique characteristics.

### 8.1 CIISI-EU Membership Restrictions

CIISI-EU is a market-driven initiative and, as such, membership is restricted to financial market 'operators'. Authorities in their capacity as regulators, overseers and/or supervisors are not part of the CIISI-EU Community and regulatory reporting on cyber incidents and data breaches are outside the scope of the intelligence sharing within the CIISI-EU Community. Central banks that are part of the CIISI-EU Community must ensure that, with regards to this CIISI-EU information exchange, an internal "Chinese Wall" separates its Security Operating Centre and its system operator function from the regulatory, oversight and supervisory functions it may have to the extent permitted by law.

This decision ensures that CIISI-EU Community members are totally comfortable in sharing information and intelligence, without any concerns that they may be subject to regulatory, oversight and/or supervisory judgement.

### 8.2 CIISI-EU Organisational Structure

Currently, the CIISI-EU members act as a like-minded community where each member is obliged to contract separately with the Third-Party Cyber Threat Intelligence Provider and with CIRCL for their provision of MISIP, based on a commonly agreed commercial contract.

As an alternative organisational structure, the CIISI-EU members discussed the future possibility of creating a separate legal entity or 'Special Purpose Vehicle' (SPV) to act as the central contractual body for undertaking procurement and other administrative

tasks. However, it was agreed not to pursue this for the moment, as an SPV would need a governance structure; legal documents such as Articles of Association; personnel; bank accounts; invoicing capabilities; etc. Although this is resource intensive, in the longer term, the members may consider such a structure to be more effective and formal, allowing a more robust structure, enhanced governance, personnel, adaptability and longevity.

### 8.3 CIISI-EU Secretariat Role

The CIISI-EU Community is served by a CIISI-EU Secretariat, which will rotate among the CIISI-EU Community members at agreed upon intervals.

The member providing the CIISI-EU Secretariat function will make available the appropriate resources during its term and will not be remunerated.

The CIISI-EU Secretariat has the following roles and responsibilities. It:

- Acts as the central contact point for the CIISI-EU Community members, the third-party cyber threat intelligence provider and CIRCL (MISP), and facilitates any decision making required for the ongoing implementation of CIISI-EU
- Facilitates the 24 month review process of the Terms of Reference and the CIISI-EU Community Rulebook, and the annual stock take of the initiative to make improvements
- Co-ordinates the monthly trusted group call and bi-annual in-person meetings, in close collaboration with the third-party cyber threat intelligence provider. This includes arranging the dates and times, setting and disseminating the agenda, chairing the calls, drafting (in conjunction with the third-party cyber threat intelligence provider) the summaries
- Liaises closely with the ECRB Secretariat, to raise any issues that require discussion at the ECRB
- Liaises with potential information and intelligence sharing communities that could forge a strategic relationship with the CIISI-EU Community
- Monitors the overall amount billed by the third-party cyber threat intelligence provider and CIRCL (MISP) to the CIISI-EU members for the provision of the CIISI-EU services

## 8.4 CIISI-EU Community Member Obligations

Despite CIISI-EU being a collection of like-minded entities agreeing to share cyber intelligence, the CIISI-EU Terms of Reference and Community Rulebook are not legally binding in nature. However, without prejudice to applicable laws, each CIISI-EU member is expected to:

- Adhere to the terms set out in the CIISI-EU Terms of Reference and in the CIISI-EU Community Rulebook
- Nominate a single point of contact (including a team, distribution list or group email account) within the member organisation that acts as a central coordination point and focus for communications
- Maintain and share with the CIISI-EU Community a list of key contacts within the institution across all stakeholders, e.g. senior management, SOC, security operations, threat intelligence, etc
- Adhere to the TLP intelligence sharing protocol when sharing information
- Participate in the monthly CIISI-EU trusted group calls
- Attend the in-person meetings, participate in discussions and provide materials / presentations on agreed upon topics of interest
- Actively use the central MISP sharing tool, to the extent possible, by sharing relevant information and intelligence, depending on significance
- Ensure that the information and intelligence that it shares with the CIISI-EU Community as part of the intelligence sharing does not contain personal data and ensure that the processing of data abides by respective national and European legal requirements, e.g. GDPR, EUDPR and the EUROPOL Regulation
- Pay their financial obligations to MISP and to the third-party cyber threat intelligence provider in a timely manner. CIISI-EU follows the principle that each CIISI-EU member bears its own costs for participating in and contributing to CIISI-EU and its community. The costs for the provision of services by the third-party providers will be borne by members on an equal basis, as set out in the contractual terms by these respective third-party providers. It is the responsibility of each member to ensure that their liabilities are paid in a timely manner and in accordance with the contractual terms. The third-party cyber threat intelligence provider and CIRCL (MISP) will provide a financial statement to the CIISI-EU Secretariat which consolidates the fees charged to each member and the associated payment status.

## 8.5 Third-Party Platform Provider - Central Shared Platform - CIRCL (MISP)

CIISI-EU Community members have committed to using CIRCL (MISP) as the central platform for information sharing, which uses STIX 2.1 (amongst others) as the industry standard data exchange protocol. Each CIISI-EU Community member will elect what information or intelligence is important enough to warrant disseminating onto the MISP shared platform.

At their own pace each CIISI-EU member can set up a MISP instance (or equivalent connection) to connect to the central CIISI-EU MISP. Each CIISI-EU Community member's MISP connection instance will synchronise with the other CIISI-EU Community members' MISP connections, and the collective will operate as a closed and trusted group

It is the responsibility of each CIISI-EU Community member to ensure the confidentiality, integrity and availability of its own MISP instance or equivalent connection, to maintain an up-to-date list of users at their organisation, and to ensure that access rights are granted, amended and/or removed to new joiners, leavers and movers as required by the organisation.

In cases where CIISI-EU Community members require training for the use of MISP, the CIISI-EU Secretariat will liaise with CIRCL to arrange such collective sessions.

## 8.6 Third-party Cyber Threat Intelligence Provider

CIISI-EU Community members have committed to using a commercial third-party cyber threat intelligence provider. This cyber threat intelligence provider plays a pivotal and unique role in CIISI-EU. The provider will have access to the trusted group and the MISP platform, to analyse the intelligence put on it, filter it and enrich it with further strategic intelligence, based on the provider's experience and skills, and its broader exposure to the financial services sector. The third-party cyber threat intelligence provider will analyse the information and intelligence, contextualise it, and enrich it from a strategic perspective and produce strategic analysis reports and dashboards, which will be shared with all the CIISI-EU Community members on an ongoing basis, as well providing intelligence support to the members and an integrated Threat Intelligence Platform which hosts the operational and strategic reporting.

The added-value of the provider is to provide more meaningful and actionable strategic information and intelligence for the different CIISI-EU Community members and reduce the resource intensiveness of analysing vast amounts of information, which would otherwise have to be done by the members.

In order to raise awareness at the highest level, the third-party cyber threat intelligence provider will also produce a higher level Board paper every six months, providing strategic analysis on the threat landscape, and share this with the ECRB members ahead of the bi-annual ECRB meetings for review, reflection and discussion.

## 9 Managing the Risks

Developing a multilateral initiative such as CIISI-EU, with such a large number of stakeholders, also carries significant project risk. In light of this, the working group noted the following risks from the inception, and ensured that steps were taken throughout the course of the project to manage them adequately.

Risk	Description	Mitigation
<b>Not Used</b>	Risk of poor operational uptake / is not used / does not reach critical mass	Executive sponsorship and strong support across all members. Formal checkpoints needed to review lessons learned and refine post rollout
<b>Volumes</b>	Risk that massive volumes of IOCs overwhelms CIISI operations	Members elect what to share on the platform, depending on significance, and this criteria is collectively agreed and documented in the CIISI-EU Community Rulebook
<b>No Value Added</b>	Risk that CIISI-EU just recycles tactical and operational IOCs offering little value-added	Approach ensures synthesis of relevant strategic intelligence, specifically via the third-party cyber threat intelligence provider
<b>Not Actionable</b>	Risk that the quality of shared intelligence is poor or not actionable	CIISI-EU Community Rulebook defines best practice based on input from SOC / CERT experts, and concept of continuously learning and evolving is defined as a core CIISI-EU objective
<b>Lock In</b>	Risk that third-party vendors initially bid cheaply then raise fees over next contracting cycle and cannot easily be swapped out	Technical IOC sharing platform is separate and distinct from the third-party cyber threat intelligence provider that provides strategic information and analysis, therefore preventing a lock-in
<b>Vendor Terms</b>	Risk that not all CIISI-EU Community members reach agreeable terms with third party vendors	Each bilateral contract is based on common terms and conditions and identical fees
<b>No Host</b>	Risk that no single CIISI-EU Community member takes	CIRCL in Luxembourg will centrally host MISP on behalf of CIISI-EU



	the responsibility to act as the central host of the platform	Community members
<b>Lack of Scale</b>	Risk that CIISI-EU cannot be scaled beyond ECRB members in the future	Approach is based on MISP, a commonly-used de-facto sharing platform with large operational capacity, rather than a specific vendor
<b>Big Bang</b>	Risk that all CIISI-EU members have to implement at the same time	Approach allows CIISI-EU Community members to implement at their own pace, but fees payable regardless of on-boarding timetable
<b>Legal</b>	Risk that sharing of information may contravene existing regulations	Continuous consultation of legal counsel and data protection officers

Although the above is not an exhaustive list of the risks, other communities looking to develop a similar multilateral initiative should take these on board from the inception and consider appropriate mitigations.

## 10 Key Success Factors

Any initiative that involves multiple stakeholders and requires the sharing of information and intelligence between them is challenging and there is always the possibility that such initiatives gradually become weak over time or diminish in value.

This can also be said about cyber information and intelligence sharing initiatives, and as such there are some key success factors that need to be monitored via indicators to ensure the initiative continues to be successful, relevant, evolve and offer value.

Some potential key success factors and indicators are as follows, although this is not an exhaustive list and will develop further over time:

Area	Key Success Factor	Indicator
<b>Trust and Openness</b>	Participating entities form part of a collective ecosystem and should understand that they do not compete on cyber resilience. Rather they have to all collectively work together to combat cyber threats, which necessitates trust and openness	Number of ad hoc queries to the third-party cyber threat intelligence provider; percentage of trusted group members not participating in more than 1 trusted group meeting or call; % of participating entities leaving the initiative; applications for new participants to join the initiative.
<b>Active Participation</b>	Active participation by all participating entities in the initiative. Over time all entities should gradually be active depending on their cyber maturity and resourcing; however, all must contribute with threat intelligence and at least speak in the trusted group calls and meetings	Monitoring of organisations not actively participating in trusted group calls and meetings (e.g. being silent); qualitative and quantitative review of the threat intelligence being shared by entities in comparison to the collective average; monitoring which entities raise ad hoc queries and introduce of new topics.
<b>Senior Management Engagement</b>	Senior Management engagement of participating entities to ensure the initiative is a priority for that entity and senior management comprehends its value.	How often do strategic threat intelligence reports and monthly dashboards go to the senior management in each entity; how frequently do they give suggestions/feedback; have their suggestions led to the creation of new workstreams or enhancements to the initiative.

<p><b>Relevancy and Value</b></p>	<p>The initiative must keep up-to-speed with the evolution of cyber threats and intelligence sharing. Input and suggestions from participating entities from multiple levels (e.g. senior, managerial, technical, etc) will be critical for the evolution of the initiative.</p>	<p>Guest speakers from other initiatives and jurisdictions, as well as threat intelligence experts and advisers; convening bespoke workshops; participating entities taking the lead for new workstreams within the initiative; number of suggestions from participating entities; number of entities wanting to leave; number of entities or other initiatives wanting to join.</p>
<p><b>Evolution</b></p>	<p>Threats are evolving and so should the information sharing initiative. The initiative should continuously enhance its existing work, based on the evolution of the threat landscape and via strategic partnerships.</p>	<p>New workstreams initiated by the initiative; increased calls of the trusted group; part of a network of strategic partnerships; interest on the initiative from other organisations; minimal entities leaving</p>

# 11 Guidance on Design, Implementation and Operationalisation Phasing

Despite having a simple objective to share cyber information and intelligence between a closed group of like-minded entities, as an implementation programme, CIISI-EU is complex with many moving parts and many stakeholders.

As guidance for entities wishing to undertake a similar path, these were the main phases of activity that CIISI-EU undertook:

- Phase 1: Working Group Formation
- Phase 2: Requirements, Ideation and Design
- Phase 3: Identification, Evaluation and Selection of the third-party platform and cyber threat intelligence provider
- Major Milestone: ECRB 'Go / No-Go' Decision
- Phase 4: Define CIISI-EU 'Terms of Reference' and 'Community Rulebook'
- Phase 5: Procurement
- Phase 6: Platform Implementation
- Phase 7: Operationalisation

These phases and the underlying activities were not always sequential and dates given below are approximate. Consideration should also be given that some of the activities were impacted, and continue to be impacted, by the Covid-19 pandemic.

## 11.1 Phase 1: Working Group Formation

In December 2018, the ECRB, comprising senior executives from each ECRB member, published a formal mandate that defined the information sharing objective and the need for a formal Working Group to effect its execution and delivery.

Facilitated by the seniority of each ECRB member, resources were quickly committed by each member to form the ECRB Information Sharing Working Group (WG), in March 2019, which was supported by the ECRB Secretariat function.

Individual WG resources were selected based on their seniority, cyber-based skill-set and pragmatism to implement the project within the compressed timeframe, as outlined in the mandate.

The WG, comprising ~20 part-time resources, was formed in February 2019. It is important to note that CIISI-EU is a market-driven initiative, for the market, by the

market. Consequently, it was important to ensure that the Chair of the WG was from the market – in the case of CIISI-EU, the Chairmanship was provided by SWIFT.

## 11.2 Phase 2: Requirements, Ideation and Design

After an initial kick-off in March 19, the WG conducted a series of calls and in-person meetings and workshops. During these meetings the WG identified requirements, defined building blocks and created an architecture and topology design.

Given the geographic diversity of WG members, and that not all members were always physically present, and to ensure all voices were heard, the WG used an online polling / voting app to gather, measure and document the various requirements priorities and appetite for the design options.

While the resultant design is now well documented, see earlier section in this paper, the process was driven by two fundamental decisions:

1. Selection of the common shared platform - MISP. MISP was selected as it is open-source, free to implement, has been specifically designed by cyber practitioners, is managed by the Computer Incident Response Centre in Luxembourg, CIRCL, and has long-established funding through the EU. Crucially, its vendor neutrality prevents longer-term 'lock-in' of the shared platform that may occur if a commercial provider were selected. In addition, several CIISI-EU members already use MISP and had in-house expertise
2. Selection of the third-party cyber threat intelligence provider - Should be made through a comprehensive RFI evaluation process. See below

The requirements, ideation and design activities were an iterative process that took place from March 2019 to June 2019.

## 11.3 Phase 3: Identification, Evaluation and Selection of the Third-party Cyber Threat Intelligence Provider

To help identify, evaluate and select the third-party cyber threat intelligence provider, the WG undertook a number of activities:

- Perform a market scan / desktop research to identify a list of candidate third-party providers. Based on the market-scan, the WG identified many suitable candidates, comprising both large well established organisations as well as smaller niche players. The WG engaged with all candidates and thereafter short-listed to a limited number of vendors
- Construct a Request for Information (RFI) for the short-listed candidates, see below. Each candidate provider provided detailed written responses to the RFI

- Invite each of the short-listed candidates to an in-person 'beauty parade', where they presented their solutions to the WG members and answered their in-depth questions
- Evaluate and 'score' each of the vendors based on the written responses to RFI criteria, their presentation and their Q&A answers
- Select the preferred third-party cyber threat intelligence provider. Selection was made by WG consensus, based on reviewing the highest scores across all of the criteria, across all candidates

The summary evaluation and 'scoring' criteria for the candidate vendors:

**Functional / Strategic Criteria:**

- Depth of functions and content / richness of analysis and reports
- Ability to maintain trusted circle
- Skill / experience of resources
- Future evolution
- Ability to support strategic partners

**Technical / Project Management Criteria:**

- Technical capability / infrastructure
- Ability to interface with MISP
- Development of cyber taxonomy – tactical, operational and strategic
- Capability to manage the project

**Commercial Criteria:**

- Contractual and commercial terms
- Bilateral flexibility on terms
- SLAs
- Pricing, including one-off costs and recurring costs: vendor implementation of topology, rules and taxonomy; platform hosting, configuration, setup and user administration; personnel training; operational support (based on predetermined number of support tickets per year) and functional enhancements (provision for limited number of enhancements, per year). All costs to be shared equally across the CIISI-EU members

This evaluation and selection phase lasted from July 2019 to November 2019.

## 11.4 Major Milestone: ECRB Committee 'Go / No-Go' Decision

All of the WG activities undertaken to date (CIISI-EU design, topology, architecture, recommendations for the platform and the vendor, risks and costs) were presented to the ECRB for a formal 'Go / No-Go' decision by each of its respective members on 27 February 2020. The ECRB unanimously approved a 'go' decision. Importantly, each member (as listed in chapter 4) agreed to be part of the CIISI-EU solution.

## 11.5 Phase 4: Define 'Terms of Reference' and the 'Community Rulebook'

With the formal 'go-ahead' of the ECRB members, the ECRB Secretariat, Chair of the WG and the third-party cyber threat intelligence provider created two anchor documents that bind the CIISI-EU members and effect the operationalisation the initiative:

- 'Terms of Reference' set out the high level framework for establishing and participating in CIISI-EU; articulate the core objectives for information sharing; and define the terms to enable the safe and effective information and intelligence sharing within the CIISI-EU Community
- 'Community Rulebook' builds on the Terms of Reference, further details on the processes and intelligence sharing protocols

These two documents, which have been published with this paper, were completed and endorsed by all members by August 2020.

## 11.6 Phase 5: Procurement

With the formal ECRB 'go-ahead', and in parallel with Phase 4 above, driven by the ECRB Secretariat, bilateral discussions with legal and procurement departments were started between:

- The third-party cyber threat intelligence provider and each of the CIISI-EU members, and
- The central platform provider (MISP / CIRCL) and each of the CIISI-EU members

As the pricing had already been addressed in the RFI, the aim of the discussions was to establish a common agreement for the contractual terms.

This procurement phase lasted from February 2020 to September 2020.

## 11.7 Phase 6: Platform Implementation

Implementation and setup of the platforms and tools at each of the CIISI-EU member sites were coordinated by the ECRB Secretariat and by CIRCL, after the procurement activities in Phase 5

MISP activities include:

- Establish and set-up the central MISP host platform at CIRCL that will store operational, technical and strategic intelligence for CIISI-EU members as a closed group. Central MISP platform was established at CIRCL in August 2020
- Support each of the CIISI-EU members to establish their own MISP instance at their own pace, which synchronises with central hosted platform. Not yet started, expected to start October 2020, pandemic notwithstanding.
- Provide MISP training to all CIISI-EU members. Not yet started, expected to start November 2020, pandemic notwithstanding
- Set up and integration of Third Party Platform with MISP

## 11.8 Phase 7: Operationalisation

In parallel with procurement activities in Phase 5 and platform implementation in Phase 6, members started the operationalisation phase. In anticipation to the establishment of the CIISI-EU Secretariat, the ECRB Secretariat coordinated the following activities:

- Establish the 'trusted group' by gathering and sharing operational contacts. The nominated 'trusted group' members have detailed cyber knowledge and can act on the shared information and are typically from the Security Operations Centre (SOC) or Threat Intelligence (TI) functions. Note that these individuals may be different from the original WG members. Contacts were gathered and shared in March 20
- Initiate the monthly calls with the CIISI-EU members and the third-party cyber threat intelligence provider. Monthly calls were started in April 2020
- Draft and agree the single commercial contract to be bilaterally signed between the members and the third-party cyber threat intelligence provider. This was a complex and iterative process, which took place between June and September 2020
- Initiate the in-person meetings. To date, due to the pandemic, these in-person meetings remain postponed
- Initiate the active sharing and consumption of IOCs intelligence using the central MISP platform, as defined in the paper. Not started – expected to start December 2020



In the longer-term, the operationalisation will also:

- Establish alerting / notification mechanisms, e.g. use of closed-group instant message services. Not started - expected Q1 2021
- Consider candidates for strategic partnerships, to enhance synergies and bridge communities. Not started – consideration expected to start Q2 2021
- Consider establishment of a dedicated legal entity to formalise CIISI-EU. Not started – consideration expected to start end 2021

## 12 Getting Further Information

The CIISI-EU target operating model is anchored around the CIISI-EU Terms of Reference and Community Rulebook, which represent a non-binding commitment of the community members to participate in the initiative and sets out the specificities of how members will operationalise the model.

### 12.1 CIISI-EU Terms of Reference

The Terms of Reference set out the high level framework for establishing and participating in CIISI-EU; articulate the core objectives for information sharing; and define the terms to enable the safe and effective information and intelligence sharing within the CIISI-EU Community.

### 12.2 CIISI-EU Community Rulebook

Building on the Terms of Reference, further details on the processes and intelligence sharing protocols are set out in the CIISI-EU Community Rulebook. Details include:

- CIISI-EU governance
- CIISI-EU administrative policies, processes and operational procedures
- Rules and roles for the CIISI-EU Community, including changes to the composition, election of representatives, meetings, calls and decision making
- Principles for information and intelligence that will be applied by the members
- Taxonomies, frameworks, terminology and conventions to be used for the sharing of information and intelligence

These documents set out a detailed approach and rules that members agree to follow in order to effectively operationalize CIISI-EU, and were drafted collectively to ensure that there is full buy-in and agreement on the collective roles and responsibilities.

Importantly, the governance arrangements anchored in the CIISI-EU Terms of Reference and the Community Rulebook have been endorsed by the senior management of each member entity. The sponsorship of senior management ensures that the initiative has full consent and will receive the required investment, vis-à-vis human resources and finance.

Although these documents have been drafted for the specific CIISI-EU Community, they can be used as a basis by other communities that intend to establish similar

information and intelligence sharing arrangements. Other prospective communities should use them as a basis, and tailor them according to the specificities of their respective community members. They are not intended to be prescriptive, and it is critical that any community designs appropriate terms and rules collectively, in a collaborative manner.

The CIISI-EU Terms of Reference and Community Rulebook have been published alongside this paper, to provide potential stakeholders with the full suite of documentation and a practical example on establishing an effective cyber information and intelligence sharing initiative.

For further information about CIISI-EU please contact [ECRB@ecb.europa.eu](mailto:ECRB@ecb.europa.eu)

### **Acknowledgements**

ECRB Secretariat, Security Alliance B.V., CIRCL (MISP) and members of the ECRB Information Sharing Working Group: the Banca d'Italia; the Banco de Espana; the Banque centrale du Luxembourg; the Banque de France; BME; CLS Bank International; the Danmarks Nationalbank; De Nederlandsche Bank; the Deutsche Börse Group; the Deutsche Bundesbank; EBA Clearing; the European Central Bank; the European Commission, ENISA; equensWorldline; European Central Counterparty N.V.; Euroclear; Europol; Iberpay; Krajowy Depozyt Papierów Wartościowych/The Central Securities Depository of Poland; London Stock Exchange Group (on behalf of LCH SA and Monte Titoli); Mastercard Europe SA; Nasdaq Nordic (on behalf of Nasdaq Clearing and Nordic Exchanges); the Nationale Bank van België/Banque nationale de Belgique; SIA; STET; SWIFT; TARGET Services and Visa Europe.

**© European Central Bank, 2020**

Postal address 60640 Frankfurt am Main, Germany  
Telephone +49 69 1344 0  
Website [www.ecb.europa.eu](http://www.ecb.europa.eu)

All rights reserved. Any reproduction, publication and reprint in the form of a different publication, whether printed or produced electronically, in whole or in part, is permitted only with the explicit written authorisation of the ECB or the authors.