Observance of CPSS-IOSCO Principles for Financial Market Infrastructures (PFMI) and Cyber Resilience of FMI

Cyber Incident Reporting & Information Sharing

EMRAN ISLAM (MCM)

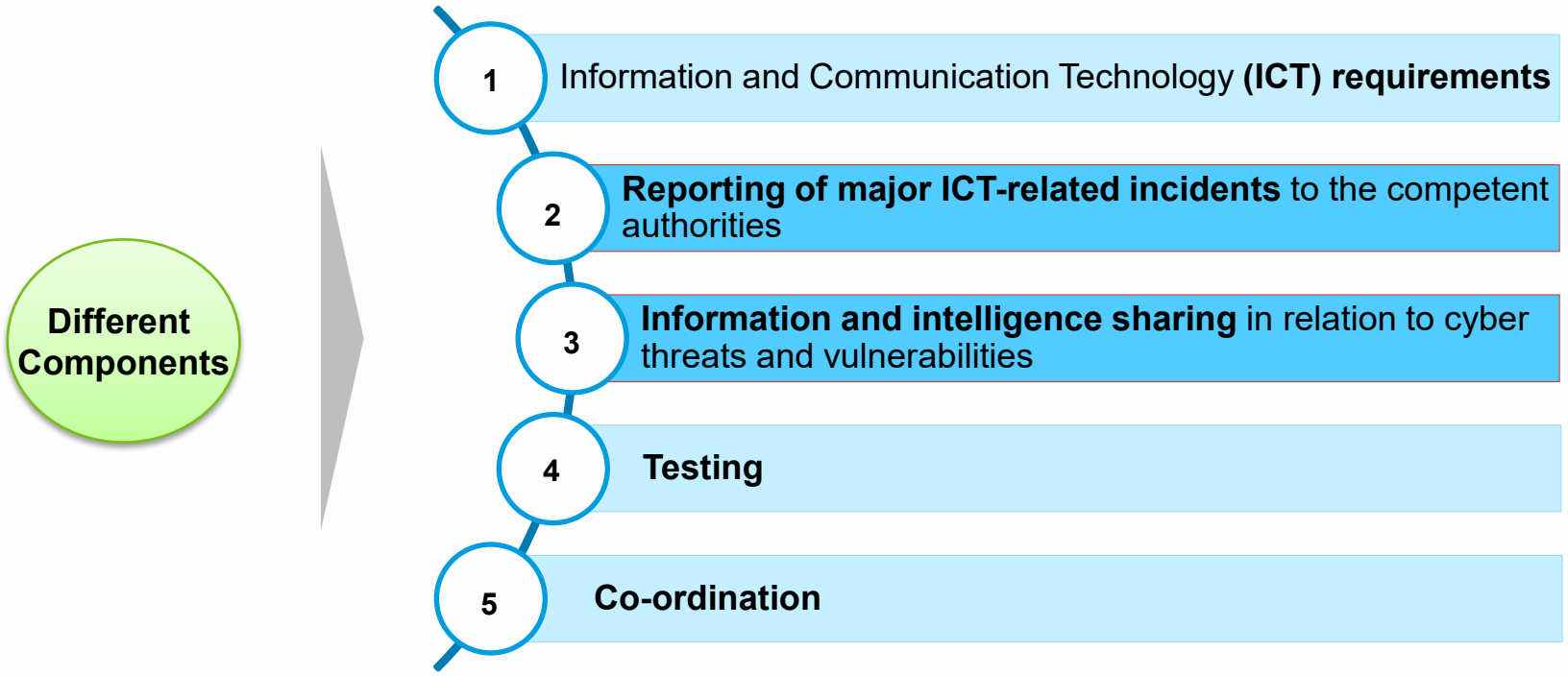
FEBRUARY 1, 2024

Agenda

1. Importance of incident reporting
2. FSB work – practical issues & operational challenges

3. Key elements of incident reporting
4. FSB recommendations
5. FIRE
6. Information Sharing

Possible high-level enablers to building cyber resilience



Incident reporting

Objective

- Regulation could aim to harmonise and streamline the reporting of ICT-related incidents
- Having a robust process of incident reporting would enhance supervisory processes and improve crisis management at national level

Contents

Proposed process could be:

- **Establish and implement a management process to monitor and log ICT-related incidents,**
- **Classify them based on criteria and materiality threshold detailed in the regulation,**
- **Only major ICT-related incidents to be reported to the competent authorities,**
- **Reporting could be processed using a common template**
- **Financial entities should submit initial, intermediate and final reports**

FSB work on cyber incident reporting – practical issues

The 2022 FSB survey augmented and refined the stocktake in 2021, delving more deeply into understanding:

(i) the most common reporting objectives for financial authorities;

(ii) the types of incident reporting used to support common objectives;

(iii) impediments to sharing information between financial authorities;

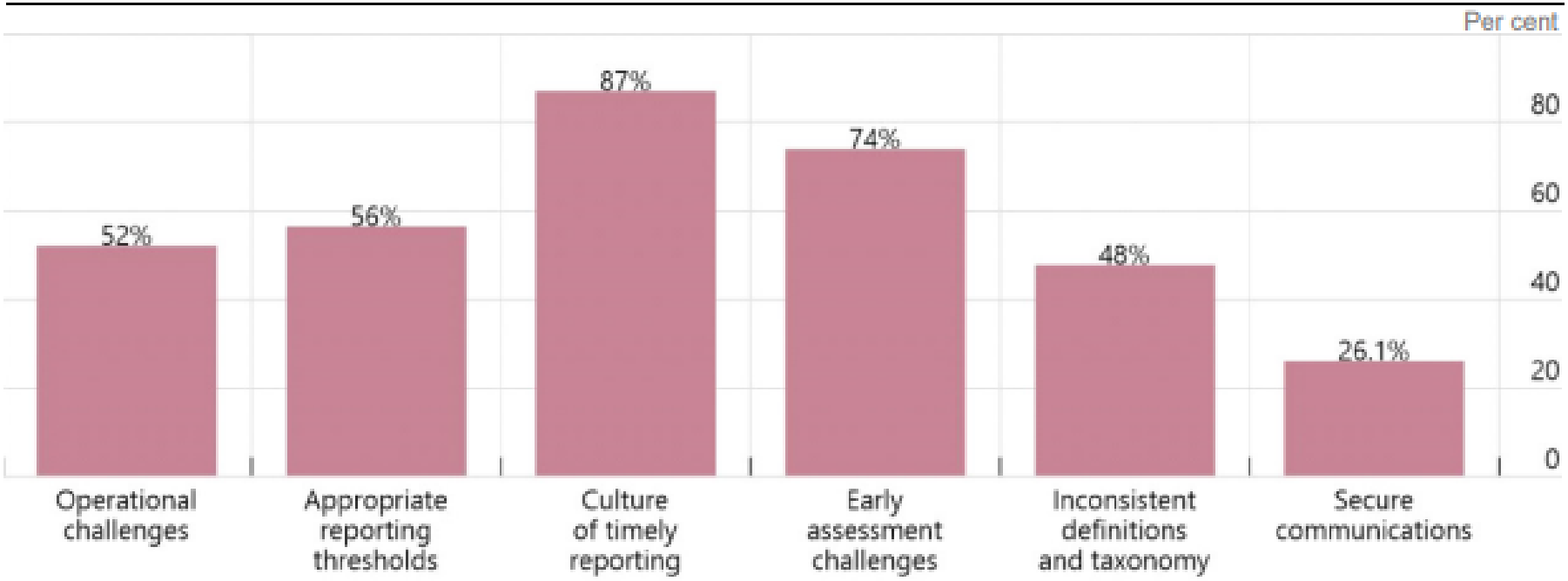
(iv) the information items exchanged as part of incident data collections;

(v) aspects considered for impact/materiality thresholds that trigger reporting obligations; and

(vi) practical issues financial authorities and FIs have in collecting or using the reported cyber information.

Survey results

Practical issues in collecting or using cyber incident information **Graph 1**



Source: 2022 FSB Survey

Operational challenges

- A **case study was developed in collaboration with a global systemically important bank (G-SIB) with large operations in Europe and the United States**. In the event of a cyber incident which triggers reporting requirements in all jurisdictions that the G-SIB operates, the G-SIB, in the first 72 hours, has to:
  - **verbally** contact five or more authorities,
  - issue between 7-13 **written notifications**,
  - complete and submit 12-14 **initial incident report forms**, and
  - enter details into 5-9 **online reporting portals**.

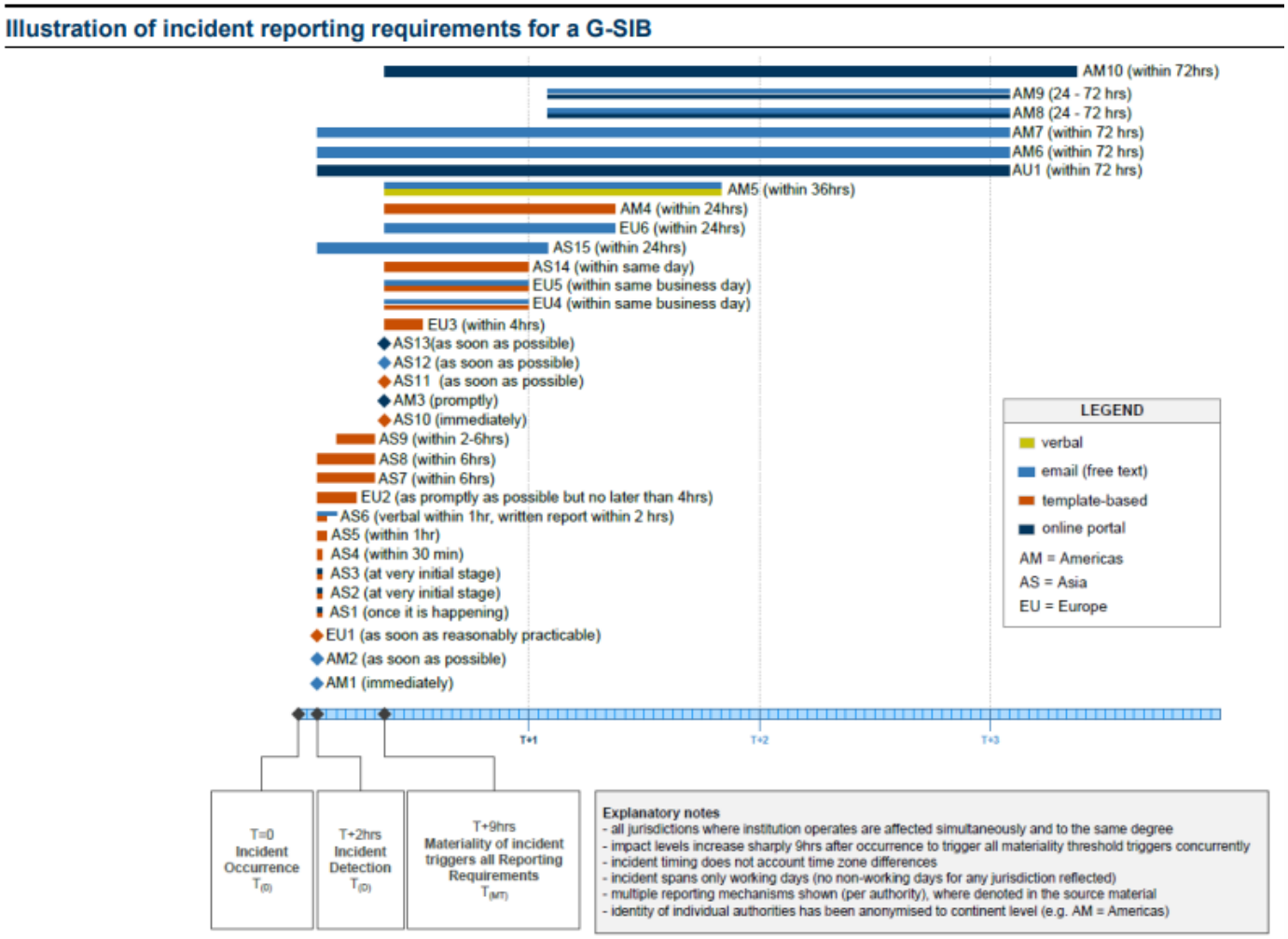
- Further, **draft text in each required communication format, style and timeframe are iterated and finalised** with the most current information available, which takes considerable time away from the relatively small-sized teams of cyber incident responders during most critical initial investigation time.

- There are also meaningful **differences in the reporting templates and reporting triggers** (i.e. detection or materiality thresholds), which require judgement by the G-SIB, and mechanisms for reporting (e.g. verbal, email, template-based, online form).

- The challenge of **materiality thresholds** as triggers for notification in the first 24 hours is further exacerbated by the uncertainty that surrounds the first hours of an event detection.

- Further, each reporting requirement may have **different governance processes**, which need to be managed while managing the incident itself.

The challenge of the GSIB



What are the key elements of incident reporting?

- Protocols and templates
- Coverage of required cyber incident reporting – which entities?
- Process and timelines for communicating cyber incidents
- Criteria for reporting
  - Definition of cyber incident - *A cyber event that: i. adversely affects the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. (FSB Cyber Lexicon)*
  - Quantitative
  - Qualitative
  - Taxonomies
  - Severity and impact
- Usage of information by financial authorities
- Cooperation and coordination

FSB recommendations for CIR

1. **Establish and maintain objectives for CIR**. Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

2. **Explore greater convergence of CIR frameworks**. Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

3. **Adopt common reporting formats**. Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

4. **Implement phased and incremental reporting requirements**. Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

5. **Select incident reporting triggers**. Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.

FSB recommendations for CIR

6. **Minimise interpretation risk**. Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, including supplementing CIR guidance with examples, and engaging with FIs.

7. **Extend materiality-based triggers to include likely breaches**. Financial authorities that use materiality thresholds should explore adjusting threshold language, or use other equivalent approaches, to encourage FIs to report incidents where reporting criteria have yet to be met but are likely to be breached.

8. **Review the effectiveness of CIR processes**. Financial authorities should explore ways to review the effectiveness of FIs' CIR processes and procedures as part of their existing supervisory or regulatory engagement.

9. **Conduct ad-hoc data collection and industry engagement**. Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.

10. **Address impediments to cross-border information sharing**. Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.

FSB recommendations for CIR

12. **Foster mutual understanding of benefits of reporting**. Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

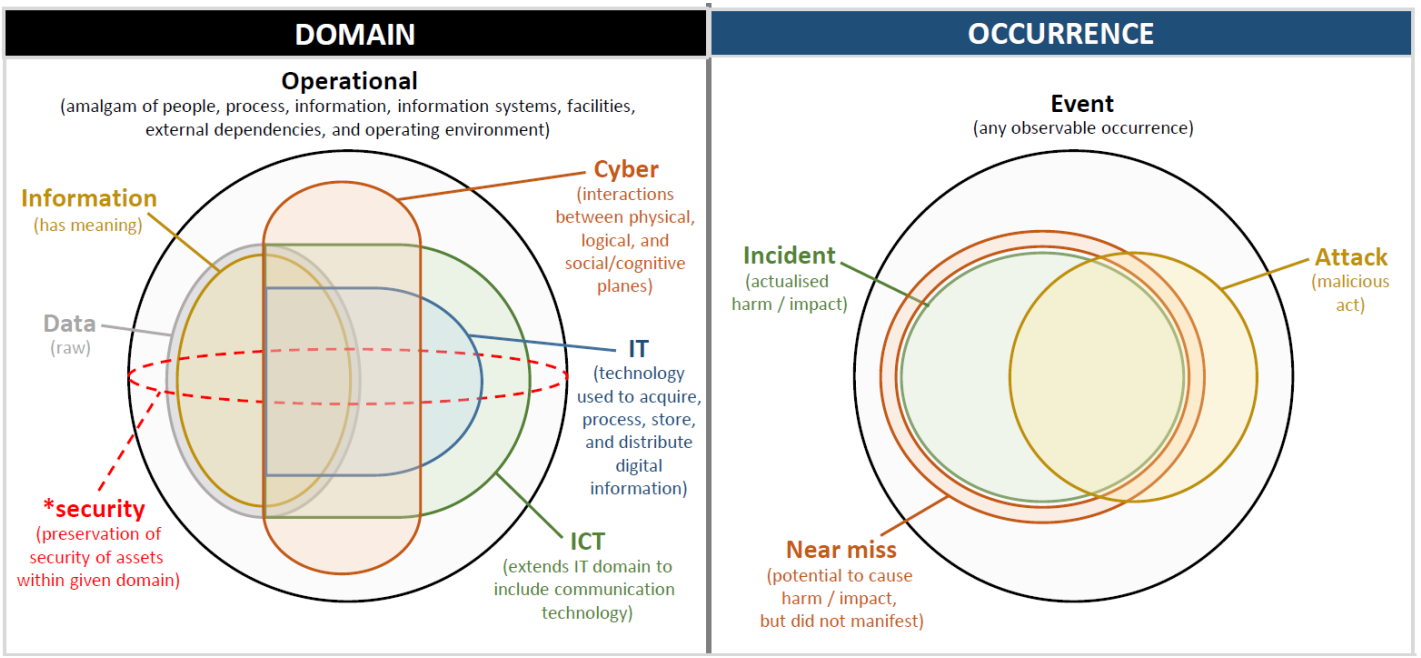
13. **Provide guidance on effective CIR communication**. Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

14. **Maintain response capabilities which support CIR**. FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

15. **Pool knowledge to identify related cyber events and cyber incidents**. Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

16. **Protect sensitive information**. Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

The issue of definition – FSB



- **Cyber* Incident : A cyber event** that adversely affects the cyber security of an information system*** or the information the system processes, stores or transmits whether resulting from malicious activity or not.**

***Cyber:** Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems

****Cyber event:** Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

*****Information systems:** Set of applications, services, information technology assets or other information-handling components, which includes the operating environment.

Format for incident reporting exchange (FIRE)

- A detailed examination of individual data fields within existing reporting templates indicated a high degree of commonality in the information requirements for cyber incident reports.
- The convergence of incident information requirements through development and adoption of a common reporting format could greatly enhance incident reporting practices on a global basis, address operational challenges and foster better communication.
- The **FIRE concept** is proposed as an approach to standardise common information requirements for incident reporting, whilst remaining flexible to a range of implementation practices.
- Authorities can decide the extent to which they wish to adopt FIRE, if at all, based on their individual circumstances. For instance, authorities could consider leveraging a subset of the features or definitions, which would promote a limited form of convergence. Even if not adopted by a single jurisdiction, it could still serve as a common baseline for FIs to map against a range of reporting requirements and assist in translating between existing frameworks.
- FIRE could also support four CIR recommendations: achieve greater convergence in CIR frameworks (#2), promote adoption of a common reporting format (#3), support implementation of phased and incremental reporting requirements (#4) and foster mutual understanding of benefits of reporting (#12).

What are the key elements of incident reporting?

1.1 Reporting Entity	1.2 Incident	1.3 Actor	1.4 Impact Assessment	1.5 Incident Closure
1.1.1 Entity Details	1.2.1 References	1.3.1 Actor Details	1.4.1 Severity Rating	1.5.1 Cause
1.1.2 Contact Details	1.2.2 Incident Details		1.4.2 Services and Resources	1.5.2 Lessons
1.1.3 Receiving Authorities	1.2.3 Change(s) since Previous Report		1.4.3 Scale	1.5.3 Supplemental Documentation
	1.2.4 Date / Time Markers		1.4.4 Impact	
Who issued the report, and to whom?	**What happened/is happening?**	**Whose or what's actions led to the incident?**	**What are the negative effects?**	**What caused the incident, and what remedial actions will be taken?**

Examples of incident types

Incident Type	Definition	Example(s)
Business Disruption, System or Execution Failure	Any type of internal or external incident that disrupts the provision of an entity's services	Technology failure, loss of third party service, Denial of Service (DoS), malware
Compromise (non-disruptive)	(Non-disruptive) Violation of the security of an information system	Account compromise, intrusion, defacement
Data Breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed	Data leakage, data loss
Financial Theft / Fraud	A deliberate act to obtain unauthorised financial benefit	Theft of funds via digital channel
Information Disorder	The spread of false or reality-based information, whether malicious or not	Misinformation, disinformation, malinformation

Examples of methods of discovery of incident

Discovery Method		Description
External	Actor Disclosure	Announced / informed by threat actor
	Authority / Agency	Reported by (national) competent authority e.g. financial authority, cyber security agency
	Law Enforcement	Reported by domestic or international law enforcement agency (LEA) e.g. police, national crime agency, Interpol
	Third Party	Reported by one of the reporting entity's external dependencies e.g. managed service provider, vendor
	Customer / Client	Reported by consumer(s) of the reporting entity's services e.g. counterparty
	Peer / Competitor	Reported by another regulated entity e.g. via collaborative information sharing platform
	Audit	Discovered following a review performed by external auditors e.g. perimeter scanning service provider
	Monitoring service	Reported by external monitoring provider e.g. security event monitoring service
	Unrelated party	Reported by party with no relationship to the reporting entity e.g. bug bounty hunter
	Unknown	Reported by anonymous or unidentified external entity
Internal	Incident Response	Discovered while responding to another incident
	Security Operations Centre	Discovered by dedicated security function as part of business as usual activities
	Existing Detection Technique	Discovered using existing monitoring tools e.g. intrusion detection, log monitoring
	Audit	Discovered following a review performed by internal auditors
	Staff	Reported by contracted staff at reporting entity
	Unknown	Reported by anonymous or unidentified internal entity
Unknown		Reported from unknown source
Other		(include within incident description)

Examples of actor types

Actor Type (shown alongside corresponding actor category)	
Internal	Executive
	Regular or customer-facing employee
	Technology staff
	Maintenance staff
	Unknown
	Other
Third Party	Outsourcing - ICT service provider
	Outsourcing - Non-ICT service provider
	Outsourcing - Sub-outsourced entity
	Outsourcing - Intragroup entity
	Non-outsourced third party
	Supply chain - Fourth (or greater) party
	Critical infrastructure / Utility provider
	Unknown
	Other
External	Activist group
	Competitor
	Customer (B2C)
	Force majeure (nature and chance)
	Nation state
	Organised or professional criminal group
	Relative or acquaintance of employee
	State-sponsored or affiliated group
	Terrorist group
	Unaffiliated person(s)
	Unknown
	Other

Examples of actor motives

Actor Motive	Description
Convenience	Convenience of expediency
Espionage	Espionage or competitive advantage
Financial	Financial or personal gain
Fun	Fun, curiosity, or pride
Grudge	Grudge or personal offense
Ideology	Ideology or protest
NA	Not Applicable (unintentional action)
Unknown	Unknown
Other	Other

Examples of service type affected

Function (and description)		Service Type
Deposit taking	Acceptance of deposits from non-financial intermediaries	Retail Current Accounts
		SME Current Accounts
		Retail Savings Accounts / Time Accounts
		SME Savings Accounts
		Corporate Deposits
Lending and loan services	Provision of funds to non-financial counterparties, such as corporates or retail customers, and can extend through to loan servicing functions	Retail Mortgages / Other Secured (Auto)
		Retail Unsecured Personal Lending
		Retail Credit Cards
		SME Lending (Secured)
		Corporate Lending
		Trade Finance
		Infrastructure Lending
		Credit Card Merchant Services
Capital Markets and Investments activities	Issuance and trading of securities, related advisory services, and related services such as prime brokerage, as well as investment of the firm's own capital in private equity or similar principal investments	Derivatives
		Trading portfolio
		Asset Management
		General Insurance
		Life insurance, pensions, investments and annuities
Wholesale Funding Markets	Lending and borrowing in wholesale markets to and from financial counterparties	Securities Financing
		Securities Lending
Payments, Clearing, Custody & Settlement	Multilateral systems among participating institutions, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions; or provision of these services as an intermediary	Payment Services
		Settlement Services
		Cash Services
		Custody Services
		Third-Party Operational Services

Examples of service disruption type

Service disruption type		Description
Availability Loss	Total	Service is completely unavailable to its users
	Partial	A subset of the service's features/components is unavailable to its users
	Intermittent	Service is occasionally unavailable (total or partial) at either regular or irregular intervals
	Degradation	Service is operating below predefined acceptable service levels
Integrity Loss	Manipulation	Creation, addition, duplication, modification, re-sequencing or deletion of information related to service
	Corruption	Information related to service in unreadable, but recoverable or can be reconstituted
	Destruction	Information related to service has been irrevocably lost
Confidentiality Loss	Unintended / Unauthorised disclosure	The exposure of information to entities not authorised access to the information (e.g. data leakage)
	Unauthorised acquisition	Gaining access to and/or retrieving information without valid authorisation (e.g. data exfiltration, interception)
Loss of Trust	Impersonation	Service identity is assumed or mimicked by an unauthorised entity (e.g. cloned identity, man-in-the-middle)
	Disinformation	Intentional dissemination of false information, with an end goal of misleading, confusing or manipulating an audience
	Rumour / Speculation	Spread of information without confirmation of its veracity
Unknown		Nature of the service disruption yet to be confirmed
Other		Service disruption type does not match pre-defined categories

Examples of impact levels and description

Impact Type vs Level	Insignificant	Minor	Moderate	Substantial	Severe
Overall	• Effects from the incident are safely contained within the entity with **no externalised impacts**	• Continue to provide services **within tolerable levels** despite noticeable disruption • Short-term consumer **inconvenience**	• Service provision **no longer meeting expectations** of one or more stakeholder groups • **Mounting consumer detriment** (disadvantaged and/or dissatisfied)	• Significant threat(s) to the **safety and soundness** of the affected entity • **Actual harm** to consumers or clients materialises • Potential to cause **significant financial** and/or **market impact**	• **Real and imminent** risk to the safety and soundness of the affected entity • **Serious harm** to consumer or client interests • Material impact to the financial system or **broader economy**
Financial	• **Inconsequential** financial loss recorded	• **Limited** financial losses arising from direct and indirect costs associated with incident	• Considerable financial losses occurring, **but can be absorbed**	• Entity in **financial difficulty**, with increased exposure to liquidity risk, or losses that can no longer be absorbed	• Entity in **financial distress or insolvent**, and is unable to meet or pay its financial obligations
Operational	• **Internal** task(s) or process(es) affected	• **Non-critical** service(s) affected	• **Deterioration** in provision of critical service(s)	• Critical service(s) affected such that **key business objectives are not met**	• Sustained operational impact preventing the entity **achieving its mission**
Reputational	• **No discernible** reputational impact	• **Isolated instance(s)** of criticism / negative reaction from a small number of external parties	• **Multiple instances** of criticism / negative reaction by external parties	• Potential for reputational damage caused by **widespread** social, national and mainstream media coverage or public scrutiny	• **Reputational damage** as a result of prolonged social, national and mainstream media coverage or public scrutiny
Legal / Regulatory	• Breach of legislation, contract or policy **that does not** have any penalty or litigation impact	• Breach of legislation, contract or policy that may have an impact on the relationship with a third party or trigger regulatory notification, **but no long lasting effect**	• Legal obligation breach which incurs monetary or non-monetary **penalties** • Heightened **regulatory** monitoring	• Legal obligation breach which leads to significant and costly **legal action** • Heightened **regulatory scrutiny** and/or compliance concerns	• Significant regulatory scrutiny and/or compliance concerns, including potential for regulatory **investigations, sanctions or fines**

Examples of causes – information system and failures

Resource	Sub-resource	Failure Type	Description
Systems and Technology	Hardware	Capacity	Inability to handle a given load or volume of information
		Performance	Inability to complete instructions or process information within acceptable parameters (speed, power consumption, heat load, etc.)
		Maintenance	Failure to perform required or recommended upkeep of the equipment
		Obsolescence	Operation of the equipment beyond its supported service life
	Software	Compatibility	Inability of two or more pieces of software to work together as expected
		Configuration management	Improper application and management of the appropriate settings and parameters for the intended use
		Change control	Changes made to the application or its configuration by a process lacking appropriate authorisation, review, and rigour
		Security settings	Improper application of security settings, either too relaxed or too restrictive, within the program or application
		Coding practices	Failures due to programming errors, including syntax and logic problems and failure to follow secure coding practices
		Testing	Inadequate or atypical testing of the software application or configuration
	Systems	Design	Improper fitness of the system for the intended application or use
		Specification	Improper or inadequate definition of requirements or failure to adhere to the requirements during system construction
		Integration	Failure of various components of the system to function together or interface correctly; also includes inadequate testing of the system
		Complexity	System intricacy or a large number or interrelationships between components
Internal Processes	Process design or execution	Process flow	Poor design of the movement of process outputs to their intended consumers
		Process documentation	Inadequate documentation of the process inputs, outputs, flow, and stakeholders
		Roles and responsibilities	Insufficient definition and understanding of process stakeholder roles and responsibilities
		Notifications and alerts	Inadequate notification regarding a potential process problem or issue
		Information flow	Poor design of the movement of process information to interested parties and stakeholders
		Escalation of issues	The inadequate or non-existent ability to escalate abnormal or unexpected conditions for action by appropriate personnel
		Service level agreements	The lack of agreement among process stakeholders on service expectations that causes a failure to complete expected actions

Planned way forward

To take this work forward, the FSB will establish a new working group comprised of financial sector authorities. The development of FIRE is expected to take place over several phases, and over the course of up to two years:

- **Mobilisation:** Identifying public and private participation and project resources, and forming the working group and its associated terms of reference.
- **Discovery:** Identifying stakeholder needs, pre-requisites, and feasibility.
- **Design:** Designing options which seek to fulfil these needs – current state
- **Consultation:** Public consultation on the identified options.
- **Publication:** Finalisation of the report, reflecting public feedback, which may include both human and machine-readable formats.

Throughout this process, the working group will collaborate with industry, including interested stakeholders outside of the financial sector, as well as authorities beyond the FSB membership

Authority stakeholders	Industry stakeholders
• FSB Member Authorities	• Regulated FIs
• Non-FSB Member Authorities	• FS Trade Associations / Collective Forums
• FSB Regional Consultative Groups (RCGs)	• Technology Service Providers
• International Organisations	• Non-FS Sector (telecoms, energy)
• Financial Standard Setting Bodies	
• National Cybersecurity Authorities	

Information and intelligence sharing

Objective

- Empower financial entities to share information and intelligence

Contents

- **To raise awareness on ICT risk, minimise its spread, support financial entities' defensive capabilities and threat detection techniques, the regulation could allow financial entities to set-up arrangements to exchange cyber threat information and intelligence amongst themselves.**

What problem are we trying to solve?

Problem Statement

1. **Cyberattacks continue** to be a major threat to financial services. Attacks are sophisticated, well-funded and coordinated

2. Financial institutions are at **different levels of maturity** in terms of usage of intelligence

3. Currently, financial institutions are **fragmented** using different services, technologies, products and intelligence data sources

4. Currently, financial institutions **do not systematically share** intelligence between themselves

A unified approach for cybersecurity information sharing across financial sector participants, given their market responsibility, is needed

What are the aims of information sharing?

Objectives

1. To **prevent, detect, respond and raise awareness** of cybersecurity threats to financial institutions
2. To enable relevant and **actionable intelligence** sharing between financial institutions, Law Enforcement and be potentially extendable to wider ecosystem
3. To encourage **active contribution** and active participation within a 'trusted circle', rather than passive consumption or weak usage
4. To synthesize and actively propagate the sharing of **strategic intelligence** in addition to operational TTPs and tactical IOCs indicators
5. To **continuously learn** and evolve, as a collective, with regard to the process of analysing, developing and sharing cybersecurity intelligence

Cyber Information Sharing Initiatives

How should we approach the problem?

Approach should …

… public-private partnership…collectively determine the **"why, what, when, how, who"** together

… not 'reinvent the wheel', should **re-use proven components** (commercial / open source) and use best practice

… 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 members

… be **ambitious**: plan big, **start small** and allow community members to **implement at their own pace**

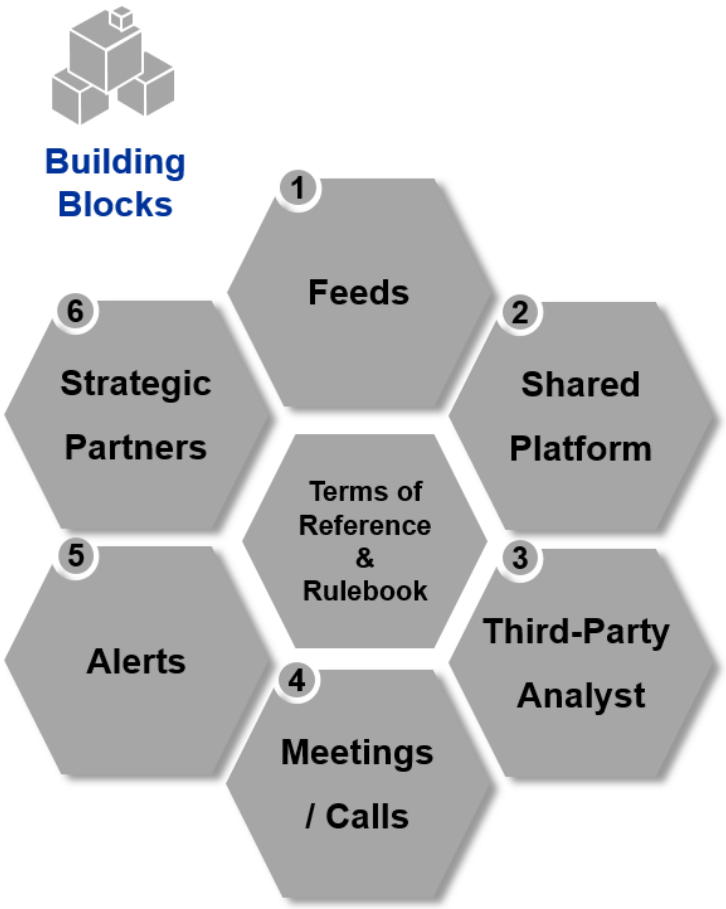
… allow any **costs to be aggregated** and shared across all community members

… focus on **sharing between community members** and should exclude regulatory / supervisory reporting, and in many cases, should exclude regulators and supervisors from the sharing community altogether

Systematic approach: What to share, with whom and when?

What		Who	When
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 organisation's threat landscape.***	E.g. Board	E.g. Quarterly
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 one 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. CISO	E.g. Daily, weekly, etc
Tactical	Tactical information/intelligence refers to 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***.	E.g. SOC, operational staff	E.g. Real-time, daily

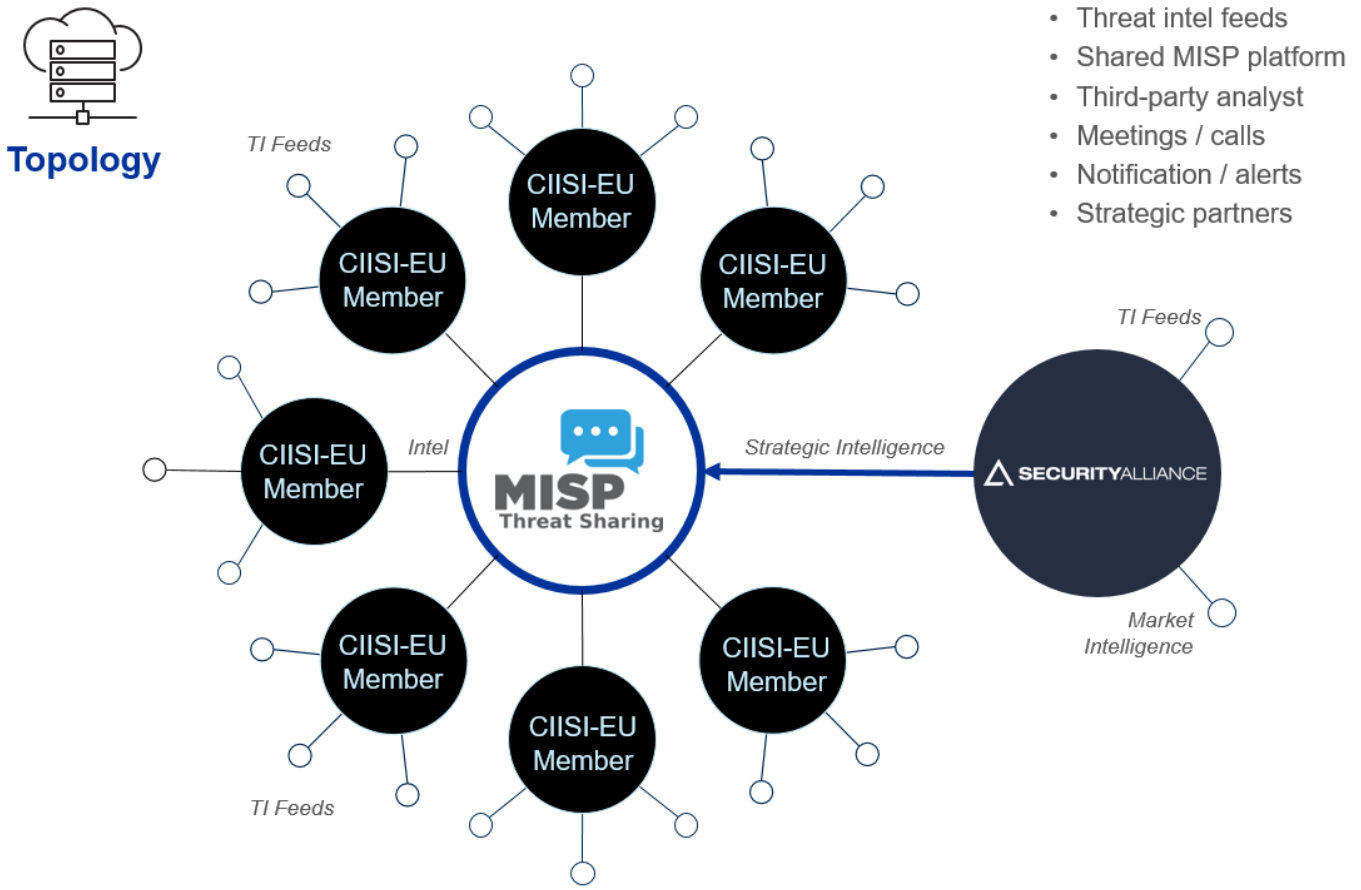
Potential building blocks – an example



1. Allow members to continue to use exist **source feeds**, commercial and/or open source
2. Utilise a **central shared platform** that stores operational and technical intelligence information, working as a 'circle of trust'
3. Contract with a **third-party cybersecurity analyst** to add value through synthesis of **strategic information**
4. Host regular TLP:RED **meetings / calls** to share information and reinforce circle of trust
5. Use simple mechanism for emergency notification and **alerts**
6. Over time, engage with **strategic partners** to enrich the information and intelligence and to bridge communities, sectors or geographies

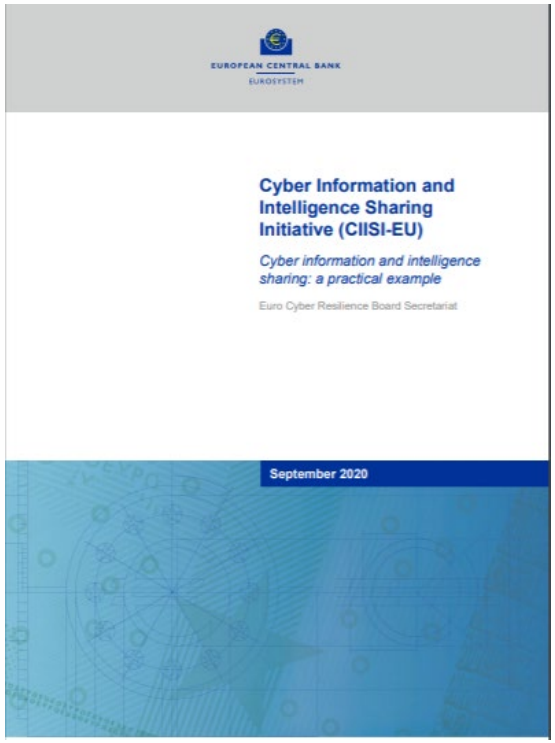
Anchor around a common **Terms of Reference & Rulebook** which describes rules of engagement including membership, usage and contact maintenance and taxonomy, principles and modalities of sharing

Working example: How does CIISI-EU work?



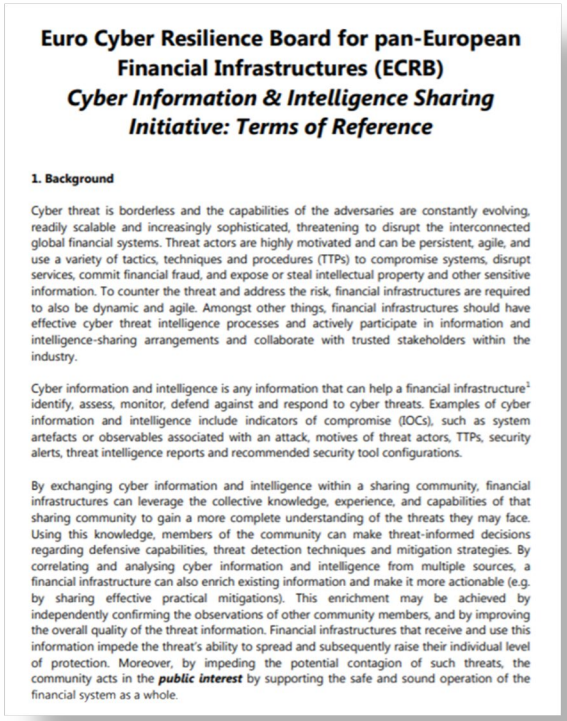
CIRCL hosts the central MISP platform. Each member connects via HTTPS browser or hosts their own sync'd MISP instance. CIISI-EU members elect what to share onto MISP, depending on significance

Consolidate Terms of Reference and Rulebook – working example for inspiration



… to operationalize the model, on a multilateral basis, critical that there are governing documents for all members – the **Terms of Reference** which informally binds all parties together (not-legally binding) and a **Rulebook** which extrapolates in detail the detailed modalities of sharing, the taxonomy, the protocols for participating, the principles of sharing, etc

… documents should be drafted together and reviewed by **legal counsel** and **data protection officers** of each member



Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)

Cyber Information & Intelligence Sharing Initiative: Terms of Reference

1. Background

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, financial infrastructures are required to also be dynamic and agile. Amongst other things, financial infrastructures 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 a financial infrastructure[1] 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, financial infrastructures 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, a financial infrastructure 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. Financial infrastructures that receive and use this information 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.

Sharing schema: Strategic, Operational and Tactical

Level	Strategic Reporting					
Description	This is inherently information and intelligence that drives decision makers and planning in the mid to long term, typically at senior level. In this instance, Strategic Intelligence supports the ECRB on setting strategy and objectives based on the changing landscape and future considerations. NATO - The level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them.					
Potential Sources	Governments, Regulators, International Institutions, Universities, Political & Strategic Studies Orgs, Geo-political analysts, Financial Market Analysts, News and Media, Human Intelligence, Trend analysis of Tact & Op data					
Preferred Dissemination Medium				**PRIMARY**	**SECONDARY**	
Intelligence Type	**What to Share**	**Required Content**	**MSC[13]**	**ThreatMatch Taxonomy**	**MISP Taxonomy**	**Note(s)**
Incidents	Incidents of a **strategic nature** not previously covered in 'Threat Incidents Tactical' or 'Threat Incidents Operational'			*TM -> Incident*	*MISP -> Event*	
		Originator	M	Show Org Name	orgc_id	
		Type of Incident	M	Incident Tag	TM:Incident MISP Taxonomy	
		Title	M	Title	info	
		Description	M	Overview	attribute > external analysis > text	
		Start DTG	S	Date	first_seen (external analysis attribute)	
		End DTG	S	Date	last seen (external analysis attribute)	
		Target	M	Targets	Text Tag	
		Target Sector	S	Sector Relevance	TM:Sector MISP Taxonomy	
		Target Geo	S	Target Geography	MISP Galaxy Geography	
		Ass. Actors	S	Associated Profiles	see SecAlliance actor profile galaxy	
		Ass. Events	C	Associated Profiles	Event ID	
		Dissemination	M	Distribution	Sharing Group	
		TLP Levels	M	TLP	TLP Tag - MISP Taxonomy	

Key components of Rulebook:

- Clear determination of **levels of information** to be shared: strategic, operational and tactical;
- Multilateral **principles** for information sharing
- **MoSCoW** principle: Must, Should, Could, Wont;
- Clearly agreed **Taxonomies, frameworks, terminology** and conventions for sharing
- Comprehensive **sharing schema**

This should be an evolving and iterative process

Recap

- Incident reporting is a key element to build cyber resilience within a technology driven environment

- Incident reporting framework enables authorities and market to manage cyber incidents more effectively and in a timely manner

- Convergence in incident reporting is important, and this will require a holistic, collaborative approach, with due consideration given to protocols, taxonomies, reporting mechanisms and public-private engagement
- Regulation and enablers can and should be multi-dimensional and have a range of different components

- Information sharing and testing are key elements to build cyber resilience within a technology driven environment

Thank you!