JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

ANNEX IV

Data glossary and instructions for notification of significant cyber threats

Data field	Description	Mandatory field	Field type
1. Name of the entity submitting the notification	Full legal name of the entity submitting the notification.	Yes	Alphanumeric
2. Identification code of the entity submitting the notification	Identification code of the entity submitting the notification. Where financial entities submit the notification/report, the identification code is to be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020. Where a third-party provider submits a report for a financial entity, they can use an identification code as specified in the Commission Implementing Regulation specifying Art. 28(9) from Regulation (EU) 2022/2554.	Yes	Alphanumeric
3. Type of financial entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report.	Yes, if the report is not provided by the affected financial entity directly.	Choice (multiselect): - credit institution - payment institution - exempted payment institution - account information service provider - electronic money institution - exempted electronic money institution - investment firm

Data field	Description	Mandatory field	Field type
			- crypto-asset service provider - issuer of asset-referenced tokens - central securities depository - central counterparty - trading venue - trade repository - manager of alternative investment fund - management company - data reporting service provider - insurance and reinsurance undertaking - insurance intermediary, reinsurance intermediary and ancillary insurance intermediary - institution for occupational retirement provision - credit rating agency - administrator of critical benchmarks - crowdfunding service provider

Data field	Description	Mandatory field	Field type
			- securitisation repository
4. Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Yes, if the financial entity is different from the entity submitting the notification.	Alphanumeric
5. LEI code of the financial entity	Legal Entity Identifier (LEI) of the financial entity notifying the significant cyber threat, assigned in accordance with the International Organisation for Standardisation.	Yes, if the financial entity notifying the significant cyber threat is different from the entity submitting the report	Unique alphanumeric 20 character code, based on ISO 17442-1:2020
6. Primary contact person name	Name and surname of the primary contact person of the financial entity.	Yes	Alphanumeric
7. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication.	Yes	Alphanumeric (
8. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Yes	Alphanumeric
9. Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity, where available.	Yes, if name and surname of the second contact person of the financial entity or an entity submitting the notification for the financial entity is available.	Alphanumeric

Data field	Description	Mandatory field	Field type
10. Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication, where available.	Yes, if email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication is available.	Alphanumeric
11. Second contact person telephone	Telephone number of the second contact person that can be used by the competent authority for follow-up communication, where available. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX).	Yes, if telephone number of the second contact person that can be used by the competent authority for follow-up communication is available.	Alphanumeric
12. Date and time of detection of the cyber threat	Date and time at which the financial entity has become aware of the significant cyber threat.	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
13. Description of the significant cyber threat	Description of the most relevant aspects of the significant cyber threat. Financial entities shall provide: - a high-level overview of the most relevant aspects of the significant cyber threat; - the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited;	Yes	Alphanumeric

Data field	Description	Mandatory field	Field type
	- information about the probability of materialisation of the significant cyber threat; and - Information about the source of information about the cyber threat.		
14. Information about potential impact	Information about the potential impact of the cyber threat on the financial entity, its clients and/or financial counterparts if the cyber threat has materialised	Yes	Alphanumeric
15. Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materialised.	Yes	Choice (multiple): - Clients, financial counterparts and transactions affected - Reputational impact - Duration and service downtime - Geographical spread - Data losses - Critical services affected - Economic impact
16. Status of the cyber threat	Information about the status of the cyber threat for the financial entity and whether there have been any changes in the threat activity. Where the cyber threat has stopped communicating with the financial entity's information systems, the status can be marked as inactive. If the financial entity has information that the threat remains active against other parties or the financial system as a whole, the status should be marked as active.	Yes	Choice: - active - inactive

Data field	Description	Mandatory field	Field type
17. Actions taken to prevent materialisation	High-level information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable.	Yes	Alphanumeric
18. Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities.	Yes, if other financial entities or authorities have been informed about the cyber threat).	Alphanumeric
19. Indicators of compromise	Information related to the significant threat that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable. The IoC provided by the financial entity may include, but not be limited to, the following categories of data: • IP addresses; • URL addresses; • Domains; • File hashes; • Malware data (malware name, file names and their locations, specific registry keys associated with malware activity); • Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); • E-mail message data (sender, recipient, subject, header, content); • DNS requests and registry configurations; • User account activities (logins, privileged user account activity, privilege escalation);	Yes, if information about indicators of compromise connected with the cyber threat are available.)	Alphanumeric

Data field	Description	Mandatory field	Field type
	• Database traffic (read/write), requests to the same file. In practice, this type of information may include data relating to, for example, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to "command and control" servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or websites observed hosting malware or exploit kits, etc.		
20. Other relevant information	Any other relevant information about the significant cyber threat	Yes, if applicable and if there is other information available, not covered in the template.	Alphanumeric