Deloitte.

DORA | RTS on ICT Incident Classification based on EBF's Position

January 2024

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Introduction

On June 19th, 2023, the European Supervisory Authorities (ESAs), EBA, EIOPA, and ESMA, published the first batch of Consultation Papers for the technical standards mandated by the Digital Operational Resilience Act (DORA) which aims at collecting market participants' feedback on their development.

The European Banking Federation (EBF) and Deloitte have held a joint workshop to gather feedback from the EBF's members, specifically around the Consultation Paper for the RTS *"on specifying the criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554*" that will be submitted to the European Commission on January 17th, 2024.

Below are reported the main key attention points raised by the EBF members during the consultation of the Draft RTS:

Unclear definition of Critical Services

Sound Application of Proportionality Principle and Risk-based Approach

The Challenges in the Notification of Significant Threats

Unclear Definition of Critical Services

According to the RTS, critical services are those financial services requiring authorization or registration in the European Union, or information and communication technology (ICT) services that support critical or important functions within a financial entity.

According to this definition, potentially all ICT services could be considered critical, since in a financial entity all ICT services would likely support critical or important functions. In addition, the very definition of critical or important functions is highly unclear creating additional confusion for the financial entity. This would lead to a risk of overreporting, considering that the criticality of the service is a primary criterion that could trigger the notification to the authority.

The materiality thresholds contribute to this risk, stating that *"Any impact on critical services which has been escalated to senior management or the management body, shall be considered as meeting the threshold of the criterion for major incidents"*. This means that potentially any incident affecting critical services and subsequently escalated internally would meet the threshold of this criterion.

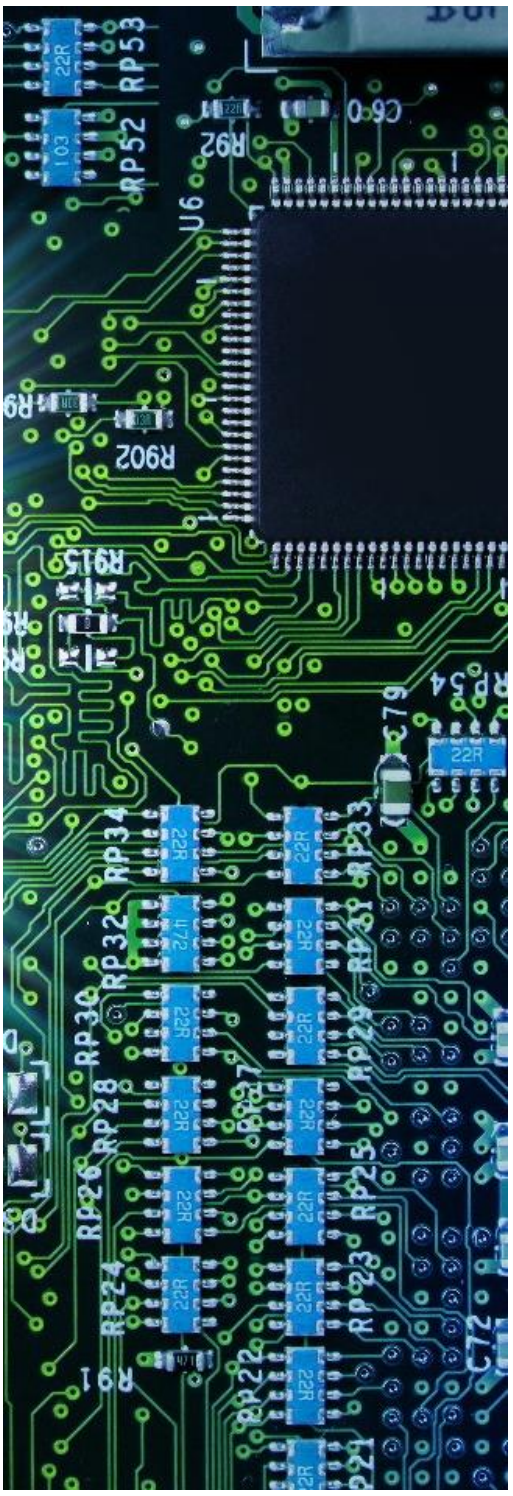
The above could also lead to a different application of the Regulation, since the internal escalation processes established by a financial entity depend on the entity's internal risk management criteria, which can vary from one entity to another.

To overcome these risks, the materiality threshold could reference a "significant impact" rather than "any impact." In this way, the financial entity would consider not only the mere escalation to the management but also the extent to which the criticality of the service will affect the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency.

Sound Application of Proportionality Principle and Risk-based Approach

Art. 4 of the DORA explicitly states that, in the application of the requisites of the incident management chapter, the financial entities should have a proportionate and risk-based approach. In light of the above, although it is necessary to classify the incident based on a set of pre-defined criteria and related thresholds, these should be always applied by financial entities considering the peculiarities of each event that occurred, taking into account the business objective of the entity, the size of the business, and the risk profile.

The regulatory authority has wisely chosen to embed the principle of proportionality directly into the criteria, involving both relative and absolute thresholds, to trigger reporting. Nevertheless, it is crucial to fine-tune the thresholds and criteria definitions, allowing financial entities the flexibility to assess incidents on a case-by-case basis. Below, some examples are presented to better illustrate this concept.



Number of clients affected

The number of clients affected is considered as a primary criterion, and its related materiality threshold according to Article 9 of the RTS is higher than 10% of all clients using the affected service of the financial entity. However, subsidiaries that have very few clients (clients with large or famous funds) can have a significant financial impact. In the case of fraud, the severity of a single customer losing €1M outweighs that of 50,000 customers losing €20 due to an internal billing error. A valuable solution could be to rely on thresholds and best practices established by current regulations; for example, for measuring the impact on clients, PSD2 indicates a threshold of 25%.

Reputational damage

The same goes for the secondary criterion of the reputational impact, which can vary depending on the size of the bank and the "scale" of the media involved. Larger banks may experience multiple levels of reputational harm compared to smaller banks. The possibility that a non-significant incident in a large financial entity attracts media attention is greater than in the case of small entities or organizations. Moreover, regarding media attention, the relevance and geographical coverage of the specific communication media where the incident has been published should also be considered. The reputational impact is different if the incident is published in media with local coverage (a specific city or region), compared to being published in media with national or international coverage.

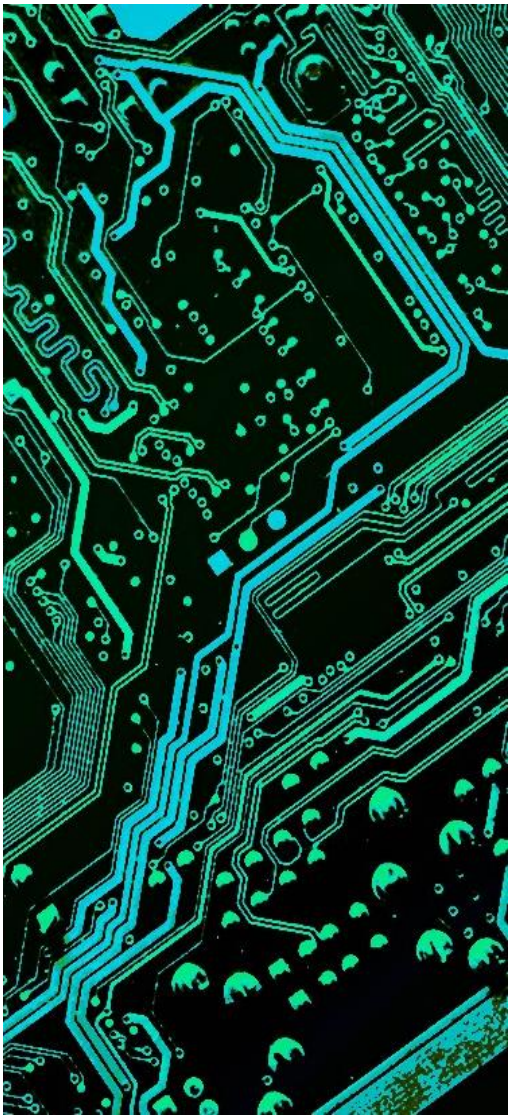
Duration and service downtime

According to the RTS, service downtime should be measured from the moment the service becomes fully or partially unavailable to clients or the financial entity itself until regular activities are restored. The RTS establishes a materiality threshold of 2 hours to resolve an incident; however, there are also qualitative elements to be considered.

Some critical business processes or services are only critical during specific timeframes. For example, the impact of service downtime will be more severe if the incident occurs during business hours than if it occurs during the night or the weekend. The threshold should be set according to the business needs of the financial entity, taking into consideration what is established in the Business Impact Analysis (BIA) or Service Level Agreements (SLA).

The same reasoning applies to the duration of the incident, measured from the moment it occurs until resolution, with a materiality threshold set at 24 hours. However, a 24-hour materiality threshold for resolving incidents may be unreasonable, particularly for certain cybersecurity incidents that do not result in service downtime.

Based on incident and problem management practices, some financial entities may not consider an incident resolved until the root cause has been determined and permanent mitigating measures have been implemented, which could take weeks or even months. On the other hand, other financial entities may deem an incident resolved as soon as normal operations are resumed. For instance, a cybersecurity incident resulting in a data breach may not likely be resolved within 24 hours. Resolving such an incident involves not only addressing the cause of the data breach but also implementing measures to minimize its impact and prevent data publication or fraudulent use.



The Challenges in the Notification of Significant Threats

Regarding the notification of significant threats, financial entities would need to establish procedures, processes, and tools to perform a thorough threat intelligence analysis to understand the potential of threats becoming major incidents. The phrasing of the RTS implies that the financial entities would need to:

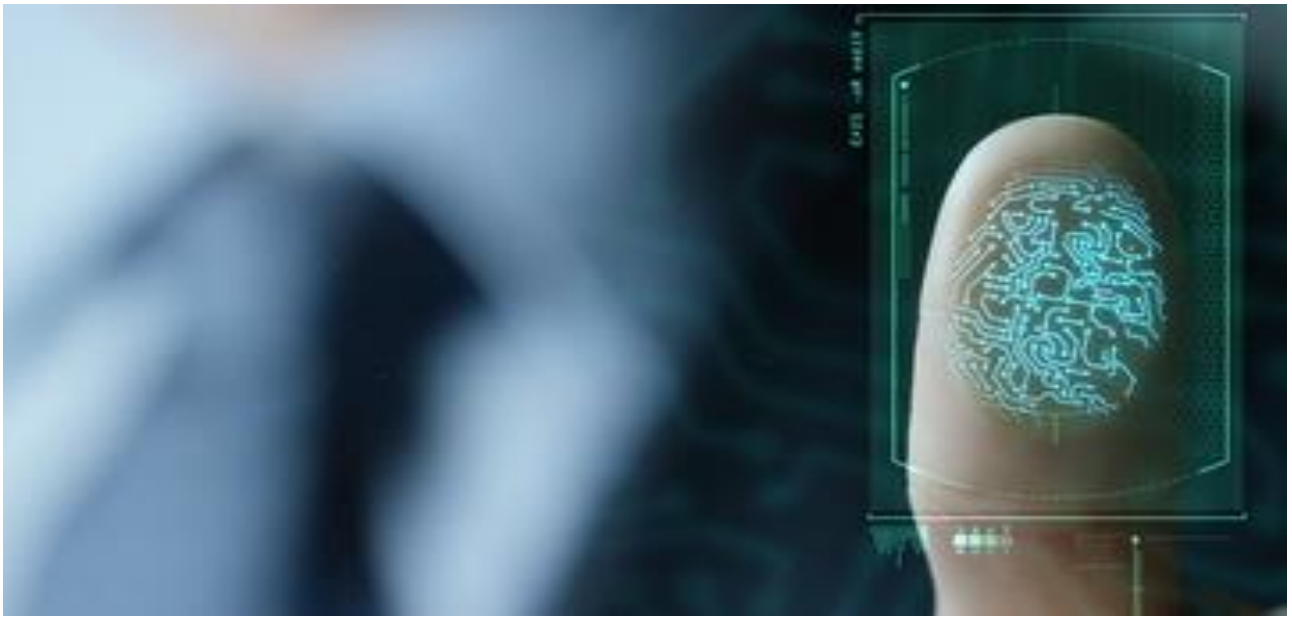
- Correlate threats and analyze the geopolitical and business landscape specific to the Financial Entity.
- Understand the interdependencies with other Financial Entities and third parties.
- Link the threats to critical or important functions within the organization.
- Gain insights into threats targeting other Financial Entities, third-party providers, clients, or financial counterparts.

Financial organizations are therefore expected to establish procedures and processes, as well as acquire tools to collect, process, and analyze information about cyber threats. Moreover, organizations should also set up mechanisms for receiving intelligence from the financial community and other external parties. This would entail resources and a level of expertise some organizations may lack.

In addition, it is important to note that the responsibility of analyzing threats typically lies with dedicated communities and intelligence organizations, rather than individual organizations themselves. Organizations may lack the resources and expertise to perform in-depth threat analysis. In the context of threat reporting, it would be important for organizations to receive input on threats from the relevant authorities, rather than the other way around.

Lastly, the financial entity should target the reporting specifically to threats that directly threaten the organization itself, considering its context and not the broader financial sector.

It should also be stressed that the nature of cyber threat reporting should remain voluntary.



Transforming mandated incident reporting into valuable Learning

The ESAs have the ultimate task of transforming the process of incident management and reporting into a valuable learning experience for organizations and the financial sector. Currently, while the market shares information with the authorities, it does not receive adequate support in return. This creates a situation where the perception of incident reporting is more associated with the possibility to impose/face sanctions rather than utilizing them as learning experiences to enhance the overall resilience of the financial sector.

The focus of incident reporting should shift towards enabling organizations to allocate resources effectively for mitigating incidents, rather than merely engaging in bureaucratic exercises and grappling with overwhelming compliance burdens that do not contribute to enhancing security and resilience. The authorities should help organizations establish clear boundaries for reporting based on common sense, encouraging continuous information sharing between the market and the authorities.

A potential solution could involve sharing anonymized data on incident. This approach would incentivize entities to join information-sharing communities, fostering collaboration between market participants and authorities.

For this transformation to occur, it is crucial for the authorities to establish an Incident Hub that facilitates coordination and effective information sharing, as established in DORA. Incident reporting should not become a burden for organizations, which have to deal not only with the incident itself but also with reporting to the authorities, fearing sanctions. Instead, it should be a collaborative experience where the authorities support financial entities by providing intelligence and information to address incidents more efficiently.

Contributors

Deloitte:

Daniele Frasca
Partner | Risk Advisory | Italy
+39 3358735381
dfrasca@deloitte.it

Diego Giordano
Director | Risk Advisory | Italy
+39 3420997270
dgiordano@deloitte.it

Susanna Savarese
Manager | Risk Advisory | Italy
+39 3452689806
ssavarese@deloitte.it

European Banking Federation:

Alexandra Maniati
Senior Director of Innovation & Cybersecurity
+32 478 901 301
a.maniati@ebf.eu

Dimos Karalis
Policy Adviser of Innovation & Cybersecurity
+32 485 523 916
d.karalis@ebf.eu

Deloitte.

The Deloitte network, a leader in professional services for businesses, is present globally in more than 150 countries worldwide. With approximately 457,000 people worldwide – united by a culture that promotes integrity, constant focus on clients, commitment to colleagues and valuing differences – Deloitte specializes in all major market sectors and accompanies companies in developing and implementing innovative, sustainable and market-to-market solutions. Deloitte offers Audit & Assurance, Consulting, Financial Advisory, Risk Advisory, Tax and Legal services in various market sectors. It also brings to its customers transversal skills and high-quality services, providing them with the necessary knowledge to face the most complex business challenges.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.