Pursuant to Article 35, paragraph 1 subparagraph 1.1 and Article 65 of the Law No. 03/L-209 on Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No.77 / 16 August 2010), as amended and supplemented by Law No. 05/L –150 (Official Gazette of the Republic of Kosovo / No. 10 / 03 April 2017) and pursuant to Article 96 paragraph 5, and article 135 of the Law No. 08/L-328 on Payment Services, the Board of the Central Bank of the Republic of Kosovo, at its meeting held on December 17, 2024, approved the following:

REGULATION ON THE NOTIFICATION OF MAJOR OPERATIONAL OR SECURITY INCIDENTS TO THE CENTRAL BANK OF KOSOVO

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose and scope

1. This Regulation lays down the criteria for the classification of major operational or security incidents by payment service providers, as well as the format and procedures they should follow to report such incidents to the Central Bank of Kosovo pursuant to Article 96 of the Law No. 08/L-328 on Payment Services.
2. This Regulation shall apply to the classification and reporting of major operational or security incidents pursuant to Article 96 of Law No. 08/L-328 on Payment Services.
3. This Regulation applies to all payment service providers that are licensed, authorized or registered to provide payment services in Kosovo in accordance with Law No. 08/L-328 on Payment Services.
4. This Regulation shall apply to all incidents that fall under the definition of "major operational or security incident", which includes both external and internal events that may be either malicious or accidental.
5. This Regulation shall also apply if the major operational or security incident originates outside Kosovo (e.g. if an incident originates in the parent company or in a subsidiary established outside Kosovo) and affects the payment services provided by a payment service provider located in Kosovo, either directly (a payment-related service is provided by the affected non-Kosovor company) or indirectly (the payment service provider's ability to continue to carry out its payment activity is otherwise jeopardized as a result of the incident).
6. This Regulation shall also apply to major incidents affecting functions outsourced by payment service providers to third parties.

Article 2
Definitions

1. The terms and definitions used in this Regulation shall have the same meaning as in the Law No. 08/L-328 on Payment Services.
2. In addition to paragraph 1 of this Article, for the purpose of implementing this Regulation, the following terms and abbreviations shall have the following meanings:
   2.1. **"availability"** means the property of payment-related services being fully accessible and usable by PSUs, according to acceptable levels predefined by the PSP;
   2.2. **"authenticity"** means the property of a source being what it claims to be;
   2.3. **"CBK"** means the Central Bank of Kosovo;
   2.4. **"confidentiality"** means the property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
   2.5. "cross-border payment transaction" means a payment transaction initiated by a payer or by or through a payee where either the payer's PSP or the payee's PSP is located in Kosovo and the other PSP is located outside Kosovo as well as within the SEPA area;
   2.6. **"integrity"** means the property of safeguarding the accuracy and completeness of assets, including data;
   2.7. **"operational or security incident"** means a singular event or a series of linked events unplanned by the PSP which has or will likely have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment-related services;
   2.8. **"payment-related services"** means any business activity with the meaning of subparagraph 1.2 of paragraph 1 of Article 4 of the Law on Payment Services, and all the necessary technical supporting tasks for the correct provision of payment services;
   2.9. **"Law on Payment Services"** means Law No. 08/L-328 on Payment Services;
   2.10. **"PSP"** means a payment service provider as defined in the Law on Payment Service;
   2.11. **"PSU"** means a payment service user as defined in the Law on Payment Service.
   2.12. "**SEPA area**" means the geographical scope of the SEPA schemes as determined by the criteria established by the EPC.

CHAPTER II
NOTIFICATION OF MAJOR OPERATIONAL OR SECURITY INCIDENTS TO THE CENTRAL BANK OF KOSOVO

Article 3
Classification as a major incident

1. PSPs should classify as major those operational or security incidents that fulfil, as set out in paragraph 4 of this Article and following the assessment set out in this Regulation, the following:

   1.1. one or more criteria at the "higher impact level"; or

   1.2. three or more criteria at the "lower impact level".

2. PSPs should assess an operational or security incident against the following criteria and their underlying indicators:

   2.1. *transactions affected*: PSPs should determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services;

   2.2. *PSUs affected*: PSPs should determine the number of PSUs affected both in absolute terms and as a percentage of the total number of PSUs;

   2.3. *breach of security of network or information systems*: PSPs should determine whether any malicious action has compromised the security of network or information systems related to the provision of payment services;

   2.4. *service downtime*: PSPs should determine the period during which the service will likely be unavailable for the payment service user or during which the payment order – within the meaning of subparagraph 1.12 of paragraph 1 of Article 4 of the Law on Payment Services – cannot be fulfilled by the PSP;

   2.5. *economic impact*: PSPs should determine the monetary costs associated with the incident holistically and consider both the absolute figure and, when applicable, the relative importance of these costs in relation to the size of the PSP (i.e. to the PSP's Tier-1 capital);

   2.6. *high level of internal escalation*: PSPs should determine whether this incident has been or will likely be reported to their executive officers;

   2.7. *other PSPs or relevant infrastructures potentially affected*: PSPs should determine the systemic implications the incident will likely have, i.e. its potential to spill over beyond the initially affected PSP to other PSPs, financial market infrastructures and/or payment schemes;

   2.8. *reputational impact*: PSPs should determine how the incident can undermine users' trust in the PSP itself and, more generally, in the underlying service or the market as a whole.

3. PSPs should calculate the value of the indicators according to the following methodology:

   3.1. transactions affected:

      3.1.1. as a general rule, PSPs should understand as "transactions affected" all national and cross-border transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (have the funds been recovered or not) or where proper execution is prevented or hampered in any other way by the incident;

      3.1.2. for operational incidents affecting the ability to initiate and/or process transactions, PSPs should report only those incidents with a duration longer than one hour. The

duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident;

3.1.3. furthermore, PSPs should understand the regular level of payment transactions to be the daily annual average of national and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. In case PSPs do not consider this figure to be representative (e.g. due to seasonality), they should use another more representative metric instead and convey to the CBK the underlying rationale for this approach in the corresponding field of the template as provided for in Annex.

3.2. PSUs affected:

3.2.1. PSPs should understand as "PSUs affected" all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected PSP that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident. PSPs should recur to estimations based on past activity in order to determine the number of PSUs that may have been using the payment service during the lifetime of the incident;

3.2.2. in the case of groups, each PSP should only consider its own PSUs. In the case of a PSP offering operational services to others, that PSP should only consider its own PSUs (if any), and the PSPs receiving those operational services should assess the incident in relation to their own PSUs;

3.2.3. for operational incidents affecting the ability to initiate and/or process transactions, PSPs should report only those incidents that affect PSUs with a duration longer than one hour. The duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident;

3.2.4. furthermore, PSPs should take as the total number of PSUs the aggregated figure of national and cross-border PSUs contractually bound with them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive PSUs.

3.3. breach of security of network or information systems:

3.3.1. PSPs should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of payment services.

3.4. service downtime:

3.4.1. PSPs should consider the period of time that any task, process or channel related to the provision of payment services is or will likely be down and, thus, prevents i) the initiation and/or execution of a payment service and/or ii) access to a payment account. PSPs should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for

business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If PSPs are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

3.5. economic impact:

3.5.1. PSPs should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, PSPs should consider expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, PSPs should only consider those that are already known or very likely to materialize.

3.6. high level of internal escalation:

3.6.1. PSPs should consider whether, as a result of the impact on payment related services, the management body as defined in the CBK Regulation on ICT and security risk management has been informed, about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, PSPs should consider whether, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

3.7. other PSPs or relevant infrastructures potentially affected:

3.7.1. PSPs should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or payment schemes that support it and the rest of PSPs. In particular, PSPs should assess whether the incident has been or will likely be replicated at other PSPs, whether it has affected or will likely affect the smooth functioning of financial market infrastructures or whether it has compromised or will likely compromise the sound operation of the financial system as a whole. PSPs should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external or whether the PSP has stopped or will likely stop fulfilling its obligations in the financial market infrastructures it is a member of.

3.8. reputational impact

3.8.1. PSPs should consider the level of visibility that, to the best of their knowledge, the incident has gained or will likely gain in the marketplace. In particular, PSPs should consider the likelihood of the incident causing harm to society as a good indicator of its potential to impact their reputation. PSPs should take into account whether i) PSUs and/or other PSPs have complained about the adverse impact of the incident, ii) the incident has impacted a visible payment service related process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.), iii) contractual obligations have been or will likely be missed, resulting in the publication of legal actions against the PSP, iv) regulatory requirements have not been complied with,

resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available, and v) a similar type of incident has occurred before.

4. PSPs should assess an incident by determining, for each individual criterion, whether the relevant thresholds in Table 1 are or will likely be reached before the incident is solved.

Table 1: Thresholds

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the PSP's regular level of transactions (in terms of number of transactions) **and** duration of the incident > 1 hour* **or** > EUR 5000,000 **and** duration of the incident >1 hour*	>25% of the PSP's regular level of transactions (in terms of number of transactions) **or** > EUR 15,000,000
PSUs affected	>5,000 **and** duration of the incident > 1 hour* **or** > 10% of the PSP's PSUs **and** duration of the incident >1 hour*	> 50,000 **or** > 25% of the PSP's PSUs
Service downtime	>2 hours	Not applicable
Breach of security of network or information systems	Yes	Not applicable

Economic impact	Not applicable	> Max (0.1% Tier-1 capital**, EUR 200,000) **or** > EUR 5,000,000
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be triggered
Other PSPs or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

* The threshold concerning the duration of the incident for a period longer than one hour applies only to operational incidents that affect the ability of the PSP to initiate and/or process transaction.

** Tier-1 capital as defined in Article 6 of Regulation on Capital Adequacy of Banks.

5. PSPs should resort to estimations if they do not have actual data to support their judgments as to whether a given threshold is or will likely be reached before the incident is solved (e.g. this could happen during the initial investigation phase).
6. PSPs should carry out this assessment on a continuous basis during the lifetime of the incident, so as to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major). Any reclassification of the incident from major to non-major should be communicated to the CBK in line with the requirement of Article 5 paragraph 4 subparagraph 4.5 of this regulation and without undue delay.

Article 4
Notification process

1. PSPs should collect all relevant information, produce an incident report by completing the template in the Annex and submit it to the CBK. PSPs should complete all fields of the template following the instructions provided in the Annex 2.
   1.1. PSPs should use the same template when submitting the initial, intermediate, and final reports related to the same incident. PSPs should therefore complete a single template in an incremental manner and update, where applicable, the information provided with previous reports;
   1.2. PSPs should further present to the CBK, if applicable, a copy of the information provided (or that will be provided) to their users, as foreseen in the paragraph 2 of Article 96 of the Law on Payment Services, as soon as it is available;

1.3. PSPs should, upon request by the CBK, provide any additional documents complementing the information submitted with the standardized template. PSPs should follow up on any requests from the CBK to provide additional information or clarifications regarding already submitted documentation;

1.4. any additional information contained in the documents provided by PSPs to the CBK, either on the initiative of the PSP or upon the request of the CBK pursuant to subparagraph 1.3, should be reflected by the PSP in the template under paragraph 1;

1.5. PSPs should always preserve the confidentiality and integrity of the information exchanged and their proper authentication towards the CBK.

2. **Initial report**

2.1. PSPs should submit an initial report to the CBK after an operational or security incident has been classified as major. The CBK should acknowledge the receipt of the initial report without undue delay and assign a unique reference code unequivocally identifying the incident. PSPs should indicate this reference code when submitting an update either to the initial report or to the intermediate and final reports related to the same incident, unless the intermediate and final reports are submitted jointly with the initial report;

2.2. PSPs should send the initial report to the CBK within four hours from the moment the operational or security incident has been classified as major. If the reporting channels of the CBK are known not to be available or operated at that time, PSPs should send the initial report as soon as the channels become available/operational again;

2.3. PSPs should classify the incident in accordance with paragraphs 1 and 4 of Article 4 in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information required for the classification of the incident is available to the PSP. If a longer time is needed to classify the incident, PSPs should explain in the initial report submitted to the CBK the reasons why;

2.4. PSPs should also submit an initial report to the CBK when a previous non-major incident has been reclassified as a major incident. In this case, PSPs should send the initial report to the CBK immediately after the change of status is identified, or, if the reporting channels of the CBK are known not to be available or operated at that time, as soon as they become available/operational again;

2.5. PSPs should provide headline-level information in their initial reports (i.e. section A of the template), thus featuring some basic characteristics of the incident and its foreseen consequences based on the information available immediately after it was classified as major. PSPs should resort to estimations when actual data are not available.

3. **Intermediate report**

3.1. PSPs should submit the intermediate report when regular activities have been recovered and business is back to normal, informing the CBK of this circumstance. PSPs should consider business is back to normal when activity/operations are restored with the same level of service/conditions as defined by the PSP or laid out externally by a service level agreement (processing times, capacity, security requirements, etc.) and when contingency measures are

no longer in place. The intermediate report should contain a more detailed description of the incident and its consequences (section B of the template);

3.2. if regular activities have not yet been recovered, PSPs should submit an intermediate report to the CBK within three working days from the submission of the initial report;

3.3. PSPs should update the information already provided in sections A and B of the template when they become aware of significant changes since the submission of the previous report (e.g. whether the incident has escalated or decreased, new causes identified, or actions taken to fix the problem). This includes the case where the incident has not been resolved within three working days, which would require PSPs to submit an additional intermediate report. In any case, PSPs should submit an additional intermediate report at the request of the CBK.

3.4. as in the case of initial reports, when actual data are not available PSPs should make use of estimations.

3.5. should business be back to normal before four hours have passed since the incident was classified as major, PSPs should aim at simultaneously submitting both the initial and the intermediate report (i.e. filling out sections A and B of the template) within the four-hour deadline.

4. **Final report**

4.1. PSPs should submit a final report when the root cause analysis has taken place (regardless of whether mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any potential estimates;

4.2. PSPs should deliver the final report to the CBK in a maximum of 20 working days after business is deemed back to normal. PSPs needing an extension of this deadline (e.g. when there are no actual figures on the impact available or the root causes have not been identified yet) should contact the CBK before the time has elapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report;

4.3. should PSPs be able to provide all the information required in the final report (i.e. section C of the template) within the four-hour window since the incident was classified as major, they should aim at providing the information related to initial, intermediate, and final reports together;

4.4. PSPs should include in their final report full information, i.e.: i) actual figures on the impact instead of estimates (as well as any other update needed in sections A and B of the template), and ii) section C of the template which includes, if already known, the root cause and a summary of measures adopted or planned to be adopted to remove the problem and prevent its reoccurrence in the future;

4.5. PSPs should also send a final report when, because of the continuous assessment of the incident, they identify that an already reported incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before the incident is resolved. In this case, PSPs should send the final report as soon as this circumstance is detected and, in any case, within the deadline for the submission of the next report. In this situation, instead of filling out section C of the template, PSPs should check the box “incident reclassified as non-major” and provide an explanation of the reasons justifying this reclassification.

Article 5
Delegated and consolidated reporting

1. Where permitted by the CBK, PSPs wishing to delegate reporting obligations under the Law on Payment Services to a third party should inform the CBK and ensure the fulfilment of the following conditions:

   1.1. the formal contract or, where applicable, existing internal arrangements within a group underpinning the delegated reporting between the PSP and the third party unambiguously defines the allocation of responsibilities of all parties. In particular, it clearly states that, irrespective of the possible delegation of reporting obligations, the affected PSP remains fully responsible and accountable for the fulfilment of the requirements set out in Article 96 of the Law on Payment Services and for the content of the information provided to the CBK;

   1.2. the delegation complies with the requirements for the outsourcing of important operational functions as set out in:

      1.2.1. Article 21 paragraph 5 of the Law on Payment Services in relation to payment institutions and electronic money institutions;

      1.2.2. the CBK Regulation on outsourcing arrangements in relation to all PSPs.

   1.3. the information is submitted to the CBK in advance and, in any case, following any deadlines and procedures established by the CBK, where applicable.

   1.4. the confidentiality of sensitive data and the quality, consistency, integrity, and reliability of the information to be provided to the CBK are properly ensured.

2. PSPs wishing to allow the designated third party to fulfil the reporting obligations in a consolidated way (i.e. by presenting one single report referring to several PSPs affected by the same major operational or security incident) should inform the CBK, provide the contact information included under "Affected PSP" in the template and ensure the following conditions are satisfied:

   2.1. include this provision in the contract underpinning the delegated reporting;

   2.2. make the consolidated reporting conditional on the incident being caused by a disruption in the services provided by the third party;

   2.3. confine the consolidated reporting to PSPs established in Kosovo;

   2.4. provide a list of all PSPs affected by the incident;

   2.5. ensure that the third party assesses the materiality of the incident for each affected PSP and only includes in the consolidated report those PSPs for which the incident is classified as major; furthermore, ensure that, in the event of doubt, a PSP is included in the consolidated report as long as there is no evidence confirming otherwise;

   2.6. ensure that when there are fields of the template where a common answer is not possible (e.g. sections B2, B4 or C3 of the template), the third party either i) fills them out individually for each affected PSP, further specifying the identity of each PSP the information relates to, or ii) uses the cumulative values as observed or estimated for the PSPs;

2.7. the third party keeps the PSP informed at all times of all the relevant information regarding the incident and all the interactions they may have with the CBK and of the content thereof, but only to the extent possible so as to avoid any breach of confidentiality as regards the information that relates to other PSPs.

3. PSPs should not delegate their reporting obligations before informing the CBK or after having been notified that the outsourcing agreement does not meet the requirements referred to in subparagraph 1.2 of paragraph 1 above.

4. PSPs wishing to withdraw the delegation of their reporting obligations should communicate this decision to the CBK, following the deadlines and procedures established by the latter. PSPs should also inform the CBK of any material development affecting the designated third party and its ability to fulfil the reporting obligations.

5. PSPs should materially fulfil their reporting obligations without any recourse to external assistance whenever the designated third party fails to inform the CBK of a major operational or security incident in accordance with Article 96 of the Law on Payment Services and with this Regulation. PSPs should also ensure that an incident is not reported twice, individually by said PSP and once again by the third party.

6. PSPs should ensure that, in the situation where an incident is caused by a disruption in the services provided by a technical service provider (or an infrastructure) which affects multiple PSPs, the delegated reporting refers to the individual data of the PSP (except in the case of consolidated reporting).

Article 6
Operational and security policy

PSPs should ensure that their general operational and security policy clearly defines all the responsibilities for incident reporting under the Law on Payment Services, as well as the processes implemented in order to fulfil the requirements defined in this Regulation.

Article 7
Annex

This regulation is comprised of Annex 1 Reporting template for payment service providers and Annex II Guidelines addressed to the competent authorities (CBK) on the criteria for assessing the relevance of the incident and the details of the incident reports to be shared with other domestic authorities

CHAPTER III
FINAL PROVISIONS

Article 8
Transitional period

All PSPs licensed, authorized or registered by the CBK shall fully adapt their activities and operations to the provisions of this Regulation within 6 months from the date of entry into force of the Regulation.

Article 9
Enforcement, Improvement Measures and Penalties

Any violation of the provisions of this Regulation shall be subject to administrative sanctions, as set out in Article 67 of Law No. 03/L-209 on the Central Bank of the Republic of Kosovo, as amended and supplemented by Law No. 05/L -150 and paragraph 2, subparagraph 2.4 of Article 124 of Law No. 08/L-328 on Payment Services.

Article 10
Entry into force

This Regulation shall enter into force 10 (ten) days after the entry into force of Law No. 08/L-328 on Payment Services.

Dr.sc. Bashkim Nurboja
Chairperson of the Board of the Central Bank of the Republic of Kosovo

ANNEX 1

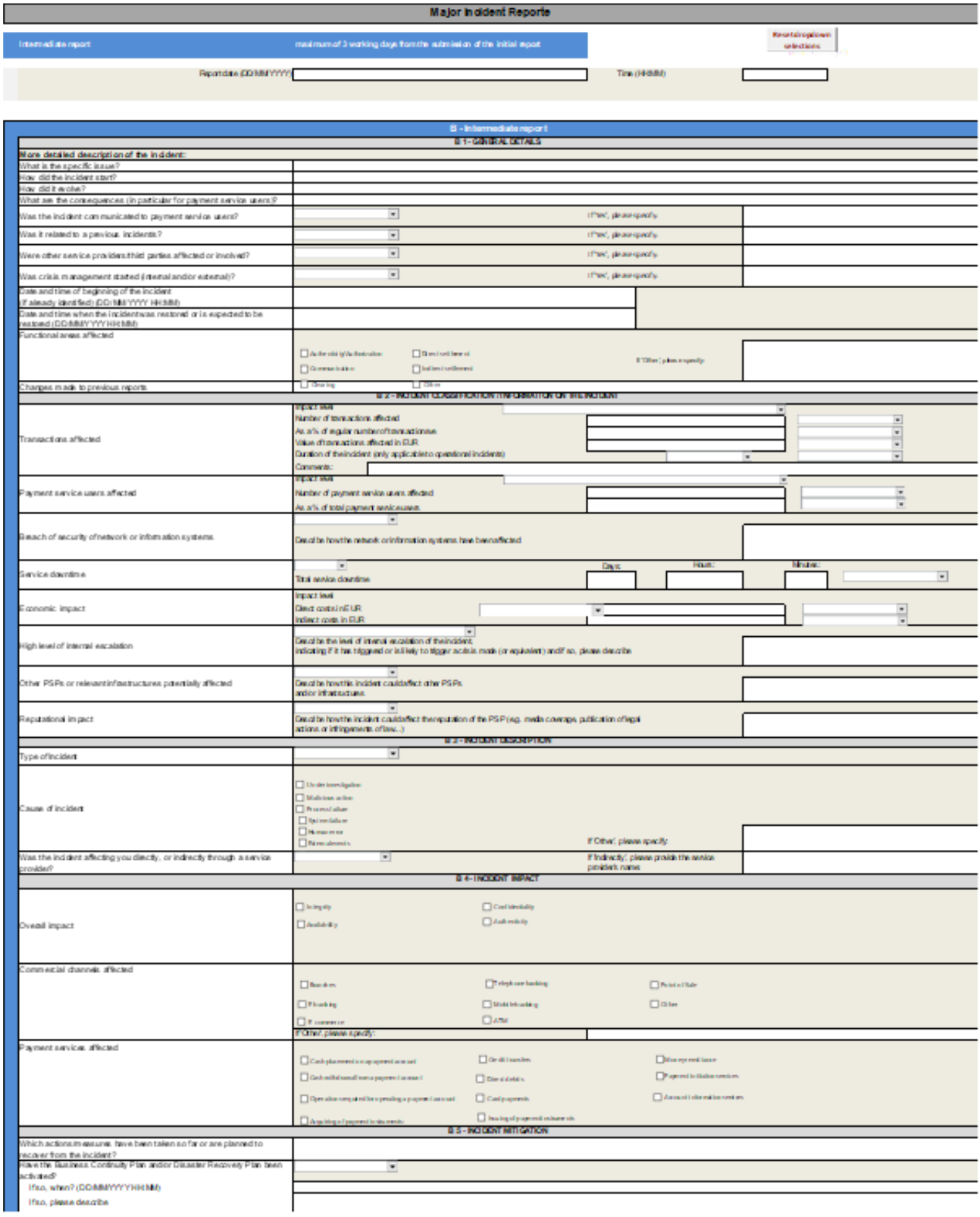
REPORTING TEMPLATE FOR PAYMENT SERVICE PROVIDERS

Initial Report

Major Incident Report		
Major Incident Report	within 20 working days after the submission of the intermediate report	Reset dropdown selections
Please describe: (applicable for incidents reclassified as non-major)		
Report date (DD/MM/YYYY)	Time (HH:MM)	

C - Final report						
If no intermediate report has been sent, please complete also section B						
C 1 - GENERAL DETAILS						
Update of the information from the initial report and the intermediate report(s)						
Changes made to previous reports						
Any other relevant information						
Are all original controls in place?						
If "No", specify which controls and the additional period required for their restoration						
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP						
What was the root cause (if already known)?	☐ Malicious action	☐ Process failure	☐ System failure	☐ Human error	☐ External event	☐ Other
Please specify:	☐ Malicious code ☐ Information gathering ☐ Intrusions ☐ Distributed/Denial of service attack (D/DoS) ☐ Deliberate internal actions ☐ Deliberate external physical damage ☐ Information content security ☐ Fraudulent actions ☐ Other	☐ Deficient monitoring and control ☐ Communication issues ☐ Improper operations ☐ Inadequate change management ☐ Inadequacy of internal procedures and documentation ☐ Recovery issues ☐ Other	☐ Hardware failure ☐ Network failure ☐ Database issues ☐ Software/application failure ☐ Physical damage ☐ Other	☐ Unintended ☐ Inaction ☐ Insufficient resources ☐ Other	☐ Failure of a supplier/technical service provider ☐ Force majeure ☐ Other	
If 'Other', please specify:						
Other relevant information on the root cause						
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known						
C 3 - ADDITIONAL INFORMATON						
Has the incident been shared with other PSPs for information purposes?	If 'Yes', please provide details:					
Has any legal action been taken against the PSP?	If 'Yes', please provide details:					
Assessment of the effectiveness of the action taken	Please provide details:					

Intermediate report



Major Incident Reporte

Intermediate report — maximum of 3 working days from the submission of the initial report

Reset dropdown selections

Report date (DD/MM/YYYY) | Time (HH:MM)

B - Intermediate report

B 1 - GENERAL DETAILS

More detailed description of the incident:

What is the specific issue?

How did the incident start?

How did it evolve?

What are the consequences (in particular for payment service users)?

Was the incident communicated to payment service users? — If "Yes", please specify.

Was it related to a previous incidents? — If "Yes", please specify.

Were other service providers/third parties affected or involved? — If "Yes", please specify.

Was crisis management started (internal and/or external)? — If "Yes", please specify.

Date and time of beginning of the incident (if already identified) (DD/MM/YYYY HH:MM)

Date and time when the incident was restored or is expected to be restored (DD/MM/YYYY HH:MM)

Functional areas affected

- Authentication/Authorisation
- Direct settlement
- Communication
- Indirect settlement
- Clearing
- Other

If "Other", please specify

Changes made to previous reports

B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT

Transactions affected

Impact level

Number of transactions affected

As a % of regular number of transactions

Value of transactions affected in EUR

Duration of the incident (only applicable to operational incidents)

Comments:

Payment service users affected

Impact level

Number of payment service users affected

As a % of total payment service users

Breach of security of network or information systems

Detail how the network or information systems have been affected

Service downtime

Total service downtime — Days: | Hours: | Minutes:

Economic impact

Impact level

Direct costs in EUR

Indirect costs in EUR

High level of internal escalation

Detail the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe

Other PSPs or relevant infrastructures potentially affected

Detail how the incident could affect other PSPs and/or infrastructures

Reputational impact

Detail how the incident could affect the reputation of the PSP (e.g. media coverage, publication of legal actions or infringements of laws...)

B 3 - INCIDENT DESCRIPTION

Type of incident

Cause of incident

- Under investigation
- Malicious action
- Process failure
- System failure
- Human error
- External events

If Other, please specify:

Was the incident affecting you directly, or indirectly through a service provider?

If Indirectly, please provide the service provider's name:

B 4 - INCIDENT IMPACT

Overall impact

- Integrity
- Confidentiality
- Availability
- Authenticity

Commercial channels affected

- Branches
- Telephone banking
- Point of Sale
- IT banking
- Mobile banking
- Other
- E-commerce
- ATM

If Other, please specify:

Payment services affected

- Cash placement on a payment account
- Credit transfers
- Money remittance
- Cash withdrawal from a payment account
- Direct debits
- Payment initiation services
- Operations required for operating a payment account
- Card payments
- Account information services
- Acquiring of payment instruments
- Issuing of payment instruments

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?

Have the Business Continuity Plan and/or Disaster Recovery Plan been activated?

If so, when? (DD/MM/YYYY HH:MM)

If so, please describe

Final report

Major Incident Report

Major Incident Report	within 20 working days after the submission of the intermediate report
Please describe: (applicable for incidents reclassified as non-major)	

Reset dropdown selections

Report date (DD/MM/YYYY) | Time (HH:MM)

C - Final report

If no intermediate report has been sent, please complete also section B

C 1 - GENERAL DETAILS

Update of the information from the initial report and the intermediate report(s)	
Changes made to previous reports	
Any other relevant information	
Are all original controls in place?	
If "No", specify which controls and the additional period required for their restoration	

C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP

What was the root cause (if already known)?

☐ Malicious action ☐ Process failure ☐ System failure ☐ Human error ☐ External event ☐ Other

Please specify:

Malicious action	Process failure	System failure	Human error	External event
Malicious code	Deficient monitoring and control	Hardware failure	Unintended	Failure of a supplier/technical service provider
Information gathering	Communication issues	Network failure	Inaction	Force majeure
Intrusions	Improper operations	Database issues	Insufficient resources	Other
Distributed/Denial of service attack (D/DoS)	Inadequate change management	Software/application failure	Other	
Deliberate internal actions	Inadequacy of internal procedures and documentation	Physical damage		
Deliberate external physical damage	Recovery issues	Other		
Information content security	Other			
Fraudulent actions				
Other				

If 'Other', please specify:

Other relevant information on the root cause	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	

C 3 - ADDITIONAL INFORMATON

Has the incident been shared with other PSPs for information purposes?	If 'Yes', please provide details:
Has any legal action been taken against the PSP?	If 'Yes', please provide details:
Assessment of the effectiveness of the action taken	Please provide details:

Annex II-Guidelines addressed to the competent authorities (CBK) on the criteria for assessing the relevance of the incident and the details of the incident reports to be shared with other domestic authorities

[refer to the original text in EBA's Guidelines – GLs 5 and 6]

Guideline 1: Assessment of the relevance of the incident

1. The CBK should assess the relevance of a major operational or security incident to other domestic authorities, taking as a basis their own expert opinion and using the following criteria as primary indicators of the importance of said incident: a.
   1.1. the causes of the incident are within the regulatory remit of the other domestic authority (i.e. their field of competence);
   1.2. the consequences of the incident have an impact on the objectives of another domestic authority (e.g. safeguarding of financial stability);
   1.3. the incident affects, or could affect, PSUs on a wide scale;
   1.4. the incident is likely to receive, or has received, wide media coverage.
2. The CBK should carry out this assessment on a continuous basis during the lifetime of the incident, to identify any possible change that could make relevant an incident that was previously not considered as such.

Guideline 2: Information to be shared

1. Notwithstanding any other legal requirement to share incident-related information with other domestic authorities, the CBK should provide information about major operational or security incidents to the relevant domestic authorities identified following the application of Guideline 1.1, as a minimum, at the time of receiving the initial report (or, alternatively, the report that prompted the sharing of information) and when they are notified that business is back to normal (i.e. the intermediate report).
2. The CBK should submit to the relevant domestic authorities the information needed to provide a clear picture of what happened and the potential consequences. In order to do so, it should provide, as a minimum, the information provided by the PSP in the following fields of the template (either in the initial or in the intermediate report):
   2.1. date and time of classification of the incident as major;
   2.2. date and time of detection of the incident;
   2.3. date and time of beginning of the incident;
   2.4. date and time when the incident was restored or is expected to be restored;
   2.5. short description of the incident (including non-sensitive parts of the detailed description).

2.6. short description of measures taken or planned to be taken to recover from the incident;

2.7. description of how the incident could affect other PSPs and/or infrastructures;

2.8. description (if any) of the media coverage;

2.9. cause of the incident.

3. The CBK should conduct proper anonymization, as needed, and leave out any information that could be subject to confidentiality or intellectual property restrictions before sharing any incident-related information with other relevant domestic authorities. Nevertheless, the CBK should provide the relevant domestic authorities with the name and address of the reporting PSP when said domestic authorities can guarantee that the information will be treated confidentially.

4. The CBK should at all times preserve the confidentiality and integrity of the information stored and exchanged and their proper authentication towards the relevant domestic authorities. In particular, the CBK should treat all information received under this Regulation in accordance with the professional secrecy obligations set out in the Law on Payment Services, without prejudice to other applicable legal requirements.