**MNB identification code: W08**

**Completion instructions**

**Financial infrastructures report on operational and security incidents**

**I. General instructions**

1. The data provider shall supply data if operational or security incidents occur.

Operational incidents are defined as one-off events or series of events related to one another taking place during the operating hours of the business service and not planned by the service provider in advance that have a negative impact on the business service provided as well as on the availability and continuity of the technical support tasks necessary for providing such service appropriately, taking into consideration the accessibility and availability of the business service, regardless of their origin (external/internal) or intentionality (intentional/unintentional).

1. Securityincidents are defined as undesired or unexpected one-off events or series of events taking place during the operating hours of the business service that entail an unfavourable change or previously unknown situation in the information system, as a result of which the confidentiality, integrity, credibility, undeniability, functionality or availability of the information carried by the electronic information system or by the electronic security system applied for the built-in control of the former gets lost or damaged, regardless of their origin (external/internal) or intentionality (intentional/unintentional). Security incidents include operational incidents detected by the security system and also the case when there has been no disruption in the service during operating the business service, but confidentiality, integrity, credibility or undeniability were damaged (leakage of company data, violation of the 4 eyes principle etc.).

In any case, the data provider shall provide information on the occurrence of an operational incident at the latest in the Closing Report to be attached to the Closing Data Provision, indicating whether any security incident has taken place. If no security incident has taken place, the data provider shall declare in the Closing Report that no security incident has taken place upon the occurrence of the operational incident.

Regarding its service provided as a payment service provider, the central securities depository under the Capital Markets Act providing payment services shall report data to the MNB concerning major operational and security incidents in the report with MNB identification code P64.

**2.** **Principles of ad hoc reporting**

a) Detailed, textual report on every operational and security incident

aa) that qualifies as operational and security event, incident, operating trouble, crisis or catastrophe according to the data provider’s business continuity, disaster recovery, incident management or other plan or public and internal rules, and

ab) that results in disruption in service, delay (e.g. decline in capacity) or damage to the expectations vis-à-vis the service (e.g. inappropriate format) during the operating of the payment system or during the performance of the clearing house, central counterparty or central securities depository activities pursuant to the Capital Markets Act (including the basic and non-bank services of the central securities depository) or during the provision of the central counterparty’s other services, as well as

ac) if – with the exception of the instant clearing – the disruption in service or delay reached or exceeded 10 minutes.

b) If the operational incident is repeated, and thus it causes disruptions or delays of less than 10 minutes in service more than once, it also shall be reported, provided that the cumulative duration of the caused disruptions in service and/or delays exceeds 20 minutes. Delays related to the performance of the activity shall also include the operational incidents that were not perceptible for the customers, but led to delays in internal working processes.

c) Damages to the functions (e.g. spare site, network services) supporting the activities and services mentioned in subpoint ab) of point a), as well as capacity and performance problems, partial loss of resources or slowdown in the service shall also be reported if they affect the aforementioned activities and services, because the capability of business continuity (e.g. switching of sites) is not ensured if the functions that support the activity are unavailable.

d) If the data provider’s report is submitted to the MNB by another organisation, the report shall indicate which data provider was affected by the operational and security incident.

e) If the operational and security incident occurred due to a reason imputable to the performing party or external service provider, the report shall indicate this fact. In this case the data report shall contain the information given by the cooperating performing party or the external service provider.

f) For full compliance with the principles of ad hoc reporting, the data provider shall attach the detailed, textual report at the latest to the ‘C – Closing Report’ table. It shall consistently contain all the information included in the Interim Report(s).

g) Since the proper operation of electronic security systems[[1]](#footnote-2) is essential for ensuring operation that is commensurate with risks, the data provider shall be obliged to pay special attention to any disruptions in the availability of electronic security systems and to report their occurrence.

1. Security incidents or events, such as operational incidents, detected by the security systems shall be reported by the data provider as security incidents, without delay.
2. The data provider is allowed to reclassify the Initial, Interim or Closing Reports sent as ad hoc report, provided that it is adequately justified and corroborated by evidence.

**3. Detailed instructions for ad hoc reporting**

An ad hoc report shall contain at least the following information:

1. with regard to the operational and security incident:

aa) its detailed description,

ab) time and duration of its occurrence, date of its closing,

ac) its location,

ad) its cause (including the description of the causes),

ae) an indication that the data provider or another party (external service provider) was responsible for the occurrence of the trouble,

af) if there is a classification system, the level of the operational and security incident,

ag) the impact of the operational and security incident on the service(s) and internal working processes, the scope of transactions concerned (e.g. types) and their size (e.g. number of pieces, or value, if applicable),

ah) naming of the IT systems concerned and the missing resources,

ai) the circumstances and time of detecting the operational and security incident,

aj) the circumstances of the decline in capacity caused by the occurrence of the operational and security incident or of the partial stoppage or deceleration of the service,

ak) the circumstances of the failure of the spare site caused by the occurrence of the operational and security incident, as at the time of an operational and security incident the service cannot be switched over,

al) business services affected by the operational and security incident;

1. indicators regarding the disruption in service:

ba) duration of the operational and security incident,

bb) duration of the disruption or delay caused, for each service (if workarounds were applied, their description, giving when they started to work),

bc) for each service, duration of the disruption in service directly perceptible for customers (if applicable),

bd) for each service, availability indicators calculated for the day(s) affected by the operational and security incident (if applicable),

be) the related extensions of operating hours, customer complaints and repairs,

bf) the duration of disruption and the availability of the business service supporting system element that failed during the disruption in service,

bg) the duration of disruption in and availability of business service in the case of a disruption in service,

bh) the way of measuring the disruption in service [automated (able to warn)/manual] in the case of the business service and the system supporting the business service,

bi) the identifier of the entity that reports the disruption in business service: a unit outside the organisation (e.g. credit institution, MNB) or organisational unit;

1. events related to the management and averting of operational and security incidents:

ca) the steps of error detection and troubleshooting,

cb) the decisions made and the necessary measures (with levels of decision-making), with their detailed description,

cc) the place, time and date of the decisions made,

cd) the error handling method, business continuity plan (hereinafter: BCP) or disaster recovery plan (hereinafter: DRP) applied,

ce) if there is no BCP or DRP applied, the documenting of the error handling method for repeatability and verifiability, the preparation of a new BCP or DRP if necessary;

1. the situation at the moment of preparing the report (in terms of the management and averting of operational and security incidents and the finding of the causes);
2. the lessons drawn from the event;
3. the description or plans of the measures taken in order to avoid similar situations or recurrences (including deadlines and people in charge) as well as the related documentation;
4. any further steps planned;
5. the internal documents created in connection with the operational and security incident (accounts, memoranda, reports as well as operating and change management documents);
6. the (planned) mode of compensating the customers for the loss they suffered and the amount of any damages already paid (if applicable);
7. if due to the event the service provider had to eliminate or ease certain (built-in preventive or detective) controls, the reason for eliminating these controls, the identification and status of the entity that requested and approved the elimination;
8. considering that during an operational incident it is a requirement to continuously control the security incidents, the data provider shall submit the report summarising the operational incident (in the form of a Closing Report in line with point II. 5) authenticated by the signatures of the heads of IT and Security.
9. since subpoint b) of this point expects the reporting of data related to the availability of business services, the data provider shall submit the report summarising the operational incident (in the form of a Closing Report in line with point II. 5) authenticated by the signature of the head of the business division;
10. a declaration whether there has been any security incident in connection with an operational incident, and a declaration whether there has been an operational incident in connection with a security incident.

**4. Principles of the quarterly reporting**

a) If no reporting obligation according to the provisions in point 1 arose for the data provider, every quarter, before the 10th working day of the month following the reference quarter the data provider shall declare that no operational and security incident – serving as the basis for reporting – has occurred.

b) If not submitted within the framework of a report with MNB identification code W08, according to this data reporting, every quarter, before the 10th working day of the month following the reference quarter the data provider shall report all the events not qualifying as subject to mandatory reporting but deemed operational or security event, incident or error in the organisation of the data provider (e.g. incident ticket, operating log, security incident), each case furnished with individual identifier, in a list. This list shall contain a short description of the cases, their start, time, current status, priority and primarily a presentation of the internal events that can be related to the circumstances of the report with MNB identification code W08 and can be listed as its cause or result.

The data provider shall attach the content of the quarterly report as part of the table ‘D – Quarterly data report’.

**5.** **The principles of ad hoc evaluation**

a) In connection with the ad hoc and quarterly reports, the data provider shall submit the following in relation to the operational and security incidents selected by the MNB:

aa) the security log evaluation and all the log files related to the event (system and components affected), in a format allowing security log evaluation and analysis in an office environment as well and

ab) the complete documentation belonging to the event (e.g. internal and external letters related to the subject matter, customer information, incident tickets).

b) In addition, the data provider shall also send the regular evaluations it prepares, which are directly or indirectly related to the ad hoc or quarterly reports it compiles, or are related to cases not qualifying as subject to mandatory reporting but deemed operational or security events, incidents or errors in the organisation of the data provider.

If the size of all the requested log files related to operational and security incidents (system and components affected) is too big, the data provider shall inform the MNB accordingly, in order to discuss an alternative format of delivering the data.

The deadline for submitting the security log evaluations concerning operational and security incidents and selected by the MNB, or prepared by the data provider, shall be 30 working days following selection by the MNB.

The data provider shall attach the content of the ad hoc evaluation as part of the table ‘E – Ad hoc evaluation’.

**II. Detailed instructions for the completion of the tables**

**1.** If the data provider failed to classify the operational and security incident within 10 minutes from detection, the operational and security incident shall be reported. If the initial report has already been sent, but it turns out before an interim report is submitted that the operational and security incident is not a reportable incident after all, an encrypted e-mail may be sent to the address [incidensek@mnb.hu](mailto:incidensek@mnb.hu) instead of filing the interim and closing reports; in this e-mail, the data provider shall notify the MNB of the classification of the operational and security incident authenticated by the signatures of the senior managers of the business, IT and security divisions, indicating the causes.

**2.** The Table **‘Header’** shall be filled in for every data supply. The data supplier shall complete the further data supply tables depending on the operational and safety incident processing status.

**3. A – Initial report**

The table summarizing the initial report of the operational and security incident shall be sent to the MNB by encrypted e-mail to [incidensek@mnb.hu](mailto:incidensek@mnb.hu) within 5 minutes of classifying the incident.

**4. B – Interim report**

This table shall be submitted to the MNB via the ERA system, first within 3 working days of the submittal of the ‘A – Initial report’ and thereafter once every week until the ‘C – Closing report’ table is sent. When submitting the first interim report, the initial report sent by encrypted e-mail shall also be uploaded into the ERA system.

**5. C – Closing report**

Standardisation of the information received during the initial and interim reporting, and updating the description of the incident.

The data supplier may deem its operations to have returned to the usual manner once its activities and operations have returned to the service level and the conditions either defined by the data supplier or stipulated externally in an agreement on service levels concerning processing times, capacities, security requirements etc., and provided that no extraordinary measures related to an operational and safety incident are still in force.

The data supplier shall submit the table via the ERA system within 30 days of closing the operational and safety incident. The ‘Closing Report’, which contains the detailed description and range of the event as well as the degree of the disruption in the business service as a separate document to be signed by the divisions affected by the incident, shall be attached as an embedded document to the ‘C – Closing Report’ table.

In its ‘C – Closing report’, the data supplier shall provide comprehensive information (for example actual figures rather than estimates to quantify the impact).

The data provider shall give the content of the report in line with the provisions in point I.2.

**5. D – Quarterly data report**

During the quarterly reporting, the data provider shall submit the data content specified below as a signed, attached document embedded in the table ‘D – Quarterly data report’:

a) if no reporting obligation according to the provisions in point 1 arose for the data provider, a declaration that no operational and security incident – serving as the basis for reporting – has occurred,

b) listing the operational and security incidents, errors and events not qualifying as subject to mandatory reporting. The data provider shall give the content of the report in line with the provisions in point I.4.

The divisions concerned shall sign the separate documents containing the quarterly data to be attached as embedded documents to the table ‘D – Quarterly data report’.

**6. E – Ad hoc evaluation**

During the ad hoc and quarterly reporting the data provider shall attach the requested data as an embedded document to the table ‘E – Ad hoc evaluation’.

The data provider shall give the content of the report as described in point I.5.

The divisions concerned shall sign the separate documents containing the ad hoc evaluations to be attached as embedded documents to the Table ‘E – Ad hoc evaluation’.

**7. F – Downgrading**

The data provider is allowed to downgrade the Initial, Interim or Closing Reports sent as ad hoc report, provided that it is adequately justified and corroborated by evidence. The data provider shall indicate the downgrading within 1 working day following the downgrading.

The divisions concerned shall sign the documents that justify and corroborate with evidence the downgrading to be attached as embedded documents to the table ‘7. F – Downgrading’.

**8. Additional data and documents to be enclosed with the data supply**

The data provider shall enclose with the particular report all available information and documentation on the operational and security incident and its resolution that it considers important for the MNB over and above those contained in the report.

1. NIST 800-35 Guide to Information Technology Security Services (<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf>) [↑](#footnote-ref-2)