30 June 2021

ROC-DSB notifications protocol pursuant to Article IV of the MOU, clause 25

Pursuant to the ROC-DSB MOU, Article IV, clause 25, all provisions below are subject to regular review and revision, preferably, at minimum, annually by mutual understanding of the ROC and DSB. This may include addition to, revisions to or removal of provisions based on need, usefulness and practicality.

Description of Major changes and Minor changes

The following represents an indicative description of Major changes and Minor changes.

Major Change.

A change shall be considered major if any of the 23 criteria listed below are met. The criteria are differentiated by impact area.

A. Impact on Workload / Costs / Resources

1. It takes greater than 99 days to deliver the change, as measured from the start of development;
2. The cost of the change is greater than EUR 250,000;
3. It requires multiple teams, including external teams, to execute the change;

B. Impact on the Industry / Reputation

4. The change requires greater than three months lead time from industry;
5. Industry will incur new / additional costs due to the change;
6. The change may benefit from consultation by ROC authorities;
7. The change has a reputational risk on ROC and/or FSB;
8. The change has a reputational risk of Board level severity;
9. The change results in an unplanned change in costs;

C. Impact on: Technology / Architecture / Operations

10. The change is non-backward compatible;
11. The change is directly related to a Board approved strategic plan;
12. The change is a public commitment to deliver within a set time-frame;
13. The change is externally mandated;

Major changes in the Technology / Architecture / Operations Category could include the following types of planned changes: (i) Commissioning of new infrastructure (physical, cloud

or hybrid) in support of a new service/solution, (ii) New systems / solutions implemented to underpin the existing service, (iii) New interfaces, integration, connectivity requirements affecting the existing service, (iv) New or changed data format affecting the existing service, (v) New software modules or third party systems affecting the existing service, (vi) New / major architectural change that impacts the existing service, or (vii) changes that requires DSB to consult the industry outside of the Industry Consultation process.

D. Impact on Data

14. The change is non-backward compatible;
15. The change is directly related to a strategic plan / is strategic in nature;
16. The change is a public commitment to deliver within a set time-frame;
17. The change is externally mandated, including to meet the UPI standards / by a designation organisation, e.g. ROC;

Major changes in the Data Category could include the following types of planned changes: (i New / major revisions to data definitions, dictionaries, reference data that result in impact to supporting systems, (ii) New / major revisions to data management systems and processes, (iii) New / major revisions to data quality, validation and integrity systems and processes, or (iv) New / major revisions to identifiers used.

E. Impact on Security

18. Any changes to networks, infrastructure, applications and services affecting cyber security;
19. Any changes to networks, infrastructure, applications and services that affect information security;
20. Any changes that require new / additional penetration, threat and vulnerability testing;
21. Any high priority items identified during penetration, threat and vulnerability testing or high priority configuration changes that require remediation;
22. Intra-year or ad-hoc changes affecting security;

F. Impact on Governance

23. Any change affecting jurisdictional neutrality.

Minor Change

A change shall be considered minor if the criteria listed below are met. The criteria are differentiated by impact area.

A. Impact on Workload / Costs / Resources

1. It takes 99 days or less to deliver the change, as measured from the start of development;
2. The cost of the change is EUR 250,000 or less;

B. Impact on the Industry / Reputation

3. The change requires less than three month lead time from industry;
4. Industry could incur some new / additional costs due to the change or fixes;
5. The change does not benefit from consultation with the ROC authorities;
6. The change does not have a reputational risk of Board level severity;

C. Impact on Technology / Architecture / Operations

7. The change is backward compatible;
8. The change is not related to a Board approved strategic plan;
9. The change is implemented by the execution of a predefined, repeatable, replayable process;

Minor changes in the Technology / Architecture / Operations Category could include the following types of planned changes: (i) Cosmetic changes, (ii) Configuration changes, (iii) Enumeration changes, (iv) Introduction of new products, (v) Scheduled patches / fixes / maintenance, (vi) Client/vendor integration via an existing service, (vii) Changes to components of the system that are passive (MIS, tooling, etc), (viii) Addition or removal of infrastructure within the existing scalable design (additional memory, storage, additional servers), (ix) Existing infrastructure (including decommissioning), (x) Existing systems and applications, (xi) Existing interfaces, integration, connectivity affecting the service, and (xii) Documentation changes (externally facing) related to the service.

D. Impact on Data

10. The change is backward compatible;
11. The change is not directly related to a Board approved strategic plan;

Minor changes in the Data Category could include the following types of planned changes: (i) Error correction e.g. data quality, validation, (ii) Data surgery, (iii) Changes that do not impact data structures or require change of functionality in a supporting system, (iv) Minor changes to data dictionaries, reference data that result in impact to supporting systems , (v) Amendments to data management systems and processes, (vi) Amendments to data quality, validation and integrity systems and processes, and (vii) Documentation changes (externally facing) related to the service.

E. Impact on Security

12. Changes related to scheduled patches / fixes affecting security;
13. Changes related to scheduled maintenance affecting security;
14. Changes related to any low/medium priority items identified during penetration, threat and vulnerability that require remediation;

F. Impact on Governance

15. Changes related to operational risk assessments, plans and mitigation as they relate to the existing service;
16. Amendments to internal audit process as they relate to the existing service;

17. Amendments to risk management processes as they relate to the existing service;
18. Amendments to change management processes as they relate to the existing service
19. Amendments to business continuity and disaster recovery plans as they relate to the existing service;
20. Amendments to security controls impacting the service (physical, environmental, personnel) as they relate to the existing service;
21. Amendments to data governance processes as they relate to the existing service.

Notifications of Major or Minor Changes

A. DSB will notify the ROC before a proposed Major change related to the below as follows:

a. DSB will provide notice a minimum of 90 calendar days ahead of the proposed change

b. ROC may provide a recommendation, if any, within 60 calendar days of notice being provided by DSB

Technology & Data Change

1. changes to infrastructure supporting the assignment, retrieval and / or maintenance of UPI codes and associated reference data, including products that have underliers from more than one asset class
2. intra-year or ad-hoc technology and data changes, whose relevance has increased from Minor to Major Change unexpectedly over time.

Operations Change

1. intra-year or ad-hoc changes to policies and controls, including security, whose relevance has increased from Minor to Major Change unexpectedly over time.

B. DSB will notify the ROC before proposed Major Changes, and through **Regular Communications** of Minor Changes, related to the below, as follows:

a. DSB will provide notice a minimum of 90 calendar days ahead of proposed Major Change, unless specified differently below.

b. ROC may provide a recommendation, if any, within 60 calendar days of notice being provided by DSB of the proposed Major Change, unless specified differently below.

c. DSB will provide notice of Minor Change for information purposes only every 90 calendar days, unless specified differently below.

Technology & Data Change

1. changes to systems (including logical solution architecture) supporting the assignment, retrieval and / or maintenance of UPI codes and associated reference data, including products that have underliers from more than one asset class;
2. changes to data exchange formats (e.g. XML, JSON, CSV) and standards as specified in Article VI clause 31 b of the MOU supporting the assignment, retrieval and / or maintenance of UPI codes and associated reference data, including products that have underliers from more than one asset class;
3. changes to business processes supporting the assignment, retrieval and / or maintenance of UPI codes, including products that have underliers from more than one asset class;
4. changes to business processes supporting / managing the reference data associated with UPI codes, including products that have underliers from more than one asset class;

5. changes impacting attributes or their values that may impact jurisdictional neutrality as defined in the section 3.1 of the CPMI-IOSCO UPI Technical Guidance;[1]
6. changes that impact the user interfaces for the UPI service;
7. changes to dependencies on, compatibility and integration with existing systems that could impact the UPI service.
8. change to the list of supported identifiers for a given underlier;
9. changes to systems supporting data management, quality and integrity;
10. changes to systems supporting data governance (including the functioning of advisory committees) such as related to third party data providers used to underpin the UPI service:

    DSB will provide notice of Minor Changes for information purposes only, on an annual basis

11. changes to data maintenance processes and operating procedures:

    DSB will provide notice of Minor Changes for information purposes only, on an annual basis

12. changes to processes, policies and standards supporting data governance (including the functioning of advisory committees) such as changes to committee Charters:

    DSB will provide notice of Minor Change annually for information purposes only, on an annual basis

C. DSB will notify the ROC after the following of Major Changes, and through **Regular Communications** of Minor Changes, related to the below, as follows:

a. DSB will provide 90 calendar days notice or after notification for Major Changes for information purposes only
b. DSB will provide notice of Minor Changes annually for information purposes only

Operations

1. new / changes to system operations (such as hardware and software change management, patch management, and event and problem management). *At*

[1] According to this principle, the harmonisation of the UPI should not, to the greatest extent practicable, depend on factors that are specific to a jurisdiction, but should be based only on the exhaustive inherent technical characteristics of products. Jurisdiction neutrality helps ensure that the UPI System is globally applicable and therefore facilitates aggregation. For the UPI to achieve jurisdiction neutrality, all values that are included in an OTC derivative product's reference data should be standardised among jurisdictions to the fullest extent practicable. The CPMI and IOSCO have developed the guidance on the standardisation of the data elements other than the UPI and UTI in parallel to the UPI guidance. Implementation of the UPI guidance should promote the standardisation of the elements in the UPI reference data, to the greatest extent practicable.

minimum, DSB to provide one single annual evidence of compliance with ITIL v4 or strong alignment to it or equivalent.

2. new / changes to requirements and controls for cyber-security, information security and physical security requirements; this could include plans for regular penetration / threat / vulnerability testing. *At minimum DSB to provide one single annual evidence of compliance with ISO27001, ISO27032, PAS555 and / or NIST CSF or at minimum if these do not exist then strong alignment to these standard(s) should be demonstrated.*
3. new / changes to requirements and controls for identification, authorisation and access to systems and networks including monitoring of misuse, unauthorised or remote third party access; training and awareness procedures. *At minimum, DSB to provide one single annual evidence of compliance with ISO27001, ISO27032, PAS555 and / or NIST CSF or at minimum if these do not exist then strong alignment to these standard(s) should be demonstrated.*
4. for business continuity and / or disaster recovery: new / changes to backup facilities (and their testing), audit processes, risk assessments, incident management plans and / or contingency sites, their supporting resources, and infrastructures as well as any capacity / performance planning. *At minimum DSB to provide one single annual evidence of compliance with ISO22301, ISO27031 or demonstrate strong alignment to these or equivalent requirements.*

D. DSB will notify the ROC **after** the changes listed below, by close of business and on regular daily intervals until the issues is resolved (unless differently specified below).

Service/Data Reports

1. security incident / breach
2. critical IT incidents (defined by DSB internal classification of critical)
3. system downtime > 1 hour
4. system downtime < 1 hour
    a. DSB will provide notice by close of business for information purposes only

E. DSB shall notify the ROC **after** Major Changes, and through **Regular Communications** of Minor Changes, related to the following:

Technology & Data Change

1. unplanned changes to infrastructure, systems supporting the assignment, retrieval and / or maintenance of UPI codes and associated reference data, including products that have underliers from more than one asset class, that have been implemented

a. DSB will provide immediate notification for Major Changes, followed by a report within 30 calendar days for information purposes only

b. DSB will provide notice of Minor Changes every 90 calendar days for information purposes only

Operations Change

2. Remediation of results of regular penetration / threat / vulnerability testing plans or rectifying other security incidents

   a. DSB will provide immediate notification post remediation/ rectification of high priority issues / incidents for Major Changes for information purposes only

   b. DSB will provide notice of Minor Changes annually for information purposes only

F. DSB will notify the ROC through **Regular Communications** of Major and Minor Changes related to the below, as follows (unless differently arranged between the parties as specified in the below text):

a. DSB will provide notice of changes every 90 calendar days for information purposes only

Technology & Data Change

2. changes to technical documentation underpinning the UPI service including (but not limited to) formats, integration and connectivity and security guidelines

3. changes to data documentation underpinning the UPI service including but not limited to) data definitions and dictionaries

Operations

4. A change to the approach used to identify and minimize sources of operational risk, to determine appropriate controls, to assess and manage operational risks (such as the risk connected to changes to the technology infrastructure);

   a. for Minor Changes, DSB will provide notice annually for information purposes only

G. DSB will notify the ROC through **Regular Communications** of Major and Minor Changes related to the below, as follows:

a. DSB will provide notice every 90 calendar days or ex-post evidence of compliance / strong alignment for Major Changes for information purposes only

b. DSB will provide notice of Minor Changes annually for information purposes only

Operations

1. new or changes to risk management and risk assessments; at minimum DSB should provide annual evidence of compliance with ISO31000 or strong alignment to it or equivalent standard
2. new or changes to internal audit programs and to the system of controls; at minimum DSB should provide annual evidence of compliance / strong alignment to International Standards set out by the Global Institute of Internal Auditors or equivalent
3. new or changes to systems development methodology (such as quality assurance and outsourcing); at minimum DSB should provide annual evidence of compliance with ISO9000 or strong alignment to it or equivalent standard.

H. DSB will provide **Regular Communications** to the ROC, every 30 calendar days, for the following:

Service/Data Reports

1. Volumes for UPI codes assigned, for each asset class and related response times by user type
2. Volumes for UPI codes retrieved (i.e. already assigned UPI codes), for each asset class and related response times by user type;
3. Number of UPI reference data records retrieved and related response times by user type.
4. Volumes for Reference Data elements assigned the value of "Other"

   Moreover,

   a. ROC may review this information no less than every 90 calendar days to determine if data changes to support "Other" products are required. Any recommendation / specification will be passed to DSB for assessment and implementation.DSB will respond within 28 calendar days of any ROC recommendation to provide an impact assessment and tentative implementation plan.
5. Detail on Reference Data elements assigned the value of "Other"

   a. ROC may review this information no less than every 90 calendar days to determine if data changes to support "Other" products are required. Any recommendation / specification will be passed to DSB for assessment and implementation.DSB will respond within 28 calendar days of any ROC recommendation to provide an impact assessment and tentative implementation plan.
6. Volumes where the product does not include specific underliers such as custom basket constituents
7. Expected level of future UPI generation

8. Volume of UPIs by status;

Service level reports

9. Service level reports detailing the number, frequency, and nature of security incidents
10. Service level reports detailing the number, frequency, and nature of critical IT incidents (defined by DSB internal classification of critical)
11. Service level reports detailing system availability metrics (e.g. cumulative downtime

I. DSB will provide **Regular Communications** to the ROC, every 90 calendar days, for the following:

Service/Data Reports

1. Data quality assessment against metrics consistent with ROC standards (i.e. the results of data quality checks to ensure integrity, completeness, and consistency of the UPI codes and UPI reference data)

   Moreover,

   a. If data quality assessment threshold/targets are breached then DSB will report within 28 calendar days of report.

The frequency and significance of users' complaints and disputes regarding

2. users' ability to have open access to the UPI service, in terms of systems' technical reliability and performance
3. users' ability to have open access to the UPI service, in terms of absence of legal restrictions or other impediments to open access[2]
4. fee model for UPI services, such as fee levels, classification of user permissions and allocation of fees across different user types, treatment of excess fees or shortfalls materialising during the year
5. policies and procedures that allow users to contest fees and issues regarding access to UPI services
6. conflicts of interest, DSB's policies to deal with conflicts of interest and DSB's adherence to those policies
7. DSB's policies and procedures governing applications for obtaining new UPIs

[2] The "open access" criterion, as defined in the FSB Governance arrangements for the UPI states that "*Access to, and use of, UPI Codes and the UPI Data Standard should be unrestricted. Authorities should have access to, and use of, the UPI Reference Data Library that is similarly unrestricted. Entities with reporting obligations and TRs should have access to, and use of, the UPI Reference Data Library in a manner that is sufficient to at least allow them to associate a specific OTC derivative product to its UPI Code in a timely manner and facilitate the discharge of reporting obligations for OTC derivatives transactions.*"

8. the ability of the UPI system to support required product definitions, attributes and allowable values.
9. the ability of the UPI system to accurately issue UPIs and maintain the appropriate state for all UPIs
10. the ability of the UPI system to accurately derive the data elements specified in the product definition