Council of the European Union

Brussels, 6 October 2020
(OR. en)

10831/20

**Interinstitutional File:**
**2020/0123 (NLE)**

**ENV 516**
**CLIMA 187**
**ENER 290**
**IND 135**
**COMPET 405**
**MI 333**
**ECOFIN 803**
**TRANS 397**
**AELE 52**
**CH 24**

**LEGISLATIVE ACTS AND OTHER INSTRUMENTS**

| | |
|---|---|
| Subject: | Draft DECISION OF THE JOINT COMMITTEE ESTABLISHED BY THE AGREEMENT BETWEEN THE EUROPEAN UNION AND THE SWISS CONFEDERATION ON THE LINKING OF THEIR GREENHOUSE GAS EMISSIONS TRADING SYSTEMS on the adoption of Common Operational Procedures (COP) |

DRAFT

**DECISION No 1/2020**
**OF THE JOINT COMMITTEE ESTABLISHED BY THE AGREEMENT**
**BETWEEN THE EUROPEAN UNION AND THE SWISS CONFEDERATION**
**ON THE LINKING OF THEIR GREENHOUSE GAS EMISSIONS TRADING SYSTEMS**

**of …**

**on the adoption of Common Operational Procedures (COP)**

THE JOINT COMMITTEE

Having regard to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems[1] ('the Agreement') and in particular Article 3(6) thereof,

[1] OJ L 322, 7.12.2017, p. 3.

Whereas:

(1) Decision No 2/2019 of the Joint Committee of 5 December 2019[1] amended Annexes I and II to the Agreement thus fulfilling the conditions for linking set out in the Agreement.

(2) Following adoption of Decision No 2/2019 of the Joint Committee and pursuant to Article 21(3) of the Agreement, the Parties exchanged their instruments of ratification or approval, since they consider all conditions for linking as set out in the Agreement to have been fulfilled.

(3) In accordance with Article 21(4) of the Agreement, the Agreement entered into force on 1 January 2020.

[1] Decision no 2/2019 of the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 5 December 2019 amending Annexes I and II to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems (OJ L 314, 29.9.2020, p. 68).

(4) Pursuant to Article 3(6) of the Agreement, the Swiss registry administrator and the Union central administrator should determine common operational procedures (COP) related to technical or other matters necessary for the operation of the link between the European Union Transaction Log (EUTL) of the Union registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry and taking into account the priorities of domestic legislation. The COP should take effect when adopted by decision of the Joint Committee.

(5) In accordance with Article 13(1) of the Agreement, the Joint Committee should agree on technical guidelines to ensure the proper implementation of the Agreement including on technical or other matters necessary for the operation of the linking and taking into account the priorities of domestic legislation. Technical guidelines may be developed by a working group set up pursuant to Article 12(5) of the Agreement. The working group should at least include the Swiss registry administrator and the Union central administrator and should assist the Joint Committee in its functions under Article 13 of the Agreement.

(6) In view of the technical nature of the guidelines and the need to adapt them to ongoing developments, the technical guidelines developed by the Swiss registry administrator and the Union central administrator should be submitted to the Joint Committee for information or, where appropriate, approval,

HAS ADOPTED THIS DECISION:

*Article 1*

The Common Operational Procedures (COP), as annexed to this Decision, are hereby adopted.

*Article 2*

Herewith, a working group shall be set up pursuant to Article 12(5) of the Agreement. It shall assist the Joint Committee in ensuring the proper implementation of the Agreement, including the development of technical guidelines for the implementation of the COP.

The working group shall at least include the Swiss registry administrator and the Union central administrator.

*Article 3*

This Decision shall enter into force on the date of its adoption.

Done at Brussels, … 2020.

*For the Joint Committee*

| *Secretary for the European Union* | *The Chair* | *Secretary for Switzerland* |
|---|---|---|

**ANNEX**

COMMON OPERATIONAL PROCEDURES (COP)
PURSUANT TO ARTICLE 3(6) OF THE AGREEMENT
BETWEEN THE EUROPEAN UNION AND THE SWISS CONFEDERATION
ON THE LINKING OF THEIR GREENHOUSE GAS EMISSIONS TRADING SYSTEMS

Procedures for Provisional Solution

1. Glossary

Table 1-1 Acronyms and Definitions

| Acronym/Term | Definition |
|---|---|
| Certificate Authority (CA) | Entity that issues digital certificates. |
| CH | Swiss Confederation |
| ETS | Emissions Trading System |
| EU | European Union |
| IMT | Incident Management Team |
| Information Asset | A piece of information that is valuable to a company or organization. |

| Acronym/Term | Definition |
|---|---|
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| ITSM | IT Service Management |
| LTS | Linking Technical Standards |
| Registry | An accounting system for allowances issued under the ETS, which keeps track of the ownership of allowances held in electronic accounts. |
| RFC | Request For Change |
| SIL | Sensitive Information List |
| SR | Service Request |
| Wiki | Website that allows users to exchange information and knowledge by adding or adapting content directly via a web browser. |

2. Introduction

The Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 23 November 2017 ('Agreement') provides for the mutual recognition of emission allowances that can be used for compliance under the Emissions Trading System of the European Union ('EU ETS') or the Emissions Trading System of Switzerland ('ETS of Switzerland'). To operationalise the link between the EU ETS and the ETS of Switzerland, a direct link between the European Union Transaction Log (EUTL) of the Union Registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry will be established, which will enable the registry-to-registry transfer of emission allowances issued under either ETS (Article 3(2) of the Agreement). To operationalise the link between the EU ETS and the ETS of Switzerland, a provisional solution shall be in place by May 2020 or as soon as possible thereafter. Parties shall cooperate to replace the provisional solution with a permanent registry link as soon as possible (Annex II to the Agreement).

Pursuant to Article 3(6) of the Agreement, the Swiss registry administrator and the Union central administrator shall determine common operational procedures (COP) related to technical or other matters necessary for the operation of the linking and taking into account the priorities of domestic legislation. The COP developed by the administrators shall take effect when adopted by decision of the Joint Committee.

The COP, as recorded in this document, is to be adopted by the Joint Committee by its Decision No 1/2020. In accordance with this Decision, the Joint Committee shall request the Swiss registry administrator and the Union central administrator to develop further technical guidelines to operationalise the link and to ensure that these are continuously adapted to technical progress and new requirements relating to the safety and security of the link and to its effective and efficient operation.

2.1. Scope

This document represents the common understanding between the Parties to the Agreement regarding the establishment of the procedural foundations of the link between the registries of the EU ETS and the ETS of Switzerland. While it outlines the overall procedural requirements in terms of operations, some further technical guidelines will be needed to operationalise the link.

For its proper functioning, the link will require technical specifications in order to further operationalise it. Pursuant to Article 3(7) of the Agreement, those matters are detailed in the Linking Technical Standards (LTS) document to be adopted separately by decision of the Joint Committee.

The objective of the COP is to make sure that IT services related to the operation of the link between the registries of the EU ETS and the ETS of Switzerland are delivered effectively and efficiently, especially for the fulfilling of service requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks according to international standards for IT service management.

For the agreed provisional solution, only the following COP will be needed, which are part of this document:

– Incident Management;

– Problem Management;

– Request Fulfilment;

– Change Management;

– Release Management;

– Security Incident Management;

– Information Security Management.

With the deployment of the permanent registry link at a later date, the COP must be adapted and supplemented where necessary.

2.2. Addressees

The target audience of these COP are the EU and Swiss registry support teams.

3. Approach and Standards

The following principle applies to all COP:

– The EU and CH agree to define the COP on the basis of ITIL (Information Technology Infrastructure Library, version 3). Practices from this standard are reused and adapted to the specific needs related to the provisional solution;

– The communication and coordination necessary for the processing of the COP between the two Parties takes place via the Registry Service Desks of the CH and EU. Tasks are always assigned within one Party;

– If there is disagreement about the handling of a COP, this will be analysed and resolved between both Service Desks. If no agreement can be reached, the finding of a joint solution is escalated to the next level.

| Escalation levels | EU | CH |
|---|---|---|
| 1st level | EU Service Desk | CH Service Desk |
| 2nd level | EU Operations Manager | CH Registry Application Manager |
| 3rd level | Joint Committee (which might delegate this responsibility considering Article 12(5) of the Agreement) | |
| 4th level | Joint Committee, if 3rd level is delegated | |

;

– Each Party can determine the procedures for the operation of its own registry system, taking into account the requirements and interfaces related to these COP;

– An IT Service Management (ITSM) tool is used to support the COP, in particular Incident Management, Problem Management and Request Fulfilment, and communication between both Parties;

– In addition, the exchange of information via e-mail is allowed;

– Both Parties ensure that the information security requirements are met in accordance with the Handling Instructions.

4. Incident management

The objective of the Incident Management process is to return IT services to a normal service level as quickly as possible following an incident and with minimum disruption to the business.

Incident Management should also keep a record of incidents for reporting purposes and integrate with other processes to drive continuous improvement.

From a global perspective, Incident Management comprises the following activities:

– Incident detection and recording;

– Classification and initial support;

– Investigation and diagnosis;

– Resolution and recovery;

– Incident closure.

Throughout the lifecycle of an incident, the Incident Management process is responsible for the constant handling of the ownership, monitoring, tracking and communication.

4.1. Incident detection and recording

An incident can be detected by a support group, by automated monitoring tools or by technical staff performing routine surveillance.

Once detected, an incident must be recorded and assigned a unique identifier allowing for proper incident tracking and monitoring. The unique identifier of an incident is the identifier assigned in the common ticketing system by the Service Desk of the Party (either EU or CH) that raised the incident, and it has to be used in every communication related to this incident.

For all incidents, the contact point should be the Service Desk of the Party that logged the ticket.

4.2. Classification and initial support

The incident classification aims at understanding and identifying what system and/or service are affected by an incident, and to what degree. To be effective, the classification should route the incident to the correct resource on the first try, in order to speed up the incident resolution.

The classification phase should categorize and prioritize the incident according to its impact and urgency, for it to be treated according to the priority relevant time frame.

If the incident has a potential impact on the confidentiality or integrity of sensitive data, and/or an impact on the system availability, the incident shall be also declared as a security incident and then managed according to the process defined in the 'Security Incident Management' chapter of this document.

If possible, the Service Desk that logged the ticket performs an initial diagnosis. For this, the Service Desk will see if the incident is a known error. If so, then the resolution path or workaround is already known and documented.

If the Service Desk is successful in solving the incident, then it will actually close the incident at this point, as the primary purpose of Incident Management has been fulfilled (namely the fast restoration of service for the end user). If not, then the Service Desk will escalate the incident to the appropriate resolver group for further investigation and diagnosis.

4.3. Investigation and diagnosis

Incident investigation and diagnosis is applied when an incident cannot be resolved by the Service Desk as part of the initial diagnosis, and is therefore escalated appropriately. Incident escalation is a full part of the investigation and diagnosis process.

A common practice in the investigation and diagnosis phase is the attempt to recreate the incident under controlled conditions. It is important when performing incident investigation and diagnosis that the proper order of events that led up to the incident be understood.

Escalation is the recognition that an incident cannot be resolved at the current support level, and must be passed to a higher level support group or to the other Party. Escalation can follow two paths: horizontal (functional) or vertical (hierarchical).

The Service Desk that recorded and triggered the incident is responsible for escalating the incident to the appropriate resource and for tracking the overall status and assignment of the incident.

The Party to which the incident has been assigned is responsible for ensuring the requested actions are performed in a timely fashion, and for providing feedback to the Service Desk of its own Party.

4.4. Resolution and recovery

Incident resolution and recovery is performed once the incident is fully understood. Finding a resolution to an incident means that a way of rectifying the issue has been identified. The act of applying the resolution is the recovery phase.

Once the appropriate resources resolve the service failure, the incident is routed back to the relevant Service Desk that logged the incident and that Service Desk confirms with the initiator of the incident that the error has been rectified and that the incident can be closed. Findings from the processing of the incident are to be recorded for future use.

Recovery can be performed by IT support staff or by providing the end user with a set of instructions to follow.

4.5. Incident closure

Closure is the final step in the Incident Management process and takes place shortly after incident resolution.

Within the checklist of activities that need to be performed during the closure phase, the following are highlighted:

– The verification of the initial categorization that was assigned to the incident;

– The proper capture of all information surrounding the incident;

– The proper documentation of the incident and update of the knowledge base;

– The adequate communication to every stakeholder directly or indirectly affected by the incident.

An incident is formally closed once the incident closure phase has been executed by the Service Desk and communicated to the other Party.

Once an incident is closed, it is not reopened. If an incident re-occurs within a short time period then, the original incident is not re-opened, a new incident must be logged instead.

If the incident is tracked by both the EU and CH Service Desks, the final closure is the responsibility of the Service Desk that logged the ticket.

5. Problem Management

This procedure should be followed whenever a problem is identified and therefore triggers the Problem Management process. Problem Management focuses on enhancing quality and reducing the volume of raised incidents. A problem can be the cause of one or more incidents. When an incident is reported, the objective of Incident Management is to restore the service as quickly as possible, possibly involving workarounds. When a problem is created, the objective is to investigate the root cause of the issue in order to identify a change that will ensure the problem and related incidents will not occur anymore.

5.1. Problem identification and recording

Depending on which Party initiated the ticket, either the EU or CH Service Desk will be the contact point for problem related matters.

The unique identifier of a problem is the identifier assigned by the IT Service Management (ITSM). It has to be used in every communication related to this problem.

A problem can be triggered by an incident or can be opened as a self-initiative act to fix issues discovered in the system at any point in time.

5.2. Problem Prioritization

Problems may be categorized according to their severity and priority in the same way as incidents in order to facilitate their tracking, taking the impact of the associated incidents and their frequency of occurrence into account.

5.3. Problem investigation and diagnosis

Each Party can raise a problem and the Service Desk of the initiating Party will be responsible for logging the problem, assigning it to the appropriate resource and tracking the overall status of the problem.

The resolver group to whom the problem was escalated is responsible for handling the problem in a timely fashion and communicating with the Service Desk.

Upon request, both Parties are responsible for ensuring the assigned actions are performed, and for providing feedback to the Service Desk of its own Party.

5.4. Resolution

The resolver group to whom the problem is assigned is responsible for resolving the problem and providing relevant information to the Service Desk of its own Party.

Findings from the processing of the problem are to be recorded for future use.

5.5. Problem closure

A problem is formally closed once the problem is fixed by implementing the change. The problem closure phase will be carried out by the Service Desk that logged the problem and informed the Service Desk of the other Party.

6. Request Fulfilment

The Request Fulfilment Process is the end-to-end management of a request for a new or existing service from the moment it is registered and approved through to closure. Service Requests are usually small, predefined, repeatable, frequent, pre-approved, and procedural requests.

The main steps that have to be followed are outlined below:

6.1. Initiate Request

The information related to a Service Request is submitted to the EU or CH Service Desk by email, phone, or through the IT Service Management (ITSM) tool or any other agreed channel of communication.

6.2. Request Logging and Analysis

For all Service Requests, the contact point should be the EU or CH Service Desk, depending on which Party raised the Service Request. This Service Desk will be responsible for logging and analysing the Service Request with the appropriate diligence.

6.3. Request Approval

The Service Desk Agent of the Party that raised the Service Request checks if any approvals are required from the other Party and if so proceeds to obtain them. If the Service Request is not approved, the Service Desk updates and closes the ticket.

6.4. Request fulfilment

This step caters for the effective and efficient handling of Service Requests. A distinction must be made between the following cases:

– The fulfilment of the Service Request only affects one Party. In this case, this Party issues the work orders and coordinates the execution.

– The fulfilment of the Service Request affects both the EU and CH. In this case, the Service Desks issue the work orders in their area of responsibility. The processing of the Service Request fulfilment is coordinated between both Service Desks. The overall responsibility lies with the Service Desk that received and initiated the Service Request.

When the Service Request has been fulfilled, it must be placed into Resolved State.

6.5. Request Escalation

The Service Desk can escalate the outstanding Service Request to the appropriate resource (third Party) if needed.

Escalations are done to the respective third Parties, i.e. the EU Service Desk will have to go through the CH Service Desk for escalation to a CH third Party, and vice versa.

The third Party to whom the Service Request was escalated is responsible for handling the Service Request in a timely fashion and communicating with the Service Desk who escalated the Service Request.

The Service Desk that logged the Service Request is responsible for tracking the overall status and assignment of a Service Request.

6.6. Request Fulfilment Review

The responsible Service Desk submits the Service Request Record to a final quality control before it is closed. The aim is to make sure that the Service Request is actually processed and that all information required to describe the request's life-cycle is supplied in sufficient detail. In addition to this, findings from the processing of the request are to be recorded for future use.

6.7. Request Closure

If the assigned Parties agree that the Service Request has been fulfilled and the requestor considers the case resolved, the next status to be set is 'Closed'.

A Service Request is formally closed once the Service Desk that logged the Service Request has executed the request closure phase and informed the Service Desk of the other Party.

7. Change Management

The objective is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives.

The Change Management process includes different steps that capture every detail about a Change Request for future tracking. These processes ensure that the change is validated and tested before it moves to deployment. The Release Management process is responsible for successful deployment.

7.1. Request for Change

A Request For Change (RFC) is submitted to the Change Management team for validation and approval. For all Change Requests, the contact point should be the EU or CH Service Desk, depending on which Party raised the request. This Service Desk will be responsible for logging and analysing the request with appropriate diligence.

Change Requests may originate from:

– An incident that causes a change;

– An existing problem that results in a change;

– An end user requesting for a new change;

– Change as a result of an ongoing maintenance;

– Legislative change.

7.2. Change Evaluation and Planning

This stage handles change assessment and planning activities. It includes prioritization and planning activities to minimize risk and impact.

If the implementation of the RFC affects both the EU and CH, the Party that logged the RFC verifies the change evaluation and planning with the other Party.

7.3. Change approvals

Any registered change request needs to be approved by the relevant escalation level.

7.4. Change implementation

Change implementation is handled in the Release Management process. The Release Management teams of both Parties follow their own processes that involve planning and testing. Change review happens once the implementation is completed. To ensure that everything has gone according to plan the existing Change Management process is constantly reviewed and updated wherever necessary.

8. Release Management

A release represents one or more changes to an IT service, collected in a release plan that will have to be authorized, prepared, built, tested, and deployed together. A release may represent a bug fix, a change to hardware or other components, changes to software, upgrades of application versions, changes to documentation and/or processes. The contents of each release are managed, tested and deployed as a single entity.

Release Management aims to plan, build, test and validate, and deliver capability to provide the designed services, which will accomplish the stakeholders' requirements and deliver the intended objectives. Acceptance criteria for all changes to the service will be defined and documented during design coordination and provided to Release Management teams.

The release will typically consist of a number of problem fixes and enhancements to a service. It contains the new or changed software required and any new or changed hardware needed to implement the approved changes.

8.1. Plan the release

The first step of the process assigns authorized changes to release packages and defines the scope and content of releases. Based on this information, the Release Planning sub-process develops a schedule for building, testing and deploying the release.

Planning should define:

– Scope and content of the release;

– Risk assessment and risk profile for the release;

– Customer/users affected by the release;

– Team responsible for the release;

– Delivery and deployment strategy;

– Resources for the release and its deployment.

Both Parties inform each other about their release planning and maintenance windows. If a release affects both the EU and CH, they coordinate the planning and define a common maintenance window.

8.2. Build and Test Release Package

The build and test step of the Release Management process establishes the approach of executing the release or release package and of maintaining the controlled environments prior to changing production, as well as testing all changes in all environments released.

If a release affects both the EU and CH, they coordinate the delivery plans and tests. This includes the following aspects:

– How and when release units and service components will be delivered;

– What the typical lead times are; what happens if there is a delay;

– How to track the progress of the delivery and obtain confirmation;

– Metrics for monitoring and determining the success of the release deployment effort;

– Common test cases for relevant functionalities and changes.

At the end of this sub-process, all required release components are ready to enter the live deployment phase.

8.3. Prepare deployment

The preparation sub-process ensures that communication plans are defined correctly and notifications are ready to be sent to all stakeholders and end users impacted, and that the release is integrated with the Change Management process to ensure that all changes are performed in a controlled manner and approved by the required forums.

If a release affects both the EU and CH, they shall coordinate the following activities:

– Change Request record for scheduling and preparing deployment to Production environment;

– Create implementation plan;

– Rollback approach, so that, in case of deployment failure, the previous state can be placed back;

– Notifications sent to all necessary Parties;

– Require approval for the implementation of the release from the relevant escalation level.

8.4. Roll back the release

In case deployment has failed or testing has identified that deployment was unsuccessful or has not met the agreed acceptance/quality criteria, the Release Management teams of both Parties will need to roll back to the previous state. All necessary stakeholders will need to be informed, including impacted/targeted end users. Pending approval, the process can restart at any of the previous stages.

8.5. Review and close release

When reviewing a deployment, the following activities should be included:

– Capture feedback on customer, user and service delivery satisfaction with the deployment (collect the feedback and consider for continuously improving the service);

– Review any quality criteria that were not met;

– Check that any actions, necessary fixes and changes are complete;

– Make sure there are no capability, resource, capacity or performance issues at the end of the deployment;

– Check that any problems, known errors and workarounds are documented and accepted by the customer, end users, operational support, and other Parties impacted;

– Monitor incidents and problems caused by deployment (provide early life support to operational teams in case the release has caused an increase in volumes of work);

– Update support documentation (i.e. technical information documents);

– Formally hand over the release deployment to service operations;

– Document lessons learnt;

– Collect the release summary document from implementation teams;

– Formally close the release after verifying the Change Request record.

9. Security Incident Management

Security Incident Management is a process for handling security incidents in order to enable incident communication to potentially impacted stakeholders; incident evaluation and prioritisation; and incident response to settle any actual, suspected or potential breach of confidentiality, availability or integrity of sensitive information assets.

9.1. Information Security Incident Categorization

All incidents impacting the link between the Union Registry and the Swiss registry shall be analysed to determine a possible breach in the confidentiality, the integrity or the availability of any sensitive information recorded in the Sensitive Information List (SIL).

If so, the incident shall be characterized as an information security incident, immediately registered in the IT Service Management (ITSM) tool and managed as such.

9.2. Information Security Incident Handling

Security Incidents are placed under the responsibility of the 3rd escalation level and resolution of the incidents will be dealt with by a dedicated Incident Management Team (IMT).

The IMT is responsible for:

– Carrying out a first analysis, categorizing and rating the severity of the incident;

– Coordinating actions between all the stakeholders including the full documentation of the incident analysis, the decisions taken to tackle the incident and any possible identified weaknesses;

– Depending on the severity of the security incident, escalating the incident in a timely manner to the appropriate level for information and/or a decision.

In the Information Security Management process, all information regarding incidents is classified at the highest level of sensitivity of the information, but in any case not lower than ETS SENSITIVE.

For an on-going investigation and/or a weakness that could be exploited, and until its remediation, the information is classified as ETS CRITICAL.

9.3. Security Incident Identification

Based on the security event type, the information security officer determines appropriate organizations to be involved and to be part of the IMT.

9.4. Security Incident Analysis

The IMT liaises with all involved organizations and the relevant members of their teams, as appropriate, to review the incident. During the analysis, the extent of an asset's confidentiality, integrity or availability loss is identified and consequences for all affected organizations are assessed. Next, initial and follow-up actions to resolve the incident and manage its impact, including the resource impact of these actions, are defined.

9.5. Security Incident Severity assessment, Escalation and Reporting

The IMT shall assess the severity of any new security incident after its characterization as a security incident and shall start immediate required action according to the severity of the incident.

9.6. Security Response Reporting

The IMT includes incident containment and recovery results in the information security incident response report. The report is provided to the 3rd escalation level using secure email or other mutually accepted means of secure communication.

The responsible Party reviews the containment and recovery results and:

– Reconnects the registry in case of prior disconnection;

– Provides incident communications to the registry teams;

– Closes the incident.

The IMT should include – in a secure manner - relevant details in the information security incident report in order to ensure consistent recording and communication and to enable prompt and appropriate action to contain the incident. Following its completion, the IMT provides the information security incident final report in due course.

9.7. Monitoring, Capacity Building and Continuous Improvement

The IMT will provide reports for all security incidents to the 3rd escalation level. The reports will be used by this escalation level to determine the following:

– Weak points in security controls and/or operation that need to be strengthened;

– A possible need to enhance this procedure to improve the effectiveness of the response to incidents;

– Training and capacity building opportunities to further strengthen the information security resilience of registry systems, reduce the risk of future incidents and minimize their impact.

10. Information Security Management

Information Security Management aims to ensure the confidentiality, integrity and availability of an organization's classified information, data and IT services. In addition to the technical components including their design and testing (see LTS), the following common operational procedures are necessary to fulfil the security requirements for the provisional solution.

10.1. Sensitive information identification

The sensitivity of a piece of information is assessed by determining the level of impact on the business (e.g. financial losses, image degradation, law infringement…) a security breach related to this information could have.

The sensitive information assets shall be identified on the basis of their impact on linking.

The level of sensitivity of this information shall be assessed according to the sensitivity scale applicable for this linking and detailed in the 'Information Security Incident Handling' section of this document.

10.2. Sensitivity levels of Information Assets

Upon its identification, the information asset is classified by applying the following rules:

– The identification of at least a single HIGH confidentiality, integrity or availability level classifies the asset as ETS CRITICAL;

– The identification of at least a single MEDIUM confidentiality, integrity or availability level classifies the asset as ETS SENSITIVE;

– The identification of only LOW confidentiality, integrity or availability levels classifies the asset as ETS LIMITED.

10.3. Assignment of Information Assets Owner

All information assets should have an assigned owner. Information assets of the ETS, belonging to or in conjunction with the link between the EUTL and the SSTL should be included in a joint asset inventory list, maintained by both Parties. Information assets of the ETS outside the link between the EUTL and the SSTL should be included in an asset inventory list, maintained by the respective Party.

Ownership of each information asset belonging to or in conjunction with the link between the EUTL and the SSTL is to be agreed to by the Parties. The owner of an information asset is responsible for assessing its sensitivity.

The owner should have a level of seniority that is appropriate to the value of the assigned asset(s). The owner's responsibility for the asset(s) and his or her obligation to maintain the required level of confidentiality, integrity and availability should be agreed and formalized.

10.4. Registration of sensitive information

All sensitive information shall be registered in the Sensitive Information List (SIL).

Where relevant, the aggregation of sensitive information that could lead to a higher impact than the impact of one single piece of information shall be taken into account and registered in the SIL (e.g. a set of information stored in the system database).

The SIL is not static. Threats, vulnerabilities, likelihood or consequences of security incidents related to the assets may change without any indication and new assets might be introduced into the operation of registry systems.

Therefore, the SIL shall be reviewed regularly and any new information identified as sensitive shall be immediately registered into the SIL.

The SIL shall contain at least the following information for each entry:

– Description of the information

– Information owner

– Sensitivity level

– Indication if the information includes personal data

– Additional information if required

10.5. Handling of sensitive information

When processed outside the link between the Union Registry and Swiss Registry, sensitive information shall be handled in accordance with the Handling Instructions.

Sensitive information processed by link between the Union Registry and Swiss Registry shall be handled in accordance with the Security requirements by the Parties.

10.6. Access Management

The objective of Access Management is to grant authorized users the right to use a service, while preventing access to non-authorized users. Access Management is sometimes also referred to as 'Rights Management' or 'Identity Management'.

For the provisional solution and its operation, both Parties need access to the following components:

– Wiki: A collaboration environment for the exchange of common information, such as release planning;

– IT Service Management (ITSM) Tool for incident and problem management (see chapter 3, 'Approach and Standards');

– Message exchange system: each Party shall provide a secure message exchange transfer system for the transmission of the messages containing the transaction data.

The Swiss registry administrator and the Union central administrator ensure that accesses are up-to-date and act as contact points for their Parties for access management activities. Access requests are handled according to the Request Fulfilment procedures.

10.7. Certificate/Key Management

Each Party is responsible for its own certificate/key management (generation, registration, storage, installation, usage, renewal, revocation, backup and recovery of certificates/keys). As outlined in the Linking Technical Standards (LTS), only digital certificates issued by a Certificate Authority (CA) trusted by both Parties shall be used. The handling and storage of certificates/keys must follow the provisions set in the Handling Instructions.

Any revocation and/or renewal of certificates and keys shall be coordinated by both Parties. This takes place according to the Request Fulfilment procedures.

The Swiss registry administrator and the Union central administrator will exchange certificates/keys via secure means of communication according to the provisions laid down in the Handling Instructions.

Any verification of certificates/keys in any means between the Parties will take place out of band.