DG TAXUD

Business continuity plan for Member States

ICS2

Date: 11/02/2021
Doc. Version: 1.00

Document Control Information

Settings	Value
Document Title:	Business continuity plan for Member States
Project Title:	ICS2
Document Author:	DG TAXUD ICS2 Project team
Project Owner:	DG TAXUD ICS2 Project team
Doc. Version:	1.00
Sensitivity:	Basic
Date:	11/02/2021

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All reviewers in the list are considered required unless explicitly listed as Optional.

Name	Role	Action	Date
ECCG		Approve	

Document history:

The Document Author is authorized to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Short Description of Changes
1.00	11/02/2021	DG TAXUD	Submitted for approval (SfA)
0.70	05/02/2021	DG TAXUD	Document updated after ITSM3 TES and Member State review
0.60	09/12/2020	DG TAXUD	Document updated after TAXUD ICS2 project team internal review
0.51	03/12/2020	DG TAXUD	Document updated based on the input from the PG held 30/11/2020
0.50	27/11/2020	DG TAXUD	Document updated based on the input from the PG held 05/11/2020 and 06/11/2020
0.41	05/11/2020	DG TAXUD	Document updated based on the input from the PG held 13/10/2020
0.30	13/10/2020	DG TAXUD	Document updated with more detailed information
0.20	11/09/2020	DG TAXUD	Document updated based on the first PG 24/07/2020 input
0.10	24/07/2020	DG TAXUD	Initial draft of the document

TABLE OF CONTENTS

1 INTRODUCTION 4

1.1 Purpose 4
1.2 Scope 4
1.3 Target Audience 4
1.4 Structure of this document 4
1.5 Reference and applicable documents 5
1.5.1 Reference Documents 5
1.6 Abbreviations and Acronyms 5
1.7 Definitions 6

2 SOURCES OF SYSTEM UNAVAILABILITY 7

3 BUSINESS CONTINUITY MEASURES AND COMMUNICATION 8

3.1 Economic operator system unavailability 8
3.2 HTI unavailability 11
3.2.1 UUM&DS Central component unavailability 11
3.2.2 UUM&DS unavailability – National Component 14
3.2.3 TAPAS unavailability 17
3.2.4 STI unavailability 20
3.3 Common Repository unavailability 23
3.4 CCN2 unavailability 28
3.5 NES Unavailability 33
3.5.1 NES (RMS) unavailability 33
3.5.2 NES (IMS) unavailability 39
3.5.3 NES (PNES) and (CNES) unavailability 42
3.6 ICS2 Message prioritisation 44
3.6.1 External domain messages 44
3.6.2 Common domain messages 45
3.7 Templates for notification of the unavailability 46
3.7.1 Economic Operator unavailability notification information template (EO to NSD or IT service provider to CSD) 46
3.7.2 ICS2 Component / NES unavailability notification information template (CSD to NSD or NSD to CSD) 47
3.7.3 ICS2 Component / NES unavailability notification information template (NSD to EO/IT service provider or CSD to IT service provider) 49
3.7.4 Business continuity plan activation notification template (NSD to EO/IT service provider) 50
3.7.5 Business continuity plan activation notification template (NSD to CSD) 50
3.7.6 Request to activate business continuity plan template (CSD) 51
3.7.7 Notification on recovery of ICS2 components 51
3.7.8 Business continuity plan is deactivated 52
3.8 Unavailability statistics 52
3.9 Scheduled unavailability 53

4 ANNEXES 54

4.1 Annex A: Statistics on ICS2 unavailability 54
4.2 Annex B: Consolidated statistics on ICS2 unavailability 54

1 INTRODUCTION

1.1 Purpose

This document describes the impact on a business process and assesses the criticality of an unavailability of a given component of the ICS2. Furthermore, it introduces measures to maintain an appropriate level of business continuity with regard to the required customs formalities on the entry of goods.

1.2 Scope

This document covers the measures for continuity of the business of ICS2 Release 1 only. Disaster recovery plans and IT protocols for technical issues are not covered by this document. These artefacts will be elaborated separately.

1.3 Target Audience

The intended audience for this document are:

- DG TAXUD Central service desk;
- National service desks of the Member States;
- Economic operators filing ENS filings;
- IT service providers;
- any person involved in the ICS2 project.

1.4 Structure of this document

The document contains the following chapters:

- **Chapter 1 – Introduction**: describes the scope and the objectives of the document;
- **Chapter 2 – Sources of system unavailability:** provides the system components of ICS2 and a brief description of the impact on the business process;
- **Chapter 3 – Business continuity measures and communication**: provides business continuity measures, communication of unavailability, and activation of the BCP and recovery of the system, as well as recovery strategy from a business perspective;
- **Chapter 4 – Annexes**: provide template for ICS2 unavailability statistics.

1.5 Reference and applicable documents

1.5.1 Reference Documents

Ref.	Title	Reference	Version	Date
R01	Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code			9/10/2013
R02	Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code			28/07/2015
R03	Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code			24/11/2015
R04	TES-RfA-SLA Availability Continuity Management		3.20	04/11/2020
R05	CD3-ICS2-HTI-Interface Control Document		2.90	25/11/2020

Table 1: Reference documents

1.6 Abbreviations and Acronyms

Abbreviation/Acronym	Definition
AEO	Authorised Economic Operator
BCP	Business continuity plan
CNES	Controls component of Member state National entry system
CSD	Central Service Desk
DNL	Do Not Load
ENS	Entry Summary Declaration
EO	Economic Operator
EU	European Union
HRCM	High Risk Cargo and Mail
ICS2	Import Control System 2
IMS	Involved Member State
MRN	Master Reference Number
MS	Member State
NES	National Entry System
NSD	National Service Desk
PNES	Presentation component of Member state National entry system
RfI	Request for Information
RfS	Request for Screening
RMS	Responsible Member State

Table 2: Abbreviations and acronyms

1.7 Definitions

Term	Description
Central component	ICS2 Common repository and CCN2
Central service desk (CSD)	The DG TAXUD contractor responsible for the central operation in ICS2 (ITSM) with two level support
IT service provider	IT service provider is entity acting as a technical sender of the messages and assuming only technical responsibility.
MS user	Customs officer, risk analyst or any other person in particular Member state using ICS2.

Table 3: Definitions

2 SOURCES OF SYSTEM UNAVAILABILITY

Depending on the source of unavailability, business continuity procedures will have to vary to some extent due to their effectiveness provided in a given case. Looking at it from an end-to-end perspective, the following causes of unavailability of an electronically supported business process were identified:

- a relevant electronic system of the economic operator is unavailable;
- a relevant electronic national customs application or supporting system is unavailable;
- a relevant common central service is unavailable.

Service providers who provide services for economic operators (e.g. network connectivity, software for electronic communication/connection with relevant customs systems etc.) are not considered being directly responsible with regard to legal requirements stemming from the customs legislation. Nevertheless, they have a responsibility to fulfil the contractual requirements of the established contract with an economic operator.

In order to implement a sufficient business continuity plan that is underpinned by effective measures the following factors are to be considered:

- What system component is not available or has a malfunction seriously affecting the business operations?
- What is the impact of the unavailability of the given system component on the end-to-end process?
- What are the available effective options for efficient and appropriate measures to overcome the impact?

The following matrix shows the relevant ICS2 system components and their impact on the business process in case of unavailability:

			CAPABILITIES																	
IT Component			Send ENS	Register and send MRN	Lifecycle validation	Prepare ENS for RA	Send e-risk request	Send e-screening request	Perform RA			Send/ Receive RA Results	Perform e-screening		Send/ Receive e-screening Results	Referrals	Assessment Complete	DNL	Presentation	Controls
EO System	Postal operators		3													3	3	2		1
	Express carriers		3													3	1	2		1
HTI	TAPAS		3													3	3	3		1
	UUM&DS	Central Component	2													2				
		National Application	2													2				
	STI		1	3	1											3	3	3		1
CR				1	3	3	3	3				3			2	3	3	3	3	3
CCN2							3	3				3			2	3			3	3
NES	NES (RMS)	Lifecycle					3					3								
		Risk Engine							1	2	3									
	NES (IMS)	Lifecycle						3							2					
		Risk Engine											1	2						
	PNES																		3	
	CNES																			3
			Category A1 - EOS impacted			Category A2 - RA impacted										Category A1 - EOS impacted			Category B - less time critical	

Impact of Component Unavailability on capability	
3	Total disfunction
2	Partial disfunction / degradation
1	Limited disfunction (non essential)
	No impact

Table 4 System unavailability

The following subsections will further describe the business continuity measures to be applied in case of unavailability of each ICS2 component and how the unavailability, BCP activation and recovery is communicated between the Central and National service desks and the economic operators and their IT service providers, if applicable.

3 BUSINESS CONTINUITY MEASURES AND COMMUNICATION

Economic operator is directly responsible to comply with legal requirements of the customs legislation. CSD, DG TAXUD and IT service provider will support the business continuity process but customs of particular MS is always the one taking a decisions and providing instructions for EO established in its country in case of unavailability of ICS2 components.

3.1 Economic operator system unavailability

The unavailability of an economic operator's system affects either one economic operator in case of an in-house IT solution or all economic operators, which are customers of an IT service provider.

The business continuity measures will depend on which part of the end-to-end process is affected – whether the ENS filing is already lodged or not.

		CAPABILITIES							
	IT Component	Send ENS	Register and send MRN	Lifecycle validation	Referrals	Assessment Complete	DNL	Presentation	Controls
EO System	Postal operators	3			3	3	2		1
	Express carriers	3			3	1	2		1

Table 5 EO System unavailability

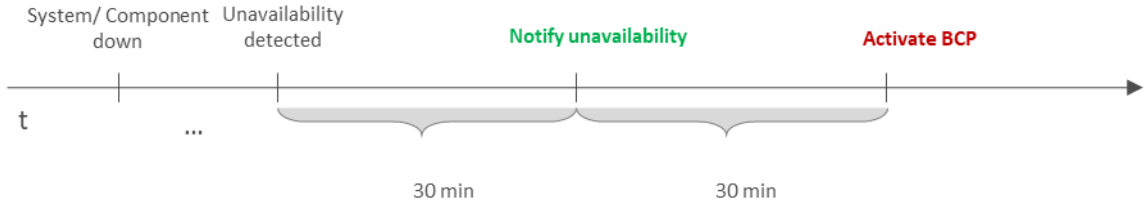

Figure 1 Business continuity plan activation timeline for EO system

Unavailable component		
Economic Operator System		
Component unavailability description		
The system of an Economic Operator is considered to be unavailable when it cannot interact (send and receive messages) as per the specifications of ICS2 regardless of the reason. If the Economic Operator System unavailability can be compensated (alternatively handled) by another facility of the Economic Operator without impact on the operations continuity, there is no reason to activate any business continuity measures by the Customs Authorities.		
Unavailability identification and notification		
Relevant EO	Once the EO has detected an unavailability in their system or system components, the unavailability needs to be notified to the NSD of the MS to which the EO has legal obligation to file ENS filings. In case of the unavailability of the IT Service provider system, the unavailability needs to be notified by IT Service provider to the CSD and to all postal operators affected. In this case CSD will notify NSD(s) on EO unavailability.	30 min

	The unavailability notification has to be sent after 30 minutes from the detection of unavailability and it has to contain all the details as elaborated in [3.7.1].	
NSD (MS to which the EO is addressing the ENS filings)	The NSD of the MS to which the EO is addressing the ENS filings notifies: • CSD (except IT service provider unavailability where IT service provider notify CSD himself) • MS user as soon as information on the unavailability of the EO system has been provided and it has to contain all the details as elaborated in [3.7.1].	asap
CSD	The CSD notifies: • In case of unavailability of the express operator's system – all NSDs; • In case of the unavailability of the IT service provider of the postal operators – all NSDs although only those MS whose postal operators are using IT service provider system are affected.	asap
Activation of Business continuity plan		
NSD	If the EO system is not restored, the business continuity plan is activated 30 minutes after the unavailability has been notified. The NSD notifies the activation of the business continuity plan and applicable measures to: • EOs that are filing their ENSs [3.7.4] • MS users The NSD notifies the CSD of the activation of the business continuity plan and the measures and it has to contain all the details as elaborated in [3.7.5].	30 min
EO	EO notifies IT service provider on activation of business continuity plan, if necessary.	asap
CSD	The CSD notifies about the activation of the BCP all NSDs.	asap
Business continuity measures		
Lodgement of new ENS		
ENS filings	No new ENS filings will be lodged during the unavailability of the EO system. If the goods (postal consignments) have already arrived to the EU and are presented to customs, the lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible. If the goods (express consignments) have already arrived to the EU and are presented to customs, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.	
Amendment	No amendments will be done on the already filed ENSs	
Invalidation	Invalidation of ENS will not be performed	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	Issued via alternative communication channels – e-mail, phone, etc.	
Referral responses from the EO	Communicated via alternative communication channels – e-mail, phone, etc.	
DNL	Issued via phone and e-mail	

Assessment complete notifications	Not communicated to the EO during the unavailability of their system	
Advance control notification to AEO	Communicated via alternative communication channels – e-mail, phone, etc.	
Presentation and controls		
Presentation information	If the goods (postal consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible.	
	If the goods (express consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.	
Recovery strategy		
Recovery communication		
Relevant EO	Once the EO system has been restored it has to be notified to the NSD of the MS to which the EO is addressing the ENS filings. In case of the IT Service provider system, the recovery needs to be notified by IT service provider to the CSD and to all postal operators affected.	asap
NSD (MS to which the EO is addressing the ENS filings)	The NSD of the MS to which the EO is addressing the ENS filings notifies deactivation of BCP to: • CSD • MS users • EO as soon as information on the recovery of the EO system has been provided.	asap
CSD	The CSD notifies all NSDs on recovery of IT service provider system.	asap
	The CSD notifies all NSDs on deactivation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has deactivated BCP.	asap
Recovery measures		
Relevant EO	EO has to lodge ENS filings for all the goods that have not yet been presented to customs immediately after the system has been restored.	
	EO can amend and invalidate the ENS filings which are not yet in the state 'Presented'.	
	Referral responses that have been provided via alternative means have to be sent via the system.	
	The messages need to be forwarded in quantities not to disrupt the regular performance of the HTI due to abnormally high levels. The resulting traffic should not exceed limits agreed on technical protocol. The messages must be distributed in accordance with the assigned priority.	
ICS2 Central components	The HTI needs to re-send the messages to the EO for which the delivery was not confirmed by the technical protocol. The re-sent messages should be sent in quantities not disrupting the EO system. To be further elaborated in the technical protocols. Statistics are gathered by the central components for the unavailability of the EO system and the delayed responses to risk analysis requests.	
NES	Risk analysis is performed to the provided ENSs even if with a delay.	

3.2 HTI unavailability

3.2.1 UUM&DS Central component unavailability

			CAPABILITIES							
			Send ENS	Register and send MRN	Lifecycle validation	Referrals	Assessment Complete	DNL	Presentation	Controls
IT Component										
HTI	UUM&DS	Central Component	2			2				
		National Application	2			2				

Table 6 UUM&DS unavailability

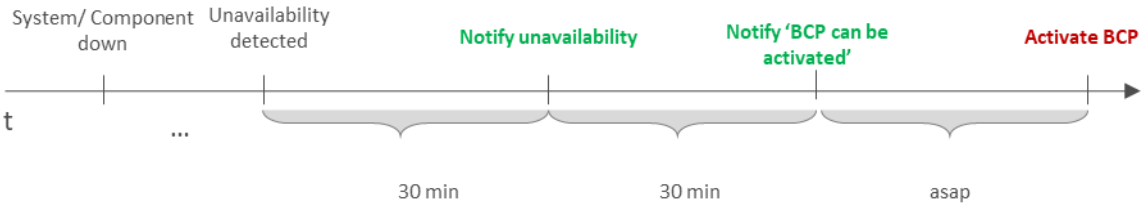

Figure 2 Business continuity plan activation timeline for UUM&DS component

Unavailable component		
UUM&DS Central Component		
Component unavailability description		
The unavailability of the UUM&DS services prevents the system from identifying and authenticating the sender of a message. The submitted messages are rejected with an error message [R05]. Consequently, the business process does not continue and messages are not registered, further processed and responded. The UUM&DS component is considered unavailable in the case of the failover domain activation failure. The UUM&DS central component information is cached in TAPAS for 24 hours. If an Economic Operator has not sent a message within the last 24 hours or is newly registered, there is no authentication information available about it in the stored cache.		
Unavailability identification and notification		
CSD	The CSD notifies: • All NSDs; • IT service provider. The unavailability notification has to be sent after 30 minutes from the detection of unavailability and it has to contain all the details as elaborated in [3.7.2, 3.7.3].	30 min
NSD (MS to which the EO is addressing the ENS filings)	The NSD of each MS affected notifies all the EOs that are filing their ENSs to their MS and it has to contain all the details as elaborated in [3.7.3].	asap
IT service provider	IT service provider notifies unavailability to all clients (postal operators) affected.	asap

Activation of Business continuity plan		
CSD	If the component is not restored, the CSD needs to notify the NSD of affected MS about the possibility of activation of the Business continuity plan. This notification needs to be communicated 30 minutes after the notification of the unavailability of the component and it has to contain all the details as elaborated in [3.7.6].	30 min
	The CSD notifies all NSDs about activation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has activated BCP.	asap
NSD	The business continuity plan is activated by the MS to which the EO is filing the ENS filings. Decision to activate the BCP needs to be taken immediately after receipt of the CSD notification allowing for BCP activation. The NSD notifies the activation of the business continuity plan and applicable measures to: • EOs that are filing their ENSs [3.7.4]; • MS users; • CSD [3.7.5].	asap
EO	EO notifies IT service provider on activation of business continuity plan, if necessary.	asap
Business continuity measures		
Lodgement of new ENS		
ENS filings	No new ENS filings will be lodged during the unavailability of the component. If the goods (postal consignments) have already arrived to the EU and are presented to customs, the lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible. If the goods (express consignments) have already arrived to the EU and are presented to customs, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.	
Amendment	No amendments will be done on the already filed ENSs.	
Invalidation	Invalidation of ENS will not be performed.	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	No impact	
Referral responses from the EO	Communicated via alternative communication channels – e-mail, phone, etc.	
DNL	No impact	
Assessment complete notifications	No impact	
Advance control notification to AEO	No impact	
Recovery Strategy		
Recovery Communication		
CSD	The CSD notifies: • All NSDs;	asap

	• IT service provider that the component has been recovered.	
	The CSD notifies all NSDs about deactivation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has deactivated BCP.	asap
NSD (MS to which the EO is addressing the ENS filings)	The NSD of each MS affected notifies: • all the EOs that are filing their ENSs to their MS • MS users that the component has been recovered and the Business continuity plan is no longer applicable.	asap
IT service provider	IT service provider notifies recovery to all clients (postal operators) affected.	asap
EO	EO notifies IT service provider on deactivation of BCP, if necessary.	asap
Recovery measures		
Relevant EO	EO has to lodge ENS filings for all the goods that have not yet been presented to customs immediately after the component has been restored.	
	EO can amend and invalidate the ENS filings.	
	Referral responses that have been provided via alternative means have to be sent via the system.	
	The messages need to be forwarded in quantities not to disrupt the regular performance of the HTI due to abnormally high levels. The resulting traffic should not exceed limits agreed on technical protocol. The messages must be distributed in accordance with the assigned priority.	
NES	Risk analysis is performed to the provided ENSs even if with a delay.	

3.2.2 UUM&DS unavailability – National Component

			CAPABILITIES							
			Send ENS	Register and send MRN	Lifecycle validation	Referrals	Assessment Complete	DNL	Presentation	Controls
IT Component										
HTI	UUM&DS	Central Component	2			2				
		National Application	2			2				

Table 7 UUM&DS unavailability

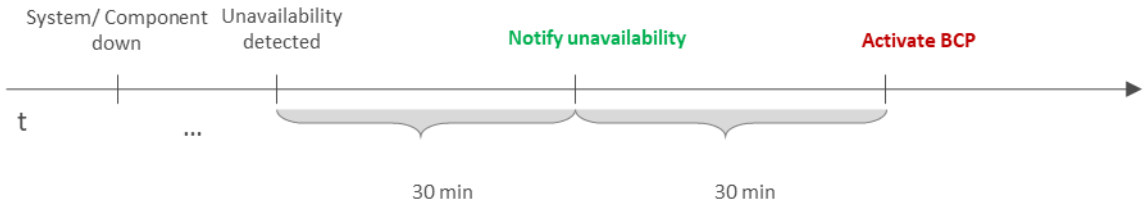

Figure 3 Business continuity plan activation timeline for UUM&DS component

Unavailable component		
UUM&DS National Component		
Component unavailability description		
The unavailability of UUM&DS National component will prevent the system from identifying and authenticating the sender of a message. The submitted messages are rejected with an error message. Consequently, the business process does not continue and messages are not registered, further processed and responded. The UUM&DS national component is considered unavailable in the case of the failover domain activation failure. The UUM&DS national component information is cached in TAPAS for 24 hours. If an Economic Operator has not sent a message within the last 24 hours or is newly registered, there is no authentication information available about it in the stored cache.		
Unavailability identification and notification		
NSD	The NSD of the affected MS notifies: • All the EOs that are filing their ENSs to the affected MS; • CSD. The unavailability notification has to be sent after 30 minutes from the detection of unavailability and it has to contain all the details as elaborated in [3.7.3, 3.7.2].	30 min
CSD	The CSD notifies all NSDs.	asap
Activation of Business continuity plan		
NSD	If the component is not restored within 30 minutes of the unavailability notification, the business continuity plan is activated by the MS. Decision to activate the BCP needs to be taken within 30 minutes after detection of the component unavailability. The NSD notifies the activation of the business continuity plan and applicable measures to: • EOs [3.7.4];	30 min

	• MS users; • CSD [3.7.5].	
CSD	CSD notifies activation of the Business continuity plan by an affected MS to all NSDs.	asap
Business continuity measures		
Lodgement of new ENS		
ENS filings	No new ENS filings will be lodged during the unavailability of the component. If the goods (postal consignments) have already arrived to the EU and are presented to customs, the lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible. If the goods (express consignments) have already arrived to the EU and are presented to customs, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.	
Amendment	No amendments will be done on the already filed ENSs.	
Invalidation	Invalidation of ENS will not be performed.	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	No impact	
Referral responses from the EO	Communicated via alternative communication channels – e-mail, phone, etc.	
DNL	No impact	
Assessment complete notifications	No impact	
Advance control notification to AEO	No impact	
Recovery Strategy		
Recovery Communication		
NSD	The NSD notifies about the recovery of the component and that the Business continuity plan is no longer applicable: • All the EOs that are filing their ENSs to their MS; • Affected IT service provider, if any; • MS users; • CSD.	asap
CSD	The CSD notifies all NSDs about the recovery of a MS component and deactivation of BCP by a particular NSD.	asap
IT service provider	IT service provider notifies recovery to all clients (postal operators) affected.	asap
Recovery measures		
Relevant EO	EO has to lodge ENS filings for all the goods that have not yet been presented to customs immediately after the component has been restored.	
	EO can amend and invalidate the ENS filings.	
	Referral responses that have been provided via alternative means have to be sent via the system.	

	The messages need to be forwarded in quantities not to disrupt the regular performance of the HTI due to abnormally high levels. The resulting traffic should not exceed limits agreed on technical protocol. The messages must be distributed in accordance with the assigned priority.
NES	Risk analysis is performed to the provided ENSs even if with a delay.

3.2.3 TAPAS unavailability

		CAPABILITIES							
		Send ENS	Register and send MRN	Lifecycle validation	Referrals	Assessment Complete	DNL	Presentation	Controls
IT Component									
HTI	TAPAS	3			3	3	3		1

Table 8 TAPAS unavailability

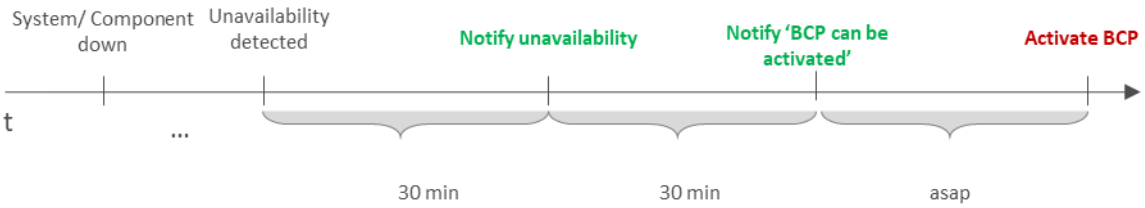

Figure 4 Business continuity plan activation timeline for TAPAS component

Unavailable component		
TAPAS		
Component unavailability description		
No message exchange between the Economic Operators and the HTI can take place.		
Unavailability identification and notification		
CSD	The CSD notifies about detected unavailability: • All NSDs; • Affected IT service provider, if any. The unavailability notification has to be sent after 30 minutes from the detection of unavailability and it has to contain all the details as elaborated in [3.7.2, 3.7.3].	30 min
NSD (MS to which the EO is addressing the ENS filings)	The NSD notifies: • all the EOs that are filing their ENSs to their MS and it has to contain all the details as elaborated in [3.7.3]; • relevant MS users.	asap
IT service provider	IT service provider notifies unavailability to all clients (postal operators) affected.	asap
Activation of Business continuity plan		
CSD	If the component is not restored, the CSD needs to notify the NSDs about the possibility of activation of the Business continuity plan and it has to contain all the details as elaborated in [3.7.6]. This notification needs to be communicated 30 minutes after the notification of the unavailability of the component.	30 min
	The CSD notifies all NSDs about the activation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has activated BCP.	asap

NSD	The business continuity plan is activated by the MS to which the EO is filing the ENS filings. Decision to activate the BCP needs to be taken immediately after receipt of the CSD notification allowing for BCP activation. The NSD notifies the activation of the business continuity plan and applicable measures to: • EOs [3.7.4]; • IT service providers [3.7.4]; • MS users; • CSD [3.7.5].	asap
Business continuity measures		
Lodgement of new ENS		
ENS filings	No new ENS filings will be lodged during the unavailability of the component. If the goods (postal consignments) have already arrived to the EU and are presented to customs, the lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible. If the goods (express consignments) have already arrived to the EU and are presented to customs, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.	
Amendment	No amendments will be done on the already filed ENSs.	
Invalidation	Invalidation of ENS will not be performed.	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	Issued via alternative communication channels – e-mail, phone, etc.	
Referral responses from the EO	Communicated via alternative communication channels – e-mail, phone, etc.	
DNL	Issued via phone and e-mail.	
Assessment complete notifications	Not communicated to the EO during the unavailability of TAPAS.	
Advance control notification to AEO	Communicated via alternative communication channels – e-mail, phone, etc.	
Recovery Strategy		
Recovery Communication		
CSD	The CSD notifies about the recovery: • All NSDs; • Affected IT service provider, if any.	asap
	The CSD notifies all NSDs about the deactivation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has deactivated BCP.	asap
NSD (MS to which the EO is addressing the ENS filings)	The NSD of each MS affected notifies: • all the EOs that are filing their ENSs to their MS; • MS users; • CSD; that the component has been recovered and the Business continuity plan is no longer applicable.	asap

IT service provider	IT service provider notifies recovery to all clients (postal operators) affected.	asap
Recovery measures		
Relevant EO	EO has to lodge ENS filings for all the goods that have not yet been presented to customs immediately after the component has been restored.	
	EO can amend and invalidate the ENS filings.	
	Referral responses that have been provided via alternative means have to be sent via the system.	
	The messages need to be forwarded in quantities not to disrupt the regular performance of the HTI due to abnormally high levels. The resulting traffic should not exceed limits agreed on technical protocol. The messages must be distributed in accordance with the assigned priority.	
ICS2 Central components	The HTI needs to re-send the messages to the EO for which the delivery was not confirmed by the technical protocol.	
NES	Risk analysis is performed to the provided ENSs even if with a delay.	

3.2.4 STI unavailability

		CAPABILITIES							
		Send ENS	Register and send MRN	Lifecycle validation	Referrals	Assessment Complete	DNL	Presentation	Controls
IT Component									
HTI	STI	1	3	1	3	3	3		1

Table 9 STI unavailability

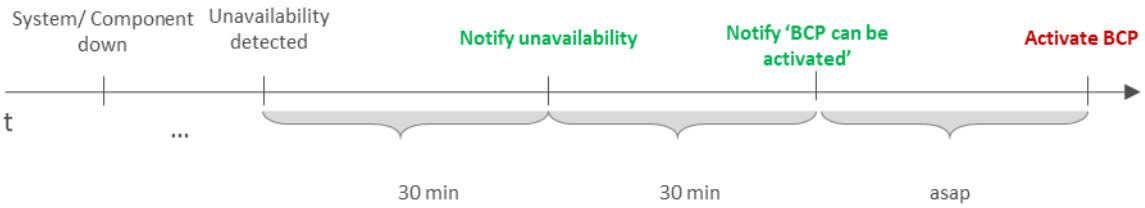

Figure 5 Business continuity plan activation timeline for STI component

Unavailable component		
Shared Trader Interface		
Component unavailability description		
No message exchange between the Economic Operators and the HTI can take place. In case of unavailability of the STI, no messages from the Economic Operators will be functionally validated, registered and further processed. Moreover, no messages are sent to the Economic Operators for the ENSs which are already in process. The messages received from the Economic Operators are stored and queued in TAPAS and can be processed when STI is available again. There is no need for the Economic Operators to re-send messages. The outgoing STI messages are queued but not sent. The operations performed by the STI are completely blocked – no MRNs are generated and communicated.		
Unavailability identification and notification		
CSD	The CSD notifies about detected unavailability: • All NSDs; • IT service provider. The unavailability notification has to be sent after 30 minutes from the detection of unavailability and it has to contain all the details as elaborated in [3.7.2, 3.7.3].	30 min
NSD (MS to which the EO is addressing the ENS filings)	The NSD notifies: • all the EOs that are filing their ENSs to their MS [3.7.3]; • relevant MS users.	asap
IT service provider	IT service provider notifies unavailability to all clients (postal operators) affected.	asap
Activation of Business continuity plan		
CSD	If the component is not restored, the CSD needs to notify the NSDs about the possibility of activation of the Business continuity plan [3.7.6].	30 min

	This notification needs to be communicated 30 minutes after the notification of the unavailability of the component.	
	The CSD notifies all NSDs about the activation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has activated BCP.	asap
NSD	The business continuity plan is activated by the MS to which the EO is filing the ENS filings. Decision to activate the BCP needs to be taken immediately after receipt of the CSD notification allowing for BCP activation. The NSD notifies the activation of the business continuity plan and applicable measures to: • EOs [3.7.4]; • IT service providers [3.7.4]; • MS users; • CSD [3.7.5].	asap
Business continuity measures		
Lodgement of new ENS		
ENS filings	New ENS filings can be lodged during the unavailability of the component. If the message load is too large the CSD may request to stop sending of the messages. If the goods (postal consignments) have already arrived to the EU and are presented to customs, the lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible. If the goods (express consignments) have already arrived to the EU and are presented to customs, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.	
Amendment	Amendments of the ENSs can be lodged, but already filed ENSs will not be amended until the system is restored.	
Invalidation	Invalidation of ENS can be requested, but will not be performed until the system is restored.	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	Issued via alternative communication channels – e-mail, phone, etc.	
Referral responses from the EO	Response messages can be sent to the system, but they will only be processed after the system is restored. For this reason they need to be communicated via alternative communication channels – e-mail, phone, etc. in addition to the messages sent via system.	
DNL	Issued via phone and e-mail.	
Assessment complete notifications	Not communicated to the EO during the unavailability of STI.	
Advance control notification to AEO	Communicated via alternative communication channels – e-mail, phone, etc.	
Recovery Strategy		
Recovery Communication		
CSD	The CSD notifies about the recovery: • All NSDs; • Affected IT service provider, if any.	asap

	The CSD notifies all NSDs about the deactivation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has deactivated BCP.	asap
NSD (MS to which the EO is addressing the ENS filings)	The NSD of each MS affected notifies: • all the EOs that are filing their ENSs to their MS; • MS users; • CSD; that the component has been recovered and the Business continuity plan is no longer applicable.	asap
IT service provider	IT service provider notifies recovery to all clients (postal operators) affected.	asap
Recovery measures		
Relevant EO	EO has to lodge only the missing ENS filings. In case the ENS filings were lodged during the unavailability the EO does not need to do any further actions.	
	EO can amend and invalidate the ENS filings. If amendment or invalidation was requested during the unavailability, no further actions from the EO are needed.	
	Referral responses that have been provided via alternative means have to be sent via the system. If referral responses were submitted via the system in addition to the other communication channels during the unavailability, no further actions from the EO are needed.	
	The messages need to be forwarded in quantities not to disrupt the regular performance of the HTI due to abnormally high levels. The resulting traffic should not exceed limits agreed on technical protocol. The messages must be distributed in accordance with the assigned priority.	
ICS2 Central components	The HTI needs to re-send the messages to the EO for which the delivery was not confirmed by the technical protocol.	
NES	Risk analysis is performed to the provided ENSs even if with a delay.	

3.3 Common Repository unavailability

IT Component	CAPABILITIES																
	Send ENS	Register and send MRN	Lifecycle validation	Prepare ENS for RA	Send e-risk request	Send e-screening request	Perform RA			Send/ Receive RA Results	Perform e-screening		Send/ Receive e-screening Results	Referrals	Assessment Complete	DNL	Presentation	Controls
CR		1	2	3	3	3				3			2	3	3	3	3	3

Table 10 Common Repository unavailability

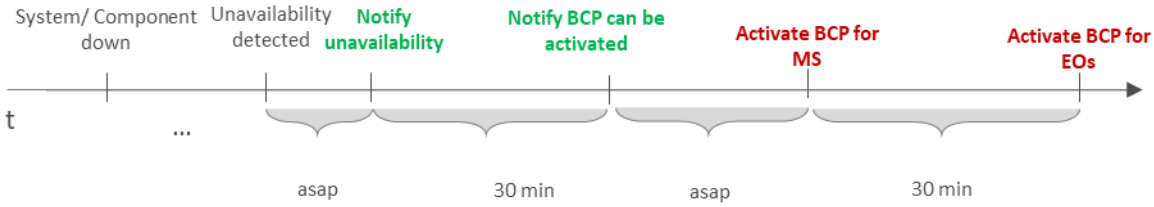

Figure 6 Business continuity plan activation timeline for CR component

Unavailable component		
Common Repository		
Component unavailability description		
CR is unable to process any message received from the EO or MS and to orchestrate the processes and send messages out. All messages sent to the CR are queued. The ENS filings will be validated by STI, registered, but no ENS life cycle validation will be performed and no risk analysis will be triggered and EO won't be informed on MRN. Communication between customs and EO on the ongoing risk analysis process, referrals and results of it via the system is not possible. Communication between the RMS and IMS on the ongoing risk analysis process is not possible.		
Unavailability identification and notification		
CSD	The CSD notifies all NSDs about detected unavailability. The unavailability notification has to be sent immediately after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	asap
Activation of Business continuity plan		
CSD	If the component is not restored, the CSD inform NSD about the need to activate the Business continuity plan and it has to contain all the details as elaborated in [3.7.6]. CSD notify NSDs 30 minutes after the notification of the unavailability of the component. CSD coordinates and orchestrates activation of business continuity plan by all the NSD at the same time.	30 min
	The CSD notifies all NSDs about the activation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has activated BCP.	asap
NSD	The NSD activated the business continuity plan immediately.	asap
	The NSD notifies the activation of the business continuity plan and applicable measures to the: • MS users; • CSD [3.7.5].	asap

	This notification is sent out immediately after activation of BCP by NSD.	
	The NSD notifies the activation of the business continuity plan and applicable measures to the EOs that are filing the ENS in their MS and IT service providers that are registered in their MS and it has to contain all the details as elaborated in [3.7.4]. This notification is sent 30 minutes after the activation of the BCP by NSD.	30 min
Business continuity measures for EO		
Lodgement of new ENS		
ENS filings	New ENS filings prior to loading can be lodged during the unavailability of the component. MRNs will be communicated to EOs after component is restored. **Measures:** No measures to be applied.	
Amendment	Amendments of the ENSs can be lodged, but already filed ENSs will not be amended until the system is restored. **Measures:** No measures to be applied.	
Invalidation	Invalidation of ENS can be requested, but will not be performed until the system is restored. **Measures:** No measures to be applied.	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	Referral request messages will not pass via the CR. **Measures:** Referral requests will be issued via alternative communication channels – e-mail, phone, etc.	
Referral responses from the EO	Response messages for referrals that were issued before the unavailability can be sent to the system, but they will only be processed after the system is restored. **Measures:** Referral responses sent via system, in addition need to be communicated via alternative communication channels – e-mail, phone, etc. Referral responses to the request issued via alternative means need to be communicated via alternative means.	
DNL	Decision to issue a DNL will not be received by the CR and DNL request will not be issued to the EO via the system. **Measures:** DNL will be issued via phone and e-mail.	
Assessment complete notifications	Assessment complete messages will not be sent by the CR. **Measures:** Assessment complete will not be communicated to the EO during the unavailability of the component.	
Advance control notification to AEO	MS decision to inform the AEO about the controls in advance will not be received by the CR and will not be communicated to the EO. **Measures:**	

	Communicated via alternative communication channels – e-mail, phone, etc.
Presentation and controls	
Presentation information / control results	MS can decide if and when they want to apply the BCP for the presentation and control process. If the goods (postal consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible.
Presentation information / control results	If the goods (express consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.
Business continuity measures for MS	
Initiation of risk assessment of newly lodged ENSs	
Preparation of ENS for risk analysis	Newly lodged ENSs will not be processed by the CR and prepared for the risk analysis. **Measures:** No measures to be applied.
Risk analysis requests	Risk analysis will not be triggered. **Measures:** No measures to be applied.
e-Screening requests	e-Screening requests will not be triggered. **Measures:** No measures to be applied.
Risk assessment of already lodged ENSs	
RMS Risk analysis hit	If RMS has a hit on an ENS, this hit will not be received by the CR. **Measures:** No measures to be applied.
Risk analysis results	RMS risk analysis results for the ENSs which were risk assessed in the NES will not be received by the CR. CR will not issue Assessment complete notifications. **Measures:** RMS needs to send their risk analysis results via the system. RMS needs to communicate risk analysis results and control recommendation to customs officials performing controls. In case MS of Control is different than RMS it needs to communicate risk analysis results and control recommendation via alternative means (e.g CRMS).
e-Screening results	IMS e-Screening results will not be received by the CR and will not be forwarded to the RMS. **Measures:** IMS needs to send their e-Screening results via the system and in addition MS needs to contact the RMS via alternative means (e.g. CRMS) to communicate confirmed e-Screening hits.

Referral requests (RFI, RFS) for the EO	Referral request messages will not pass via the CR. **Measures:** RMS issues referral requests via alternative communication channels – e-mail, phone, etc. Referral for amendment of an ENS cannot be used. Instead Referral for additional information should be used.
Referral responses from the EO	Response messages for referrals that were issued before the unavailability can be sent to the system, but they will only be processed after the system is restored. RMS will not receive these messages until the system is restored. **Measures:** Referral responses sent via system, in addition will be communicated by the EO via alternative communication channels – e-mail, phone, etc. Referral responses to the request issued via alternative means will be communicated by the EO via alternative means.
DNL	Decision to issue a DNL will not be received by the CR and DNL request will not be issued to the EO via the system. **Measures:** RMS issues the DNL via phone and e-mail.
Advance control notification to AEO	MS decision to inform the AEO about the controls in advance will not be received by the CR and will not be communicated to the EO. **Measures:** Communicated via alternative communication channels – e-mail, phone, etc.
Presentation and controls	
Presentation information	CR will not receive the presentation information from the NES. In case of diversion the CR will not provide the ENS data, risk analysis results and control recommendations to the MS of presentation. **Measures:** If the ENS data with risk analysis results and control recommendations are available to the MS of presentation, then controls, if necessary, can be performed. The results of control can be sent by the NES to the CR. If the ENS data and/or risk analysis results and/or control recommendations are not available to the MS of presentation, then security and safety risk assessment is done on another customs declaration, e.g. temporary storage, if needed, and control decisions are made by the MS of presentation.
Control results	Control result messages cannot be received by the CR, they will be queued and processed once the component is recovered. **Measures:** Control results can be sent by the MS for all the goods for which an ENS was lodged and risk analysis completed prior to the unavailability of the component. The messages will be queued and processed once the component is recovered. If the ENS was lodged but the risk assessment was not completed and the control is done, the results of control will have to be sent to the CR once the system is recovered and risk assessment is completed.
Recovery Strategy	
Recovery Communication	

CSD	The CSD notifies all NSDs about the recovery.	asap

	The CSD notifies all NSDs about the deactivation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has deactivated BCP.	asap
NSD	The NSD notifies: • EOs that are filing the ENS in their MS; • IT service providers that are registered in their MS; • relevant MS users; • CSD; that the component has been recovered and the Business continuity plan is no longer applicable.	asap
Recovery measures		
Relevant EO	Referral responses that have been provided via alternative means have to be sent via the system after the referral request is communicated via the system. If referral responses were submitted via the system in addition to the other communication channels during the unavailability, no further actions from the EO are needed.	
ICS2 Central components	Once the CR is recovered, the message queues will be processed. There is no need of the messages from the EO and MS to be re-sent. The sequence of message processing based on priority: RMS hit notifications, e-screening results, referral requests/responses, RA results, DNLs, Assessment complete notifications, timers expiration, Presentation, Request for RA/e-screening, Control recommendations, Amendments, new ENSs in the pipeline, invalidations, control results, advance control notifications.	
NES (RMS)	Risk analysis is performed on the provided ENSs that were lodged but not processed by the CR during the unavailability. The referrals that were issued via alternative means only, need to be issued also via the system.	
NES (IMS)	e-Screening is performed on the provided ENSs that were lodged but not processed by the CR during the unavailability.	
NES (PNES)/(CNES)	Presentation information for the goods for which an ENS was lodged but not received by the NES and which were presented during the unavailability needs to be submitted to the CR. Control results that were not sent to the CR are sent.	

3.4 CCN2 unavailability

IT Component	CAPABILITIES															
	Send ENS	Register and send MRN	Lifecycle validation	Prepare ENS for RA	Send e-risk request	Send e-screening request	Perform RA			Send/ Receive RA Results	Perform e-screening		Send/ Receive e-screening Results	Referrals	Assessment Complete	DNL	Presentation	Controls
CCN2					3	3				3			2	3			3	3

Table 11 CCN2 Unavailability

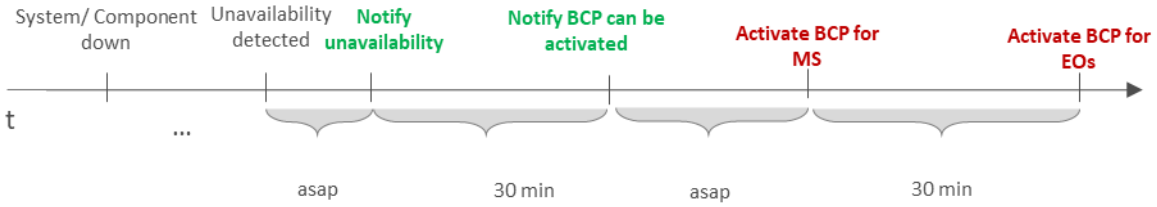

Figure 7 Business continuity plan activation timeline for CCN2 component

Unavailable component		
CCN2		
Component unavailability description		
The messages between the CR and the NESs are exchanged via the CCN2 network. In case of its unavailability, the CR cannot forward the messages to the NESs and cannot receive any messages from the NESs. Consequently, no ENS filing data can be forwarded to the NESs for risk analysis/e-screening and no referrals can be processed, as well as the CR cannot receive risk analysis hit notifications, risk analysis results, control recommendations, presentation information and control results from the NESs. The NESs can accumulate the messages in their queues waiting for the recovery of the CCN2 network, the messages do not need to be re-sent. If the NES does not have queues to accumulate the messages, then those messages will have to be re-sent. The CR queues the outbound messages to NESs.		
Unavailability identification and notification		
CSD	The CSD notifies all NSDs about detected unavailability. The unavailability notification has to be sent immediately after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	asap
Activation of Business continuity plan		
CSD	If the component is not restored, the CSD inform NSD about the need to activate the Business continuity plan and it has to contain all the details as elaborated in [3.7.6]. CSD notify NSDs 30 minutes after the notification of the unavailability of the component. CSD coordinates and orchestrates activation of business continuity plan by all the NSD at the same time.	30 min
	The CSD notifies all NSDs about the activation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has activated BCP.	
NSD	The NSD activated the business continuity plan immediately.	asap
	The NSD notifies the activation of the business continuity plan and applicable measures to the:	asap

	• MS users; • CSD [3.7.5]. This notification is sent out immediately after activation of BCP by NSD.	
	The NSD notifies the activation of the business continuity plan and applicable measures to the EOs that are filing the ENS in their MS and IT service providers that are registered in their MS and it has to contain all the details as elaborated in [3.7.4]. This notification is sent 30 minutes after the activation of the BCP by NSD.	30 min
Business continuity measures for EO		
Lodgement of new ENS		
ENS filings	New ENS filings prior to loading can be lodged. **Measures:** No measures to be applied.	
Amendment	Amendments of the ENSs can be lodged. **Measures:** No measures to be applied.	
Invalidation	Invalidation of ENS can be requested. **Measures:** No measures to be applied.	
Risk assessment of already lodged ENSs		
Referral requests (RFI, RFS) for the EO	Referral request messages will not reach the CR. **Measures:** Referral requests will be issued via alternative communication channels – e-mail, phone, etc.	
Referral responses from the EO	Response messages for referrals that were issued before the unavailability can be sent to the system, but they will only be sent to NES after the system is restored. **Measures:** Referral responses sent via system, in addition need to be communicated via alternative communication channels – e-mail, phone, etc. Referral responses to the request issued via alternative means need to be communicated via alternative means.	
DNL	Decision to issue a DNL will not be received by the CR and DNL request will not be issued to the EO via the system. **Measures:** DNL will be issued via phone and e-mail.	
Assessment complete notifications	Assessment complete messages will be sent by the CR. **Measures:** No measures to be applied.	
Advance control notification to AEO	MS decision to inform the AEO about the controls in advance will not be received by the CR and will not be communicated to the EO. **Measures:** Communicated via alternative communication channels – e-mail, phone, etc.	
Presentation and controls		

Presentation information / control results	MS can decide if and when they want to apply the BCP for the presentation and control process. If the goods (postal consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible.
Presentation information / control results	If the goods (express consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.
Business continuity measures for MS	
Initiation of risk assessment of newly lodged ENSs	
Preparation of ENS for risk analysis	Newly lodged ENSs will be processed by the CR and prepared for the risk analysis. **Measures:** No measures to be applied.
Risk analysis requests	Risk analysis will be triggered, but will not be received by the NES. **Measures:** No measures to be applied.
e-Screening requests	e-Screening requests will be triggered, but will not be received by the NES. **Measures:** No measures to be applied.
Risk assessment of already lodged ENSs	
RMS Risk analysis hit	If RMS has a hit on an ENS, this hit will not be received by the CR. **Measures:** No measures to be applied.
Risk analysis results	RMS risk analysis results for the ENSs which were risk assessed in the NES will not be received by the CR. CR will issue Assessment complete notifications after expiry of the timer for completion of risk analysis. **Measures:** RMS needs to send their risk analysis results via the system. RMS needs to communicate risk analysis results and control recommendation to customs officials performing controls. In case MS of Control is different than RMS it needs to communicate risk analysis results and control recommendation via alternative means (e.g CRMS).
e-Screening results	IMS e-Screening results will not be received by the CR and will not be forwarded to the RMS. **Measures:** IMS needs to send their e-Screening results via the system (will be queued and processed later) and in addition MS needs to contact the RMS via alternative means (e.g. CRMS) to communicate confirmed e-Screening hits.
Referral requests (RFI, RFS) for the EO	Referral request messages will not pass via the CR. **Measures:**

	RMS issues referral requests via alternative communication channels – e-mail, phone, etc. Referral for amendment of an ENS cannot be used. Instead Referral for additional information should be used.
Referral responses from the EO	Response messages for referrals that were issued before the unavailability can be sent to the system, but RMS will not receive these messages until the system is restored. **Measures:** Referral responses sent via system, in addition will be communicated by the EO via alternative communication channels – e-mail, phone, etc. Referral responses to the request issued via alternative means will be communicated by the EO via alternative means.
DNL	Decision to issue a DNL will not be received by the CR and DNL request will not be issued to the EO via the system. **Measures:** RMS issues the DNL via phone and e-mail.
Advance control notification to AEO	MS decision to inform the AEO about the controls in advance will not be received by the CR and will not be communicated to the EO. **Measures:** Communicated via alternative communication channels – e-mail, phone, etc.
Presentation and controls	
Presentation information	CR will not receive the presentation information from the NES. In case of diversion the CR will not provide the ENS data, risk analysis results and control recommendations to the MS of presentation. **Measures:** If the ENS data with risk analysis results and control recommendations are available to the MS of presentation, then controls, if necessary, can be performed. The results of control can be sent by the NES to the CR. If the ENS data and/or risk analysis results and/or control recommendations are not available to the MS of presentation, then security and safety risk assessment is done on another customs declaration, e.g. temporary storage, if needed, and control decisions are made by the MS of presentation.
Control results	Control result messages cannot be received by the CR, they will be queued and processed once the component is recovered. **Measures:** Control results can be sent by the MS for all the goods for which an ENS was lodged and risk analysis completed prior to the unavailability of the component. The messages will be queued and processed once the component is recovered. If the ENS was lodged but the risk assessment was not completed and the control is done, the results of control will have to be sent to the CR once the system is recovered and risk assessment is completed.
Recovery Strategy	
Recovery Communication	

CSD	The CSD notifies all NSDs about the recovery.	asap

	The CSD notifies all NSDs about the deactivation of BCP by a particular NSD. This notification is to be sent immediately after particular NSD has deactivated BCP.	
NSD	The NSD notifies: • the EOs that are filing the ENS in their MS; • IT service providers that are registered in their MS; • relevant MS users; • CSD; that the component has been recovered and the Business continuity plan is no longer applicable.	asap
Recovery measures		
Relevant EO	Referral responses that have been provided via alternative means have to be sent via the system after the referral request is communicated via the system. If referral responses were submitted via the system in addition to the other communication channels during the unavailability, no further actions from the EO are needed.	
ICS2 Central components	Once the CCN2 is recovered, the message queues will be processed. There is no need of the messages from the EO to be re-sent. The sequence of message processing based on priority: RMS hit notifications, e-screening results, referral requests/responses, RA results, DNLs, Assessment complete notifications, timers expiration, Presentation, Request for RA/e-screening, Control recommendations, Amendments, new ENSs in the pipeline, invalidations, control results, advance control notifications.	
NES (RMS)	If the NESs can accumulate the messages in their queues waiting for the recovery of the CCN2 network, the messages do not need to be re-sent. If the NES does not have queues to accumulate the messages, then those messages will have to be re-sent. Risk analysis is performed on the provided ENSs that were lodged but not processed by the CR during the unavailability. The referrals that were issued via alternative means only, need to be issued also via the system.	
NES (IMS)	If the NESs can accumulate the messages in their queues waiting for the recovery of the CCN2 network, the messages do not need to be re-sent. If the NES does not have queues to accumulate the messages, then those messages will have to be re-sent. e-Screening is performed on the provided ENSs that were lodged but not processed by the CR during the unavailability.	
NES (PNES)/(CNES)	If the NESs can accumulate the messages in their queues waiting for the recovery of the CCN2 network, the messages do not need to be re-sent. If the NES does not have queues to accumulate the messages, then those messages will have to be re-sent. Presentation information for the goods for which an ENS was lodged but not received by the NES and which were presented during the unavailability needs to be submitted to the CR. Control results that were not sent to the CR are sent.	

3.5 NES Unavailability

The NES of a MS is composed of various components with different functionality, which varies from MS to MS depending on national decisions on system architecture and assignment of functionalities. In general a NES consists of the following functional blocks:

- Message and business process lifecycle management
- Risk analysis
- Presentation of goods
- Control decision and control performance management
- (optional arrival of means of transport management)

3.5.1 NES (RMS) unavailability

With regard to the role of RMS the message and business process lifecycle management (NES Lifecycle) and risk analysis (NES Risk engine) components are relevant. Where the message and lifecycle management is unavailable, the risk analysis requests are not processed and therefore not forwarded in the defined in-house format to the risk analysis system. In case of unavailability of the risk analysis system the risk analysis request data received from the message and lifecycle management is not analysed. In both cases, the risk analysis results are not produced and communicated back to the CR. Moreover contributions from IMSs cannot be taken into account. Consequently, the business processes are blocked and the required results will not be available when the means of transport arrives or the goods are presented.

			CAPABILITIES																	
			Send ENS	Register and send MRN	Lifecycle validation	Prepare ENS for RA	Send e-risk request	Send e-screening request	Perform RA			Send/ Receive RA Results	Perform e-screening		Send/ Receive e-screening Results	Referrals	Assessment Complete	DNL	Presentation	Controls
IT Component																				
NES	NES (RMS)	Lifecycle					3					3								
		Risk Engine							1	2	3									

Table 12 NES (RMS) unavailability

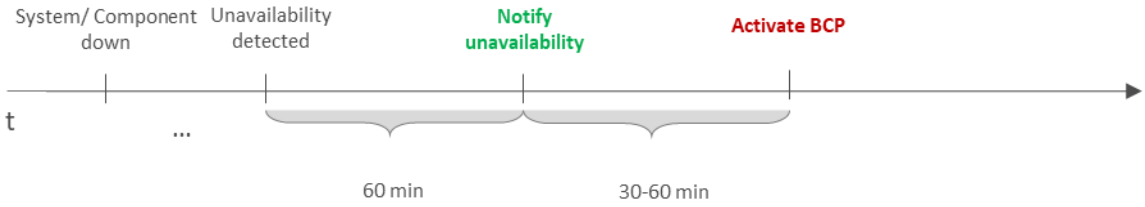

Figure 8 Business continuity plan activation timeline for NES (RMS) component

Unavailable component		
NES (RMS)		
Component unavailability description		
The RMS System is considered not to be available when either its risk engine or the ENS lifecycle processing component are not operational. In case the ENS lifecycle processing component is unavailable the RMS does not receive e-risk analysis requests and cannot send risk analysis results, DNL and referrals. It also cannot receive e-Screening contributions from the IMS. When the risk engine is not functioning, the RMS cannot perform automatically the risk analysis for the received ENS data.		
Unavailability identification and notification		
NSD (RMS)	The NSD notifies CSD about detected unavailability.	60 min

	The unavailability notification has to be sent 60 minutes after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	
CSD	The CSD notifies all NSDs about detected unavailability. The unavailability notification has to be sent immediately after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	asap
Activation of Business continuity plan		
NSD (RMS)	If the component or part of it is not restored, the NSD activates the Business continuity plan and notifies CSD [3.7.5]. BCP is activated 30-60 minutes after the notification of the unavailability of the component.	30-60 min
	The NSD notifies the activation of the business continuity plan and applicable measures to the MS users. This notification is sent out immediately after activation of BCP by NSD.	asap
	The NSD notifies the activation of the business continuity plan and applicable measures to the EOs that are filing the ENS in their MS and IT service providers that are registered in their MS and it has to contain all the details as elaborated in [3.7.4]. This notification is sent immediately after the activation of the BCP by NSD.	asap
CSD	The CSD notifies the activation of the business continuity plan and applicable measures to all NSDs and it has to contain all the details as elaborated in [3.7.6]. This notification is sent out immediately after activation of BCP by NSD.	asap
All other NSDs	The NSD notifies the activation of the business continuity plan and applicable measures to the MS users. This notification is sent out immediately after notification was received from CSD.	asap

Business continuity measures for EO	
Lodgement of new ENS	
ENS filings	New ENS filings prior to loading can be lodged during the unavailability of the component. **Measures:** No measures to be applied.
Amendment	Amendments of the ENSs can be lodged. **Measures:** No measures to be applied.
Invalidation	Invalidation of ENS can be requested. **Measures:** No measures to be applied.
Risk assessment of already lodged ENSs	
Referral requests (RFI, RFS) for the EO	If NES Lifecycle component is unavailable, referral request messages will not be sent. **Measures:** Referral requests will be issued via alternative communication channels – e-mail, phone, etc.

Referral responses from the EO	If NES Lifecycle component is unavailable, response messages for referrals that were issued before the unavailability can be sent to the system, but they will only be received by the NES after the system is restored. Response received is stored in Central repository and available for MS user in Central repository user interface. In case response provided is not sufficient and there is a need for additional information it should be requested via alternative means. **Measures:** Referral responses to the request issued via alternative means need to be communicated via alternative means.
DNL	If NES Lifecycle component is unavailable, decision to issue a DNL will not be sent to the CR and DNL request will not be issued to the EO via the system. **Measures:** DNL will be issued via phone and e-mail.
Assessment complete notifications	Assessment complete messages will be sent. **Measures:** No measures to be applied.
Advance control notification to AEO	If NES Lifecycle component is unavailable, MS decision to inform the AEO about the controls in advance will not be sent to the CR and will not be communicated to the EO. **Measures:** Communicated via alternative communication channels – e-mail, phone, etc.
Presentation and controls	
Presentation information	If the goods (postal consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage, if possible.
	If the goods (express consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.
Business continuity measures for MS	
Initiation of risk assessment of newly lodged ENSs	
Preparation of ENS for risk analysis	Newly lodged ENSs will be processed by the CR and prepared for the risk analysis. **Measures:** No measures to be applied.
Risk analysis requests	Risk analysis will be triggered by the CR, however it will not be received by the NES, if NES Lifecycle component is unavailable **Measures:** Risk assessment is delayed.
	Risk analysis will be triggered by the CR, it will be received by the NES, but no risk analysis will be performed, if the NES Risk engine is unavailable. **Measures:**

	Risk assessment is delayed.
e-Screening requests	e-Screening requests will be triggered. **Measures:** No measures to be applied.
Risk assessment of already lodged ENSs	
RMS Risk analysis hit	If NES Lifecycle component is unavailable, Risk hit will not be sent to the CR even if it is produced by the NES Risk engine. After expiration of the timer for completion of the risk analysis, the CR will send Assessment complete message to the EO. **Measures:** Risk assessment is delayed.
	If NES Risk engine is unavailable, no risk hit will be triggered by this component. **Measures:** Risk assessment is delayed.
Risk analysis results	RMS risk analysis results for the ENSs which were risk assessed in the NES will not be received by the CR. CR will issue Assessment complete notifications after expiration of timer. **Measures:** In case serious risk is confirmed RMS needs to send their risk analysis results via the system. RMS needs to communicate risk analysis results and control recommendation to customs officials performing controls. In case MS of Control is different than RMS it needs to communicate risk analysis results and control recommendation via alternative means (e.g CRMS).
	If NES Risk engine is unavailable, the RMS risk analysis results will not be received by the NES Lifecycle component and made available to the risk analyst. **Measures:** No measures to be applied.
e-Screening results	IMS e-Screening results will not be received by the NES, if NES Lifecycle component is unavailable. **Measures:** IMS needs to send their e-Screening results via the system and in addition MS needs to contact the RMS via alternative means (e.g. CRMS) to communicate confirmed e-Screening hits.
	If NES Risk engine is unavailable, the IMS e-Screening results will be received by the NES Lifecycle component and made available to the risk analyst. **Measures:** No measures to be applied.
Referral requests (RFI, RFS) for the EO	If NES Lifecycle component is unavailable, the referral request messages will not be issued. **Measures:** If RMS is in the process of manual assessment of the ENS and the referrals need to be issued, the RMS issues referral requests via alternative communication channels – e-mail, phone, etc. Referral for amendment of an ENS cannot be used. Instead Referral for additional information should be used.

	If NES Risk engine is unavailable, referral requests can be issued. **Measures:** No measures to be applied.
Referral responses from the EO	If NES Lifecycle component is unavailable, referral response messages will not be received by the NES. RMS will not receive these messages until the system is restored. **Measures:** Referral responses sent via system, in addition will be communicated by the EO via alternative communication channels – e-mail, phone, etc. Referral responses to the request issued via alternative means will be communicated by the EO via alternative means.
	If NES Risk engine is unavailable, referral responses can be received. **Measures:** No measures to be applied.
DNL	If NES Lifecycle component is unavailable, decision to issue a DNL will not be sent to the CR and DNL request will not be issued to the EO via the system. Also won't be communicated to all MS. **Measures:** RMS issues the DNL to the EO via phone and e-mail.
	If NES Lifecycle component is unavailable, decision to issue a DNL will not be sent to the CR and DNL request will not be issued to the EO via the system. Also won't be communicated to all MS. **Measures:** RMS informs about issued DNL all the MSs via phone and/or e-mail and CRMS.
	If NES Risk engine is unavailable, DNL can be issued. **Measures:** No measures to be applied.
Advance control notification to AEO	If NES Lifecycle component is unavailable, MS decision to inform the AEO about the controls in advance will not be sent to the CR and will not be communicated to the EO. **Measures:** Communicated via alternative communication channels – e-mail, phone, etc.
Presentation and controls	
Presentation information	If the goods (postal consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, lodgement of an ENS is waived and the risk assessment for security and safety purpose is done on another customs declaration, e.g. temporary storage.
	If the goods (express consignments) have already arrived to the EU and are presented to customs: • If the ENS for the goods was lodged, no further actions • If ENS for the goods was not lodged, the lodgement of the PLACI is waived. ENS will be lodged in ICS1.

Recovery Strategy		
Recovery Communication		
NSD (RMS)	The NSD notifies the CSD about the recovery of the system and deactivation of BCP.	asap
	The NSD notifies the MS users that the component has been recovered and the Business continuity plan is no longer applicable.	asap
	The NSD notifies the EOs that are filing the ENS in their MS and IT service providers that are registered in their MS that the component has been recovered and the Business continuity plan is no longer applicable.	asap
CSD	The CSD notifies all NSDs about the recovery and deactivation of BCP by a particular NSD.	asap
All other NSDs	The all other NSDs notifies their MS users about the recovery and deactivation of BCP. This notification is sent out immediately after notification was received from CSD.	asap
Recovery measures		
Relevant EO	Referral responses that have been provided via alternative means have to be sent via the system after the referral request is communicated via the system. If referral responses were submitted via the system in addition to the other communication channels during the unavailability, no further actions from the EO are needed.	
ICS2 Central components	Once the NES is recovered, the message queues will be processed. There is no need for the messages to be re-sent. The sequence of message processing based on priority: RMS hit notifications, e-screening results, referral requests/responses, RA results, DNLs, Assessment complete notifications, timers expiration, Presentation, Request for RA/e-screening, Control recommendations, Amendments, new ENSs in the pipeline, invalidations, control results, advance control notifications.	
NES (RMS)	Risk analysis is performed on the provided ENSs that were not processed by the NES during the unavailability. The referrals and DNL that were issued via alternative means only, need to be issued also via the system.	
NES (IMS)	None.	
NES (PNES)/(CNES)	None.	

3.5.2 NES (IMS) unavailability

For the role of IMS, the same functional blocks are relevant as mentioned above for the RMS.

When the message and lifecycle management is unavailable, the requests for e-screening are not processed and therefore not forwarded in the defined in-house format to the risk analysis system.

In case of unavailability of the risk analysis system the e-screening request data received from the message and lifecycle management is not analysed.

In both cases, the contribution results are not produced and communicated back to the CR. Hence follows that risks identified by the IMS are not available to the RMS and therefore cannot be taken into account for the risk analysis results. Although the continuation of the process workflow is not interrupted, it means definitely a loss of quality of the risk analysis results, in particular where the IMS is the MS of destination of the goods. Since an IMS will provide feedback only where a risk was identified the volumes are considered to be much lower than from the RMS that would have to provide risk analysis results in any case, even where the risk analysis result is determined as 'no risk'.

			CAPABILITIES																
			Send ENS	Register and send MRN	Lifecycle validation	Prepare ENS for RA	Send e-risk request	Send e-screening request	Perform RA			Send/ Receive RA Results	Perform e-screening		Send/ Receive e-screening Results	Referrals	Assessment Complete	DNL	Presentation	Controls
IT Component																			
NES	NES (IMS)	Lifecycle						3							2					
		Risk Engine											1	2						

Table 13 NES (IMS) unavailability

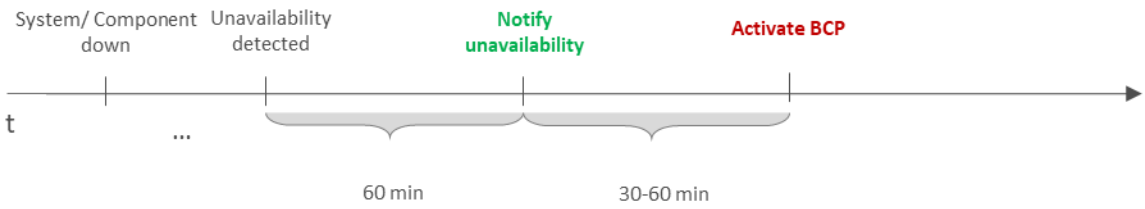

Figure 9 Business continuity plan activation timeline for NES (IMS) component

Unavailable component		
NES (IMS)		
Component unavailability description		
The IMS System is considered not to be available when either its risk engine or the ENS lifecycle processing component are not operational. In case the ENS lifecycle processing component is unavailable the IMS does not receive e-screening requests and cannot contribute to risk analysis result. When the risk engine is not functioning, the IMS cannot perform automatically the e-screening for the received ENS data.		
Unavailability identification and notification		
NSD (IMS)	The NSD notifies CSD about detected unavailability. The unavailability notification has to be sent 60 minutes after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	60 min
CSD	The CSD notifies all NSDs about detected unavailability. The unavailability notification has to be sent immediately after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	asap
Activation of Business continuity plan		
NSD (IMS)	If the component or part of it is not restored, the NSD activates the Business continuity plan and notifies CSD [3.7.5].	30-60 min

	BCP is activated 30-60 minutes after the notification of the unavailability of the component.	
	The NSD notifies the activation of the business continuity plan and applicable measures to the MS users. This notification is sent out immediately after activation of BCP by NSD.	asap
CSD	The CSD notifies the activation of the BCP by a particular NSD and applicable measures to all NSDs and it has to contain all the details as elaborated in [3.7.6]. This notification is sent out immediately after activation of BCP by NSD.	asap
Business continuity measures for MS		
Initiation of risk assessment of newly lodged ENSs		
e-Screening requests	e-Screening will be triggered by the CR, however it will not be received by the NES, if NES Lifecycle component is unavailable **Measures:** e-Screening is delayed.	
	e-Screening will be triggered by the CR, it will be received by the NES, but no e-Screening will be performed, if the NES Risk engine is unavailable. **Measures:** e-Screening is delayed.	
Risk assessment of already lodged ENSs		
e-Screening execution	If NES Lifecycle component is unavailable, IMS e-Screening will not be performed. **Measures:** e-Screening is delayed.	
	If NES Risk engine is unavailable, the IMS e-Screening will not be performed. **Measures:** No measures to be applied.	
e-Screening results	If NES Lifecycle component is unavailable, IMS e-Screening results will not be sent to the CR. **Measures:** If IMS has performed e-Screening but is not able to send their e-Screening results via the system, the MS needs to contact the RMS via alternative means (e.g. CRMS) to communicate confirmed e-Screening hits.	
Recovery Strategy		
Recovery Communication		
NSD (IMS)	The NCD notifies the CSD about the recovery of the system and deactivation of BCP.	asap
	The NSD notifies the MS users that the component has been recovered and the Business continuity plan is no longer applicable.	asap
CSD	The CSD notifies all NSDs about the recovery and deactivation of BCP by a particular NSD.	asap
Recovery measures		
ICS2 Central components	Once the NES is recovered, the message queues will be processed. There is no need for the messages to be re-sent.	

	The sequence of message processing based on priority: RMS hit notifications, e-screening results, referral requests/responses, RA results, DNLs, Assessment complete notifications, timers expiration, Presentation, Request for RA/e-screening, Control recommendations, Amendments, new ENSs in the pipeline, invalidations, control results, advance control notifications.
NES (RMS)	None.
NES (IMS)	e-Screening is performed on the provided ENSs that were not processed by the NES during the unavailability. The IMS can decide on sequence how e-screening is performed. Risks identified are assessed and communicated to CR. If necessary communication can be performed via e.g. CRMS.
NES (PNES)/(CNES)	None.

3.5.3 NES (PNES) and (CNES) unavailability

When the presentation system is unavailable, the presentation MS might not be able to submit the presentation information to the CR. The desynchronization between the real state of the goods and the state stored in the CR still allows the economic operator to amend ENS filings or request invalidation of ENS filings that are related to the presented goods although this is legally excluded. Later submission and processing of presentation information data may result in inconsistencies of the affected datasets in the CR.

When the control management system is unavailable, the control MS might miss to perform a decided control.

		CAPABILITIES																
	IT Component	Send ENS	Register and send MRN	Lifecycle validation	Prepare ENS for RA	Send e-risk request	Send e-screening request	Perform RA			Send/ Receive RA Results	Perform e-screening		Send/ Receive e-screening Results	Referrals	Assessment Complete	DNL	Presentation	Controls
NES	PNES																	1	
	CNES																		1

Table 14 NES (PNES) and (CNES) unavailability

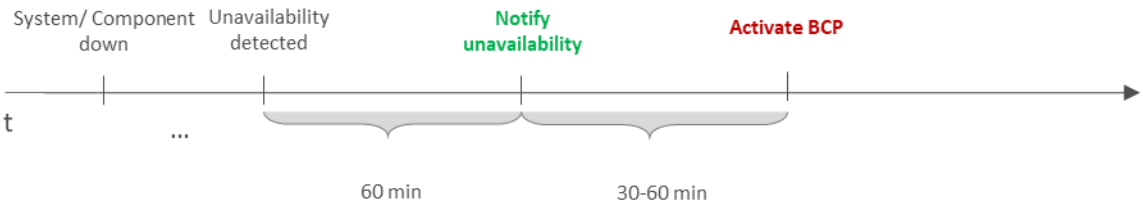

Figure 10 Business continuity plan activation timeline for NES (PNES) and (CNES) components

Unavailable component		
NES (PNES)/(CNES)		
Component unavailability description		
The NES (PNES) is considered not to be available when the presentation component of a NES where the goods are presented is not operational and the presentation notification cannot be lodged by the Economic Operator and cannot be forwarded to the CR. The NES (CNES) System is considered not to be available when the control component of a NES where the goods are presented is not operational and the control results cannot be registered.		
Unavailability identification and notification		
NSD (PNES)/(CNES)	The NSD notifies CSD about detected unavailability for information only. The unavailability notification has to be sent 60 minutes after the detection of unavailability and it has to contain all the details as elaborated in [3.7.2].	60 min
Activation of Business continuity plan		
NSD (PNES)/(CNES)	MS can decide if and when they want to apply the BCP for the presentation and control process. If the component or part of it is not restored, the NSD activates the Business continuity plan. It is recommended that BCP is activated 30-60 minutes after the notification of the unavailability of the component but it's up to MS to decide.	30-60 min
	The NSD notifies the activation of the business continuity plan and applicable measures to the: • MS users; • CSD. This notification is sent out immediately after activation of BCP by NSD.	asap

	The NSD notifies the activation of the business continuity plan and applicable measures to the EOs that are filing the ENS in their MS and IT service providers that are registered in their MS and it has to contain all the details as elaborated in [3.7.4]. This notification is sent immediately after the activation of the BCP by NSD.	asap
Business continuity measures for MS		
Presentation and controls		
Presentation information	NES cannot not send presentation notification to the CR. If the MS was already assigned the role of the MS of presentation, if should have the ENS data, risk analysis results and control recommendations. Control decision is made on the data available, however, it cannot be communicated to the CR. **Measures:** Sending of the presentation information is delayed.	
	In case of diversion, NES cannot receive the ENS data, risk analysis results and control recommendations. **Measures:** If the ENS data and/or risk analysis results and/or control recommendations are not available to the MS of presentation, then security and safety risk assessment is done on another customs declaration, e.g. temporary storage, if needed, and control decisions are made by the MS of presentation.	
Control results	If the MS was already assigned the role of the MS of presentation, if should have the ENS data, risk analysis results and control recommendations. Control decision is made on the data available, however, it cannot be communicated to the CR. Control result messages cannot be sent by the NES. **Measures:** Control results sending to the CR is delayed.	
Recovery Strategy		
Recovery Communication		
NSD (PNES)/(CNES)	The NCD notifies the CSD about the recovery of the system and deactivation of BCP for information only.	asap
	The NSD notifies the MS users that the component has been recovered and the Business continuity plan is no longer applicable.	asap
	The NSD notifies the EOs that are filing the ENS in their MS and IT service providers that are registered in their MS that the component has been recovered and the Business continuity plan is no longer applicable.	asap
Recovery measures		
ICS2 Central components	Once the NES is recovered, the message queues will be processed. There is no need for the messages to be re-sent. The sequence of message processing based on priority: RMS hit notifications, e-screening results, referral requests/responses, RA results, DNLs, Assessment complete notifications, timers expiration, Presentation, Request for RA/e-screening, Control recommendations, Amendments, new ENSs in the pipeline, invalidations, control results, advance control notifications.	
NES (PNES)/(CNES)	If the ENS was lodged and the control is done, the results of control will have to be sent to the CR once the system is recovered. Presentation information for the goods for which an ENS was lodged but not received by the NES and which were presented during the unavailability needs to be submitted to the CR.	

3.6 ICS2 Message prioritisation

3.6.1 External domain messages

Priority	Message ID	Name	Full name	Process where it is used
B	IE3Fxx	E_ENS_xxx_DEC	ENS filing	L4-ICS2-01 Register filing
B	IE3Axx	E_ENS_xxx_AMD	ENS filing amendment	L4-ICS2-07 Amend filing
A	IE3Q01	E_DNL_REQ	Do Not Load request	L4-ICS2-03 Perform risk analysis
B	IE3Q02	E_REF_RFI_REQ	Additional information request	L4-ICS2-03-01 Send referral
A	IE3Q03	E_REF_RFS_REQ	High Risk Cargo & Mail screening request	L4-ICS2-03-01 Send referral
C	IE3Q04	E_INV_REQ	Invalidation Request	L4-ICS2-08 Invalidate filing
B	IE3R01	E_ENS_REG_RSP	ENS Registration Response	L4-ICS2-01 Register filing
B	IE3R02	E_REF_RFI_RSP	Additional information response	L4-ICS2-03-01 Send referral
A	IE3R03	E_REF_RFS_RSP	High Risk Cargo & Mail screening response	L4-ICS2-03-01 Send referral
C	IE3R07	E_INV_ACC_RSP	Invalidation Acceptance Response	L4-ICS2-08 Invalidate filing
B	IE3N01	E_ELF_VLD_NOT	ENS lifecycle validation error notification	L4-ICS2-01 Register filing
A	IE3N03	E_ASM_CMP_NOT	Assessment complete notification	L4-ICS2-03 Perform risk analysis
C	IE3N09	E_AEO_CON_NOT	Authorised Economic Operator control notification	L4-ICS2-06-01 Handle AEO notification
C	IE3N10	E_AMD_NOT	Amendment Notification	L4-ICS2-07 Amend filing
B	IE3N99	E_ERR_NOT	Error notification	L4-ICS2-01 Register filing
				L4-ICS2-04 Process arrival of means of transport
				L4-ICS2-07 Amend filing
				L4-ICS2-08 Invalidate filing

3.6.2 Common domain messages

Priority	Message ID	Message Name	Message name full	Process where it is used	Equivalent ED message
B	IE4Fxx	C_ENS_xxx_DEC	ENS filing	L4-ICS2-01 Register filing	IE3Fxx
B	IE4Axx	C_ENS_xxx_AMD	ENS filing amendment	L4-ICS2-07 Amend filing	IE3Axx
B	IE4Q01	C_ESC_REQ	e-Screening request	L4-ICS2-03 Perform risk analysis	
B	IE4Q02	C_ERA_REQ	e-risk analysis request	L4-ICS2-03 Perform risk analysis	
A	IE4Q03	C_DNL_REQ	Do Not Load request	L4-ICS2-03 Perform risk analysis	IE3Q01
B	IE4Q04	C_REF_RFI_REQ	Additional information request	L4-ICS2-03-01 Send referral	IE3Q02/IE3N04
A	IE4Q05	C_REF_RFS_REQ	High Risk Cargo & Mail screening request	L4-ICS2-03-01 Send referral	IE3Q03/IE3N05
C	IE4Q06	C_INV_REQ	Invalidation request	L4-ICS2-08 Invalidate filing	IE3Q04
B	IE4Q07	C_OMS_REQ	OMS request to perform e-Screening	L4-ICS2-09 e-Screening by OMS	
C	IE4Q08	C_PRS_RVK_REQ	Presentation revocation request	L4-ICS2-12 Revoke presentation of goods	
B	IE4Q10	C_ENS_QUE	Query for ENS	L4-ICS2-14 Query for ENS	
B	IE4R01	C_ENS_ACC_RSP	ENS acceptance response	L4-ICS2-02 Prepare ENS for risk analysis	
B	IE4R02	C_REF_RFI_RSP	Additional information response	L4-ICS2-03-01 Send referral	IE3R02
A	IE4R03	C_REF_RFS_RSP	High Risk Cargo & Mail screening response	L4-ICS2-03-01 Send referral	IE3R03
C	IE4R04	C_INV_ACC_RSP	Invalidation acceptance response	L4-ICS2-08 Invalidate filing	IE3R07
B	IE4R05	C_ENS_QUE_RES	ENS query results	L4-ICS2-14 Query for ENS	
B	IE4S01	C_ESC_ASM_RES	e-Screening results	L4-ICS2-03 Perform risk analysis	
A	IE4S02	C_RSK_RES	Risk analysis results	L4-ICS2-03 Perform risk analysis	
C	IE4S03	C_CON_RES	Control results	L4-ICS2-04 Process arrival of means of transport	
				L4-ICS2-06 Process control decision and results	
B	IE4N01	C_ELF_VLD_NOT	ENS lifecycle validation error notification	L4-ICS2-02 Prepare ENS for risk analysis	IE3N01
A	IE4N03	C_ERA_HIT_NOT	e-risk analysis hit notification	L4-ICS2-03 Perform risk analysis	
A	IE4N04	C_ASM_CMP_NOT	Assessment complete notification	L4-ICS2-03 Perform risk analysis	IE3N03
B	IE4N05	C_CON_RCM_NOT	Control recommendation notification	L4-ICS2-03 Perform risk analysis	
				L4-ICS2-04 Process arrival of means of transport	
				L4-ICS2-05 Process presentation of goods	
				L4-ICS2-06 Process control decision and results	
B	IE4N06	C_REF_AMD_NOT	Amendment after referral reception notification	L4-ICS2-03-01 Send referral	
B	IE4N10	C_PRS_INF	Presentation information	L4-ICS2-05 Process presentation of goods	
C	IE4N11	C_AEO_CON_NOT	Authorised Economic Operator control notification	L4-ICS2-06-01 Handle AEO notification	IE3N09
C	IE4N12	C_AMD_NOT	Amendment completion notification	L4-ICS2-07 Amend filing	IE3N10
C	IE4N13	C_INV_NOT	ENS filing invalidation notification	L4-ICS2-08 Invalidate filing	IE3N99
B	IE4N99	C_ERR_NOT	Error notification	L4-ICS2-07 Amend filing	
				L4-ICS2-08 Invalidate filing	
				L4-ICS2-12 Revoke presentation of goods	

3.7 Templates for notification of the unavailability

Main means how to communicate unavailability is:

- in case of scheduled unavailability information between CSD and NSD will be exchanged via ICS2 Monitoring user interface (MON UI);
- in case of scheduled unavailability information between CSD and IT service provider or between NSD and EO will be exchanged via e-mail;
- in case of unscheduled unavailability via e-mail.

If e-mail should be used to communicate unavailability you can:

- use templates described in this section (file format MS Word or pdf);
- indicate all the details elaborated in the templates as a free text.

3.7.1 Economic Operator unavailability notification information template (EO to NSD or IT service provider to CSD)

Template or all the details elaborated in template is to be used by:

- EO to notify NSD on scheduled/unscheduled unavailability of EO system;
- IT service provider to notify CSD on scheduled/unscheduled unavailability of EO system.

This template can be reused by:

- NSD to notify CSD and other NSDs on unavailability of EO system;
- CSD to notify NSDs on unavailability of IT service provider.

1.	EO name notifying the unavailability:	
1.1.	Type of EO:	☐ Postal operator ☐ Express carrier ☐ IT service provider
1.2.	In which country impacted EO is located (*IT service provider can indicate one or several countries)*:	☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
2.	Unavailability type:	☐ scheduled ☐ unscheduled
3.	Which is the unavailable component/ functionality?	
4.	Which is the impacted ICS2 related business process:	
	☐ Sending information to ICS2: ☐ Lodgement of ENS Filings ☐ ENS Filings Amendment ☐ Invalidation request ☐ RfI Response ☐ RfS Response	☐ Receiving information from ICS2: ☐ ENS Registration response ☐ Invalidation Acceptance Response ☐ Amendment Notification ☐ RfI Requests ☐ RfS Requests ☐ DNL ☐ Assessment complete ☐ Advanced Control Notification
5.	Identified start date and time of the unavailability?	
6.	Expected end date and time of the unavailability?	

Table 15 EO Unavailability notification information template

1.	EO name notifying the unavailability:	Valsts akciju sabiedrība "Latvijas Pasts"
1.1.	Type of EO:	☒ Postal operator ☐ Express carrier ☐ IT service provider
1.2.	In which country impacted EO is located (*IT service provider can indicate one or several countries)*:	☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☒ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
2.	Unavailability type:	☐ scheduled ☒ unscheduled
3.	Which is the unavailable component/ functionality?	Referrals handling component cannot send information, but the incoming messages are successfully received.
4.	Which is the impacted ICS2 related business process:	
	☒ Sending information to ICS2: ☐ Lodgement of ENS Filings ☒ ENS Filings Amendment ☐ Invalidation request ☒ RfI Response ☒ RfS Response	☐ Receiving information from ICS2: ☐ ENS Registration response ☐ Invalidation Acceptance Response ☐ Amendment Notification ☐ RfI Requests ☐ RfS Requests ☐ DNL ☐ Assessment complete ☐ Advanced Control Notification
5.	Identified start date and time of the unavailability?	23.10.2020 09:00
6.	Expected end date and time of the unavailability?	23.10.2020 22:00 (tentative)

Table 16 EO Unavailability notification information example

3.7.2 ICS2 Component / NES unavailability notification information template (CSD to NSD or NSD to CSD)

Template or all the details elaborated in template is to be used by NSD and CSD to notify each other on unscheduled unavailability of ICS2 central/national components. CSD can reuse the template to notify other NSD on unscheduled unavailability.

1.	Unavailability detected in:	☐ ICS2 Central components ☐ NES components: ☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
1.1.	Which is the detected unavailable component?	
	☐ UUM&DS central component ☐ UUM&DS national component ☐ TAPAS ☐ STI	☐ Common repository ☐ CCN2 ☐ NES (RMS) ☐ NES (IMS)

		☐ NES (PNES) ☐ NES (CNES)
1.2.	If partial unavailability which functionality is affected?	
2.	Impacted business functionality:	
2.1.	Impacted ICS2 central components:	
	☐ Receiving information in ICS2: ☐ Lodgement of ENS Filings ☐ ENS Filings Amendment ☐ Invalidation request ☐ RfI Requests ☐ RfS Requests ☐ RfI Response ☐ RfS Response ☐ DNL ☐ Advanced Control Notification ☐ e-risk analysis results ☐ e-screening results ☐ presentation notification ☐ presentation revocation request ☐ control results ☐ ENS consultation request ☐ OMS request to perform screening	☐ Sending information from ICS2: ☐ ENS Registration response ☐ Invalidation Acceptance Response ☐ Amendment Notification ☐ RfI Requests ☐ RfS Requests ☐ DNL ☐ Assessment complete ☐ Advanced Control Notification ☐ e-risk analysis request ☐ e-screening request ☐ ENS consultation results ☐ Error notification
2.2.	NES impacted business functionality:	
	☐ Sending information to ICS2: ☐ RfI Requests ☐ RfS Requests ☐ DNL ☐ Advanced Control Notification ☐ e-risk analysis results ☐ e-screening results ☐ presentation notification ☐ presentation revocation request ☐ control results ☐ ENS consultation request	☐ Receiving information from ICS2: ☐ Invalidation Acceptance Response ☐ Amendment Notification ☐ RfI Response ☐ RfS Response ☐ e-risk analysis request ☐ e-screening request ☐ ENS consultation results
3.	Identified start date and time of the unavailability?	
4.	Expected end date and time of the unavailability?	

Table 17 ICS2 Unavailability notification information

3.7.3 ICS2 Component / NES unavailability notification information template (NSD to EO/IT service provider or CSD to IT service provider)

Template or all the details elaborated in template is to notify EO and/or IT service provider on unavailability for one or several ICS2 components. IT service provider can be notified by NSD or CSD but EO will always be notified by NSD.

1.	EO(s) to be notified about unavailability:	☐ Postal operator ☐ Express carrier ☐ IT service provider
2.	Unavailability type:	☐ scheduled ☐ unscheduled
3.	Unavailable component(s)?	☐ ICS2 central component: ☐ UUM&DS Central component ☐ TAPAS ☐ STI ☐ UUM&DS National component: ☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
4.	Which is the impacted ICS2 related business process for EO(s):	
	☐ Sending information to ICS2: ☐ Lodgement of ENS Filings ☐ ENS Filings Amendment ☐ Invalidation request ☐ RfI Response ☐ RfS Response	☐ Receiving information from ICS2: ☐ ENS Registration response ☐ Invalidation Acceptance Response ☐ Amendment Notification ☐ RfI Requests ☐ RfS Requests ☐ DNL ☐ Assessment complete ☐ Advanced Control Notification
5.	What is the identified start date and time of the unavailability?	
6.	What is the expected end date and time of the unavailability?	

Table 18 ICS2 Unavailability notification information

3.7.4 Business continuity plan activation notification template (NSD to EO/IT service provider)

Template or all the details elaborated in template is to be used by NSD to notify EO and/or IT service provider on activation of business continuity plan for one or several ICS2 components and business continuity measures to be activated.

1.	MS notifying the Business continuity plan activation:	☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
2.	Who to notify for Business continuity plan activation:	☐ Postal operator ☐ Express carrier ☐ IT service provider
3.	To which ICS2 components Business continuity plan is activated by NSD:	
	☐ EO system ☐ UUM&DS central component ☐ UUM&DS national component	☐ TAPAS ☐ STI ☐ Central component ☐ NES (RMS)
4.	When NSD activated Business continuity plan (start date and time)?	
5.	What are the business continuity measures to be activated?	☐ Lodgement of new ENS ☐ Risk assessment of already lodged ENS ☐ Presentation ☐ Control
5.1.	Additional information on business continuity measures.	

Table 19 ICS2 BCP activation notification template (NSD to EOs)

3.7.5 Business continuity plan activation notification template (NSD to CSD)

Template or all the details elaborated in template is to be used by NSD to notify CSD on activation of business continuity plan for one or several ICS2 components and business continuity measures to be activated. CSD can reuse it to notify other MS NSDs.

1.	MS notifying the Business continuity plan activation:	☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
2.	Who to notify for Business continuity plan activation:	☐ CSD ☐ Other MS
3.	To which ICS2 components Business continuity plan is activated by NSD:	
	☐ EO system ☐ UUM&DS central component ☐ UUM&DS national component ☐ TAPAS	☐ Common repository ☐ CCN2 ☐ NES (RMS) ☐ NES (IMS)

	☐ STI	☐ NES (PNES) ☐ NES (CNES)
4.	When NSD activated Business continuity plan (start date and time)?	
5.	What are the business continuity measures to be activated?	☐ Lodgement of new ENS ☐ Risk assessment of already lodged ENS ☐ Presentation ☐ Control ☐ Initiation of risk assessment of newly lodged ENS
5.1	Additional information on business continuity measures.	

Table 20 ICS2 BCP activation notification template (NSD to CSD)

3.7.6 Request to activate business continuity plan template (CSD)

Template or all the details elaborated in template is to be used by CSD to notify NSD on necessity to activate business continuity plan for one or several ICS2 components and which business continuity measures to be activated. To activate business continuity plan NSD must use template described in section 3.7.5.

1.	National service desk responsible for activation of Business continuity plan:	☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
2.	To which ICS2 components Business continuity plan can be activated by NSD:	☐ Common repository ☐ CCN2 ☐ UUM&DS central component ☐ UUM&DS national component ☐ TAPAS ☐ STI
3.	What are the business continuity measures to be activated?	☐ Lodgement of new ENS ☐ Risk assessment of already lodged ENS ☐ Presentation ☐ Control ☐ Initiation of risk assessment of newly lodged ENS
4.	Additional information on business continuity measures.	

Table 21 BCP activation notification template (CSD to NSD)

3.7.7 Notification on recovery of ICS2 components

Template or all the details elaborated in template is to be used by CSD, EO and/or IT service provider to notify NSD on availability of one or several ICS2 components. On the bases of information received NSD will make a decision to deactivate business continuity plan.

1.	Who notifies availability of ICS2 components:	☐ CSD ☐ Economic operators ☐ IT service provider
2.	Which ICS2 components are available again:	

	☐ Central components ☐ UUM&DS central component ☐ TAPAS ☐ STI	☐ EO system
3.	When ICS2 components were available again (date and time)?	

Table 22 ICS2 components are recovered

3.7.8 Business continuity plan is deactivated

Template or all the details elaborated in template is to be used by NSD to notify CSD, EO and/or IT service provider on deactivation of business continuity plan for one or several ICS2 components.

1.	National service desk deactivating Business continuity plan:	☐ AT ☐ BE ☐ BG ☐ CH ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IT ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK ☐ UK
2.	To which ICS2 components Business continuity plan is deactivated:	
	☐ EO system ☐ UUM&DS central component ☐ UUM&DS national component ☐ TAPAS ☐ STI	☐ Central components ☐ NES (RMS) ☐ NES (IMS) ☐ NES (PNES) ☐ NES (CNES)
3.	When Business continuity plan is deactivated (date and time)?	

Table 23 BCP deactivation notification template

3.8 Unavailability statistics

NSDs and CSD are going to collect statistics on scheduled and unscheduled unavailability:

- NSDs are going to collect statistics per:
  - National components;
  - EO components (optional);
  - Member state;
  - Economic operator;
  - Duration of unavailability ;
  - Type of unavailability.
- CSD is going to collect statistics per:
  - Component (central components only);
  - Duration of unavailability;
  - Type of unavailability.

All the statistics will be collected on a monthly bases and NSD should share their statistics with CSD within 15 days after end of each month. CSD will consolidate statistics received from NSDs in Annex B and provide this statistics to DG TAXUD.

3.9 Scheduled unavailability

MSs and CSD is going to use ICS2 Monitoring user interface (MON UI) to notify each other about scheduled unavailability. Scheduled unavailability should be organised in time windows when there is less operational activity and should be recorded in MON UI one week in advance for national components (not later than 48 hours in advance) [R04].

MON UI does not support dissemination of these notifications to EOs, therefore:

- NSD should provide this information to impacted EOs;
- CSD should provide this information to IT service provider [3.7.3].

NSD should be notified on scheduled unavailability of Economic operator systems not later than 48 hours in advance.

Activation of business continuity plan in case of scheduled unavailability:

- NSD can decide whether and when to activate business continuity plan in case of Economic operators scheduled unavailability;
- NSD should activate business continuity plan only in case of long scheduled unavailability (more than 3 hours). CSD coordinates and orchestrates activation of business continuity plan by all the NSD.

4 ANNEXES

4.1 Annex A: Statistics on ICS2 unavailability

UnavailabilityStatistics.xlsx

4.2 Annex B: Consolidated statistics on ICS2 unavailability

UnavailabilityStatistics_consolidated.xlsx

End of document