Node Operators Operational Book (NOOB)

Any reference to duties or obligations of the EBSI Service Desk within this document, shall be understood as a non-binding statement made in good faith, which is not legally enforceable against the European Commission, and which creates no binding obligation of result or legal recourse against the European Commission in case of breach of such duties or obligations.

Date: 30/03/2022

1 Glossary

The key terms used in this NOOB are defined in: EBSI Terminology

1.1 Additional Definitions

The following are key terms used solely in this NOOB which have not yet been included in the aforementioned glossary.

Term	Definition
EBSI Nodes	The EBSI Software and the servers used by the Node Operator to run the EBSI Node Software. They are designated by the EBP Members.
Validator Node	An EBSI Node in charge of guaranteeing the consensus of the network and the block generation. To do this, they run the consensus algorithm. Validator Nodes can also be referred to as *Consensus Nodes*, in Hyperledger Fabric as *Orderers*, etc.
Regular Node	An EBSI Node that participate in the network by replicating the blockchain, accepting blocks generated by Validators Nodes and executing transactions included in blocks by Validator Nodes. Regular Nodes also provide EBSI Network access to EBSI Application Service Providers. Sometimes Regular Nodes are referred to as *non-validating nodes* or *ledger nodes*.
Validator Set	The set of Validator Nodes that can execute the consensus algorithm. The Validator Set is managed by the participants of the network and its composition is fairly stable over time. At a given time, the Validator Set is split in: • Active Validator Set: The subset of nodes within the Consensus Set that are executing the consensus algorithm at a given time (i.e.: for the next block). • Stand-by Validator Set: The subset of Consensus Nodes that for some reasons (e.g. maintenance, SLA not compliance or Validator Set number higher than the maximum limit allowed by the consensus algorithm) are temporarily excluded from executing the consensus algorithm in order to avoid affecting the performance of the network. Validator Set is can also be referred to as Consensus set.

Term	Definition
Proposer Node	The Validator Node in the Active Validator Set that acts as a leader at a given moment. In IBFT a new Proposer is chosen each block in a round-robin way using lexicographic order of the node IDs in the Active Validator Set.
EBSI Service Desk	The services of the European Commission’s Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT), tasked with facilitating the EBP’s work to develop the EBSI Software, and tasked with the on-boarding, off-boarding and connection of EBSI Node Operators.
EBP	The European Blockchain Partnership that supports the delivery of cross-border digital public services, as defined at: https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership
EBP Member	Country which has signed the Joint Declaration creating the European Blockchain Partnership (EBP).
EBSI	European Blockchain Services Infrastructure project, which is a joint initiative between the EBP Members with the support of the European Commission to facilitate EBP-wide, domestic and/or cross-border public services with the use of distributed ledger technologies, as defined in Article 2(1) of Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (DLT Pilot Regime), including blockchain, through large-scale deployment, as defined at https://ec.europa.eu/digital-building-blocks/wikis/display/ebsi.
EBSI Network	A network of distributed nodes across Europe in all or parts of EBP Members, comprising public permissioned blockchain applications and distributed databases. They jointly enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.
Node Operator(s)	A public or private entity to host and operate an EBSI Node and by signing the EBSI Node Operator General Conditions detailing the technical and governance requirements for the EBSI Node Operators. The Node Operator enables and ensures the execution of transactions, by e.g., keeping a copy of the EBSI ledgers, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.
Compliance Process	The process of assessing systems to ensure their compliance with security standards, as well as with regulatory policies and requirements.
Sponsoring EBP Member	The EBP Member in whose jurisdiction a Node Operator has its legal seat inside the European Economic Area.

Date: 30/03/2022

Term	Definition
EBSI Application Service Provider	A natural or a legal person who provides one or more services to Use Case Owners using the EBSI Network, for instance by operating a digital wallet or for creating digital credentials, and who has entered into an agreement with the EBP Member by signing the EBSI Application Service Provider General Conditions.
EBSI Services	The services made available by the European Commission to the public as funded under the applicable funding Regulation and Work Programmes as well as under the EBSI Governance framework. This may include services such as specifications, software, support or testing services to enable access to and use of the EBSI Network.
EBSI Software	EBSI Node software package released by the European Commission under Commission Decision Ares (2022)404785 - 19/01/2022 and running on a server which is connected to the EBSI blockchain(s) using protocols that allows communication with other nodes on the network, as well as disseminating information held in distributed ledger database about transactions and blocks, accessible here: https://ec.europa.eu/digital-building-blocks/code/projects/EBSI.
Information Security Event	An occurrence indicating a possible breach of information security or failure of controls.
Information Security Incident	One or multiple related and identified Information Security Events that can harm an organization's assets or compromise its operations.
Intellectual Property Rights	All patent rights, copyrights, trademark rights, rights in trade secrets, database rights, moral rights,and any other intellectual and/or industrial property rights (registered or unregistered) throughout the world.
Node Services	The set of activities performed by the EBSI Nodes.
NOOB	Node Operators Operational Book, which is a set of standard processes for an EBSI Node Operator to follow in order to operate as such.
Personal Data	Any information related to an identified or an identifiable natural person as defined in the General Data Protection Regulation No (EU) 2016/679.

2 Purpose

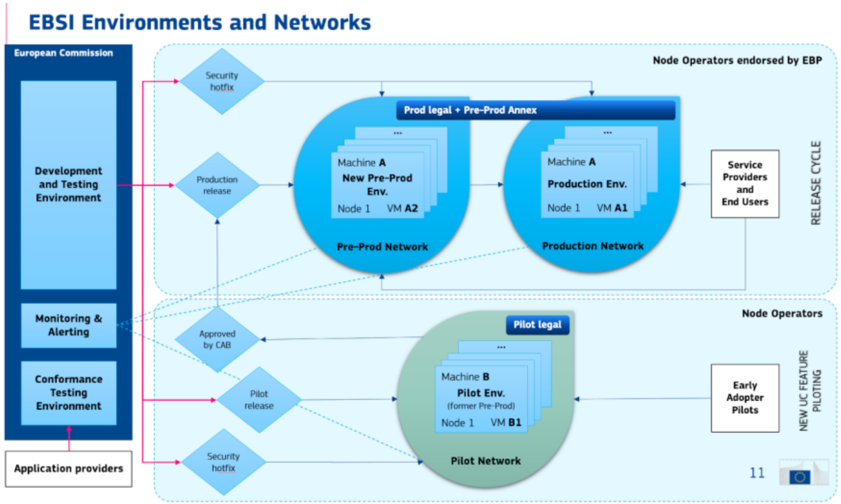
This book provides the standard processes for a Node Operator to operate as an EBSI Node Operator. It has the key objective of improving operations by reducing errors, increasing clarity and efficiency, as well as creating a safe working environment through the implementation of standardisation among Node Operators in the way of resolving issues in the daily execution and performance of an EBSI Node.

It is intended as an operation manual for Node Operators in key circumstances and contains the main processes for the Node Operators to know what to do in those circumstances.
It does not define how to execute the tasks as the individual procedures pertain to each Node Operator. However, it represents a guideline as to what are the general steps required to be followed.
These processes cover the operational aspects of incident management, vulnerability management, risk management, configuration management, and deploy management.

3 Minimum Technical Requirements (for an EBSI V2.0 Node)

3.1 EBSI Environments

In order to assure that software components and new features are tested appropriately prior to development, EBSI will follow the DTAP standard. As a consequence, 3 different networks (i.e., environments) are foreseen in the release orchestration for EBSI. When an environment is not specified in the present document, requirements must be assumed as generic for all environments. Node Operators are able to choose to operate a single or combination of networks. See below



The available network combinations that can be hosted by Node Operators are detailed below:

3.1.1 Only Pilot environment

Commitment to host one Virtual Machine with the following resource allocation and conform to applicable SLA & MTRs (Minimum Technical Requirements):

- **Pilot**
- - 4 vCPU, 32 GB RAM, 80 GB Disk + 256 GB Disk - Pilot SLA

3.1.2 Only Pre-Production and Production environments

Commitment to host two Virtual Machines with the following resource allocation and conform to applicable SLAs & MTRs:

- **Pre-Production**
- - 4 vCPU, 32 GB RAM, 80 GB Disk + 256 GB Disk - Pre-Production SLA
- **Production**
- - 8 vCPU, 64 GB RAM, 80 GB Disk + 500 GB Disk - Production SLA

3.1.3 Pre-Production, Production and Pilot environments providing with hardware separation of the Pilot environment.

Commitment to host **3 Virtual Machines provided with hardware separation** of Pilot environment with the following resource allocation and conform to applicable SLAs & MTRs:

- **Pre-Production**
- - 4 vCPU, 32 GB RAM, 80 GB Disk + 256 GB Disk - Pre-Production SLA
- **Production**
- - 8 vCPU, 64 GB RAM, 80 GB Disk + 500 GB Disk - Production SLA
- **Pilot**
- - 4 vCPU, 32 GB RAM, 80 GB Disk + 256 GB Disk - Pilot SLA

In case of hosting Pre-Production and Production environments, the Pilot environment must be provided with hardware separation.

3.2 Environment Requirements

An EBSI v2.0 node requires a minimum of **3 virtual hosts** all with access to the Internet and with individual **fixed IPV4 public IP addresses.**

These can be either physical server computers or virtual machines running in a self-hosted data-center infrastructure, a private cloud, or a public cloud, located in Europe.

For the EBSI project are foreseen 3 different environments (meaning 3 different networks). Each Virtual host will be used to join a different environment - one virtual host per environment.

Before joining the EBSI Network, all 3 hosts will have to pass a technical check to validate that all the minimum requirements are respected.

For the whole duration of the hosts being part of the EBSI network, all minimum requirements must be respected. A Node Operator can upgrade the performance, but can't lower it down at any moment.

3.3 Hardware

Each computer host – virtual machine – must have these minimum specifications:

EBSI V2 **Pilot Environment** VM	**EBSI V2 Pre-Production Environment VM**	**EBSI V2 Production Environment VM**
• **4 vCPU *** • **32 GB of RAM** • **80 GB for the operating system**** • **256 GB for data volume****	**4 vCPU *** **32 GB RAM** **80 GB for storage Operating System**** **256 GB for Data Volume****	**8 vCPU *** **64 GB RAM** **80 GB for storage Operating System**** **500 GB for Data Volume****

** data center CPU (not consumer CPU), newer than 2018 generation, not having any vulnerability listed in the CVE database (https://cve.mitre.org/cve/search_cve_list.html) unless the vendor-supplied mitigation has been applied*
*** minimum 2000 IOPs*

The host for Pilot Environment must be hosted on a different physical host and network than the hosts provisioned for the Pre-Production and Production Environments

3.4 Network

Each host must have a public IP address and must be connected to the Internet in order to get updated and communicate with other EBSI Nodes.

The minimum specifications are:

- 3 fixed public IPs v4 (one for each environment).
- 100 Mbits/second for bandwidth (Internet)
- maximum latency 100ms (Internet),
- 1 GB Ethernet (local network),

3.5 EBSI VM Deliverables

EBSI provides two options for node operators:

- OVA image for Vmware ESX (minimum ESX 6.7)
- qcow2 images for qemu/KVM based systems (Ovirt, ect)

The VM images are pre-configured with all the needed software stack to easily bootstrap the node.

3.6 Firewall Settings

Each virtual machine (host) must use the following configuration for the **external firewall.**

The table lists all the inbound firewall rules that must be implemented on the external firewall of the Internet connection used by each MS node host.:

3.6.1 For Pilot Environment

Number	Source IP(s)	Destination Port(s)	Protocol(s)	Action	Description
1	0.0.0.0/0	443	TCP	ACCEPT	TLS Core APIs & APPs
2	0.0.0.0/0	48733	TCP	ACCEPT	Besu P2P
3	0.0.0.0/0	48733	UDP	ACCEPT	Besu P2P
4	3.124.208.144	48722	TCP	ACCEPT	SSH*

*if this port cannot be opened, you will then need to ensure the availability of a system administrator during working hours, for troubleshooting cases

3.6.2 For Pre-Production Environment

Number	Source IP(s)	Destination Port(s)	Protocol(s)	Action	Description
1	0.0.0.0/0	443	TCP	ACCEPT	TLS Core APIs & APPs
2	0.0.0.0/0	48733	TCP	ACCEPT	Besu P2P
3	0.0.0.0/0	48733	UDP	ACCEPT	Besu P2P

3.6.3 For Production Environment

Number	Source IP(s)	Destination Port(s)	Protocol(s)	Action	Description
1	0.0.0.0/0	443	TCP	ACCEPT	TLS Core APIs & APPs
2	0.0.0.0/0	48733	TCP	ACCEPT	Besu P2P
3	0.0.0.0/0	48733	UDP	ACCEPT	Besu P2P

All Outbound traffic (Outbound Firewall rule) must be allowed without any proxy. A direct internet connection is required.

Based on the future evolution of the EBSI project, additional opened ports might be needed. In this case, you will be informed by the EBSI support team.

3.7 Hosting requirements

3.7.1 Security

A Node Operator is responsible for Node's security compliance. Node Operators hosting PreProd and Prod nodes **must** provide evidence of a valid ISO 27001 certification, or an equivalent national or regional standard approved by the EBP Member Country where the Node Operator is located. The certification requirement does not apply for the hosted Pilot environment.

Node Operator must protect their nodes against **Distributed Denial of Service attacks** and must apply **Web Application Firewall** to protect the nodes.

All traffic towards the node must always be adequately terminated by the designated TLS Certificate and all HTTP connections must be redirected towards HTTPS. The actual entry for the node is HTTP but this cannot be exposed as such and must be protected by TLS.

3.7.2 Domains

A domain must always start with the sub-domain parts of **"convention"** and must not have any extra path variables as a suffix, thus it should follow the template of "convention". The domain name cannot contain any words which can be considered rude or have any negative impact

The nodes will expose APIs documented in the EBSI API Catalog, where the paths will start immediately after the selected domain. A single node must have a single domain name, and multiple nodes can operate either under multiple sub-domains, multiple domains, or in a combination of these.

Node Operators must own and be able to control the domain name(s) and the associated TLS certificates. The TLS Certificates must be maintained and kept up to date by the Node Operator. Considering there are multiple subdomains, a Wildcard certificate is recommended.

The naming convention for the domains

Pilot	Pre-Production	Production

`api-pilot.ebsi.[FREELY_CHOSEN.DOMAIN.TLD]`
`app-pilot.ebsi.[FREELY_CHOSEN.DOMAIN.TLD]`
	`api-preprod.ebsi.[FREELY_CHOSEN.DOMAIN.TLD]`
	`app-preprod.ebsi.[FREELY_CHOSEN.DOMAIN.TLD]`
		`api.ebsi.[FREELY_CHOSEN.DOMAIN.TLD]`
		`app.ebsi.[FREELY_CHOSEN.DOMAIN.TLD]`

3.7.3 Recommendations

Node Operators should monitor the used CPU, disk space, memory, and network bandwidth and scale the resources if needed.

In the case of multiple nodes, Node Operators should consider re-routing traffic to other nodes upon disaster events.

4 Processes

In the context of the NOOB, the objective of security and all security related activities is to safeguard the node(s) operated by the node operator, and to limit potentially negative impact on other nodes. As consequence, in the context of the NOOB, the scope of security is the set of all elements (people, processes, technologies) that keep the node(s) operated by the node operator from harm, including those elements that stop and/or limit potential negative effects from propagating through the network.

In the context of the above, it is important that Node Operators are aware that the node they operate does include sensitive information that is unique to their node, including the node's private keys. These private keys are only known to the individual node operators and need to be backed-up by them. A node operator needs to have a tested backup and recovery plan/procedure in place for its node.

Any reference to duties or obligations of the EBSI Service Desk within this document, shall be understood as a non-binding statement made in good faith, which is not legally enforceable against the European Commission, and which creates no binding obligation of result or legal recourse against the European Commission in case of breach of such duties or obligations.

4.1 3PS01 - Node Operator Signing Process

4.1.1 GOAL

This process describes the necessary steps a potential Node Operator should perform to become part of the EBSI Network since they first get in touch with the EBSI ecosystem until they accept the legal documents, the privacy statement and launch the connection request procedure.

4.1.2 SCOPE

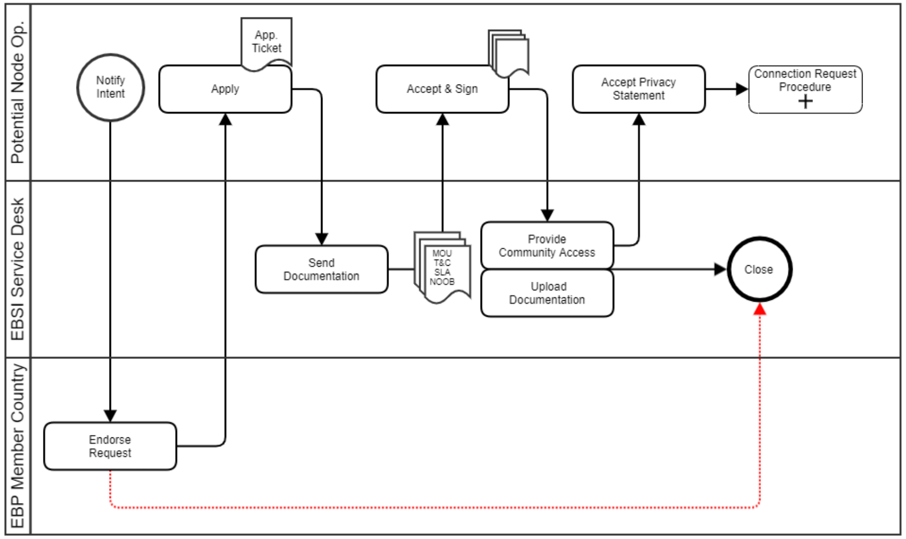
The process includes all the steps and the first onboarding. It includes the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management, regardless of who they are provided by.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI Network and released as open-source or put in operation by the European Commission.

The node connection to the network is not included but triggered as result of the last step, Connection Request Procedure.

4.1.3 THE PROCESS

The process actors and their steps are presented in the following diagram:



4.1.4 PROCESS DESCRIPTION

- ***Step 1. Notify Intent****<Potential Node Operator>* sends a notification of his intention to become a Node Operator indicating the environments they wish to be part of. If the Node operator intends to be part of the preprod and production environments the request needs to be endorsed by the EBP Member country as well as its Security Certification (ISO27001 or equivalent) must be sent to the EBP Member Country (EBP MC) where the Node Operator is or will be located. For the pilot environment the endorsement of the security certification is not needed.

- ***Step 2. Endorse Request***<*EBP Member Country*> reviews the notification and the security certification sent by the <*Potential Node Operator*> and decides whether to endorse this application or not. The <*EBP Member Country*> may not endorse these documents separately. They either endorse both the <*Potential Node Operator*> and their Security Certification, or the do not endorse the <*Potential Node Operator*>.Should the <*EBP Member Country*> decide not to endorse this application or Security Certification, the process is terminated at this point. The choice to notify the <*Potential Node Operator*> of this decision and its reasons (and if applicable how to do so) belongs to the <*EBP Member Country*> and is outside of the scope of this process.
  Should the <*EBP Member Country*> decide to endorse this application and Security Certification, it must provide a formal endorsement in the form of a document that the <*Potential Node Operator*> can attach in the application to be sent in the next step (e.g. email exchange with a written approval from the EBP MC).

- ***Step 3. Apply***<*Potential Node Operator*> sends an application on the EBSI website, which creates a Jira Ticket. In this Ticket, the <*Potential Node Operator*> must attach the endorsement document received from the <*EBP Member Country*>.

- ***Step 4. Send Documentation***<*EBSI Service Desk*> via the *Support Office* replies to the application ticket by explaining the procedure of accepting the legal documentation to be able to participate in EBSI Production phase. And providing the links to the required documentation to be accepted by <*Potential Node Operator*>, comprised of: MoU, T&C, SLA, NOOB.
  Step 5. Accept & Sign<*Potential Node Operator*> reads the documentation, and if it still wishes to continue with the application process accepts and sign the documentation through EUSurvey. By going forwards with this action the <*Potential Node Operator*> is accepting the MoU, the T&C and commits to the SLA and the NOOB. Any objection, partial or total, to any document will translate into a termination of this process.

- ***Step 6. Provide Community Access***<*EBSI Service Desk*> grants community access to the <*Potential Node Operator*> by providing the defined permissions to the NO Community space and explaining the next steps to request the access to the EBSI network.

- ***Step 7. Upload Documentation***<*EBSI Service Desk*> uploads the acceptance of the documentation provided by the <*Potential Node Operator*> to the NO Community space.

- ***Step 8a. Close***<*EBSI Service Desk*> considers this process closed and proceeds to close the ticket.

- ***Step 8b. Accept Privacy Statement***<*Potential Node Operator*> enters the community space and accepts the privacy statement.

- ***Step 9. Connection Request***<*Potential Node Operator*>, after accepting the privacy statement, launches the Connection Request Procedure via the link on the homepage of the NO Community.

4.1.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering new configurations for their proper handling in accordance to the established policies.
- notifying all relevant parties of the new configuration to be deployed.
- keeping an updated record of all configurations in the form of a Configuration Registry.

EBP Member Country refers to a country participating in the European Blockchain Partnership, who holds sovereignty over the territory in which a Potential Node Operator will operate.

Their responsibilities within this process include (but not limited to):

- assess the Potential Node Operator to realise the application and provide, if needed, feedback on the legal documents signature process in accordance with the established policies.
- assess the Potential Node Operator's Security Certification.

Potential Node Operator refers exclusively to those who manifest their intention to become EBSI Node Operators who will become stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- properly applying to become EBSI Node Operators via a valid application request.
- providing a valid Security Certification (ISO27001 or equivalent)
- accepting and signing the documents needed to become EBSI Node Operators.
- requesting to be connected to the network to finalise the process.

4.2 3PS03 - Connection Request Process

4.2.1 GOAL

This procedure describes the necessary steps to onboard and connect a node to the network. This procedure is never triggered on its own, but as result of a 3PS01 - Node Operator Signing Process, despite its key role to create a strong network in the EBSI platform.

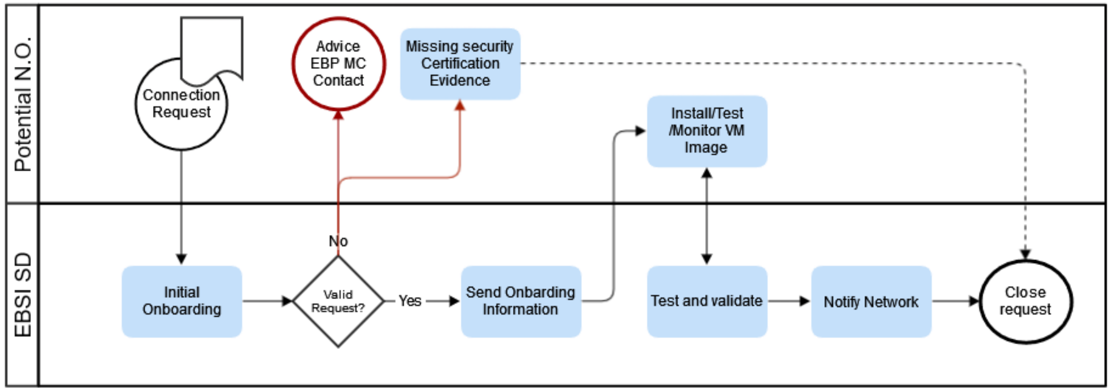
4.2.2 SCOPE

This procedure defines all possible aspects and evaluations during the promotion of a potential new node to the EBSI network and it covers the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management.
- **Hardware** - operated by Node Operators.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI Network and released as open-source or put in operation by the Commission.
- **Virtual Machines** - provided by EBSI.

4.2.3 THE PROCESS

The main actors of the procedure and their steps are presented in the following diagram:



4.2.4 PROCESS DESCRIPTION

- **Step 1. Connection Request**

<Potential Node Operator> submits a request via Support Ticket after a successful signing process that is reflected on the Jira ticket (see 3PS01 - Node Operator Signing Process)

The ticket indicates (among other basic identifying information):

1. if the Potential Node Operator would like to be a validator
2. confirmation they have read the minimum technical requirements, more info here. This includes the IP address to be whitelisted as per Minimum Technical Requirements for EBSI V2.0 Node.
3. the EBP member country name who approved their request to join the network
4. evidence of EBP member country endorsement

5. Information Security Certification evidence.

- **Step 2. Valid Request?**

<EBSI Service Desk> receives the request and validates the following:

1. information on the ticket (as listed in step 1)
2. the signed legal documentation in the Node Operator's Community who was uploaded in the 3PS01 - Node Operator Signing Process (Potentially MoU, T&C, SLA, NOOB)
3. ensure there is an information security certification attached to the request

- **Step 2a. <if no> Advice EBP MC Contact or Notify Security Certification is missing or invalid**

<EBSI Service Desk> notifies the <Potential Node Operator> of the missing elements and required steps to comply with a valid request following the 3PS01 - Node Operator Signing Process

- **Step 3. <if yes> Send On-boarding information**

<EBSI Service Desk> sends the image to be installed to the <Potential Node Operator> and any required extra guidance - ongoing open point to determine where to put image/improve security on access to image

The access to Node Operators community should be granted during the 3PS01 - Node Operator Signing Process

- **Step 4. Install VM Image**

<Potential Node Operator> downloads and Installs Node image, implement the IP firewall rules (update Node ID JSON)

- The node operator needs to create a private/public key (DID keys)
- This DID is communicated to the Support Office
- Node operators must share their public keys with EBSI via an authenticated channel (can be mTLS) to issue them a Verifiable Authorisation
- **Step 4b. Test & Monitor**

<Potential Node Operator> confirms installation and the <Support Office> monitors and performs tests

Tests to confirm minimum technical requirements and connectivity

- **Step 5. Test and Validate**

<EBSI Service Desk> validates if the hardware and connectivity Node testing is successful

Steps 4b and 5 will repeat until all issues are fixed according with the terms defined in the SLA.

- **Step 6. Notify Network**

<EBSI Service Desk> will start the procedure for the new node to be included in the Network.

- **Step 7. Close request**

Once node is connected <EBSI Service Desk> informs New node and closes the ticket

4.2.4.1 ROLES & RESPONSIBILITIES

Potential Node Operator refers exclusively to those who manifest their intention to become EBSI Node Operators who will become stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities include (but are not limited to):

- properly applying to become EBSI Node Operators via a valid application request.
- accepting and signing the documents needed to become EBSI Node Operators
- requesting to be connected to the network to finalise the process.

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities in this process are limited to:

- identifying, controlling and registering new configurations for their proper handling in accordance with the established policies.
- notifying all relevant parties of the new configuration to be deployed.
- keeping an updated record of all configurations in the form of a Configuration Registry.

4.3 3PS04 - Incident Management Process

This process is responsible for managing security incidents within the EBSI Network.

4.3.1 GOAL

The goal of this process is to ensure the use of standardised methods and procedures for efficient and prompt handling of all EBSI related incidents by Node Operator(s), in order to minimise their impact upon service quality and manage events that may impact information systems' confidentiality, integrity, or availability.

4.3.2 SCOPE

This process covers the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Hardware** - EBSI infrastructure components.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI and released as open-source or put in operation by the European Commission.

4.3.3 THE PROCESS

The Incident Management Process actors and their steps are presented in the following diagram:

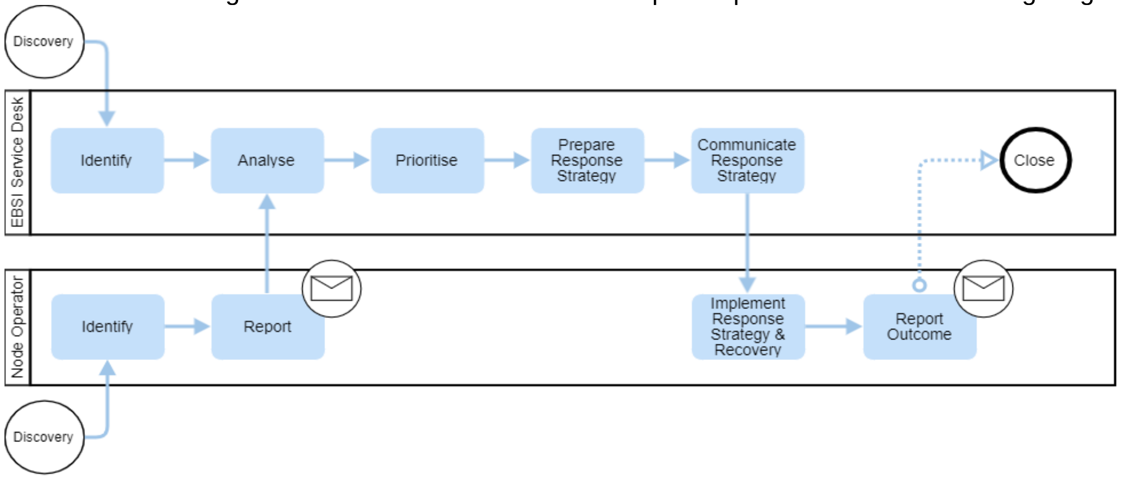


Figure 1: Incident Management Process

4.3.4 PROCESS DESCRIPTION

- ***Discovery:*** The starting point of this process is the discovery of an incident by one of the actors, be these Node Operator(s) or EBSI Service Desk personnel.
- ***Identify:*** Identification of an Incident by either actor, implies the registration of the incident through the <Incident Report>, and completion of all the relevant information for the proper analysis of said incident.
- ***Report:*** <Node Operator> sends the <Incident Report>, via the established secure channels, to <EBSI Service Desk> ensuring all mandatory information is complete and as much optional information as possible is provided.

- ***Analyse:*** <EBSI Service Desk> performs a thorough analysis of the received information about the incident with aims at providing enough insight to prioritise and prepare a response strategy further on. To this end, the <Incident Report> is further completed ensuring all potential threats and implications of the incident are mentioned. All relevant information is included in the <Incident Log>.
- ***Prioritise:*** <EBSI Service Desk> prioritises the preparation of a Response Strategy for the reported incident, based on it's severity (Low, Medium, High, Critical) according to the information provided within the <Incident Report>.
- ***Prepare Response Strategy:*** <EBSI Service Desk> prepares a response strategy to for the Node Operator(s) to deal with the incident in accordance to the established standards and Incident Management Policies. <EBSI Service Desk> updates the <Incident Log> with the Response Strategy.
- ***Communicate Response Strategy:*** <EBSI Service Desk> informs the Node Operator(s) via the established secure channels, which is the response strategy for the incident, by use of the <Incident Response Strategy Template>. This communication may well be extended to all Node Operators fulfilling a certain criteria, depending on the incident type and scope.
- ***Implement Response Strategy & Recovery:*** <Node Operator(s)> executes the response strategy and ensures the system has been completely recovered.
- ***Response Report:*** <Node Operator(s)> informs <EBSI Service Desk> via the <Incident Response Report>, the outcome of the Response Strategy execution.
- ***Close:*** <EBSI Service Desk> registers the response in the <Incident Log> closing the incident or sends the report back to step 4 in case of Response Strategy execution failure.

4.3.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- registering discovered incidents for the proper handling in accordance to the established policies.
- preparing the response strategies.

- notifying all relevant parties of the discovered incidents.
- notifying all relevant parties of response strategies.
- keeping an updated record of all incidents, response strategies and contingency actions in the form of an Incident Log.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- reporting discovered incidents to EBSI Service Desk for the proper handling in accordance with the established policies.
- implementing response strategies and recovering from the incident.
- reporting back the taken actions and their result to EBSI Service Desk.

4.4 3PS05 - Vulnerability Management Process

This process is responsible for the management of vulnerabilities within the EBSI Network, from discovery to closure through response strategies and their communication to Node Operators.

4.4.1 GOAL

The goal of this process is to ensure the use of standardised methods and procedures for efficient and prompt handling of vulnerabilities detected on the EBSI Network, to minimise and mitigate their impact upon service quality, and manage events that may impact information systems' confidentiality, integrity, or availability.
Starting through the discovery of a vulnerability, the process follows the steps from identification to response strategy ensuring Node Operator(s) have taken the established measures.

4.4.2 SCOPE

This process covers the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Hardware** - EBSI infrastructure components.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI DSIs and released as open-source or put in operation by the European Commission.

4.4.3 THE PROCESS

The EBSI Vulnerability Management Process actors and their steps are presented in the following diagram:

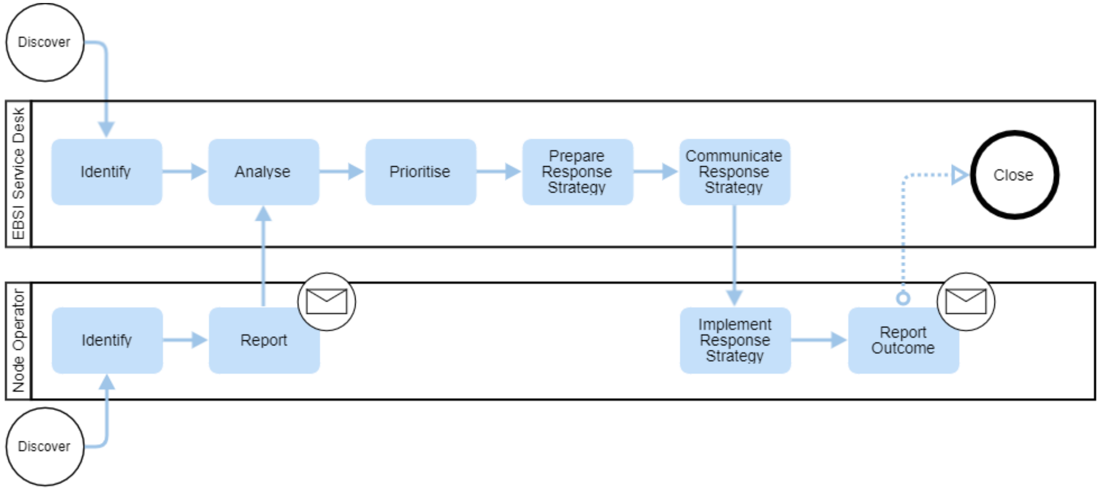


Figure 1: EBSI Vulnerability Management Process

4.4.4 PROCESS DESCRIPTION

- ***Discover:*** The starting point of this process is the discovery of a vulnerability by one of the actors, be these Node Operator(s) or EBSI Service Desk personnel.
- ***Identify:*** Identification of a vulnerability by either actor implies the registration of the vulnerability through the Vulnerability Report, and completion of all the relevant information for the proper analysis of said vulnerability.
- ***Report:*** <Node Operator> sends the Vulnerability Report, via the established secure channels, to <EBSI Service Desk> using the Vulnerability Report Template, ensuring all mandatory information is complete and as much optional information as possible is provided.
- ***Analyse:*** <EBSI Service Desk> performs a thorough analysis of the received information about the vulnerability with aims at providing enough insight to prioritise and prepare a Response Strategy further on. To this end, the Vulnerability Report is further completed ensuring all relevant information is provided, including severity and impact. <EBSI Service Desk> registers the vulnerability in the Vulnerability Log.
- ***Prioritise:*** <EBSI Service Desk> prioritises the preparation of a Response Strategy for the reported vulnerability based on it's severity and impact according to the information provided within the Vulnerability Report.
- ***Prepare Response Strategy:*** <EBSI Service Desk> prepares a Response Strategy for the Node Operator(s) to deal with the vulnerability by means in accordance to the established standards and the Vulnerability Management Policies. <EBSI Service Desk> updates the Vulnerability Log with the Response Strategy.
- ***Communicate Response Strategy:*** <EBSI Service Desk> communicates the Response Strategy for the reported vulnerability including the corresponding contingency actions to the Node Operator(s) via the established secure channels, by use of the Vulnerability Response Strategy Template. This communication may well be extended to all Node Operators fulfilling a certain criteria, depending on the vulnerability type and scope.
- ***Implement Response Strategy:*** <Node Operator(s)> executes the Response Strategy ensuring the contingency actions defined for the vulnerability have been set in place.
- ***Report Outcome:*** <Node Operator(s)> informs <EBSI Service Desk> via the Vulnerability Response Report, the outcome of the Response Strategy implementation, acknowledging their responsibility on acting upon the vulnerability and taking the necessary contingency actions. The reported outcome must include confirmation of the vulnerability removal or a detailed explanation of the issues and errors encountered while implementing the Response Strategy.
- ***Close:*** <EBSI Service Desk> registers the response in the Vulnerability Log.

4.4.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- registering discovered vulnerabilities for the proper handling in accordance to the established policies.
- preparing the response strategies and contingency actions.
- notifying all relevant parties of the discovered vulnerabilities.
- notifying all relevant parties of response strategies and contingency actions.
- keeping an updated record of all vulnerabilities, response strategies and contingency actions in the form of a Vulnerability Log.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include:

- reporting discovered vulnerabilities to EBSI Service Desk for the proper handling in accordance with the established policies
- successfully implementing response strategies
- successful application of contingency actions
- reporting back the taken actions and their result to EBSI Service Desk

4.5 3PS06 - Risk Management Process

This process is responsible for the management of all risks within the EBSI Network, from discovery to closure through response strategies and their communication to Node Operators.

4.5.1 GOAL

The goal of this process is to ensure the use of standardised methods and procedures for efficient and prompt handling of all EBSI related risks which affect the Nodes Network, in order to minimise and mitigate their impact upon service quality, and consequently to improve the day-to-day operations of the organisation.
Starting through the discovery of a risk, the process follows the steps from identification to response strategy, and subsequently ensuring Node Operator(s) have taken the appropriate measures.

4.5.2 SCOPE

This process covers the following items:

- **Documents** - textual artifacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Hardware** - EBSI infrastructure components.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI and released as open-source or put in operation by the Commission.

4.5.3 THE PROCESS

The Risk Management Process actors and their steps are presented in the following diagram:

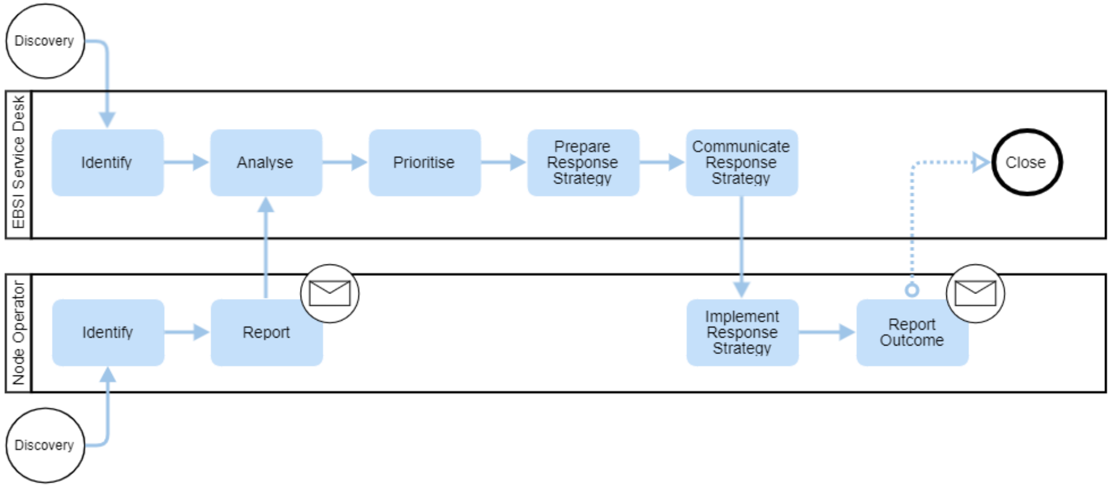


Figure 1: Risk Management Process

4.5.4 PROCESS DESCRIPTION

- ***Discovery:*** The starting point of this process is the discovery of a risk by one of the actors, be these Node Operator(s) or EBSI Service Desk personnel.
- ***Identify:*** Identification of a risk by either actor, implies the registration of the risk through the <Risk Report>, and completion of all the relevant information for the proper analysis of said risk.
- ***Report:*** <Node Operator> sends the <Risk Report>, via the established secure channels, to <EBSI Service Desk> using the <Risk Report Template>, ensuring all mandatory information is complete and as much optional information as possible is provided.
- ***Analyse:*** <EBSI Service Desk> performs a thorough analysis of the received information about the risk with aims at providing enough insight to prioritise and prepare a response strategy further on. To this end, the <Risk Report> is further completed ensuring all relevant information is provided; including severity, impact and probability of occurrence. All this information is updated in the <Risk Log>.
- ***Prioritise:*** <EBSI Service Desk>prioritises the preparation of a Response Strategy for the reported risk, based on it's severity, impact and probability of occurrence according to the information provided within the <Risk Report>.
- ***Prepare Response Strategy:*** <EBSI Service Desk> prepares a response strategy for the Node Operator(s) to deal with the risk by means of mitigation strategies, in accordance to the established standards and Risk Management Policies. <EBSI Service Desk> updates the <Risk Log> with the Response Strategy.
- ***Communicate Response Strategy:*** <*EBSI Service Desk*> communicates the Response Strategy for the reported risk, including the corresponding contingency actions to the Node Operator(s) via the established secure channels, by use of the <Risk Response Strategy Template>. This communication may well be extended to all Node Operators fulfilling a certain criteria, depending on the risk type and scope.
- ***Implement Response Strategy:*** <Node Operator(s)> executes the response strategy ensuring the mitigation strategies defined for the risk have been set in place, and the risk owners are informed of the mitigation actions and the necessary contingency actions in case the risk triggers.
- ***Response Report:*** <Node Operator(s)> informs <EBSI Service Desk> via the <Risk Response Report>, the outcome of the Response Strategy implementation, acknowledging their responsibility for mitigating the risk and taking the necessary contingency actions in case the risk triggers.
- ***Close:*** <EBSI Service Desk> registers the response in the <Risk Log>, recording the Node Operator(s) risk owner.

4.5.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission’ Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members’ work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering new configurations for their proper handling in accordance to the established policies.
- notifying all relevant parties of the new configuration to be deployed.
- keeping an updated record of all configurations in the form of a Configuration Registry.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include:

- reporting identified risks to EBSI Service Desk for the proper handling in accordance to the established policies.
- implementing response strategies and mitigation strategies defined by EBSI Service Desk.
- applying contingency actions successfully when risks are triggered.
- reporting back the taken actions and their result to EBSI Service Desk.

4.6 3PS07 - Support Request Management Process

This process is responsible for handling support requests to the Service Desk by reviewing, registering, replying and closing them.

4.6.1 GOAL

The goal of this process is to ensure proper and standard review and registration of all EBSI support requests, for them to be timely replied to and provide a knowledge base for future reference on all matters that have required support, and/or assistance of the Service Desk. This will facilitate future requests on matters that have been previously attended and, through registration facilitate metrics, requests, and replies.

4.6.2 SCOPE

This process covers the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Hardware** - EBSI infrastructure components.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI DSIs and released as open-source or put in operation by the Commission.

4.6.3 THE PROCESS

Process activities are presented in the following diagram:

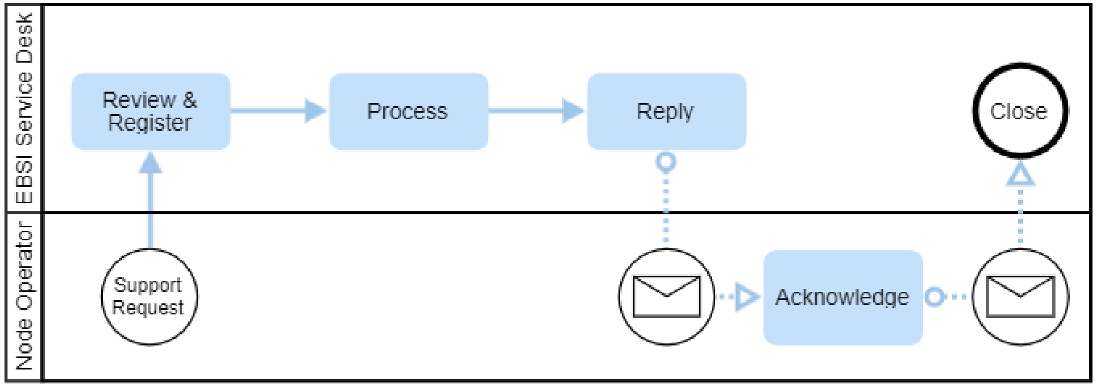


Figure 1: Support / Help-Desk Management Process

4.6.4 PROCESS DESCRIPTION

- ***Support Request:*** <Node Operator(s)> sends a Support Request via the designated communication support channels.
- ***Review & Register:*** <EBSI Service Desk> receives, reviews and registers the support request, ensuring it enters the support request queue.
- ***Process:*** <EBSI Service Desk> processes the support request accordingly, which may lead to other processes depending on the request type.
- ***Reply:*** <EBSI Service Desk> responds to the <Node Operator(s)> once the processing of the support request is completed.
- ***Acknowledge:*** <Node Operator(s)> receives the reply to the support request and sends the acknowledgement of the reception indicating acceptance or refusal of the reply.

- ***Close:*** <EBSI Service Desk> closes the support request, with the acknowledgement sent by the <Node Operator(s)>. In the case of a refusal from the <Node Operator(s)>, this leads back to the Review & Register step.

4.6.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- reviewing, registering, processing and replying to support requests for their proper handling in accordance to the established policies.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- properly requesting support through a valid support request.
- acknowledging the received reply.

4.7 3PS08 - Configuration Management Process

This process responsible for identifying, controlling, registering, and communicating configuration information to Node Operators, for them to perform the necessary steps to apply new configurations, and report back the results.

4.7.1 GOAL

The goal of this process is to ensure the use of standardised methods and procedures for efficient and prompt handling of all EBSI configuration related matters, such as applying new configuration components, and/or removing obsolete ones, be these related to software, hardware, or virtual hardware; to minimise the impact of configuration-related incidents upon service quality and improving the day-to-day operations of the EBSI Network.

4.7.2 SCOPE

This process covers the following items:

- **Hardware** - EBSI infrastructure components.
- **Services** - provided by EBSI.
- **Software** - applications developed and maintained within the EBSI Network and released as open-source or put in operation by the Commission.
- **Virtual Machines** - provided by EBSI.

4.7.3 THE PROCESS

The Configuration Management Process actors and their steps are presented in the following diagram:

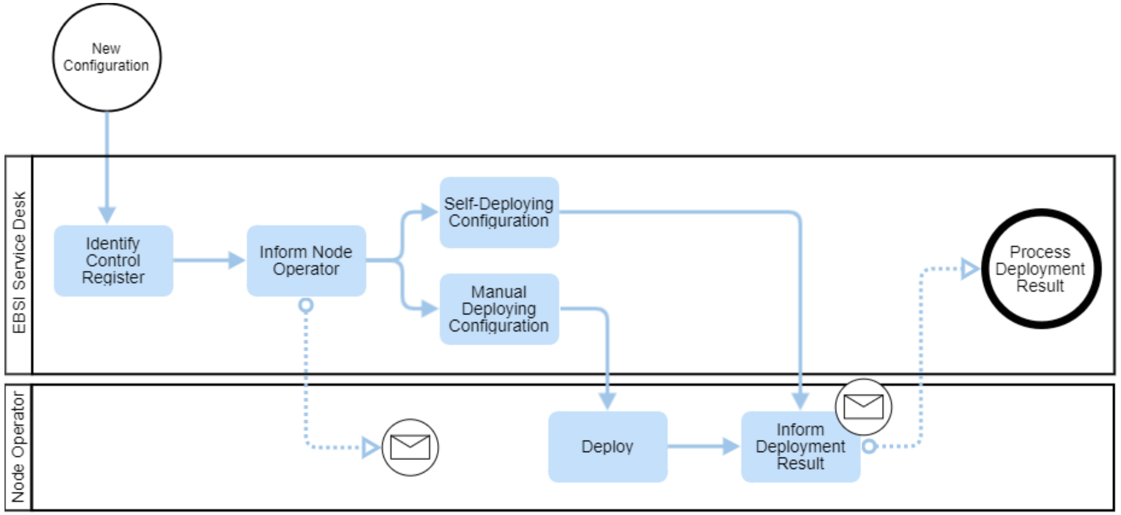

New Configuration
EBSI Service Desk
Identify Control Register
Inform Node Operator
Self-Deploying Configuration
Manual Deploying Configuration
Process Deployment Result
Node Operator
Deploy
Inform Deployment Result

Figure 1: Configuration Management Process

4.7.4 PROCESS DESCRIPTION

- ***New Configuration:*** The starting point of this process is the reception of a New Configuration to be deployed automatically or manually by the Node Operator(s). This trigger encompasses all types of new configurations for all possible reasons, such as a new configuration to resolve a vulnerability, prepare an environment for a new release, configuring an environment after a release, or any other typified or not typified configuration trigger.
- ***Identify / Control / Register:*** <EBSI Service Desk> identifies the New Configuration, verifies, and records the new configuration in the <Configuration Registry> with its corresponding Id (version).

- ***Inform Node Operator:*** <EBSI Service Desk> communicates the location and identification of the configuration to deploy to the Node Operator(s) via the <New Configuration Report>, informing whether this configuration is self-deploying or has to be manually deployed by the Node Operator(s).
- ***Self-Deploying Configuration:*** This is an automatic step, for the cases of self-deploying configurations, in which the Node Operator(s) are notified that a self-deploying configuration process will be executed on the nodes, via the established remote configuration tools.
- ***Manual Deploying Configuration:*** <Node Operator> receives the <New Configuration Report>, with Manual Deployment instructions, and the steps to perform the manual deployment of the new configuration.
- ***Deploy:*** <Node Operator> performs the steps for the manual deployment of the new configuration following the Manual Deployment instructions received within the <New Configuration Report>.
- ***Inform Deployment Result:*** <Node Operator> informs the result of the deployment back to <EBSI Service Desk> via the <Deployment Result Report>, with either a Success Result or the errors obtained from the Deployment process.
- ***Process Deployment Result:*** <EBSI Service Desk> receives the <Deployment Result Report> and acts accordingly by either registering the successful deployment in the <Configuration Registry> or resuming this process at the Inform Node Operator step.

4.7.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering new configurations for their proper handling in accordance to the established policies.
- notifying all relevant parties of the new configuration to be deployed.
- keeping an updated record of all configurations in the form of a Configuration Registry.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network.

They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- deploying new configurations according to EBSI Service Desk requests.
- reporting back the taken actions and their result to EBSI Service Desk.

4.8 3PS09 - Deploy Management Process

This process is responsible for notifying Node Operators of changes that have been released and ready to be deployed, receiving the deployment report and acting accordingly.

4.8.1 GOAL

The goal of this process is to ensure the use of standardised methods and procedures for efficient and prompt handling of all EBSI related deployments by Node Operators, be they automated or manual, in order to minimise their impact upon service quality, and improve the day-to-day operations of the EBSI Network.

4.8.2 SCOPE

This process covers the following items:

- **Software -** applications developed and maintained within the EBSI and released as open-source or put in operation by the Commission;
- **Hardware** - EBSI infrastructure components;
- **Services -** provided by EBSI;

4.8.3 THE PROCESS

The Deploy Management Process actors and their steps are presented in the following diagram:

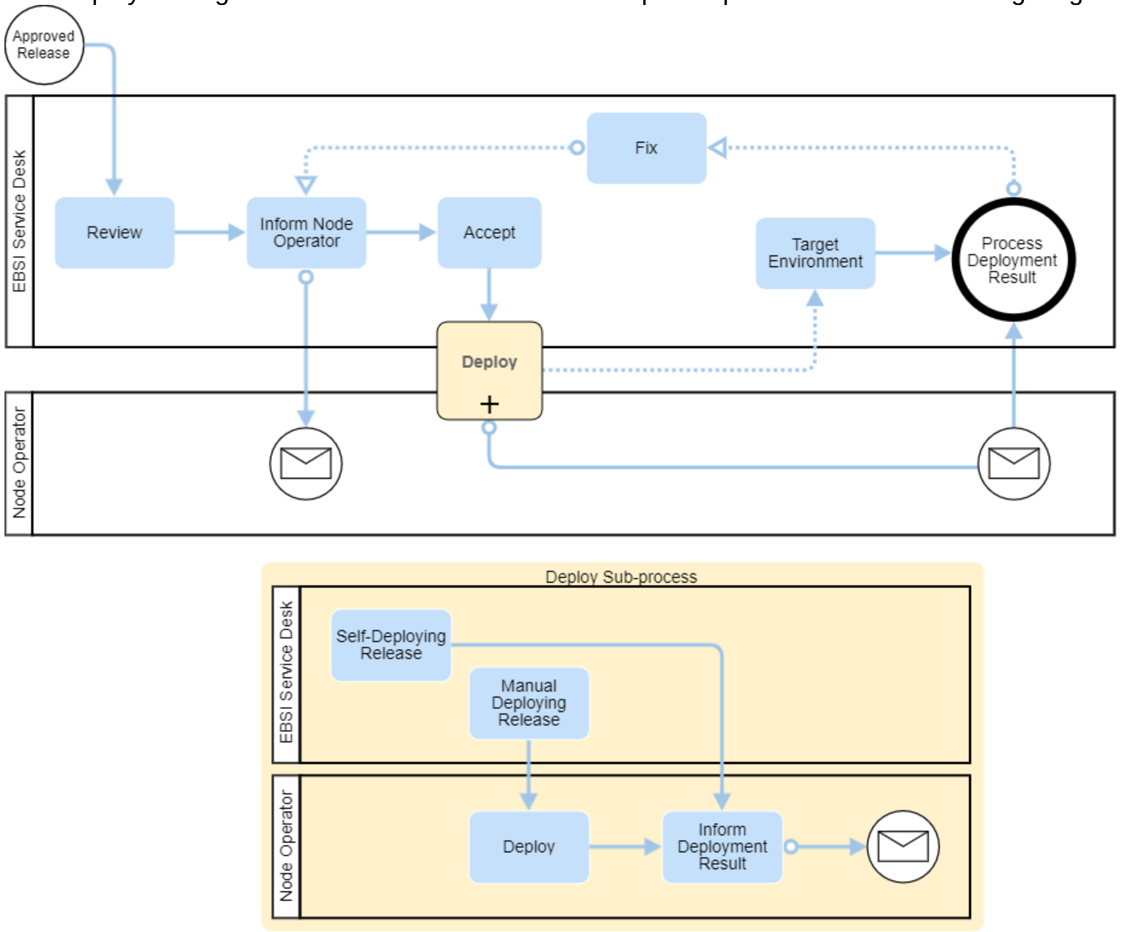


Figure 1: Deploy Management Process

4.8.4 PROCESS DESCRIPTION

- ***Approved Release:*** The starting point of this process is the reception of an Approved Release to be deployed automatically or manually by the Node Operator(s). This trigger encompasses all types of releases for all possible reasons, such as a release to resolve a vulnerability, incident, implementation of new functionality, or any other typified or not typified release trigger.
- ***Review:*** <EBSI Service Desk> performs a review of the release to be sent to the Node Operator(s) and registers the release in the <Release Registry>, including all relevant information.
- ***Inform Node Operator:*** <EBSI Service Desk> communicates the location and identification of the release to deploy to the Node Operator(s) via the <Release Report>, informing whether this release is self-deploying or has to be manually deployed by the Node Operator(s).
- ***Accept:*** <EBSI Service Desk> registers the release acceptance in the <Release Registry>.
- ***Self-Deploying Release:*** This is an automatic step, for the cases of self-deploying releases, in which the Node Operator(s) are notified that a self-deploying release process will be executed on the nodes, via the established remote tools.
- ***Manual Deploying Release:*** <Node Operator(s)> receives the <Release Report>, with Manual Deployment instructions, and the steps to perform the manual deployment of the release.
- ***Deploy:*** <Node Operator(s)> performs the steps for the manual deployment of the release following the Manual Deployment instructions received within the <Release Report>.
- ***Inform Deployment Result:*** <Node Operator(s)> communicates the result of the deployment back to <EBSI Service Desk> via the <Deployment Result Report>, with either a Success Result or the errors obtained from the Deployment process.
- ***Process Deployment Result:*** <EBSI Service Desk> receives the <Deployment Result Report> and acts accordingly by either registering the successful deployment in the <Release Registry> or resuming this process at the Inform Node Operator step.

4.8.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission’ Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members’ work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering new releases for their proper handling in accordance with the established policies.
- notifying all relevant parties of the new releases to be deployed.
- keeping an updated record of all releases in the form of a Release Registry.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- deploying new releases according to EBSI Service Desk requests.
- reporting back the taken actions and their result to EBSI Service Desk.

4.9 3PS10 - Archiving & Backup Management Process

This process is responsible for identifying, controlling, registering, and communicating archiving and backup information to Node Operators, for them to perform restore operations, and report back the results.

4.9.1 GOAL

The goal of this process is to ensure the use of standardised methods and procedures for efficient and prompt handling of archiving and backup access needs. Communicating them to Node Operators, and acting accordingly to their response, minimising the impact of related activities on service quality and ensuring the integrity of the EBSI network.

4.9.2 SCOPE

This process covers the following items:

- **Documents -** textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Software** - applications developed and maintained within EBSI and released as open-source or put in operation by the European Commission.
- **Services** - provided by EBSI.
- **Virtual Machines** - provided by EBSI.

4.9.3 THE PROCESS

The Archiving and Backup Management Process actors and their steps are presented in the following diagram:

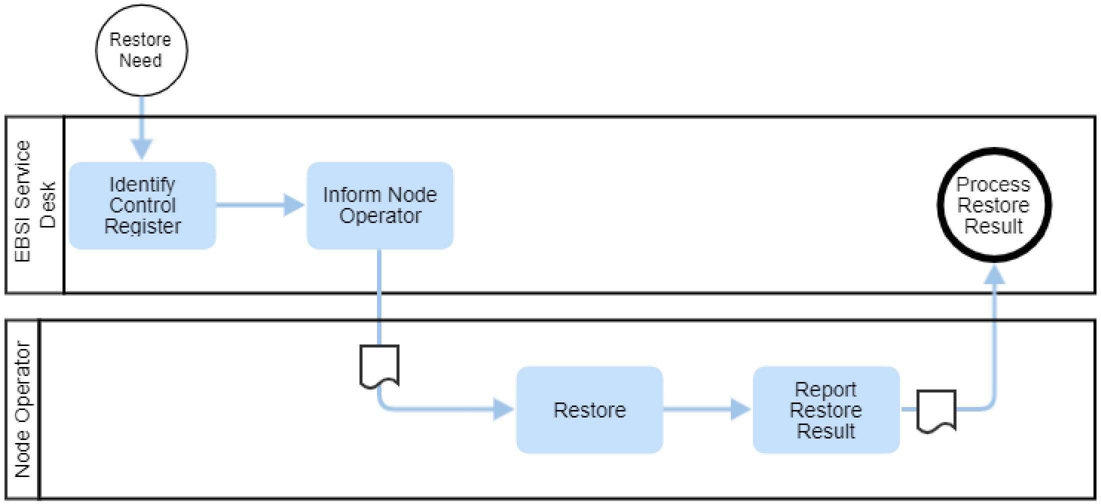


Figure 1: EBSI Archiving & Backup Management Process

4.9.4 PROCESS DESCRIPTION

- ***Restore Need:*** The starting point of this process is the reception of a restore need, which represents a trigger, message, situation, and/or any other form of communication related to restoring a backup.
- ***Identify, Control, Register:*** <EBSI Service Desk> identifies the backup to be restored, controls said backup ensuring that it corresponds with the necessary restore, and registers the action to be taken by the Node Operator(s) to maintain traceability of backup restoration.
- ***Inform Node Operator:*** <EBSI Service Desk> notifies the Node Operator(s) of the restore request, including the location and identification of the backup to be restored.
- ***Restore:*** <Node Operator> proceeds to execute the restoration of the backup received in the communication sent in the previous step, ensuring that the location and identification match.
- ***Report Restore Result:*** <Node Operator> informs the result of the restore process back to <EBSI Service Desk> via the Restore Result Report, with either a Success Result or the errors obtained from the restore process.
- ***Process Restore Result:*** <EBSI Service Desk> receives the Restore Result Report and acts accordingly by either requesting the successful restore by the Node Operator(s) or resuming this process at the Inform Node Operator step.

4.9.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering restore needs and backups for the proper handling in accordance to the established policies.
- notifying all relevant parties of the backup location and the need for a restore.
- keeping an updated record of backup locations, restore requests and results.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- execute EBSI Service Desk restore requests.
- reporting back the taken actions and their result to EBSI Service Desk.

4.103PS11 - Voting Process

This process is responsible for defining the voting action within the EBSI Network.

4.10.1 GOAL

This process describes the necessary steps to realise a voting procedure, necessary to create a consensus on actions involving other nodes of the EBSI Network.

4.10.2 SCOPE

This process covers the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Software** - applications developed and maintained within EBSI and released as open-source or put in operation by the European Commission.
- **Services** - provided by EBSI.
- **Virtual Machines** - provided by EBSI.

4.10.3 THE PROCESS

The Voting Process actors and their steps are presented in the following diagram:

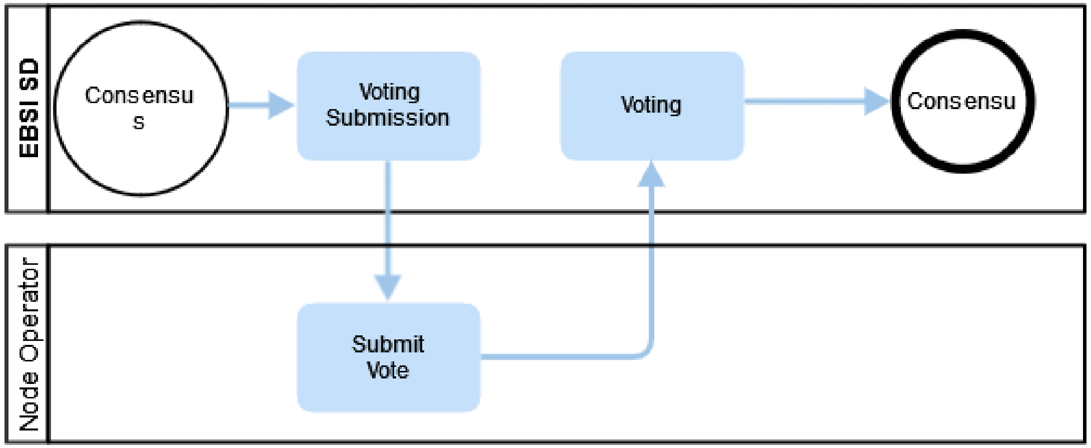


Figure 1: EBSI Voting Process

4.10.4 PROCESS DESCRIPTION

- ***Consensus Needed.*** <EBSI Service Desk> receives a request to push for a voting round.
- ***Voting Submission.*** <EBSI Service Desk> creates the voting process and notifies <Node Operators>.
- ***Submit Vote.*** <Node Operators> submit their vote within agreed SLA target timeframe.
- ***Voting Resolution.*** <EBSI Service Desk> computes the voting resolution.
- ***Consensus.*** <EBSI Service Desk> confirms consensus is reached.

4.10.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering restore needs and backups for the proper handling in accordance to the established policies.
- notifying all relevant parties of the backup location and the need for a restore.
- keeping an updated record of backup locations, restore requests and results.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- execute EBSI Service Desk restore requests.
- reporting back the taken actions and their result to EBSI Service Desk.

4.113PS12 - Suspension/disconnection response Process

4.11.1 GOAL

This process describes the process of restoring service to a node that has been taken offline due to a pending solution to be implemented.

4.11.2 SCOPE

This process covers the following items:

- **Documents** - textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Software** - applications developed and maintained within EBSI and released as open-source or put in operation by the European Commission.
- **Services** - provided by EBSI.
- **Virtual Machines** - provided by EBSI.

4.11.3 THE PROCESS

The Issue Resolution Process actors and their steps are presented in the following diagram**:**

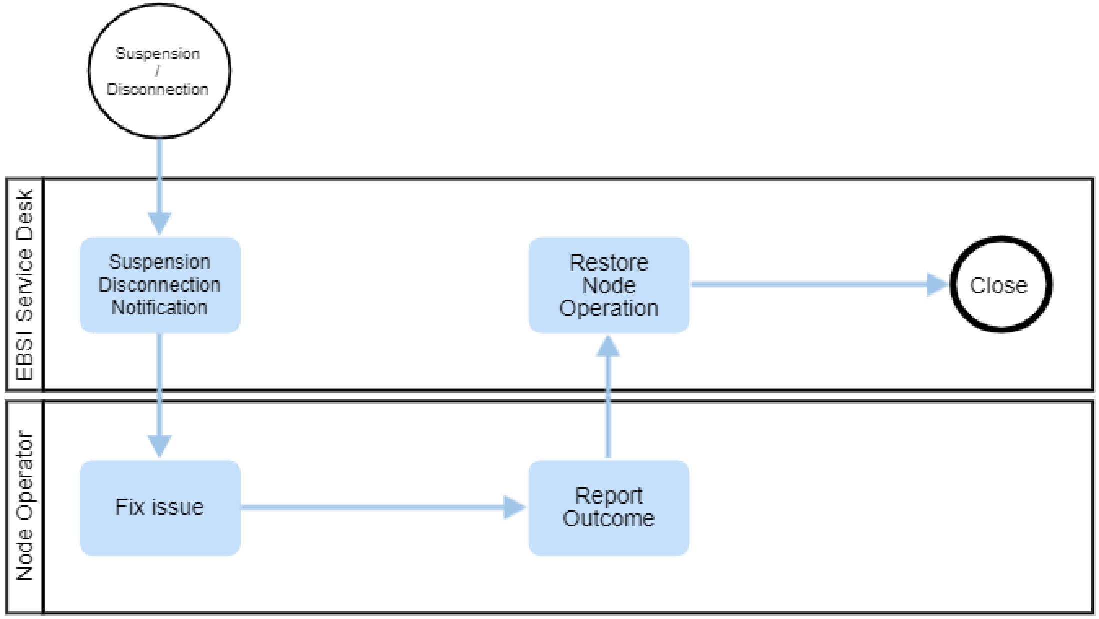


Figure 1: EBSI Suspension/Disconnect Response Process

4.11.4 PROCESS DESCRIPTION

- ***Step 0. Trigger: Node Suspension/Disconnection***

<*EBSI Service Desk*> receives a request via a Ticket including the reason for the disconnection/suspension and the attached evidence for the reason.

- ***Step 1. Suspension/Disconnection Notification***

<*EBSI Service Desk*> sends a notification to <*Node Operator*> informing they will be disconnected or suspended and includes the reasons and the evidence (if applicable) in the notification.

- ***Step 2. Fix issue***

<Node Operator> Applies a fix successfully solving the reported issue.

- ***Step 3. Report Outcome.*** <Node Operator> provides evidence of the fixed issue.
- ***Step 4. Restore Node Operation***

If the Node is suspended, <Node Operator> contacts <*EBSI Service Desk*> via a Unsuspend Request Jira Ticket where they must include:

· A reference to the suspension notification ticket they received when they were suspended.
· Evidence (attached to the ticket) proving that they have solved whatever cause granted the suspension.

If the Node is disconnected, <Node Operator> start the 3PS03 - Connection Request Process.

- ***Step 4. Close***

<Node Operator> closes the process.

4.11.5 ROLES & RESPONSIBILITIES

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are limited to:

- identifying, controlling and registering restore needs and backups for the proper handling in accordance to the established policies.
- notifying all relevant parties of the backup location and the need for a restore.
- keeping an updated record of backup locations, restore requests and results.

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- execute EBSI Service Desk restore requests.
- reporting back the taken actions and their result to EBSI Service Desk.

4.12 3PS13 - Validator Promotion Request Process

This process is responsible for the handling of requests to become a validator node validator.

4.12.1 GOAL

The goal of this process is to establish the prerequisites and steps to request, process, and keep track of validator nodes that participate in the network.

4.12.2 SCOPE

This process covers the following items:

- **Documents -** textual artefacts placed under a controlled life cycle management, e.g. specifications, project charters, rules of procedure.
- **Hardware** - EBSI infrastructure components.
- **Services** - provided by EBSI.

- **Software** - applications developed and maintained within the EBSI DSIs and released as open-source or put in operation by the European Commission.

4.12.3 THE PROCESS

Process activities are presented in the following diagram:

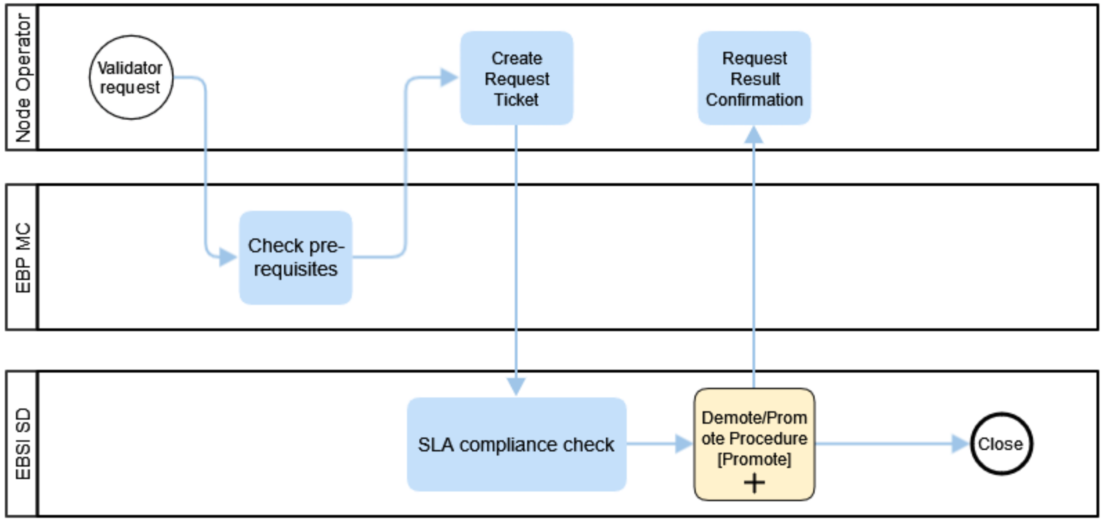


Figure 1: Validator Promotion Request

4.12.4 PROCESS DESCRIPTION

- ***Validator Request:*** <Node Operator> requests <EBP MC> to become validator.
- ***Check prerequisites***: <EBP MC> Checks that the NO complies with the prerequisites as per the Terms&Conditions.
- ***Create Request Ticket:*** On acceptance from <EBP MC> <Node Operator>, creates a ticket for <EBSI Service Desk> to validate and solve the request.
- ***SLA compliance check***: , <EBSI Service Desk> validates that the node meets the SLA targets.
- ***Demote/Promote Procedure:*** <EBSI Service Desk> follows the Demote/Promote Procedure (Promote action) to effectively promote the node as validator..
- ***Request Result Confirnation*** <EBSI Service Desk> communicates the result of the request to the <Node Operator>.
- ***Close:*** <EBSI Service Desk> closes the <validator request>

4.12.5 ROLES & RESPONSIBILITIES

Node Operator(s) refers exclusively to EBSI Node Operators who are stakeholders of the network and their dedicated devices (i.e. servers) authorised by the EBP to participate and run the EBSI Network in their capacity as operators of such devices. All these Operators together constitute the EBSI Network. They enable and ensure the execution of transactions, by e.g., keeping a copy of the blockchain ledger, accepting and producing new blocks, guaranteeing the consensus of the network and the integrity of the chain and transactions.

Their responsibilities within this process include (but not limited to):

- reporting discovered incidents to EBSI Service Desk for the proper handling in accordance with the established policies.
- implementing response strategies and recovering from the incident.
- reporting back the taken actions and their result to EBSI Service Desk.

EBP Member Country refers to a country participating in the European Blockchain Partnership, who holds sovereignty over the territory in which a Potential Node Operator will operate.

Their responsibilities within this process include (but not limited to):

- Assess the potential new NO to realise the application and provide, if needed, feedback on the legal documents signature process in accordance to the established policies.

EBSI Service Desk means the technical support services provided by the European Commission' Directorate-General for Informatics (DG DIGIT) and Directorate-General for Communications Networks, Content and Technology (DG CNECT) to facilitate the EBP members' work in developing the EBSI Software as funded under applicable funding Regulation and Work Programmes and the EBSI governance framework set out in these ToR. This may include support services such as providing specifications, software, support or testing services to enable access to and use of the EBSI Network under guidance of the EBP.

Their responsibilities within this process are:

- checking SLA compliance of nodes.
- following the procedure to promote/demote nodes.

Date: 30/03/2022