ECHA/2016/400

Title: Framework Contract for the provision of IT infrastructure services to the European Chemicals Agency in Helsinki (ECHA)

Competitive Procedure with Negotiation

Annex 4.1.1 Technical Specifications

Contents

1 INTRODUCTION 5

2 OBJECTIVES OF THE FRAMEWORK CONTRACT 6

2.1 Background 6
2.2 ECHA's goals 6
2.3 Elements for consideration 6

3 SERVICES IN SCOPE OF THIS FRAMEWORK CONTRACT 8

3.1 Current Mode of Operations (CMO) 9
3.2 Future Mode of Operation (FMO) 10
3.2.1 Cloud and infrastructure services 10

4 GENERAL ELEMENTS FOR IMPLEMENTATION OF THE FRAMEWORK CONTRACT 12

4.1 Methodologies 12
4.2 Language requirements 12
4.3 Services calendar 12
4.4 Audit 13

5 SECURITY 14

5.1 ECHA IT security model 14
5.2 IT security principles 14
5.2.1 Defence in depth / layered security 14
5.2.2 Least privileges and access 14
5.2.3 Risk driven 14
5.2.4 Weakest Link 15
5.2.5 Simplicity and standardisation 15
5.2.6 Continuous improvement 15
5.3 IT security objectives 15
5.3.1 Concept of perimeter 15
5.3.2 Network perimeter protection 16
5.3.3 Security of internal network 19
5.3.4 Operating System (OS) security 20
5.3.5 Data protection 21
5.3.6 Email security 21
5.4 Security requirements on the Contractor's operations 22
5.4.1 Service delivery facilities 22
5.4.2 Personnel security 22
5.4.3 Contractor's access to ECHA dedicated systems and Contractor's shared systems where ECHA data is stored or processed 22

6 SERVICES 25

6.1 Cloud and Infrastructure Services 26
6.1.1 Managed Datacentre Service 26
6.1.2 Managed ECHA LAN and WAN 36
6.1.3 Office automation 37
6.1.4 Backup and restore services 41
6.2 Service Management Portal 42
6.2.1 Service Catalogue 43
6.2.2 Service Management Tools 43
6.2.3 Technical Monitoring and Reporting 44
6.3 Service management 45
6.3.1 RACI matrix for Service Management 45
6.3.2 Service Desk 47
6.3.3 Set-up of the service/Termination of the service 48
6.3.4 Event management 48
6.3.5 Incident management 48

6.3.6 Problem Management *49*
6.3.7 Service Request Fulfilment *49*
6.3.8 Change Management *50*
6.3.9 Required Requests *51*
6.4 Consultancy services 54
6.4.1 Project Manager *55*
6.4.2 Consultant/senior consultant *56*
6.4.3 Junior Consultant *56*
6.4.4 Senior Engineer/Architect *57*
6.4.5 Junior Engineer/Administrator *58*
6.4.6 Trainer *58*
6.5 Transformation services 59
6.6 Security Services 60
6.6.1 Vulnerability management service *60*
6.6.2 Security monitoring *61*
6.6.3 Security incident response service *63*

7 IT BUSINESS CONTINUITY 65

7.1 Business continuity requirements on the Contractor's operations 65

8 TRANSITION OF SERVICES 67

8.1 Transition in 67
8.1.1 Model for transition *67*
8.1.2 Transition plan *68*
8.1.3 Service model *69*
8.1.4 User acceptance testing *70*
8.2 Transition out 71

9 GOVERNANCE 72

9.1 Roles 72
9.2 Levels of cooperation 72
9.2.1 Steering Committee Level *72*
9.2.2 Operational level *73*
9.3 Working with third parties 74
9.4 Knowledge sharing, documentation management, ticket management, performance monitoring 74
9.5 Customer satisfaction management and poor performance claim 75
9.6 Innovation 76

10 CONTINUOUS OPTIMISATION AND COST REDUCTION OVER TIME 77

11 SLA AND PRICING 78

11.1 Service Level Agreement 78
11.1.1 Service Bands *78*
11.1.2 Incident management *80*
11.1.3 Service and Change Requests *81*
11.1.4 Penalties *83*
11.2 Pricing 90
11.2.1 Price Catalogue *90*
11.2.2 Service Fees *90*
11.2.3 Daily fees and Effort Bands *92*
11.2.4 Separately billable services *93*
11.2.5 Acceptance of Service Readiness and Periodic Review *94*
11.2.6 Transition-in project *94*
11.2.7 Transformation services *95*
11.2.8 Invoicing and financial management *95*

12 ACCEPTANCE PROCEDURE 98

13 ANNEXES 99

14 GLOSSARY **100**

List of tables

Table 1 Current management of R4BP application (CMO) 8
Table 2 Future management of R4BP application (FMO) 8
Table 3 Security objectives, inbound traffic 16
Table 4 Security objectives, outbound traffic 19
Table 5 Security objectives, internal network 20
Table 6 Security objectives, operating systems 20
Table 7 Security objectives, data protection 21
Table 8 Security objectives, email 21
Table 9 Overview of services and their main actors 25
Table 10 Allowed tenancy in the FWC services 27
Table 11 RACI matrix for Service Management 46
Table 12 Incident classification. 48
Table 13 Required Requests 51
Table 14 Definition of Service Bands 78
Table 15 Services and their defined Service Bands 79
Table 16 Incident timers 81
Table 17 Request timers 82
Table 18 Combined impacts example 89
Table 19 Effort Bands definitions 92
Table 20 Example of the Effort Bands in conjunction with Service Bands 93
Table 21 Payment model for Transition-in project 94
Table 22 Transformation services volume discount table 95
Table 23 Example of a financial management hierarchy that would meet ECHA's needs 96

1 Introduction

This document is an integral part of the procurement documentation for Framework Contract ECHA/2016/400 for the provision of IT infrastructure services to the European Chemicals Agency in Helsinki (ECHA), and details the Technical Specifications.

This document is divided into several chapters as follows:

- Chapter 2 Objectives of the Framework Contract summarises the objectives that ECHA places to this Framework Contract.
- Chapter 3 Services in scope of this Framework Contract provides an overview of the services in scope and points to the documents describing the Current Mode of Operations (CMO).
- Chapter 4 General elements for implementation of the Framework Contract explains the horizontal requirements of the Framework Contract.
- Chapter 5 Security describes ECHA security model, principles and objectives, as well as defines security requirements for the Contractor to deliver the services in context of the Framework Contract.
- Chapter 6 Services details the required services of the Framework Contract.
- Chapter 7 IT Business Continuity contains the requirements on support services for the ECHA IT Business Continuity and Disaster Recovery activities and ECHA requirements on the relevant Contractor's operations.
- Chapter 8 Transition of services details ECHA's requirements for transitioning from the Incumbents' services to the Contractor's services.
- Chapter 9 Governance describes the governance model for the implementation of this Framework Contract.
- Chapter 10 Continuous optimisation and cost reduction over time describes the mechanism to manage efficiency improvement.
- Chapter 11 SLA and pricing defines the SLA targets and measurements and the pricing model.
- Chapter 12 Acceptance procedure defines the default acceptance procedure.
- Chapter 13 Annexes includes the list of annexes that are referred to in this document and are part of these specifications.
- Chapter 14 Glossary includes a glossary of the main terms used in this document.

To ensure coherence with requirements, modal verbs will be used as follows:

- **MUST/MUST NOT**: The definition or statement is a **minimum** requirement of the services.
- **SHALL/SHALL NOT**: The definition or statement is a requirement of the Specifications.
- **SHOULD/SHOULD NOT**: The definition or statement is a recommendation.
- **MAY**: The definition or statement is fully optional.

2 Objectives of the Framework Contract

2.1 Background

In 2012 ECHA started a transition towards outsourced hosting services, which was progressively implemented over three years. In particular, ECHA currently sources infrastructure services provided by one outsourcer (Incumbent), in conjunction with a second contractor (Networks Incumbent) managing the networks, based on two external datacentres and external service delivery centres.

In 2015 ECHA adopted an ICT asset-free strategy and transitioned its entire computing capacity to Infrastructure-as-a-service (completed in 2016). Such transition does not currently cover the network equipment.

Services under the existing agreements are secured for a time period that ECHA considers sufficient to establish this new Framework Contract (FWC) through competition and in order to complete the transition of services.

In parallel ECHA is performing a re-design of its networks in order to simplify and streamline the network managed services, on the one hand, and to facilitate the completion of the transition to full Infrastructure-as-a-service to cover also network-as-a-service, on the other. The aim is that this FWC will start when such transformation has already been completed or be very close to completion.

While the quality of the services to be provided by the Contractor are an important part of the FWC, clear focus will be put on awarding the Contract to a provider that can dramatically reduce the total cost of ownership of infrastructure services, including ECHA's internal resources (e.g. contract management, service management, issue follow-up, etc.). That being said, continuity of ECHA's existing infrastructure service portfolio is a top priority.

2.2 ECHA's goals

Therefore, this FWC is of strategic importance to ECHA. There are four key objectives that ECHA puts on it:

1. Providing secure access to high-quality, secure and state-of-the-art services for consumption by ECHA and its third parties.

2. Ensuring a cost effective and low-risk transition from ECHA's current infrastructure services in to the services available on this FWC.

3. Lowering the total cost of ownership of infrastructure services, including efforts made by ECHA staff for e.g. Contract and Service Management.

4. Streamlining of the service delivery via lean service management and effective governance, automation and standardisation of service delivery and integration of services in a multiparty ecosystem.

ECHA expects that the Contractor is in a position to achieve all these objectives.

2.3 Elements for consideration

There are some elements in the context of this FWC that are not totally defined at the moment of drafting the procurement documents of the procedure.

The leasing of the current ECHA office premises expires in 2019 and ECHA plans to relocate to new facilities in Helsinki by 1st January 2020. The new location will remain in Helsinki; however, the details of the new premises are not yet available. These aspects will, however, be spelled out in the course of this procurement procedure and factored into the potential negotiation phase.

As mentioned in the “background”, in this text and in Annex 1: IT Infrastructure Architecture (CMO), a target network topology (a.k.a. Net 2.0) is described. Whereas ECHA will target to have completed the transformation to this topology by the time this FWC will start, delays are possible. The impact of any delay would largely be the need of some legacy networks to be configured in the FMO infrastructure (ref. 3.2 Future Mode of Operation (FMO)). These aspects will, however, be spelled out in the course of this procurement procedure and factored into the potential negotiation phase. The Net 2.0 transformation will deliver a fundamental change to the current network infrastructure (ref. CMO in Annex 1: IT Infrastructure Architecture (CMO)).

3 Services in scope of this Framework Contract

ECHA is seeking a long partnership with a dynamic and proactive service provider to enable ECHA's next paradigm shift in its vision for sourcing cloud infrastructure services.

In this text, the service delivery mode expected to be provided by the Contractor will be called **Future Mode of Operations** (FMO). The on-going services (most of which are provided by the current outsourcers) are here called the **Current Mode of Operations** (CMO).

After transition and set-up, the Contractor **shall** deliver the service according to the FMO. ECHA targets transition without any major transformation of the services and related performance aspects during transition. However, the technical solutions in the background chosen by the Contractor **may** be different from those that ECHA currently uses.

Transition to FMO with minimum effort, time, required adaptation of services and cost is key to a successful bid. The level of automation (expectation: high) and use of human resources (expectation: low) play a crucial role, particularly the use of ECHA human resources. Below is an example of the envisaged change from CMO to FMO for the service stack for the ECHA bespoke application Registry for Biocidal products (R4BP).

Table 1 Current management of R4BP application (CMO)

Service	Actor
Application development	Third party
Application management	Incumbent (production environment only) Third party (non-production environments)
Database management	Incumbent (production environment only) Third party (non-production environments)
Authentication services **Hardware token based authentication service**	Incumbent (production environment only) Network Incumbent
OS management	Incumbent
IaaS	Incumbent
Managed network services	Network Incumbent

Table 2 Future management of R4BP application (FMO)

Service	Actor
Application development	Third party
Application management	Third party
Database management	Third party
Authentication services **RSA authentication**	Third party Contractor
OS management	Contractor

Service	Actor
Cloud and infrastructure services	Contractor
~~**Managed network services**~~	~~N/A~~

Due to the duration of this FWC and the fast evolution of the market in scope, it is likely that further transformation projects will be sourced via this FWC and it is also possible that the application of the innovation mechanism described in section 9.6 Innovation will become necessary.

Important note: The CMO annexes will be available only in Phase II for selected candidates

3.1 Current Mode of Operations (CMO)

The CMO is described in more detail in the following CMO annexes:

- Annex 1: IT Infrastructure Architecture (CMO)
- Annex 2: Network Service Model (CMO)
- Annex 3: IT BCP - IT Continuity Technical Preparedness Plan (CMO)
- Annex 4: ICT Change Management (CMO)

ECHA sources infrastructure capacity services as IaaS. Such services cover compute and storage capacity, but not yet Network-as-a-Service. The IaaS platform consists of a private cloud and back-up to disk. The Incumbent hosts such a platform in two datacentres (PDC/A and PDC/B) connected via dark fibre, DWDM and dual Internet uplinks. ECHA is also connected to the datacentres via another set of dark fibres and DWDM.

Other still ECHA-owned infrastructure, such as core networking equipment and s-TESTA equipment, are co-located there.

The Incumbent's private cloud infrastructure uses VMware based virtualisation with synchronous storage replication between 2 VCE vBlocks, both hosted in different datacentres.

In conjunction with the IaaS, ECHA uses the Incumbent's dedicated DataDomain system for backup-to-disk. The services are delivered in two datacentres for cross-datacentre backups.

Operating systems, of mainly Windows Server 64-bit and Red Hat Enterprise Linux 64-bit flavours, are to a large extent managed by the Incumbent for ECHA.

Furthermore, the Incumbent manages the following ECHA systems:

- Microsoft Exchange
- Windows DFS & SMB (File Shares)
- NFS
- Windows Active Directory
- Windows DNS
- Windows DHCP
- Windows PKI

- Microsoft Terminal Services for System Administration.

The Incumbent also provides:

- Off-site back-up tape staging and storage
- Consultancy services.

The datacentre networking hardware is still largely owned by ECHA. The Network Operations Centre (NOC) services and management of the network hardware and related services are outsourced to another party, in this text called the Network Incumbent. The Network Incumbent also manages ECHA's LAN and provides on-premise and off-premise support and maintenance.

3.2 Future Mode of Operation (FMO)

The focus on innovation for the FMO will be on providing also datacentre-Network-as-a-service.

ECHA believes that lowering the Total Cost of Ownership (TCO) for the services is achievable mainly through automation, standardisation, continual improvement and integration, lean service management and effective governance.

While the initial set of services to be provided is to ensure a fast and smooth transition with minimal transformation, it is to be expected that ECHA's appetite for further improvement and streamlining of service delivery to grow. Such improvements will be pursued through transformation projects and the rolling plan for optimisation (ref. section 6.5 Transformation services and chapter 10 Continuous optimisation and cost reduction over time).

ECHA wishes to utilize a set of highly automated and standardised Cloud Services (primarily private cloud, but also Trusted Community) and infrastructure services.

The private cloud infrastructure **must** be provided on a state-of-the-art cloud platform for ECHA to ensure performance and to mitigate the need for a major hardware refresh for the length of the FWC. This platform **must not** have been used for service delivery for ECHA before.

Furthermore, ECHA wishes to the highest extent possible to facilitate repeatable provisioning of services with minimum effort and error. While ECHA has certain constraints and requirements for delivery of services, where automation and standardisation is possible ECHA is willing to adapt its processes to facilitate lowered TCO. The driving force behind this is to allow the Contractor (the winning Tenderer) to provide their best possible service at the best possible price to ECHA and its multiparty ecosystem.

Utilisation of human resources **shall** be kept to a minimum wherever possible to avoid duplication of work, knowledge transfer, risk of error, general overhead and cost.

The aforementioned services will to a large extent be consumed by other ECHA contractors/third parties, for example, providers for software development and application management services. The ability of the Contractor to handle issues related to this integration of service delivery channels is therefore crucial.

3.2.1 Cloud and infrastructure services

The cloud and infrastructure services are the core services of the FWC. The Contractor **shall** provide all datacentre, infrastructure and connectivity services required to run ECHA's virtual datacentre, including LAN and WAN services and remote connectivity. Enabling IT business continuity is part of these services.

The Cloud Services **shall** provide "networking as a service" based on the "Net 2.0" topology as described in Annex 1: IT Infrastructure Architecture (CMO).

Furthermore, office automation services are to be included, for the most part Windows AD and Exchange services.

The services **shall** be manageable to the largest possible extent via a Service Management Portal (ref. section 6.2 Service Management Portal) that includes service management tools.

4 General elements for implementation of the Framework Contract

This chapter refers to some general elements that underpin the implementation of the FWC

4.1 Methodologies

The methodology used by ECHA for project management is based on Prince2. For the service management, the Agency is using ITIL good practices.

The use of a methodology based on PMI/Prince2, ISO2700x and ITIL is needed for the provision of this FWC professional services.

Whenever providing consultancy services in the context of projects or services run by ECHA the Contractor undertakes to perform in accordance with ECHA guidelines, procedures and tools, as disciplined in the related specific contracts.

ECHA has endeavoured over the years to standardise, and avoid complexity where possible, largely concentrating the complexity into the Applications. This has enabled the organisation to standardise on for example computing requirements and Operating System flavours.

To be noted, ECHA has services in its portfolio that are outside the scope of the FWC that depend heavily on services within the scope of the FWC. Most notable are Active Directory, DNS and Load Balancing services. ECHA expects the Contractor to develop an understanding of the full ECHA IT landscape to understand the interdependencies, and to take a pro-active role in those areas. The Contractor **shall** act as an expert in the technologies in the FWC, taking a leading role and acting as a partner with ECHA. In other words, a factory approach to only implement what is requested by ECHA and not understand the impact of those requests on ECHA's complete IT landscape would not be appropriate (ref. section 9.3 Working with third parties).

The Contractor **shall** endeavour to understand ECHA as an organisation, understand the needs of the organisation and understand the IT landscape. The Contractor **should** establish a methodology to ensure this level of understanding is achieved, and specifically how it would be maintained in the Contractor's organisation.

4.2 Language requirements

The working language of the Agency is English. The English language **shall** be used throughout the execution of this FWC for all communication, reports and other documentation.

Therefore, it is required that all members of the Contractor's staff involved in the FWC have working knowledge of spoken and written English, at level B2 as a minimum.[1] ECHA reserves the right to request the replacement of a resource if s/he does not have the adequate knowledge of English as deemed necessary for the execution of the tasks.

4.3 Services calendar

As a rule, work at ECHA premises (i.e. on-site) will be carried out on normal working days for at least 8 working hours between 8:00 and 20:00. For Times and Means contracts, the days and hours worked per resource will be verified by ECHA against the Agency's time-recording system.

For on-site work, normal working days are Monday to Friday, except for ECHA holidays as published on ECHA website. Such holidays can differ from national ones, and will be notified every year in advance for the upcoming year. In exceptional cases and only upon ECHA request, work could be ordered outside that window and/or on week-ends.

---

[1] According to Common European Framework of Reference for Languages: Learning, Teaching, Assessment (CEFR). See self-assessment grid in https://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr

4.4 Audit

As provided for in Articles I.22 and II.24 of the draft FWC, the Contractor undertakes to accept ECHA audits, including third party audits on behalf of ECHA, related to the scope of this FWC and to collaborate, at no charges for ECHA, by providing access to their internal procedures, to the records thereof, to their facilities including data centres and service delivery centres.

The Contractor undertakes to collaborate with ECHA, at no charges, in the analysis of the audit findings, potentially supplementing the information and documentation provided during the audit for the sake of clarification.

The Contractor undertakes to timely address – at no cost for ECHA - the audit findings whenever they regard matters of incompliance with the provisions of this FWC or a valid specific contract. Such commitment **shall** be sustained until a successful closure of the audit findings, normally ascertained in a follow-up audit.

The Contractor commits to addressing the other audit findings too, on request by ECHA. In this case, the agreed implementation tasks will be handled as “transformation project” and can be chargeable to ECHA at the conditions agreed for transformation projects.

5 Security

5.1 ECHA IT security model

ECHA applies an IT security model driven by a set of IT *security principles* (ref. section 5.2 IT security principles) and *security objectives* (ref. section 5.3 IT security objectives). Furthermore, a set of *security requirements* for operations (ref. section 5.4 Security requirements on the Contractor's operations) are provided.

In this section we describe the principles and their application to ensure the identified security objectives and the security requirements that **must** be followed. The Contractor **shall** play the role indicated in the following sections in the pursuit of the security objectives.

The Contractor **shall** provide the specific security services defined in section 6.6 Security Services and, where appropriate, any of the security related components of other services that are described in chapter 6 Services.

5.2 IT security principles

The Contractor **shall** ensure that ECHA's IT security principles below are followed during the execution of the FWC. These are the minimum set of IT security principles that ECHA requires and are not to be seen as limiting the Contractor to have other principles as well.

5.2.1 Defence in depth / layered security

The principle of defence-in-depth is that layered security mechanisms increase security of the system as a whole. The idea is that if one security layer fails, other layers still protect the system. For example, protection of a critical ECHA internal asset against external threats does not rely only on one layer (e.g. a firewall), as this layer (e.g. the firewall) can usually be circumvented by a determined attacker. Instead, several security mechanisms are in place to complement the protection.

ECHA applies the defence–in-depth principle by following a risk driven approach: the number of layers in place depends on which asset is protected (impact of the risk) and on the probability that the relevant threats can bypass the protection layers (likelihood of risk occurrence). However, whenever critical ECHA assets are protected, single points of failure are always avoided by applying multiple protection layers.

The layered security approach is not only for strong prevention but also for helping the implementation of effective detection and reaction; attacks can be much easier to detect if several protection layers need to be broken and there is enough time to react to intrusions before the final target is attained.

5.2.2 Least privileges and access

The principle of least privilege states that a subject be given only those privileges needed for it to complete its task. This means, for example, that every program, process and user of a system operates using the least set of permissions and privileges necessary to complete their job. Primarily, this principle limits the damage that can result from unauthorised, unintentional or improper uses of privileges. While the principle is more related to (secure) software development and user access management it is also applied in operating system hardening and network access control.

5.2.3 Risk driven

Security choices are to be based on likelihood and impact of the relevant risks and cost of mitigating the risk. Risk management objectives are the key drivers for the selection of security controls.

5.2.4 Weakest Link

Overall security can be only as effective as the weakest link in the chain from end-to-end. Thus, the weakest link principle states that the whole chain be adequately protected by similar level of protection.

5.2.5 Simplicity and standardisation

As complexity is often an enemy of security and a friend of attackers, one of security principles is simplified architecture. Therefore unnecessary complexity, both from a design perspective and from an implementation perspective, is to be avoided and the security mechanisms be pervasive, simple, scalable, and easy to manage.

While complexity increases the risk of problems, also the risk of security problems, it cannot be completely avoided. Also, the simplification can be a conflicting principle with the defence in depth and least privileges. If the principles have conflicts, a risk-driven approach is applied to find a balance between the principles.

5.2.6 Continuous improvement

IT security requires continuous improvement. Only ongoing improvement allows ECHA to sustain the state of information security at the current, acceptable level. While operational level improvements happen frequently based on evolution of the threats, continuous improvements cover also mid- and long-term tactical and strategic security aspects.

5.3 IT security objectives

The Contractor **shall** ensure that ECHA's IT security objectives below are fulfilled during the execution of the FWC. These are the minimum set of IT security principles that ECHA requires and are not to be seen as limiting the Contractor to have other principles as well.

5.3.1 Concept of perimeter

The ECHA (internal) IT infrastructure is located inside the virtual perimeter and (non-public) ECHA data is stored and processed within the virtual perimeter.

While internal IT services can be accessed only from inside the ECHA perimeter, a selected set of ECHA's public services (e.g. the website) are accessible from outside the perimeter.

In the context of this FWC, ECHA (non-public) information is encrypted against unauthorised access when transmitted or stored outside of the perimeter (e.g. data transmitted between data centres).

Extensions of the perimeter:

- Client/user/IT-environment can be **within ECHA perimeter** either by being physically (or logically) part of ECHA's internal network or virtually by being compliant with ECHA's requirements for remote access.
- Thus, a **virtual perimeter** is an extension of the physical/logical perimeters and the security objectives are not reduced.

ECHA users

ECHA users, when they use their ECHA client, there are two options work inside the perimeter:

- A client is directly connected to ECHA's office LAN. Then their client is inside the network perimeters and behind the perimeter protection.
- A client located outside the office LAN has a VPN connection to ECHA internal network over the internet. In this case, it logically belongs to the internal network and the network perimeter protection is still effective[2].

[2] As VPN tunnel forces all the traffic through the office network, the traffic to/from the external addresses goes through the security measures in the network perimeters.

Authorities' users

ECHA grants access over the internet to some of its IT systems to Competent Authorities in the EU member States ("Authorities" in the text). These users never have a direct connection to the ECHA LAN. However, if they are fully compliant with the ECHA standard security requirements they are granted access to a limited set of ECHA IT services (according to the principle of least privileges), via a secure remote access solution. Therefore, they are within the ECHA virtual perimeter. One of the mandatory security requirements is that the Authorities have adequate perimeter protection in place to protect their IT environment used to access ECHA IT systems.

IT Contractors' users

IT Contractors' personnel working offsite do not have direct connection to the ECHA office LAN. If they comply with ECHA policy on IT contractors remote access, they are granted access, based on the access level category they belong to. Therefore, they are within the ECHA virtual perimeter. One of the mandatory security requirements is that the Contractor have adequate perimeter protection in place to protect their IT environment used to access ECHA IT systems.

As IT contractors usually need to have privileged access to a high number of back-end production systems, an additional security layer is in place to control IT contractors' remote access (ECHA terminal server concept) in addition to the standard remote access solution.

Note: The technical concept of ECHA remote access, is described in Annex 1: IT Infrastructure Architecture (CMO); requirements on remote access are in section 6.1.1.8 Remote Access.

5.3.2 Network perimeter protection

5.3.2.1 Inbound traffic

- Inbound connections over the internet/other networks are allowed only to ECHA public IT services (all other traffic is blocked), applying **network level access controls** with the necessary security features (packet level filtering, state-full filtering, application layer filtering) with two devices/applications fulfilling dual (internal and external) firewall functionalities
- A **centralised access point** for accessing all the public ECHA web based IT services in order to:
  - terminate the connections and provide a network stack (that will not be vulnerable in the same ways as web server) for clients instead of the web servers;
  - application level logging;
  - capability to implement (application level) access controls and filters separately from the web servers if needed
  - terminate SSL/TLS encrypted connections
- The **content of the permitted network traffic is monitored**, attacks and malicious traffic is blocked. We apply signature based detection for requests/traffic to public web based services.

Table 3 Security objectives, inbound traffic

Security objective	Requirement (high level how)	Contractor	ECHA	Principles
Allow access from the internet only to public services, prevent access to the internal network environment	Provide network access control Implement dual firewall scheme Preferably firewall technology from two different vendors; it provides an added level of security against a software-specific exploitable vulnerability	Provide as service component; 6.1.1.10.1 External Firewall Provide as service component;6.1.1.10.2 Internal Firewall	Define rules/policies	Defence in depth; Least privileges and access
Prevent the direct network connections from Internet to the public services; provide a secure network stack (that will not be vulnerable in the same ways as web server) for clients	Provide a centralised point of access to public web-based services; Implement reverse proxy Implement application level logging and provide ECHA and third parties access to the application level logs	Provide as service component;6.1.1.10.4 Reverse Proxy	Define rules/policies	Defence in depth; Simplicity and standardisation
Enable centralised security monitoring at perimeter level for encrypted traffic;	Provide capability to terminate /TLS encryption in a centralised point	Provide as service component;6.1.1.10.4 Reverse Proxy	Provide public SSL certificates Internal SSL certificates are part of the PKI	Simplicity and standardisation

Security objective	Requirement (high level how)	Contractor	ECHA	Principles
Support mitigation actions against vulnerabilities related to web-based services	Provide capability to activate application level access controls and filters separately from the web servers, e.g. "virtual patching" (i.e. if a vulnerable application cannot be updated immediately, exploitation of the known vulnerability is prevented by activating an access control or a filter e.g. by using a feature in web application firewall)	Provide as service component;6.1.1.10.3 Web Application Firewall	Request activation	Defence in depth
Attacks and malicious traffic against public ECHA services is detected and automatically blocked (in defined cases)	Implement detection of attacks and malicious traffic to public web based services	Provide as service component;6.1.1.10.3 Web Application Firewall Provide as service component; 6.6.2 Security monitoring	Define rules and policies	Defence in depth / layered security

5.3.2.2 Outbound traffic

- **Network level access control** for outgoing traffic to the internet applying **network level access controls** with the necessary security features (packet level filtering, state-full filtering, application layer filtering) with two devices/applications fulfilling dual (internal and external) firewall functionalities
- No direct internet connections; clients have access to the internet only through the centralised control point fulfilling the following security requirements:
    - Website category based filtering; blocking access to blacklisted categories
    - Investigation for downloaded content

Table 4 Security objectives, outbound traffic

Security objective	Requirement (high level how)	Contractor	ECHA	Principles
Allow only defined network traffic to the internet. By default, clients have internet access only through the centralised control point, i.e. no direct connections to internet	Provide network access control Implement dual firewall scheme Preferably firewall technology from two different vendors; it provides an added level of security against a software-specific exploitable vulnerability	Provide as service component;6.1.1.10.2 Internal Firewall Provide as service component 6.1.1.10.1 External Firewall	Define rules/policies	Defence in depth; Least privileges and access
Allowed traffic to the internet happens only through a centralised control point	Provide capability to control which application level protocols have internet access Provide capability to hide clients from the internet Inside perimeter connections to the internet are channelled through the client proxy	Provide as service component; 6.1.1.10.5 Client Proxy		Simplicity and standardisation; Defence in depth
Block access to malicious or inappropriate web sites	Provide category based content filtering for websites	Provide as service component; 6.1.1.10.5 Client Proxy	Define categories	Defence in depth
Filter out malicious content downloaded from the internet	Provide capability to detect malicious content in downloads	Provide as service component; 6.1.1.10.5 Client Proxy Recommend best practices		Defence in depth

5.3.3 Security of internal network

The main security measures:

- **Segregation of networks** based on their security level (trust zone) and, within the same security level, based on purpose of the network. ECHA has implemented system administration networks, server networks, client networks, guest networks, conference centre networks and a DMZ network. Occasionally ECHA requires changes to such configurations. Systems are located to the virtual networks based on their security level/ requirements and role/purpose. Internal ECHA networks are completely separated from external ECHA networks.

- Network **access controls for traffic between segregated networks** (inter – VLAN traffic)
    - Network and system specific access rules
    - User specific access rules
- Wireless network **(Wi-Fi) security**

ECHA has a guest wireless network and an internal wireless network. The security level is different.

Internal wireless network:

- Network Access Control (access granted only to authorised ECHA clients)

Both wireless networks:

- Protection of confidentiality and integrity of network traffic over the wireless radio link (WPA2 with AES encryption)

Table 5 Security objectives, internal network

Security objective	**Requirement (high level how)**	**Contractor**	**ECHA**	**Principles**
Systems connected to ECHA networks are adequately segregated and protected with network level controls against the threats inside the network.	Provide the capability to control the traffic between internal segregated networks based on the internal firewall (default denied) Such capability to support logging	Provide as service component; 6.1.1.10.1 Internal Firewall	Define rules	Defence in depth; Least principle and access
Wireless networks (Wi-Fi) are adequately protected against unauthorised access	Provide Network Access Control for the internal Wi-Fi based on device certificates Such capability to support logging	Provide as service component; 6.1.2.1 Managed ECHA LAN	Manage device certificates	Defence in depth; Weakest link
Confidentiality and integrity of network traffic sent over the wireless radio link adequately protected	Provide strong encryption over the wireless radio link	Provide as service component; 6.1.2.1 Managed ECHA LAN		Defence in depth; Weakest link

5.3.4 Operating System (OS) security

Security measures:

- System hardening / secure configuration
- Malware protection

Table 6 Security objectives, operating systems

Security objective	Requirement (high level how)	Contractor	ECHA	Principles
OSs are securely configured against unauthorised access, misuse of privileges and inappropriate use	Configure OS according to state-of-the-practice hardening guidelines (taking into account justified exceptions due, for example, to tailored applications)	Provide as service component; 6.1.1.5 Managed OS	Validate the secure configuration for compatibility with other IT services	Defence in depth
Operating systems are protected against malware infections	Provide antivirus running on Windows servers Regularly patch OSs	Provide as service component; 6.1.1.5 Managed OS		

5.3.5 Data protection

Security measures:

- Secure disposal of data media

Table 7 Security objectives, data protection

Security objective	Requirement (high level how)	Contractor	ECHA	Principles
Data media, including backups, are adequately secured against unauthorised physical access	Provide physically secured place for all data media stored provide encryption capabilities (also to be applied as an alternative to physically secured storage place) Data media are securely disposed	Provide as service component; 6.1.1.2 Managed Datacentre Facilities	Classification of data	Simplicity and standardisation; Defence in depth

5.3.6 Email security

Table 8 Security objectives, email

Security objective	Requirement (high level how)	Contractor	ECHA	Principles
Filter out malicious emails	Provide capabilities for detection and out-filtering of spam, phishing and malware messages, at least at two layers (e.g. gateway and server)	Provide as service component; 6.1.3.1 Email and calendaring service		Defence in depth
Protect confidentiality of e-mail traffic between ECHA and selected parties	Provide capabilities to encrypt emails and/or email traffic to implement transparent encryption for users (e.g. using forced SSL/TLS tunnels between e-mail servers)	Provide as service component; 6.1.3.1 Email and calendaring service		

5.4 Security requirements on the Contractor’s operations

The Contractor **must** ensure that ECHA’s IT security requirements below are fulfilled during the execution of the FWC. These are the minimum set of requirements that ECHA requires and are not to be seen as limiting the Contractor to have other in place as well.

5.4.1 Service delivery facilities

5.4.1.1 Datacentres

The datacentre facilities **must** be located within the territory of EU member states during the whole lifetime of service.

The datacentres **must** be strictly protected against unauthorised physical access. The Contractor **must** have a formal policy and clear instructions as to how visitors are managed. Only visitors with clear business justification are allowed to visit the data centres. Visitors’ identities **must** be checked and they **must** be formally registered before entered to datacentres. Contractor’s staff **must** escort and oversee the visitors at all times during their visit.

The physical access control **must** be implemented and maintained according to the relevant industry best practices, covering preventive, detective and reactive security measures. In particular, verification of the clean criminal record, or an equivalent background check as allowed by the legislation of the relevant EU member state (ref. section 5.4.2 Personnel security) **must** be performed for those having access rights to the data centre facilities (including e.g. cleaners and facility management staff, if not managed as visitors).

The datacentre facilities and related services **must** be audited at least annually by independent third party auditors. A SOC 2 (or equivalent) audit report **must** be made available to ECHA after the completion of the audit.

5.4.1.2 Other service delivery facilities

Any other service delivery facility **must** be located within the territory of the EU member states. They **must** be adequately protected against unauthorised physical access. The Contractor **must** have a formal policy and clear instructions as to how visitors are managed and controlled during their visits to such facilities.

5.4.2 Personnel security

The Contractor **must** maintain an up-to-date list of their service delivery personnel who have access to ECHA dedicated systems and Contractor’s shared systems where ECHA data is stored or processed.

The Contractor **must** verify the background of its personnel, by performing a visual verification of a clean criminal record, or an equivalent background check as allowed by the legislation of the relevant EU member state, before authorising such access.

The Contractor **must** have formal HR processes and practices in place (e.g. for recruitment, change of job descriptions and termination of employment) and manage any related security risks.

5.4.3 Contractor’s access to ECHA dedicated systems and Contractor’s shared systems where ECHA data is stored or processed

Access **must not** be allowed outside the territory of the EU member states.

Without mutual agreement, ECHA data **must not** be copied outside of such systems, not even for temporary purposes, except for data generated in the performance of managed services: for example, Contractor log data, monitoring data, asset/CMDB info etc.

Teleworking access from outside the Contractor’s service delivery facilities (ref. 5.4.1 Service delivery facilities) **must** be explicitly authorised by ECHA. In such assessment, ECHA will consider: the justification (e.g. on-call work outside of normal working hours; staff policies of the Contractor) and compliance with ECHA's security rules for teleworking (indicative teleworking rules are presented in Annex 5: ECHA Indicative teleworking rules and requirements for IT hosting contractor).

Only the Contractor’s authorised users with valid business justification can have access to ECHA dedicated systems and Contractor’s shared systems where ECHA data is stored or processed (with the exception of public services available from the internet). The Contractor **must** have an access policy applying the principle of least privilege and keep the access rights up-to-date. The Contractor **must** keep an audit trail of which access rights have been granted to whom for the duration that services are delivered to ECHA.

The Contractor’s logical access (except to public services available from Internet) for service delivery purposes is allowed only from a dedicated environment (the “system management environment”), i.e. access from the Contractor’s normal office automation IT-environment **must** be blocked.

The “system management environment” **must** be highly secure and sufficiently isolated from the Contractor’s other IT environments, according to the following requirements:

- Only authorised service delivery staff members can have access to the “system management environment”. Access to this environment is managed according to the Contractor’s formal access right management process.
- Access is opened only on successful multi-factor (min. two) authentication and log-on/gain access to the “system management environment”.
- Only personal (i.e. non-shared) user accounts are permitted.
- The “system management environment” is not used for any other purposes than system administration and management (e.g. web browsing). Access to the office email and other similar services are blocked.
- Controls are in place to automatically lock out or block access to the “system management environment” after a reasonably short inactivity period.
- All the systems in the “system management environment” are adequately protected, security hardened and regularly patched
- In the “system management environment”, risks related spreading of malwares or malicious software run are strictly mitigated. Application installation and running is controlled, and only applications with justified business reasons are allowed to run in that environment.
- In order to detect potential vulnerabilities and weaknesses, and continuously improving security, security of the “system management environment” are regularly (at least once a year) verified by performing audits and penetration testing
- Adequate access and audit logs from the “systems management environment” are kept to identify who has accessed such environment and further proceeded to ECHA dedicated systems or Contractor’s shared systems where ECHA data is stored or processed
- Access and audit logs are protected from unauthorised tampering or removal and regularly monitored in order to detect unusual activities
- The “system management environment” is under continuous security monitoring and intrusion detection. Detected suspected intrusions and unusual activities are promptly investigated and responded to.

The Contractor **must** be able to map access to an individual person (individual user accounts). Non-personal accounts (e.g. root) are allowed to be used only when strictly necessary. The

Contractor **must** have a system/procedure in place to formally manage credentials related to non-personal accounts, usage of these accounts **must** be controlled, and who has been using the accounts identified.

The Contractor **must** adequately monitor the access and activities of their personnel, particularly those with privileged access rights.

6 Services

The services in scope for the FWC are presented in the sections below.

The table below provides an overview of the services and main their actors.

Table 9 Overview of services and their main actors

Service	Scope	Supply	Demand
6.1.1 Managed Datacentre	Managed Datacentre Facilities Managed Datacentre WAN Cloud Service Managed OS Managed Load Balancing Internet Access Datacentre hosting of ECHA owned hardware Security components of the Managed Datacentre Service	Contractor (and related sub-contractors/suppliers/vendors)	ECHA, third parties
6.2 Service Management Portal	Service Catalogue Service Management Tools Technical Monitoring and Reporting	Contractor (and related sub-contractors/suppliers/vendors)	ECHA, third parties
6.1.1.8 Remote Access	Access as if inside perimeter over the internet	Contractor (and related sub-contractors/suppliers/vendors)	ECHA, third parties
6.1.2 Managed ECHA LAN and WAN	Managed ECHA LAN Managed ECHA WAN Security components of the Managed Datacentre Service	Contractor (and related sub-contractors/suppliers/vendors)	ECHA, third parties
6.1.3 Office automation	Managed Email and calendaring service Managed Active Directory Services Managed DNS Service Managed file shares (	Contractor (and related sub-contractors/suppliers/vendors)	ECHA, third parties

Service	Scope	Supply	Demand
	DFS & SMB) Managed DHCP service Managed Public Key Infrastructure (PKI)		
6.1.4 Backup and restore services	Managed Backup according to ECHA backup policy Restore-from-backup service Managed Backup and restore services according to ECHA backup policy	Contractor (and related sub-contractors/suppliers/vendors)	ECHA
6.3 Service management	Service Desk Service management processes	Contractor (and related sub-contractors/suppliers/vendors)	ECHA, third parties
6.4 Consultancy services	Provision of consultants either at ECHA premises or off-premises Transformation projects	Contractor (and related sub-contractors/suppliers/vendors)	ECHA
6.6 Security Services	Vulnerability management service Security monitoring Security incident response service	Contractor (and related sub-contractors/suppliers/vendors)	ECHA

6.1 Cloud and Infrastructure Services

After the completion of the transition project, the Contractor **shall** own and manage the IT infrastructure components required to deliver Cloud and Infrastructure Services to ECHA, with the exception of the IT infrastructure for delivering the LAN services.

The Contractor **shall** also provide all required software licenses and related maintenance unless explicitly so specified in the sections below.

6.1.1 Managed Datacentre Service

The Managed Datacentre Service **shall** provide all required datacentre facilities, connectivity solutions, hardware and software to deliver highly automated cloud infrastructure services to ECHA, in the form of a **virtual private datacentre** running on a cloud infrastructure and, in the case of multi-tenancy, properly segregated from possible other tenants or the Contractor's management tools on all layers of the managed datacentre.

6.1.1.1 Tenancy requirements

Some services in the scope of the FWC have special conditions regarding the tenancy. The following terminology will be used:

- Private
- Trusted Community
- Shared

Private: means single-tenancy with ECHA as the single tenant. The Contractor **must not** give access to anyone else than ECHA, it's agreed third parties, the Contractor themselves and the agreed subcontractors and vendors.

Trusted Community: means multi-tenancy with multiple tenants that are the Contractor's customer, fulfil the same or equivalent security requirements and belong to the following categories: other EU institutions, EU Member States public administrations or international governmental organisations.

Shared: means multi-tenancy with multiple tenants that are the Contractor's customers.

Important note: The IT security principles (ref. 5.2 IT security principles) **shall**, the IT security objectives (ref. 5.3 IT security objectives) **shall** and the IT security requirements (ref. 5.4 Security requirements on the Contractor's operations) **must** be respected regardless of tenancy.

The table below depicts ECHA's current requirements for tenancy. These **may** be changed later upon agreement.

Table 10 Allowed tenancy in the FWC services

Service	**Private**	**Trusted Community**	**Shared**
6.1 Cloud and Infrastructure Services			
6.1.1 Managed Datacentre			
6.1.1.2 Managed Datacentre Facilities	Yes	Yes	Yes
6.1.1.3 Managed Datacentre WAN	Yes	Yes	Yes
6.1.1.4 Cloud Service	Yes	Yes (upon agreement)	No
6.1.1.5 Managed OS	Yes	Yes	No
6.1.1.6 Managed Load Balancing	Yes	Yes (upon agreement)	Yes (upon agreement, conditional)
6.1.1.7 Internet Access	Yes	Yes (upon agreement)	No
6.1.1.8 Remote Access	Yes	Yes (upon agreement)	No
6.1.1.9 Datacentre hosting of ECHA owned hardware	Yes	Yes	Yes
6.1.1.10 Security components			

Service	Private	Trusted Community	Shared
6.1.1.10.1 External Firewall	Yes	Yes (upon agreement)	Yes (upon agreement, conditional)
6.1.1.10.2 Internal Firewall	Yes	Yes (upon agreement)	No
6.1.1.10.3 Web Application Firewall	Yes	Yes (upon agreement)	No
6.1.1.10.4 Reverse Proxy	Yes	Yes (upon agreement)	Yes (upon agreement, conditional)
6.1.1.10.5 Client Proxy	Yes	Yes (upon agreement)	No
6.1.2 Managed ECHA LAN and WAN			
6.1.2.1 Managed ECHA LAN	Yes	No	No
6.1.2.2 Managed ECHA WAN	Yes	N/A	Yes (upon agreement, if traffic is encrypted)
6.1.3 Office automation			
6.1.3.1 Email and calendaring service	Yes	Yes (upon agreement)	No (yes only for messaging security)
6.1.3.2 Windows services	Yes	Yes (upon agreement)	No
6.1.4 Backup and restore	Yes	Yes (upon agreement)	No. Offline backup service can be shared if data in backups is encrypted
6.2 Service Management Portal	Yes	Yes (upon agreement)	No
6.6 Security Services			
6.6.1 Vulnerability management service	Yes	Yes	Yes
6.6.2 Security monitoring	Yes	Yes	Yes (recommended)
6.6.3 Security incident response service	Yes	Yes	Yes

6.1.1.2 Managed Datacentre Facilities

The Contractor **shall** provide two secure, modern and state-of-the-art datacentres of equal and sufficient quality to host the infrastructure underpinning the virtual private datacentre. These two datacentres will be referenced to as CDC-1 and CDC-2 (Cloud Datacentre 1 & 2) in this text, to clearly differentiate them from ECHA's current datacentre naming convention (PDC-A and PDC-B). These datacentres **shall** be "lights out" datacentres to minimise human activity in them.

To ensure that the requirements of a modern datacentre are met, the Contractor **shall** follow structured and documented datacentre guidelines or standards (for example ANSI/TIA-942-A/B or equivalent) for design of its datacentres and this **shall** apply to CDC-1 and CDC-2 as well. ECHA requires at least N + 1 resiliency for the critical datacentre equipment in the managed datacentres and that documented guidelines or standards, e.g. the Uptime Institute Tier Classification System or equivalent, are followed. The Contractor **shall** make clear to ECHA which guidelines and standards they follow and the classification that CDC-1 and CDC-2 have. On request, the Contractor **shall** be able to demonstrate that they follow such guidelines and standards.

CDC-1 and CDC-2 **shall** be separated by geographical distance to provide adequate datacentre redundancy. In order to be able to benefit from datacentre-level redundancy if and when needed (e.g. in local and regional-scale disaster-recovery situations), CDC-1 and CDC-2 **shall** be separated by a reasonable and adequate geographical safety margin.

The actual magnitude of physical separation between those sites **shall** offer adequate risk mitigation, and hence be based on due diligence and a qualified assessment of the risk exposure prevailing at and around the respective area or country. All commonly and widely known risk elements **shall** be considered and taken into account where appropriate, be they physical/natural or man-made/industrial, including also aspects of general and infrastructure-stability, and balancing and addressing their likelihood and impact on service delivery under this contract.

The Contractor **shall** upon request provide evidence that an adequate and comprehensive risk analysis has been done, and that corresponding, protecting and/or mitigating measures, and plans, for business continuity and disaster recovery are in place, and will be maintained throughout the duration of the Contract. Likewise, where appropriate, the quality management (including e.g. recurrent and regular testing) of such plans **shall** be addressed.

Please see Annex 3: IT BCP - IT Continuity Technical Preparedness Plan (CMO) for more details on ECHA's current solutions.

To ensure Managed ECHA WAN performance (e.g. throughput, latency, migration time, etc.), the datacentres used for delivery of private cloud and infrastructure services **shall** have adequate proximity to ECHA's premises. This is further elaborated in the Managed ECHA WAN service (ref. 6.1.2.2 Managed ECHA WAN).

The need for proximity of the datacentres is further justified by the need to ensure appropriate accessibility for ECHA providers, and possibly ECHA, for hosted ECHA hardware.

Finally, the need for proximity is also justified by the offline backup service (ref. 6.1.4.2 Offline backups).

Important note: ECHA does not wish to impose a strict distance requirement for the proximity of the datacentres. However, by signing the FWC the Contractor agrees to provide services that will deliver the required performance to ECHA. If the required performance cannot be achieved, the Contractor shall put into place an action plan (ref. section 9.5 Customer satisfaction management and poor performance claim). This includes, if so required, relocating to other datacentres closer to ECHA.

The Contractor **may** choose to provide a Trusted Community Cloud Service in datacentres at a greater distance from ECHA's premises. Usage of such services and datacentres are subject to analysis of suitability.

6.1.1.3 Managed Datacentre WAN

The Contractor **shall** provide highly available, encrypted and secure WAN connectivity between the CDC-1 and CDC-2, supporting real-time/synchronous data replication between datacentres. The links **shall** recover automatically from failure and allow upgrade and downgrade of the bandwidth without loss of service. The WAN connectivity **must** securely segregate ECHA networks form possible other non-ECHA networks (e.g. other customers' networks).

The WAN services **shall not** be delivered over the public internet, but rather with private networks or point-to-point connections. The hardware, carrier and any other possible systems required for WAN **shall** be provided by the candidate without exception.

The WAN connections' **shall not** be a bottleneck constraining the technological solution chosen by the Contractor to provide the Managed Datacentre services. The Managed Datacentre WAN **shall** enable fail over of selected (by ECHA) services between datacentres and infrastructures via automation for near zero second Recovery Point Objective (RPO) and an aggressive Recovery Time Objective (RTO) to support ECHA's business continuity requirements. The Contractor **shall** describe what limitations are in place for their service and how the aforementioned near zero second RPO is achieved.

6.1.1.4 Cloud Service

The Contractor **shall** provide **Compute, Storage and Network as-a-service** based on a Cloud infrastructure that supports high levels of automation, standardization, scalability and flexibility. Such infrastructure contains all required server, storage and datacentre network hardware, including datacentre network routing and segregation capabilities, maintenance and licenses required for provisioning compute, storage and network capacity (in short: infrastructure capacity) to ECHA.

The Contractor **shall** follow structured and documented guidelines for Cloud Service delivery, e.g. CSA STAR, EuroCloud Star or equivalent. The Contractor **shall** make clear to ECHA which guidelines and standards they follow. On request, the Contractor **shall** be able to demonstrate that they follow such guidelines and standards.

To be noted is that ECHA does not specifically require that all components of the infrastructure to be "inside one box". Regardless of how the actual physical resources are provided, the components and services provided to ECHA **shall** always be compatible with other services to the highest degree possible.

Compute is defined as computing resources in CPU and RAM. Both CPU and RAM **may** be overprovisioned, over-committed and shared in the underlying infrastructure as long as the services relying on the Compute components do not suffer adversely. The Compute resources **should** be cold- and hot-swappable for "hot add" functionality for VMs (thus requiring no reboot).

The platform **should** support configuration of VM restart order at least to some extent.

The platform **should** support at least the following maximum configurations:

- 64 vCPU per VM
- 1024 GB of RAM per VM
- attachable disk/device size of 16 TB

The Contractor **shall** present at least three tiers, e.g. Gold, Silver and Bronze. **Storage shall** be made available in tiers that have different features, e.g. spindle vs. SSD, different IOPS, different pricing, etc.

In the example tiers above the minimum specifications of the tiers would be:

- Gold comparable to high-end SSD (e.g. 6 Gbit/s), or better

- Silver comparable to high-end 15 000 RPM SAS, or better
- Bronze comparable to 10 000 RPM SATA, or better

Real-time/synchronous, and if available asynchronous, data replication across datacentres **shall** be made available for at least top, but preferably **should** also be available for middle, tiers. Encryption at rest **should** be available as a selectable option when provisioning a VM instance.

The Contractor **shall** provide a highly automated solution for failover of services between datacentres utilizing the data replication between datacentres. To enable controlled failover between datacentres, being able to enforce datacentre affinity for VMs is **should** be available to Business Continuity Planning. Therefore, the platform **shall** make it possible to change the storage tiers of already provisioned Storage resources, preferably in real-time without outage.

To avoid overprovisioning, the offered cloud platforms **should** start from a minimal configuration of e.g. 1 vCPU, 2 GB RAM, 20 GB disk. It **shall** then be possible to select various resource sizes as well as the guest operating system.

The Contractor **shall** manage all aspects of the **Network** required for the cloud infrastructure and all integration with the other Contractor platforms in scope of this FWC. The initial topology (NET 2.0, ref. Annex 1: IT Infrastructure Architecture (CMO)) **shall** be implemented by the Contractor as part of the configuration of the platform. Such topology is aimed to serve ECHA's networking requirements for several years. However, the topology **shall** be changeable in the future through a possible transformation project as part of the Continuous optimisation and cost reduction (ref. chapter 10 Continuous optimisation and cost reduction over time).

While ECHA has no specific requirements for physical segregation for hardware from a security perspective, the Contractor **must** ensure ECHA's networks and virtual machines are securely segregated, whether via virtual or hardware boundaries.

A separate DMZ network **must** be made available for ECHA's Internet facing workloads. This DMZ **shall** be adequately segregated from other networks to ensure the security of the overall platform. More than one DMZ network **should** be supported.

The bandwidth of the underlying cloud infrastructure network **shall** be high enough to meet ECHA's requirements. This **shall** include any possible redundancy configurations and **shall** thus be read as actual usable bandwidth. For ECHA's current network requirements, see Annex 1: IT Infrastructure Architecture (CMO).

There **should not** be any limit to IP or name spaces or VLAN IDs and ECHA **should** be able to define this at will. DHCP **should** be enabled and ECHA **should** be able to define the IP ranges to be used. Preferably, Layer 2 VLAN stretching between the Incumbent's and the Contractor's network **should** be possible to avoid IP changes during transition.

The platform **shall** also support running of Docker Containers with Docker Overlay Networks (VXLAN).

The Compute, Storage and Network components create the basics of the virtual machines that ECHA will provision on the platform. The time to provision **shall** be short, as the level of automation used in the platform **shall** be high. The provisioning **shall** be simultaneous as opposed to sequential.

Important note: ECHA currently uses Oracle DBMSs and Oracle Data Integrator (ODI).

For the current number of ODI and Oracle DBMS licences see Annex 1: IT Infrastructure Architecture (CMO).

The Contractor **shall** ensure that ECHA is compliant with Oracle's licensing model and that ECHA is not required to increase the amount of licenses for Oracle products when running the services in the managed datacentre.

6.1.1.5 Managed OS

Virtual machines will primarily be provisioned from operating system templates provided by the Contractor. Operating system flavours and versions made available to ECHA **shall** always be supported by the vendor of the operating system. The Contractor **shall** provide “two-generation” supported operating systems (N - 1). When operating systems are provisioned, they **should** be automatically joined to the relevant directory service (e.g. AD).

The operating systems in scope of the FWC are split into three categories:

1. Contractor templates
2. Supported operating systems
3. Virtual appliances

Contractor templates are operating systems that can be provisioned instantaneously from a Contractor managed image file (or similar). All Contractor templates **shall** be supported to run in the managed datacentre. ECHA **may** request certain software and/or agents (for which ECHA will provide poss. licenses) to be present in the template.

Supported operating systems are the set of operating system flavours that are at any given time supported to run in the managed datacentre. These operating systems are not necessarily built with Contractor templates, although it is ECHA’s intention to use Contractor templates to the greatest extent possible.

Virtual appliances are operating systems that cannot be managed in a standard manner by ECHA or the Contractor; they are “black boxes” provided by a supplier for a specific purpose. The Contractor **shall** support running virtual appliances in the managed datacentre.

The Contractor’s services **should** support exporting of the above categories, but also for provisioned VMs.

The Contractor will primarily manage all ECHA operating system instances. The Contractor **shall**:

- Maintain supported Contractor OS templates/images as a service.
- Maintain patching/upgrade system in place for all supported OS images as a service.
- Run general OS maintenance tasks such as: anti-virus, log rotation, file system management and monitoring, system tuning, kernel parameter, specification, debugging, trouble-shooting, etc.

As the management of the OS will be done by the Contractor, the Contractor **shall** ensure that ECHA and its third parties have **sufficient operating system level privileges** to perform their respective duties, e.g. application management. Provisioning and delivery of these privileges **shall** be done in a secure manner.

In the case ECHA or one of its third parties require elevated privileges such as root or administrator access to the OS instance, the Contractor **shall** provide a secure and preferably automated mechanism for enabling this. Also, the mechanism **shall** have a capability to disable or terminate the use of the provided privileges when the validity of the justification for having such privileges ends. An audit trail of provisioned/de-provisioned privileges **shall** be maintained all the time.

Any OS instance deployed from Contractor templates **shall** technically support the Service Management tools (ref. section 6.2.2 Service Management Tools). ECHA templates **should** preferably also support this. Were this technically unfeasible, an exception **shall** immediately be reported to ECHA.

The Contractor **shall** maintain and patch systems for all supported OS instances. The patching services **should** be automated, standardised and centralised to the greatest extent possible to minimise error and effort.

Important note: The Contractor **shall** make OS licenses from its own pool available to ECHA as a service. ECHA **may** use its own OS licenses if ECHA so chooses.

6.1.1.6 Managed Load Balancing

Managed Load balancing services, primarily layer 7, **shall** be available for any IP, DNS or URL targets in the managed datacentre, for both internal and external connections. These services are likely to be used by applications outside the scope of this FWC.

The Contractor should be able to transfer ECHA's CMO configuration to the services.

6.1.1.7 Internet Access

The internet uplinks serve two purposes: connectivity from inside ECHA perimeter to the internet; connectivity over the internet to the ECHA public services.

The same link **may** be shared by both use cases, however separate reporting and metrics **shall** be available. The Contractor **shall** ensure that ECHA client usage cannot saturate the link in this case (e.g. QoS).

The internet uplinks **shall** consist of a minimum of two links with either redundancy or load balancing (preferred). The initial uplinks capacity (upgradeable and downgradeable) **shall** ensure minimum throughput of 400 Mbit/s. ECHA **should** be able to pay for the actual throughput ordered, regardless the full capacity of the uplinks. The Contractor **shall** handle all static route changes, etc.

The current architecture is described in the Annex 1: IT Infrastructure Architecture (CMO).

As ECHA has its own Autonomous Number and Provider Independent IP addresses for external usage, the services **shall** support such configuration.

The Internet uplinks **shall** have in place DDoS protection.

6.1.1.8 Remote Access

For providing inside perimeter access to ECHA IT services over the internet (e.g. for the teleworking of ECHA staff, for secure access of ECHA third parties etc.) the Contractor **shall** provide **managed services** for the following solutions (or equivalent):

1. IPsec tunnels towards routable Internet addresses to ensure LAN-to-LAN type tunnels. The current infrastructure, owned by ECHA, is described in Annex 1: IT Infrastructure Architecture (CMO). Since IPsec tunnels management is a feature of ECHA external firewall ECHA's requirements are defined in Section 6.1.1.10.1 External Firewall. VPN tunnels **shall** support integration with the other services in the FWC.

2. SSL VPN based on Pulse Secure Access (SSL VPN). Two factor authentication is based on ECHA SecurID token authentication provide by RSA virtual servers; ECHA owns the physical tokens and the current infrastructure, owned by ECHA, is described in Annex 1: IT Infrastructure Architecture (CMO). The SSL VPN and RSA authentication service tunnels **should** support integration with the other services in the FWC.

3. For system administration purposes (remote and local system administration) ECHA has put in place a terminal server solution to offer a single point of entry to ECHA IT systems; the current infrastructure, owned by ECHA, is described in Annex 1: IT Infrastructure Architecture (CMO).

As regards solution no. 2 the Contractor **shall** take over the management of the solution **based also on the current appliances that will be hosted in the Contractor's datacentres** (ref. section 6.1.1.9 Datacentre hosting of ECHA owned hardware). Initially, ECHA will still own the physical appliances, the licences and maintenance contracts, the physical tokens, whereas the Contractor will be responsible for the managed services. During the implementation of the FWC ECHA can decide to transform such infrastructure towards an as-a-service model (according to which the Contractor will own any appliance, licence etc. as means to providing a service) through a transformation project; the scope of the managed services remaining the same. Therefore, the Contractor **shall** provide a price offer for the managed services in the ECHA owned model and in the as-a-service model.

6.1.1.9 Datacentre hosting of ECHA owned hardware

The Contractor **shall** provide hosting of specialised hardware owned by ECHA (network equipment for the EU institutions network TESTA-ng, CCTV recorders, etc.) co-located in the aforementioned datacentres, and provide network connectivity for the hosted devices.

Services **shall not** be restricted to "server hardware", but **shall** apply equally to other types of (rack-mountable) hardware typically found in data centres (e.g. appliances, switches and other network devices).

The hosting location **shall** always be the most appropriate of the Contractor's datacentres available under the FWC.

The Contractor **shall** grant third party and ECHA access to the datacentre facilities if required for the maintenance of the ECHA owned hardware.

6.1.1.10 Security components of the Managed Datacentre Service

As part of the service, the Contractor **shall** provide the at least the security components described in this section. All hardware, maintenance, software licenses, hosting, etc. related to such components **shall** be included in the Service Fee. The Contractor **may** consolidate these service components, even into a single device or application, and **may** virtualise them. Integration into the cloud infrastructure is also possible, for example if the Contractor offer a Software Defined Datacentre.

The security components **shall** be integrated with the security services described in section 6.6 Security Services.

6.1.1.10.1 External Firewall

The Contractor **shall** provide and manage a state-of-the-art, scalable, highly available external firewall service component to protect the ECHA perimeter (for the concept of perimeter ref. Section 5). The main purpose of the external firewall function is to:

a) protect the systems that reside in the DMZ by ensuring that only explicitly allowed incoming traffic can enter the ECHA perimeter;

b) Provide layered protection against unauthorised access to ECHA inside perimeter;

c) Manage IPsec VPN tunnels. ECHA expects the Contractor to be able to incorporate steep growth of the number of VPN tunnels in the near future (depending on the architecture decisions of on-going ECHA projects) and be able manage up to few hundreds of VPN tunnels.

The external firewall **shall** deny all traffic except explicitly allowed traffic. The Contractor **shall** migrate ECHA's current external firewall configuration (ref. Annex 1: IT Infrastructure Architecture (CMO)), for both incoming and outgoing traffic, to its best of breed external firewall service.

6.1.1.10.2 Internal Firewall

The Contractor **shall** provide and manage a state-of-the-art, highly available internal firewall service component to protect the ECHA perimeter (for the concept of perimeter ref. Section 5).

The Contractor **shall** take over ECHA's existing configuration (ref. Annex 1: IT Infrastructure Architecture (CMO)) and migrate it to the offered service.

In particular, ECHA uses AD integration to power the internal firewall rules. Therefore, the offered internal firewall function **shall** support integration with the ECHA's Active Directory for automatic firewall ruleset creation based on AD users, groups and computer accounts. This functionality **shall** also be applicable to access from the LAN network to the managed datacentre.

6.1.1.10.3 Web Application Firewall

The Contractor **shall** provide a state-of-the-art, highly-available Web Application Firewall service component to protect selected internet-facing web applications indicated by ECHA.

The Contractor **shall** be able to take ECHA's current Web Application Firewall (F5 ASM) configuration and migrate it to the offered service to the greatest extent possible. This configuration is currently applied to few ECHA critical applications. This migration **shall** be part of the Transition Project.

The Web Application Firewall detects and blocks attacks primarily based on the attack signatures provided by the Web Application Firewall suppliers. On request of ECHA or ECHA third party, the Contractor **shall** collaborate to define the appropriate configuration of the Web Application firewall (Normal Change).

The Contractor **should** provide reports or a dashboard view on the detection activity of the Web Application Firewall to the ECHA third party in charge of the application management.

It is understood that these services are based on largely emerging technologies. Thus, ECHA expects that the Contractor will provided added value by proposing more advanced and efficient ways of leveraging the potential of the technology. Such proposal could very well fit in the rolling plan for optimisation (ref. chapter 10 Continuous optimisation and cost reduction over time).

6.1.1.10.4 Reverse Proxy

The Contractor **shall** provide a state-of-the-art, highly available reverse proxy service component targeted at preventing direct network connections from the internet to the public services.

The reverse proxy **shall** act as an extra layer of security on top of the external firewall. SSL/TLS termination, support for multiple certificates and configuration of host headers (e.g. X-Forwarded-Host, X-Forwarded-Proto) **shall** be available.

The Contractor **shall** take over ECHA's existing configuration and migrate it to the offered service.

6.1.1.10.5 Client Proxy

The Contractor **shall** provide a state-of-the-art, highly available client proxy service component. The client proxy will act as an extra layer of security for connections going out from ECHA's clients towards the internet or other services inside the ECHA perimeter. The Contractor **shall** take over ECHA's existing configuration and migrate it to its offered service.

The client proxy **shall** support:

- Category based and content based web site filtering
- Identification of users (AD integration)
- Whitelisting / blacklisting based on the requests
- SSL/TLS termination
- Sandboxing for uploaded files

- Anti-virus.

6.1.2 Managed ECHA LAN and WAN

Networking solutions outside the Contractor's datacentres are divided into Local Area Networks (LAN) and Wide Area Networks (WAN) services.

WAN services are currently provided by the Incumbent and LAN services by the Network Incumbent.

6.1.2.1 Managed ECHA LAN

The Contractor **shall** provide managed services on the existing infrastructure owned by ECHA (ref. Annex 1: IT Infrastructure Architecture (CMO)).

The LAN is used to provide end-user connectivity. All ECHA staff have a laptop device, and to enable mobility use Wi-Fi to connect to the network. There are wired connections over Ethernet for Printing devices, and Audio Visual equipment. Therefore, it is expected that the Contractor will need to provide on-site support, at least to some degree. The Contractor **shall** take this into account in its service.

The LAN service is split up into cabled Ethernet and Wi-Fi. These two groups together build up the logical part of the network which is located in ECHA premises.

The Contractor **shall** take over the management of any and all systems and devices required to provide the service, however the hardware, basic maintenance contracts and software licenses for the service will be owned by ECHA.

The wired Ethernet is the ground level network in ECHA premises and it consists of traditional access switches and distribution switches.

The Wi-Fi service provides wireless network access for internal and external users covering all the ECHA premises. Wi-Fi Access Points are dependent on the cabled Ethernet switches and the WLAN Controllers are dependent on the core network. The Contractor **shall** provide management of these devices and related systems.

Expected change requests include, but are not limited to:

- port/interface configuration changes
- static route changes
- small configuration changes to OSPF / BGP configuration
- small configuration parameter changes e.g. DNS, NTP
- install/change device certificates
- hardware installation work e.g. install / remove switch, access point
- modify cabling
- adjust WLAN coverage

The ECHA LAN consists of many network components with different purposes including switches, controllers and access points. They are covered with basic maintenance, which is the lowest possible maintenance level available via ECHA's hardware vendor. It provides ground level services i.e. software downloads from vendors and Return Material Authorisation (RMA). However it does not cover all the required services such as proper software updates or on-site service for device replacements.

Therefore, the Contractor **shall** provide advanced maintenance services, covering the following services:

- Software updates for ECHA network devices including planning, testing and scheduling in co-operation with ECHA's Change Management and fulfilling requirements for ECHA's Change Management process. In case of major update, it is required that the update is managed as a project on Contractor's side providing proper documentation and project plan approved by ECHA.

- On-site work to repair or replace a broken part or device including independent incident management and RMA process.

The Contractor **shall** collect information from all LAN network devices owned by ECHA with a discovery tool to produce a comprehensive report of network hardware and software status. The report **should** be human readable and understandable with concrete actions, suggestions and observations together with the raw data collected and reviewed jointly twice per year. The report **shall** be aligned with the latest end-of-support announcements from vendors to provide valuable output for designing network changes in long term (2+ years).

Important note: Changes are likely to occur once ECHA is relocated via the building project (ref. section 2.3 Elements for consideration). Any changes required to facilitate such change be handled in due time either during the negotiation phase of this procurement procedure or in the form of a transformation project.

6.1.2.2 Managed ECHA WAN

The ECHA WAN service **shall** provide secure, highly available (preferably active-active with automatic failover) and encrypted network traffic between the ECHA premises and the Contractor's datacentres and possibly service delivery centres.

The Managed ECHA WAN services **shall not** be delivered over the public internet, but rather with private networks or point-to-point connections. The hardware, carrier and any other possible systems required for WAN **shall** be provided by the Contractor without exception.

The WAN connections' **shall not** be a bottleneck constraining the technological solution chosen by the Contractor to provide the Managed Datacentre services. In particular, the roundtrip latency of the Managed ECHA WAN connections **shall** support client computing, including low-latency applications such as desktop as a service, video conferencing, VoIP, etc. The latency of the connection **shall not** negatively affect the experience of the users. The bandwidth **shall** be a minimum of 1 Gbit/s, but **shall** be upgradeable if so required.

The Contractor **should** investigate possibility of providing GÉANT[3] connectivity. This could be the subject for innovation of the services in the FWC (ref. section 9.6 Innovation)

Internet connectivity for ECHA client traffic **shall** also be provided (ref. section 6.1.1.7 Internet Access). The Contractor **may** use the same connection as the Internet uplink for the managed datacentre, but in this case **shall not** charge for it "twice".

Important note: All WAN connections are likely to be affected by the building project (ref. section 2.3 Elements for consideration). Any changes required to facilitate this change will be handled in due time either as part of the negotiation phase of this procurement procedure or as part of the transition project. Were the building project incurs substantial delays, changes could be addressed as a future transformation project.

6.1.3 Office automation

This is the service for provisioning certain office automation components.

[3] https://www.geant.org/

6.1.3.1 Email and calendaring service

ECHA currently has an on-premise installation of Microsoft Exchange managed by the Incumbent. The Contractor **shall** take over this service from the Incumbent and provide a similar service to ECHA.

The email service **shall** provide a performant and stable platform for message delivery and calendaring compatible with MS Office Outlook.

The Contractor **shall**:

- Manage all aspects of configuration for Microsoft Exchange (including, but not limited to, transport rules, connectors, virtual directories, database availability groups and databases).
- Manage all aspects of configuration for Exchange Online Protection.
- Manage all aspect of configuration for Exchange Online and a hybrid scenario.
- Install new certificates.
- Manage all aspects of configuration of Active Directory related to the operation and configuration of Exchange.
- Manage all aspects of Windows operating system management for the servers hosting Exchange at ECHA (if so required).
- Manage additional Anti-Virus and Spam\Malware protection software on ECHA's on-premises Exchange servers.
- When required, upgrade Exchange installation to newer version.
- Troubleshoot and fix client connectivity issues.
- Provide support for integrating other 3rd party solutions with the email service (e.g. via APIs).
- Provide reports on messaging volume, mailbox counts, database sizes and storage consumption.

The Contractor **shall** provide a state-of-the-art and highly-available messaging security function. The Contractor **shall** take over ECHA's existing configuration and migrate it to the offered service.

The Contractor **shall** provide for the following security features:

- Anti-virus
- Anti-malware
- Anti-spam

The Contractor **should** provide suggestions for improvements in the existing Exchange infrastructure and messaging security function.

6.1.3.2 Windows services

Windows services will be managed as one environment, as the services are very closely related.

6.1.3.2.1 Active Directory Services

ECHA uses Microsoft Active Directory which is managed by the Incumbent. The Contractor **shall** take over these services from the Incumbent and provide a similar service to ECHA.

The Active Directory service **shall** provide a performant and stable platform for authentication and authorization for applications that are compatible with LDAP. The service **shall** also provide centralised configuration for Windows operating systems both Client and Server through group policies and scripts.

The Contractor **shall**:

- Maintain the Active Directory services
- Manage all aspects of configuration for Active Directory services.
- Create custom attributes and classes in Active Directory schema(s) and applying schema updates
- Create scripts for batch operations.
- Manage all aspects of Windows operating system management for the servers hosting Active Directory services (if so required).
- Manage Anti-Virus and Spam\Malware protection for ECHA's Active Directory services.
- When required, upgrade AD installation to newer version.

The Contractor **should** install and configure any additional native Active Directory service available from Microsoft. The Contractor **should** also provide suggestions for improvements in the existing Active Directory Service environment

6.1.3.2.2DNS Service

ECHA uses Windows Server for DNS which is managed by the Incumbent. The Contractor **shall** take over these services from the Incumbent and provide a similar service to ECHA.

The service **shall** provide a performant and stable platform for DNS record management. The platform **shall** be compatible with Active Directory and support service\text records.

The Contractor **shall**:

- Maintain the DNS service.
- Manage all aspects of configuration for Active Directory services related to DNS.
- Manage all aspects of configuration for DNS service on Windows Server operating system (if so required).
- Manage all aspects of Windows operating system management for the servers hosting DNS services (if so required).
- Manage Anti-Virus and Spam\Malware protection for DNS services (if so required).

The Contractor **should** provide suggestions for improvements in the existing DNS Service environment.

6.1.3.2.3 DFS & SMB (File Shares)

ECHA has both AD integrated and stand-alone DFS namespaces which are connected to Shared folders, both managed by the Incumbent. The Contractor **shall** take over these services from the Incumbent and provide a similar service to ECHA.

The File Share service **shall** provide a performant and stable platform for storing and accessing files compatible accessible via SMB and DFS.

The Contractor **shall**:

- Maintain the DFS and File Shares
- Manage all aspects of configuration for Distributed File System.
- Manage all aspects of configuration for SMB file shares.
- Manage all aspects of configuration for quota administration.
- Manage all aspects of configuration of Active Directory related to the operation and configuration of DFS.
- Manage all aspects of Windows operating system management for the servers hosting DFS and SMB (if so required).
- Manage Anti-Virus and Spam\Malware protection for ECHA's DFS and SMB services.
- When required, upgrade environment to newer version.

The Contractor **should** provide suggestions for improvements in the existing DFS and SMB environment

6.1.3.2.4 DHCP service

ECHA uses Windows Server for DHCP which is managed by the Incumbent. The Contractor **shall** take over these services from the Incumbent and provide a similar service to ECHA.

The service **shall** provide a performant and stable platform to provide dynamic assignment of IP address to client devices on both wired and wireless connections.

The Contractor **shall**:

- Maintain the DHCP Servers
- Manage all aspects of configuration for DHCP.
- Creating, modifying and removing scopes (IPv4\IPv6)
- Setting scope options
- Manage all aspects of Windows operating system management for the servers hosting DHCP services (if so required).
- Manage Anti-Virus and Spam\Malware protection software for DHCP services (if so required).

The Contractor **should** provide suggestions for improvements in the existing DNS Service environment

6.1.3.2.5 PKI service

ECHA uses Microsoft Active Directory Certificate services, which are managed by the Incumbent. The Contractor **shall** take over these services from the Incumbent and provide a similar service to ECHA.

The service **shall** provide a performant and stable platform for issuing and managing certificates for ECHA internal services.

The Contractor **shall**:

- Maintain the KPI infrastructure

- Manage all aspects of configuration for Active Directory Certificate services.
- Manage all aspects of Windows operating system management for the servers hosting Active Directory Certificate services at ECHA.
- Manage Anti-Virus and Spam\Malware protection software on servers hosting Active Directory Certificate services (if so required).
- Install and configure any additional native Active Directory Certificate service component available from Microsoft.
- When required, update or upgrade any component of the Active Directory Certificate service.

The Contractor **should** provide suggestions for improvements in the existing Active Directory Service environment

6.1.3.2.6 Terminal server services

ECHA has implemented Terminal Server Services mostly for IT system administration purposes. The platform is Windows Server where Remote Desktop Services are enabled. The Contractor **shall** take over these services from the Incumbent and provide a similar service to ECHA. The CMO for such services is described in Annex 1: IT Infrastructure Architecture (CMO). The Contractor **shall** also, when required, be able to update the solution to a newer version.

The Contractor **should** provide suggestions for improvements in the solution.

6.1.4 Backup and restore services

The Contractor **shall** provide backup and restore service ensuring continuity of the Current Mode of Operations (CMO) and applying the ECHA backup retention policy as described in Annex 1: IT Infrastructure Architecture (CMO). The backups **shall** be done in a cross-datacentre manner.

Backup services **shall** be available at file level for all supported operating system flavours. Clients **shall** be installed on servers requiring backup and backups will be agent based backups and not image-level backups. Restore **shall** be possible for server, name space, target, drive, folder and single item.

For non-supported operating system flavours, image based backups **shall** be supported.

Furthermore, application aware backups **shall** be supported for all managed services in scope of the FWC and furthermore for at least the following services:

- Oracle
- MS-SQL
- Exchange
    - Restore **shall** be possible for server, database, mailbox, folder and single item.
- SharePoint.

Specific requirements for backups in the following areas:

- Active Directory
    - Restore **shall** be possible for Forest, Domain, Domain Controller, Service component configuration, database, schema, multiple objects, single object and deleted object.
    - For Active Directory Certificate services restore **shall** be possible for server,

configuration and database.

- DNS
  - Restore **shall** be possible for (server), configuration, zone, and record.
- DHCP
  - Restore **shall** be possible for server, configuration, scope and reservation.

The Contractor **may** use any optimisations for backup storage (e.g. incrementals, differentials, compression, deduplication, etc.).

During the transition phase, the Contractor **shall** take over the latest full backup data in the sense that restore of data **shall** be possible.

Taking of backups and restores due to Incidents shall be part of the Service Fee. Restores not related to Incidents shall be charged in Effort Bands.

6.1.4.1 Restore-from-backup service

Upon request of ECHA or a third party authorised by ECHA (normally one of the IT contractors of ECHA responsible for software development and operations services), the Contractor **shall** initiate restore and make the backup data for restore available in the appropriate environment.

The Recover Point Objectives (RPO) (ref. Annex 1: IT Infrastructure Architecture (CMO)) **shall** be measured accordingly.

The requestor of the restore – ECHA or a third party authorised by ECHA – **shall** be granted access to the data for restore as long as needed for completing restoration.

Such model can be used by ECHA or a third party authorised by ECHA to actually replicate data from a source environment to a replica environment.

6.1.4.2 Offline backups

To cover a potential data loss due to severe human errors and deliberate destruction of active (on system) and/or passive (on disk backup) data, the Contractor **shall** offer a separate offline backup service equivalent to the one described in Annex 1: IT Infrastructure Architecture (CMO). In order to mitigate the risk related to storing and transportation off-site, offline backups stored outside the Contractor’s datacentres **shall** be encrypted.

The Contractor shall take special note of the possible transport distances related to the service.

6.2 Service Management Portal

The Contractor **shall** provide a Service Management Portal (SMP). Through this portal, ECHA **shall** manage the services under the scope of the FWC. Currently, ECHA does not have an equivalent functionality. Therefore, the Contractor **should** foresee time and resources to aid ECHA in defining the minutiae of requirements during the transition project. In this section are the functionalities that ECHA foresees. The Contractor **may** offer more and better functionalities if they are available.

The SMP **shall** contain all pertinent information for the entire service portfolio under the FWC.

The SMP **shall** provide the following functionalities:

- Service Catalogue
- Service Management and Tools

- Monitoring and Reporting
- Billing and Invoicing.

Most services **shall** support automated provisioning via Service Requests fulfilment and be manageable via the SMP to the greatest extent possible. The Contractor **shall** strive for the highest level of automation to significantly drive down the cost of service provisioning and management. All Service Requests **should** support approval workflows, to be activated if ECHA so requests.

The SMP **shall** be provided as a browser based web application, compatible with MS Internet Explorer and Mozilla Firefox, or a set of integrated web applications. It **should** be accessible also via mobile and small form-factor devices (e.g. smartphones, tablets, etc.). It **should** utilise open standards (e.g. HTML5) and minimize use of proprietary plugins.

The SMP **shall** offer AD integration features in order to implement single sign-on (SSO), and also local identity management, for ECHA users and third parties and **shall** provide RBAC. The RBAC solution **shall** be granular to allow differentiation between ECHA and third parties and **should** support this via tagging of the resources.

It is also ECHA's expectation that the SMP **shall** expose industry standard API's (for example OpenStack, Cloud Foundry) allowing ECHA and ECHA's third parties to programmatically interface the SMP to trigger Service Requests. These APIs **shall** support SSL/TLS.

6.2.1 Service Catalogue

The SMP **shall** foresee a section providing as main functionality a centralised Service Catalogue. The Service Catalogue **should** contain all defined services of the FWC that can be ordered, via Service Request or otherwise.

Many of these services **shall** be available to be requested by users directly without authorisation or change management via Service Requests.

Service Request fulfilment for services in the Service Catalogue **shall** be automated. Non-automated requests **shall** be classified as either Standard or Normal Changes and follow the appropriate process, e.g. open a ticket. This process **shall** be explained in the Contractor's offer.

This Service Catalogue **shall** list and describe the characteristics of each selectable service, including but not necessarily limited to, its options, costs and SLAs. As an example, the Cloud service description **would** include the sizing parameters (such as vCPU, RAM, disk space), the deployable mode, the available security level, the guaranteed SLA (e.g., availability), price and expected time to deliver (if applicable).

It **should** be possible to add new services to the Service Catalogue. This could be a small addition, like the addition of a new functionality or updated service, or a larger addition such as a completely new service.

6.2.2 Service Management Tools

The SMP **shall** provide service management functionalities, where the user accounts, the provided services and the related resources are managed. The SMP **shall** also contain online help, e.g. FAQs, etc.

The Contractor **shall** provide as far as possible a complete set of service management/operation tools for ECHA to ensure that ECHA has the appropriate tools and interfaces to efficiently consume services. Such tools **shall** be integrated and in or available from the SMP with the same web based GUI requirements.

The Contractor can read about ECHA's current toolset in Annex 1: IT Infrastructure Architecture (CMO).

The Contractor **shall** provide at least the following Service Management Tools:

- users/group management for the SMP, according to a role based access control model, including account management logging (e.g. create, delete, provision, de-provision, security component changes, etc.)
- metadata tagging of VMs and other pertinent services, including forced tags that cannot be excluded.
- start/stop/redefine the computing resources or services
- monitoring and reporting (see section 6.2.3 Technical Monitoring and Reporting)
- service provisioning and de/provisioning via service requests fulfilment; requesting changes and report and track incidents. Primarily, ECHA wishes to use its own ticketing system for reporting incidents or requesting changes. The Contractor **may** use its tools of choice to provide these interfaces; however, in this case the Contractor **shall** integrate seamlessly with ECHA's ticketing systems (currently BMC Remedy) in the best way possible, minimising human intervention (e.g. no manual copy-pasting of data). The status of any change request or ticket **should** be visible also in ECHA's ticket system.
    - The minimum acceptable integration is to allow ECHA to create a ticket/change request in the ECHA ticketing system from which the ticket is transferred to the Contractor automatically. In this scenario, any requests for information to ECHA and the closure of the ticket **shall** be propagated to the ECHA ticketing system.
- searching and filtering of provisioned items in the SMP user interface to ensure proper inventory management, also on tags.

The Contractor **should** offer more functionalities if they are available. ECHA **may** request more functionality to be developed later as a transformation project; therefore, the Contractor **shall** have the capabilities and the capacity to perform such projects.

In the SMP, the Contractor **should** provide a dashboard with a consolidated view of all the provisioned services and resources. Drilldown functionalities **should** allow to "zoom-in" from the consolidated view down to the display of the details *relevant* for ECHA service management of a single resource, service instance or other items.

The platform **should** provide policy based management, e.g. patching adherence, backup and restore, password expiration, etc. The SMP **should** also have the ability to monitor the patch level of all supported operating systems and to alert ECHA in case of non-compliance to the patching policy.

The Contractor **shall** have a CMDB in use and it **shall** be updated when ECHA triggers Service Requests and Changes.

Upon dispute or otherwise ECHA's request, the Contractor **shall** provide change logs, service request records, incident records and problem records from its own systems. If pertinent, to achieve this the Contractor **should** provide read-only access to its CMDB for CIs related to service provisioning or provide reports where CIs can be located.

6.2.3 Technical Monitoring and Reporting

The Contractor **shall** provide technical monitoring and reporting information on the services in scope of the FWC via the SMP. This is a clear distinction from monitoring of individual systems or their behaviour. While the Contractor monitors its systems to deliver the services, ECHA **should** be able to run reports on preferably all attributes related to a service.

At least the following reports **shall** be provided in real time for services and their components:

- Service availability
- SLA adherence

- Major and security incident reports when applicable
- Request fulfilment incl. request/fulfilment time
- Service performance
    - Historical data **should** be made available to enable trending of the performance of individual services. For example reports on Reliability, the mean time between incidents on a particular service, and Maintainability, the average time to recover an incident on a particular service.
    - Trend reports of previous 12 months covering number of service requests and incidents
    - Support desk report (number and type of calls, dates, assignees, response and resolution times, SLA outcome)
- Detailed service consumption for, at least:
    - Cloud service
    - Backup and restore
    - Email and calendaring
    - including financial consumption (ref. section 11.2.8 Invoicing and financial management)
        - XML/CSV/etc. export **shall** be available
- Policy adherence (where applicable)
    - e.g. backup and patching policy
- Success rate of service execution (where applicable)
    - e.g. backups and restores.

The Contractor **should** enable that all pertinent SNMP traps related to the services are available for propagation to ECHA's own or ECHA's third parties monitoring tools, if so required.

ECHA **may** request more reports to be developed later as a transformation project, therefore the Contractor **shall** have the capabilities and the capacity to perform such projects.

6.3 Service management

In this section we illustrate what "managed service" entails in the context of this FWC. Such definition is coherent with ITIL and, in doubt, **are to** be interpreted by the Contractor accordingly; deviations are specifically described.

For the services in scope of the FWC, it is expected that whereas the Contractor will largely be responsible and accountable for implementation of Normal Changes, ECHA will approve changes. The Contractor **shall** provide a proposal and toolset to ensure that this can happen (ref. section 6.2.2 Service Management Tools).

Standard Changes and Service Requests can be defined by ECHA and/or proposed by the Contractor (e.g. as part of the recurrent optimisation plan, ref. chapter 10 Continuous optimisation and cost reduction over time). Once agreed they will be added to be added to the SMP. The approval of the list of Standard Changes or Service Requests and related updates will be handled through the FWC governance.

6.3.1 RACI matrix for Service Management

The service management responsibilities are defined via RACI matrix as follows:

- **R (responsible):** Those who do the work to achieve the task.
- **A (accountable):** The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible.
- **C (consulted):** Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.
- **I (informed):** Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Table 11 RACI matrix for Service Management

Process	R	A	C	I	Example
Event management	Contractor	Contractor	N/A	N/A	“Link failover to HA pair”
Set-up of the service/termination of the service	Contractor	Contractor	ECHA Third parties	ECHA	"A service is transitioned to FMO” “A service is decommissioned”
Incident management					
Incident	Contractor	Contractor	ECHA Third parties	ECHA Third parties ECHA	“A VM is stuck and cannot reboot”
Major Incident	Contractor	Contractor	ECHA Third parties ECHA	ECHA Third parties ECHA	“30 VMs have crashed”
Crisis Escalation	Contractor	Contractor	ECHA ECHA Third parties	ECHA Third parties	“All systems down”
Problem Management	Contractor	Contractor	ECHA	ECHA Third parties	“Deployment fails for new template.”
Service Request Fulfilment	ECHA third parties	Contractor	N/A[4]	ECHA Third	“Build VM from template”

[4] ECHA **may** choose to use the Contractor’s workflow engine for approval of certain Service Requests. This depends largely on the Contractor’s ability to implement and provide financial management tools.

Process	R	A	C	I	Example
	ECHA			parties ECHA	
Change Management					
Standard Change	Contractor	Contractor	N/A	ECHA ECHA Third parties	“Add a RSA super administrator”
Normal Change	Contractor	Contractor	ECHA	ECHA Third parties	“Build a new VLAN”
Emergency change	Contractor	Contractor	ECHA	ECHA Third parties	“roll-back new SMP software version”

6.3.2 Service Desk

The Contractor **shall** implement Service Desk functions and processes for ECHA and its third parties. This Service Desk will be the Single Point of Contact (SPOC) for ECHA’s service teams or authorised third party’s service teams.

The Service Desk **shall** be accessible via phone line (reachable via local national number or VOIP), instant messaging (reachable through e.g. the SMP) and email.

In line with the relevant ITIL processes, ECHA intends to structure the support services in several layers implementing separation of concerns, increasing the efficiency of the support service and facilitating the access and use of support services from the end user perspective.

Services can be generally categorized in:

- User facing support service
- Back-office support services

The default position is that ECHA will provide the function of user facing support for its “end users”, and the Contractor **shall** perform the Back-office support services. ECHA **may** under certain circumstances utilise the Contractor also for User facing support.

6.3.2.1 End user facing support services

The services under this category include the day-to-day responsibility for operating and managing the first-line support for all services related issues for end-users of the IT services.

The user facing support service is also in charge of the follow-up of the support activities.

6.3.2.2 Back-office support services

Typical activities of the Back-office support services include:

- Incident management
- Troubleshooting

- Configuration changes (minor)
- Ticket analysis
- Feedbacks into existing Change Management processes in the area affected
- Appraisal of critical and urgent issues and support to their resolution
- Problem management, problem definition, analysis and resolution, knowledge management activities, creating and maintaining knowledge.

If requested by ECHA, the Contractor **shall** provide a SPOC for a given ticket. For example, if ECHA assigns a ticket to the Contractor team X, and the Contractor sees the need for other teams to perform work to resolve the ticket, the Contractor will be responsible for requesting and coordinating that the necessary work is performed, and then collect and collate the results of this work, and then the Contractor team X will report back to ECHA. Typical areas which require an investigation spanning different parties can include performance issues, or errors associated with passing data between integrated systems.

6.3.3 Set-up of the service/Termination of the service

The Contractor **shall** be responsible for service set-up and service termination.

Service set-up includes, for example, activities like integrating the service in the SMP and into horizontal services like monitoring or security services.

Service termination convers the activities needed to decommission the services (it does not include transition out, for which ref. section 8.2 Transition out)

6.3.4 Event management

The Contractor **shall** have responsibility of all Event Management. The Contractor **shall** have a formal Event Management process in place and adequate tools. ECHA only expects to be informed of incidents, so events that do not classify as incidents do not need to be communicated to ECHA unless otherwise specified or agreed by both parties.

6.3.5 Incident management

The Incident and Major Incident Management process will clearly involve both ECHA and the Contractor, but also ECHA third parties. The Contractor **shall** have formal processes in place and **shall** ensure that its processes can adapt to this.

6.3.5.1 Definition of Incidents and their Priority

Incidents are defined in four categories as per the table below.

Table 12 Incident classification.

Priority	Cloud Service impact	Other service impact
Major incident	More than 20 % of service severely affected	ECHA's ability to meet legal obligations or deadlines is put in jeopardy.
Priority 1	More than 10 % of service severely affected	Incident has • a wide impact, for example a critical service is not at all available, or • a considerable amount of users are prevented from using the service, or • a considerable part of the functionality of the service is not available.
Priority 2	5 % - 10 % of service	Incident has medium impact (based on elements defined in priority 1 impact)

Priority	Cloud Service impact	Other service impact
	affected	
Priority 3	Less than 5% of service affected	Incident has low impact (based on elements defined in priority 1 impact)

If appropriate, more details on incident classification will be provided at the level of specific contract.

6.3.5.2 Incident

Incidents **shall** be detected rapidly after they occur by implementing proper Event and Incident Management processes. Typically it is the Contractor who detects an Incident, however, occasionally it could be that ECHA or one of its third parties detects an Incident and informs the Contractor.

In case the Incident was not properly detected by monitoring, after the Incident has been closed, a Problem **shall** be logged and analysed for further improvement of the service.

The Contractor **shall** respond to ECHA with confirmation that a ticket has been logged and the remedial action procedure has been triggered. The response **shall** inform ECHA of the ticket number assigned to the Incident. This response **may** be an automated response.

6.3.5.3 Major Incident

A Major Incident is an Incident that fits the Major Incident definition above. A Major Incident **shall** trigger Crisis Escalation to the ECHA appointed service owner and outsourcing service manager.

6.3.6 Problem Management

Re-occurring Incidents will require the Contractor to carry out problem management to ensure that such Incidents are avoided in the future. All Incidents and Problems **shall** be correctly logged for further analysis according to a documented Problem Management process that the Contractor **shall** have in place.

6.3.7 Service Request Fulfilment

In the scope of this FWC Service Requests and Request Fulfilment will be based on ITIL.

ECHA requires that the fulfilment of such Service Requests **shall** be:

- low risk
- highly automated or follows a documented standard process.

In fact, Service Requests require no assessment, authorisation or scheduling from the point of view of the Contractor and will be implemented as soon as possible by the Contractor (within the requirements set by the SLA), preferably always with automation and without any human activity except for the requesting user.

An example of a Service Request would be provisioning of a managed Operating System or a data backup. On the contrary, creating a new VLAN rule would not be a Service Request and would require creation of a Request For Change (RFC) and implementation of a Normal Change.

As Service Requests can be submitted by either ECHA or on behalf of ECHA by a third party, e.g. one of ECHA's contractors for software development, traceability of fulfilment **should** be available to allow ECHA to control if and when a Service Request is implemented, if ECHA so chooses.

The Contractor **shall** also strive to continually improve automation and standardisation, thus promoting Standard Changes to Service Requests.

The Contractor **shall** explain in their offer which Service Requests are available to ECHA via the SMP.

6.3.8 Change Management

ECHA's change management procedures are documented in the following ECHA IQMS documents:

- Annex 4: ICT Change Management (CMO)

In the scope of this FWC, three types of changes, largely based on ITIL, are defined: Standard, Normal and Emergency.

The Change Management process will clearly involve both ECHA and the Contractor, but also ECHA third parties. The Contractor **shall** have formal processes in place and **shall** ensure that its processes can adapt to this.

6.3.8.1 Standard Change

Standard change: a recurrent, well known type of change, for which a standardised implementation procedure exists. A standard change is pre-approved to be made under specific circumstances or as a response to a specific situation.

For the services in the scope of this FWC, the changes following the Standard Change process is usually the result of a provisioning of a service in the Service Catalogue, but with less automation and standardisation than a Service Request. Thus, a Standard Change **shall** require very little, if not no, assessment, authorisation or scheduling after the request has been submitted.

6.3.8.2 Normal Change

Normal change: a request for something new or a request to change something that already exists.

Normal Changes are all changes that do not fit into the other Change Management categories. These changes **shall** have at least a formal Request For Change (RFC) and Change Impact Assessment (CIA) submitted. Traceability of fulfilment of the RFC **shall** be available to ECHA for control purposes or Incident or Problem Management.

ECHA and the Contractor both appoint a Change Manager. If agreement cannot be reached at change manager level, the change is escalated to the appropriate Change Advisory Board (CAB).

If the CAB cannot come to agreement, the change will be escalated to the steering committee (ref. section 9 Governance).

The steering committee is the last possible body to approve a change. If the change cannot be approved in this board, the change is by default rejected. The change managers will be responsible for facilitating the decision making at all escalation levels, for example by providing risk analysis based on the CIA elements.

The number of escalations to the CAB and the steering committee **shall** be formally recorded.

The Contractor **shall** also continually analyse Normal Changes and look for opportunities to promote Normal Changes to Standard Changes or even Service Requests. The Contractor **shall** explain their approach to this in their tender.

6.3.8.3 Emergency Change

An Emergency Change can be requested by any party. However, Emergency Changes will normally only be raised in the case of a Priority 1 or Major Incident.

Emergency change: a change that needs to be implemented in the fastest possible yet controlled way (e.g. an issue with high critical business impact and for which there is no realistic workaround).

Defining a change as an emergency does not automatically entail the change will be implemented.

The change will be assessed by the Change Managers in both organisations and agreement is required to be reached if the situation warrants an Emergency Change. If the Change Managers cannot make a decision on the change, an emergency meeting of the Change Advisory Board will be called. If the board cannot make a decision the change, it will be escalated through the hierarchy of both organizations (as opposed to the FWC governance).

6.3.9 Required Requests

ECHA's expectation is that the following list of Requests will utilise automation to the highest degree possible and that achieving the expected output of such Requests **shall** require no ECHA manual intervention except for triggering the request.

If an item cannot be implemented as a Service Request, it **shall** be provided as a Standard Change. ECHA's requirement is that Standard Changes are well documented and follow a repeatable procedure ensuring a high probability of achieving expected outcome.

ECHA's expectation is that Standard Changes **should** over time mature into Service Requests utilising automation to the highest degree possible. Likewise, repeated Normal changes of a similar nature **should** mature into Standard Changes.

Table 13 Required Requests

Service	**Request**	**Initial min. level of maturity**	**Required after transition**
6.1.1.2 Managed Datacentre Facilities	Secure media disposal Access by ECHA or Vendor to hosted devices.	Standard Change	**Yes**
6.1.1.4 Cloud Service	Provision of VM with attributes (e.g. description, cost centre, OS template, Managed OS, OS license, patching schedule) Edit VM attributes (e.g. description, cost centre, patching schedule) Change VM running state (start, stop, restart, suspend/hibernate) Configure VM (e.g. CPU, RAM, Disks & tiers, Network/VLAN incl. DMZ(s), Disaster recovery/RPO) De-provision VM, all associated add-on services also to be de-provisioned. Request failover of services from one	**Service Request**	**Yes**

Service	Request	Initial min. level of maturity	Required after transition
	datacentre to another (in case of emergency).		
6.1.1.5 Managed OS	Minor change to a template Deploy patches/defer patching on specific VM upon request	Standard Change	**Yes**
6.1.1.6 Managed Load Balancing	Provision load balanced IP/DNS name/URL	Standard Change	**Yes**
6.1.1.7 Internet Access	Provision/de-provision public DNS record	Standard Change	**Yes**
6.1.1.8 Remote Access	Provision/de-provision RSA user Provision/de-provision RSA token Provision/de-provision Super Admin Provision/de-provision Pulse web bookmark	Standard Change	**Yes**
	Resynchronise RSA token	**Service Request**	**Yes**
6.1.1.10.1 External Firewall	Implement defined rules/policies for Internet access. Define rules/policies for connectivity between different networks/VLANs based on source and target network addresses/masks and network protocol with AD integration.	Standard Change	**Yes**
6.1.1.10.2 Internal Firewall	Implement defined rules/policies for connectivity between IP/DNS name that are in different networks/VLANs based on source and target network addresses/masks and network protocol.	Standard Change	**Yes**
6.1.1.10.3 Web Application Firewall	Request to fine-tune rules based on a false positive Request to adjust or customise rules for bespoken application Request white/blacklisting	Standard Change	**Yes**
6.1.1.10.4 Reverse Proxy	Request implementation of defined rules/policies/targets.	Standard Change	**Yes**
6.1.1.10.5 Client Proxy	Request activation of standard rules (whitelists, blacklists, malicious content). Manage changes to categories.	Standard Change	**Yes**

Service	Request	Initial min. level of maturity	Required after transition
	Block access to specific website		
6.1.3.1 Email and calendaring service	Creating, modifying and removing mailboxes (personal\shared\archive\resource) Enabling and disabling online archiving	**Service Request**	**Yes**
	Configure capabilities to encrypt emails models that implement transparent encryption for users (e.g. using forced SSL/TLS tunnels between e-mail servers) Change parameters of filtering of spam, phishing and malware messages, at least at two layers (e.g. gateway and server) Creating, modifying and removing distribution lists (dynamic\static) Creating, modifying and removing connectors (send\receive) Creating, modifying and removing transport rules Creating, modifying and removing accepted domains	Standard Change	**Yes**
6.1.3.2.1 Active Directory Services	Creating, modifying and removing objects (such as users\groups\organizational units\group policy objects)	**Service Request**	**Yes**
6.1.3.2.2 DNS Service	Creating, modifying and removing zones (forward\reverse) Configuring forwarding and conditional forwarding	Standard Change	**Yes**
	Creating, modifying and removing records (A, CNAME, Reverse, TXT, SVR)	**Service Request**	**Yes**
6.1.3.2.3 DFS & SMB	Creating, modifying and removing DFS name spaces.	Standard Change	**Yes**
	Creating, modifying and removing folders (DFS\SMB (File shares)). Setting and removing permissions for shared folders. Creating, modifying and removing quota settings.	**Service Request**	**Yes**
6.1.3.2.4 DHCP service	Creating, modifying and removing reservations	**Service Request**	**Yes**

Service	Request	Initial min. level of maturity	Required after transition
6.1.3.2.5 PKI service	Creating, modifying and removing certificate templates	Standard Change	**Yes**
	Issuing and revoking certificates	**Service request**	**Yes**
6.1.4 Backup and restore services	Provision VM backups, filesystem backups, application aware backups. Configure backups via either RPO or ECHA backup policy	**Service Request**	**Yes**
	Restore from backups not related to Incident.	Normal Change	**Yes**
6.2.2 Service Management Tools	Manage add/remove/manage SMP users/groups, etc.	**Service Request**	**Yes**
6.2.3 Technical Monitoring and Reporting	Produce technical real-time report	**Service Request**	**Yes**
6.6.1 Vulnerability management service	Request vulnerability scan of target.	**Service Request**	**Yes**
6.6.2 Security monitoring	Request activation of standard rules for intrusion detection and prevention.	Standard Change	**Yes**
11.2.8 Invoicing and financial management	Produce financial real-time report	**Service Request**	No

6.4 Consultancy services

The Contractor **shall** be ready to deploy the professional profiles described in this section either onsite or offsite. The consultancy services can be required during normal ECHA working hours as well as outside ECHA normal working hours up to 7 days per week.

ECHA **may** ask for consultancy for all types of services and technologies in scope for this FWC, at any stage of the development of a service: in ITIL terms, this consultancy can be used when in service strategy, service design, service transition, service operations and continual improvement.

Typical examples are:

- Definition of requirements
- Requirements analysis and solution design
- Development of service catalogues
- Architecture of a service
- Writing of technical documents

- Transition to revamped service
- Market analysis and comparison of different technologies
- Test of solutions / elaboration of test/validation
- labs / pilots of services
- Service release management
- Incident management
- Configuration management
- Advanced installations and upgrades
- Engineering of existing or new solutions
- Training.

ECHA can request service integration advisory consultancy services. The Contractor **shall** have the capabilities and the capacity to provide such services. Such consultancy services can involve, among others:

- support in the establishment of an IT service integration function
- advice in the assessment of an integrated tooling solution(s) for incidents, reporting, ticketing, etc. used in a multi-party technical environment
- support in designing and aligning technical requirements in SLAs that will be used by various third parties of the Agency.

In order to perform such consulting services, the Contractor **should** be in a position to deploy various capabilities, particularly in the area of service design, both from the perspective of the individual hardware/software/service components involved as well as from the view of the performance of the resulting service vis-a-vis the business stakeholders of the service.

Professional profiles:

- Project Manager
- Consultant/senior consultant
- Junior Consultant
- Senior Engineer or architect
- Junior Engineer or administrator
- Trainer

The description of the profiles is not exhaustive and **should** be regarded as indicative.

6.4.1 Project Manager

Profile type	**Project Manager**
Job description	• Planning, execution and delivery of IT infrastructure projects • Resource planning, follow-up of staff activities • Project planning, definition of deliverables and milestones • Risk and problem analysis • Project reporting and monitoring, reporting • Involvement in ITIL design, transition and/or continual service improvement phases
Qualifications	• Certification or extensive experience in a project management framework • ITIL Certification or extensive experience in ITIL service management best practices

Profile type	Project Manager
Experience	• Minimum 6 years relevant hands-on experience acting as project manager for large IT infrastructure projects
Knowledge and skills	• Project management skills • Budgeting, organizational skills and analytical ability • Knowledge of project management and office automation tools • Presentation, communication and leadership skills • Understanding of systems management & technologies in scope of the contract • Solid documentation skills in English • Working knowledge, written and spoken, of English required.

1664 ### 6.4.2 Consultant/senior consultant

Profile type	Consultant/senior consultant
Job description	• High Level consultancy for infrastructure solutions in the scope of the contract • Solution oriented market watch on new technologies in the sector of the contract • Advise to customers on strategic orientation for current and future customer portfolio • Definition and development service portfolio • Provide technical lead • Involvement in ITIL strategy, design and/or continual service improvement phases
Qualifications	• Extensive experience on in networking and/or security technologies • Thorough knowledge of market and technology trends
Experience	• Minimum 6 years of experience as consultant for the services and technologies in scope of the FWC • Certification in a project management framework highly desirable • ITIL Certification highly desirable
Knowledge and skills	• Designing of enterprise architectures • Depending on the scope of the contract • Technologies in scope of the of the FWC • Excellent oral and written communication skills • Solid documentation skills in English. • Working knowledge, written and spoken, of English required.

1665 ### 6.4.3 Junior Consultant

Profile type	Junior Consultant
Job description	• Definition of customer reference configurations • Definition and planning of customer projects • Supervision of execution and delivery of projects • Risk and problem analysis • Provide a document framework with templates to ensure quality and a homogeneous approach concerning business documentation • Involvement in ITIL design and/or continual service

Profile type	**Junior Consultant**
	improvement phases
Qualifications	• Certification in the relevant technology field desirable • ITIL Certification desirable
Experience	• Minimum 2 years of experience as consultant in relevant technologies and services
Knowledge and skills	• Relevant technologies for the contract • Very good understanding of fundamental and advanced security concepts • Good experience with designing and maintaining SLAs (Service Level agreements) for solutions in scope the FWC • Organizational skills and analytical ability • Presentation, communication and leadership skills • Solid documentation skills in English. • Working knowledge, written and spoken, of English required.

1666 ### 6.4.4 Senior Engineer/Architect

Profile type	**Senior Engineer**
Job description	• Design and implementation of (converged) solutions in the scope of the FWC. Ensure that best practices adapted to the environment are applied. Security by design solutions • Handling of multiple simultaneous delivery and installation projects • Works under general direction of a Consultant • Provides technical lead for all systems • Define and assist in the implementation of policies on systems use and services, with the corresponding policy checks mechanisms.
	• Oversee installation, provisioning, troubleshooting and reporting with operational teams • Foster, develop and maintain relationships with technical counterparts at key manufacturer partners. • Prepare request for changes to the environment in the particular domain of expertise, and be peer reviewer of changes introduced by operational team. • Collaborate with the Consultant in the definition of the High Level Architecture. • Develop and enforce procedures to ensure high level of standardization/industrialization within operational team(s). • Coach junior engineer/Administrators. • Ensure that adequate systems monitoring is in-place and that alerting and reporting integrates into other technical teams and centralized monitoring systems. • Coordinate and implement proactive health-checks of components. • Report availability, capacity and performance metrics, with corresponding trends for the future. • Maintain technical documentation and provide feedback on possible improvements. • Schedule and manage changes and maintenance activities.

Profile type	**Senior Engineer**
	• Maintain required technical knowledge and certifications as specified by management • In collaboration with the customer develop the technical service catalogue and define KPI's • Provide a document framework with templates to ensure quality and a homogeneous approach concerning business documentation • Involvement in ITIL design, transition, operation and/or continual service improvement phases
Qualifications	• Architect certifications or extensive experience with network architectures
Experience	• Minimum 6 years relevant experience in projects within the scope of contract • Experience in multi-manufacturer environments • Experience in team-leading highly desirable
Knowledge and skills	• Excellent presentation, communication, analytical, organizational, time management and problem solving skills • Ability to communicate and collaborate in multi-culture environments • Solid knowledge of technologies relevant for the contract • Solid documentation skills in English • Working knowledge, written and spoken of English required • Good understanding of fundamental security concepts

1667
6.4.5 Junior Engineer/Administrator

Profile type	**Junior Engineer**
Job description	• Administer and operate solutions in scope of the FWC. • Involvement in ITIL transition, operation and/or continual service improvement phases • Manage Request for Changes and schedule maintenance activities. • Interface with manufacturer support • Leads field teams • Involvement in ITIL, transition, operation and/or continual service improvement
Experience	• Minimum 1 years relevant hands-on experience in projects within the scope of the contract
Knowledge and skills	• Good organizational and problem solving skills • Knowledge of technologies relevant for the contract • Understanding of fundamental and advanced security concepts • Presentation and communication skills are a plus • Solid documentation skills in English. • Working knowledge, written and spoken, of English required.

1668
6.4.6 Trainer

Profile type	**Trainer**
Job description	• Definition of training plans

Profile type	**Trainer**
	• Construction of training scenarios and courses • Writing training material • Training coordination and execution • Preparation of quality control reporting • Give training courses
	• Preparation of training materials/handouts • Feedback collection and quality control
Qualifications	• Post-secondary education studies of minimum three years in computer science or related field certified by diploma or 3 years of experience in addition to the experience 5-year experience requirement below.
Experience	• Minimum of 3 years of relevant training experience
Knowledge and skills	• Excellent communication skills • Good writing skills • Ability to cope with fast evolving technologies • Working knowledge, written and spoken, of English required. • Capability of working in an international/multicultural environment

6.5 Transformation services

ECHA can order work aimed at achieving specific objectives to be performed in project mode. By nature such work **shall** be one-off, that is: it starts when the objectives, the plans to achieve them and the resourcing have been agreed and it ends upon acceptance that the delivered work has attained the objectives, normally through the release of a number of deliverables defined and agreed by both parties.

Typically project mode will be applied to transformations of the portfolio or the underlying ICT infrastructure capacity. Examples of transformations are: upgrade of one of the services (e.g. due to technology changes), implementation of new service management tools (e.g. for monitoring), integration projects with other IT contractors of ECHA (e.g. integration of service management tools).

To support such projects the Contractor **shall** provide the following:

Transformation project management, covering: project analysis and definition, project planning, coordination of the execution of the plans, reporting, risk management and corrective action. The focus of such service **shall** be on business impact management, integration of all the actors involved and integration of the transformation into the FWC portfolio. In particular, this service **shall** identify the project deliverables and agree the acceptance criteria with ECHA, according to the principles of incremental delivery and milestone driven project management.

Solution architecture, covering the analysis and specification of appropriate technical architectures. The focus of such service **shall** be on impact analysis, integration with the other solutions in the portfolio and at ECHA. This service **shall** engage vendor's experts as necessary to validate the design, and adherence to the latest good practice, and possibly certify correct the solutions at no additional cost for ECHA.

Test coordination, covering the definition and planning of verification (correct implementation according to specifications) and validation (adequate implementation against customer's requirements) activities – potentially in consultation with ECHA and other IT contractors working for ECHA – executing of the test plans, reporting and corrective action.

Support to acceptance, covering the activities needed to facilitate ECHA's application of the acceptance criteria to the contractual deliverables.

On ECHA's request (*ECHA initiated transformation*), the Contractor **shall** provide adequate profiles (according to the requirements specified under section 6.4 Consultancy services) and sufficient resources to perform such services, normally under the terms set in a specific contract.

The Contractor also undertakes to perform their own transformations (*Contractor initiated transformations*, not necessarily requested by ECHA but necessary to keep adequate performance in the portfolio) through the appropriate combinations of the services described in this section, and giving visibility to ECHA of such initiatives. Typically own transformations are low if any impact for ECHA services and **shall not** be charged to ECHA.

Examples of *ECHA initiated transformations* could be:

- Transformation of ECHA's email system to Office 365.
- Expanding or replacing completely RSA based authentication with SMS based one-time passwords
- Replacement of Pulse Secure Access with for example OpenVPN or similar
- Refactoring of ECHA's on-premise networks and services to allows for higher latency and lower bandwidth between ECHA and the Contractor's datacentres to reduce WAN costs.
- Deployment of large volumes of Docker overlay networks as opposed to traditional topology.
- Deployment of desktop virtualization solutions (e.g. VDI, presentation/application/user virtualization).

6.6 Security Services

This sections illustrates the requirements for the specific security services; requirements related to the security components of other services are illustrated under the relevant chapter.

6.6.1 Vulnerability management service

6.6.1.1 Scope

The vulnerability management service **shall** cover the entire IT service portfolio for the FWC. The following tasks **shall** be performed in the scope of this service:

- **Vulnerability monitoring** (proactive security monitoring)
    - Continuous monitoring of different security sources of vulnerability information to identify new published software vulnerabilities. Also, active monitoring of new information[5] related to older vulnerabilities which are still open (=not yet remediated).
    - Regular (at least quarterly) vulnerability checks, e.g. by performing vulnerability and network scans, for all the systems belong to IT service portfolio, including managed networks. Missing security patches, misconfiguration and obsolete technologies **shall** belong to the scope of the checks.
- **Vulnerability analysis**. All the vulnerabilities **shall** be analysed without delay. ECHA specific criticality and urgency of the remediation actions **shall** be assessed by contextualising the vulnerability in ECHA environment and by taking into account (other) security measures and compensating factors in place. The criticality and urgency assessment **shall** be updated if further information is disclosed
- **A proposal for remediation actions** (e.g. remediated as a part of the standard regular patching or by initiating an emergency patching, a configuration change as a standard or emergency change etc.) **shall** be prepared and clearly communicated to ECHA. In case

[5] for example if an exploit to abuse the vulnerability is published or if there is a new malware widely spreading via this hole

that a primary remediation action is not yet available or cannot be applied to a critical vulnerability (e.g. if a patch is not yet available), possible temporary mitigation actions **shall** be assessed and proposed

- **Follow-up and metrics**. The Contractor **shall** follow up the remediation actions and maintain a list of the open vulnerabilities. The Contractor **shall** adopt metrics on vulnerability management (e.g. number of open vulnerabilities or mitigation time for the critical vulnerabilities). Whenever the metrics reveal systematic issues, a root cause assessment **shall** be carried out according to the model for *Problem Management* defined in ITIL.

6.6.1.2 Objectives

The main objective of the service is to detect and remediate vulnerabilities that exist in the service portfolio and to propagate that information to the relevant services.

6.6.1.3 Output

The service is delivered successfully when:

- All the new vulnerabilities relevant for ECHA are identified and analysed promptly after their publication (at least within 24 hours)
- Vulnerability checks (e.g. vulnerability scans) are performed regularly (at least quarterly) covering the entire IT service portfolio
- For critical vulnerabilities, which require urgent mitigation actions, remediation proposals are prepared and communicated to relevant parties immediately. For other vulnerabilities, remediation proposals are prepared and communicated in a timely manner.
- Practical metrics to control the vulnerability management process are defined and used to measure, and to improve when needed, the related processes and practices.
- At any given time, knowledge and documented records of which (known) vulnerabilities exist is available.

As an evidence of successfully delivery of the service, the Contractor **shall** share with ECHA an on-going list of relevant vulnerabilities and related information (e.g. criticality, proposed actions, remediation status etc.). This **should** be achieved by e.g. providing continuous online access to a tool or by monthly reporting.

Performed regular vulnerability checks (e.g. vulnerability scans) and the relevant results **shall** be reported to ECHA quarterly. Measured metrics and improvements **shall** be regularly (at least quarterly) reported to ECHA. In the reports, a unique CVE (Common Vulnerabilities and Exposures) identifier **shall** be linked to each publicly known security vulnerabilities.

While security checks (e.g. vulnerability scans) can be performed over network, the service **shall** cover also locally exploitable vulnerabilities.

6.6.2 Security monitoring

6.6.2.1 Scope

The security monitoring service encompasses reactive detective activities, such as real-time and log monitoring, correlation and analytics. In other words, the service is related to events that are in progress or have already occurred, for example intrusions, malware infections and misuse of computing systems. As security incident response service is defined as a separate service, the response actions are not in the scope of the security monitoring service.

Security monitoring service **shall** cover the whole IT service portfolio provisioned under this

FWC. Workstations and application level security monitoring is limited to the related network traffic.

The security monitoring service **shall** cover the following activities:

- Orchestration (management of the security monitoring solutions):
    - Provide and manage a centralised solution for collecting, processing and monitoring security events (e.g. SIEM)
    - Collect security events from all the relevant sources across the infrastructure (e.g. network devices, operating systems, security solutions) to the centralised solution, including configuration of the sources, if needed
    - Provide solutions (e.g. IDS) to generate security events in addition to existing sources
- Automated processing and analysis of the collected information:
    - Correlation of events
    - Alerting based on different factors (signatures/IOC, thresholds to detect unusual activities, etc.)
    - Visualising and providing relevant information in a format understandable for humans
- Human based monitoring by security experts
    - Monitoring alerts, dashboards and other output provided by monitoring system
    - Analyses of alerts and other relevant information in order to determine actual suspected cases and false positives
- Escalation and reporting
    - (Suspected) security incidents escalated to Security Incident Response service
    - Regular reporting

6.6.2.2 Objectives

The primary purpose of the security monitoring service is to detect intrusions and other security incidents at an early stage and activate incident response. Thus, the goal is to provide visibility of security events and ongoing activities, in order to reveal any malicious and unusual activity reliably and quickly. The longer an attacker operates undetected, the greater the long-term impact on the ECHA business will be and higher the probability of unauthorised access to the most sensitive business information.

Effective security monitoring service means a high detection ratio of occurred incidents or attempts (i.e. low false-negative) and low number of false-positive events. The service requires continual improvements, optimisation and fine-tuning.

6.6.2.3 Output

Security incident cases with the relevant details promptly identified, accurately analysed and swiftly moved to the security incident response service.

Regular (monthly) reports **shall** be provided at least with the following details:

- A list of the source systems (list of log sources and real time monitoring sources)

    - Number of alerts and other cases analysed, number of cases moved to security incident response

Improvements, optimisations and fine-tunings conducted for the monitoring system and service **shall** be reported quarterly.

6.6.2.4 Requirements

The services **shall** be provided by using state-of-the art tools and technologies.

6.6.3 Security incident response service

6.6.3.1 Scope

The security incident response service **shall** cover all the security incidents related to the entire IT service portfolio of this FWC. Thus, the main activities in the scope of the service are:

- Initial assessment of the situation.
- Collecting evidence.
- Investigation and analysis.
- Containment actions.

  ECHA **shall** indicate which containment actions can be implemented without ECHA's approval.

- Recovery and improvements.
- Reporting to ECHA.

Whilst identifying and collecting suspected malwares and other malicious components is part of the incident response service, malware analysis work is out of the scope of the service.

If the attack is targeted to or mostly affects the IT service portfolio in the scope of this FWC, the Contractor **shall** coordinate the whole technical incident response. Otherwise, the Contractor's role is limited to support[6] the incident response coordinated/managed by another party. In such supportive role, the Contractor does not usually perform all the actions listed above, but only what coordinator requests.

Usually the service request is triggered by the security monitoring service but in some case might be requested by ECHA or another contractor of ECHA.

In the case of a data breach the Contractor **must** inform ECHA without undue delay. Specifically, in the case of personal data breach the Contractor **must** inform ECHA no later than 24 hours after detection (c.f. Article II.9.10).

6.6.3.2 Objectives

The main goal of the service is to help minimising the impact of occurring security incidents by prompt and effective response actions before the attacker has broken the last layer of defence and achieved access to ECHA's most sensitive business information. In addition to securing confidential information, the service helps a quicker recovery from security incidents (e.g. ransomware or other malware cases).

An objective of the service is also to help prevent similar issues in the future and make correct improvements by identifying how and why security incident has occurred and which weaknesses were exploited. It is also important to determine which confidential business information is

[6] For example investigate network logs related to the case

potentially accessed, stolen or leaked as a result of the incident.

6.6.3.3 Output

A detailed investigative report, with the following content, **shall** be provided at the end of every security incident response coordinate by the Contractor:

- Management summary
- A detailed description of the incident with a timeline of malicious activities and impact on ECHA (with details of affected systems, networks, user accounts etc. as well as which information is accessed or stolen). It **shall** contain the root cause assessment
- A detail description of response actions and proposed improvements: containment and recovery actions and includes recommendations to enhance security controls.

All the collected evidences **shall** be delivered to ECHA if requested.

The Contractor **shall** have deep technical capabilities (skills, experts available and tools) to investigate security incidents, including live response, forensic, network traffic and log analysis.

All the forensic evidence **shall** be collected and preserved so that formal requirements for law enforcement and prosecution are fulfilled.

7 IT Business Continuity

ECHA has developed its own IT Business Continuity Preparedness Plan (IT-BCP, ref. Annex 3: IT BCP - IT Continuity Technical Preparedness Plan (CMO)). The Plan covers the architecture put in place to ensure resilience and recovery targets. The Business Units of ECHA have developed BC plans. The IT-BCP supports those business BC plans.

It is expected that the Contractor collaborates with ECHA to improve the relevant IT-BCP aspects by helping to develop strategies to minimize and mitigate the risk for specific events concerning this FWC and for which the involvement of the Contractor is necessary. Such collaboration **shall** be done at no cost for ECHA.

The Contractor **shall** cooperate as well in the testing of the disaster recovery plans (desk or live exercises). The provider accepts the obligation to contribute to the recovery of the ECHA services in case the IT-BCP is invoked.

In this chapter we illustrate two aspects:

- How ECHA IT has achieved and maintained preparedness to support the business continuity objectives of the organisation and how such preparedness is regularly tested. This represents contextual information relevant for the services in scope of this FWC. A comprehensive description is provided in Annex 3: IT BCP - IT Continuity Technical Preparedness Plan (CMO). In this context, the Contractor, on demand, **shall** be ready to provide consultancy services to support ECHA's testing activities;

- The requirements related to business continuity management on the Contractor's operations.

7.1 Business continuity requirements on the Contractor's operations

The Contractor **shall** integrate this FWC into its own BCP and will be asked to provide a document describing the relevant part of their Business Continuity Plan. It will specify the Recovery Time Objective (RTO) for the services so that ECHA can take it into account in its own IT-BCP.

In particular, the Contractor **shall**:

- Create or amend and maintain Business Continuity and Disaster Recovery Plans (BC/DRPs), based on scenarios and as described in the Service Description for the Services. Such plans **shall** be made available to ECHA for review, on demand, and then refined where required (i.e. taking into account legitimate expectations of, and feedback from ECHA).

- Explain in the above BC/DRPs, with respect to all service delivery facilities envisaged to be engaged in contract implementation (except data-centres and facilities already accepted under the FWC), how resilience of service delivery and service continuity, i.e. protection against site-failure, will be achieved throughout contract implementation. Note that this not only refers to technical solutions facilitating system (e.g. VM or storage) fail-over, but also to all other and organisational matters, also across countries where applicable.

- In close liaison with ECHA, document the BC/DR testing strategy and perform regular BC/DR tests (including service failover across data-centres and across other service delivery sites, as appropriate). Submit a testing report to ECHA.

- Regularly audit the above BC/DRPs practices, e.g. against the standard ISO 22301.

The document **shall** include clear crisis management and contingency operation procedures. If a crisis is triggered by the Contractor, affecting the services for ECHA, the document will clarify the way in which ECHA (IT Business Continuity manager) will be notified and the timeframe. In such case, the Contractor **shall** produce an action plan in collaboration with the ECHA IT Business Continuity Manager. The Contractor **shall** ensure that regular updates about the crisis situation are given to ECHA IT Business Continuity Manager and relevant ECHA Service Manager(s).

8 Transition of services

Transition of services is divided into two parts, transition in and transition out (exit).

8.1 Transition in

The transition in of the services in scope **shall** be done with the absolute minimum amount of required transformation. In other words, the Contractor **shall** clearly identify in their offer how well the CMO described in the CMO Annexes (ref. section 3.1 Current Mode of Operations (CMO)) can be migrated to FMO and the amount of transformation of the CMO services needed.

8.1.1 Model for transition

Transition will be done in the form of a transition project the aim of which is to establish the FMO. The Contractor will be responsible for the transition project (including the interaction with the Incumbent(s)) and submit an initial plan as part of their offer. In such offer the Contractor **shall** specify requirements for exit tasks on the Incumbent(s). To this effect the Contractor is expected to carefully analyse the CMO Annexes (ref. section 3.1 Current Mode of Operations (CMO)).

As soon the FWC is signed ECHA will engage the Contractor in the preparation of:

1. Governance Contract, a refinement of the governance model specified in section 9 Governance
2. Transition project Contract, a refinement of the plan provided in the offer
3. Exit agreement with the Incumbent, based on the requirements expressed by the Contractor and their compatibility with the contractual obligations of the Incumbent(s).

Regular Service Contract(s) will follow.

ECHA envisages **a full transition to FMO in nine months after signature of the FWC** at least the following milestones in the transition project:

- M1 Readiness of the cloud infrastructure provided by the Contractor for migration of services; no later than six months after the signature of the FWC;
- M2 Migration of services complete; no later than three months after M1
- M3 services ready in the FMO (and complying with the required requests table, ref. 6.3.9 Required Requests); no later than three months after M1;
- M4 SMP ready for use; no later than three months after M1.

Readiness include successful acceptance testing and successful Disaster Recovery testing when applicable. The numbering of the milestones does not mean sequencing. However, the FMO is considered "established" on achievement of M3 and M4.

> **Note**: The Incumbent for most services in scope is bound by ECHA's current FWC (ECHA/2010/95) to actively collaborate with the Contractor to *"ensure the smooth transitioning or interconnection of the services, to minimise costs and to guarantee the continuity of services for the Agency, especially when the Framework Contract will be nearing its end."*
>
> Furthermore, the Incumbent shall provide any information, documentation and other materials, support, training, consultation, cooperation and help in the transition of services as can reasonably be expected. Most of this documentation is in a Microsoft SharePoint knowledge base in electronic format, which ECHA requires to be migrated.
>
> Finally, the Incumbent shall in cooperation with ECHA provide a phase-out transition plan *"setting forth (in such detail as may reasonably be required) the measures, processes and procedures required to ensure a successful and smooth transition of the services."*
>
> Likewise, for managed network services, ECHA has another Incumbent (here called Network Incumbent) who is bound by a Contract (ECHA/2017/058) to

> *"… provide termination assistance as requested and ordered by ECHA.*
>
> *The Contractor shall assist and contribute in all reasonable ways to guarantee the successful and smooth transition of required services to a new service provider as well as to provide any information, documentation and other materials, support, training, consultation, cooperation and help in the transition of services as can reasonably be expected and as required by ECHA."*
>
> The Network Incumbent shall also in cooperation with ECHA provide a transition plan *"setting forth (in such detail as may reasonably be required) the measures, processes and procedures required to ensure a successful and smooth transition of the services."*

The aim of the transition work stream is to minimize interruptions to services during the transition from the Incumbents.

Depending on the Contractor's proposal, it is possible that **the Contractor's datacentres have to be temporarily connected to the Incumbent's datacentres for migration purposes during the transition-in project**. The tasks related to commissioning, testing, using and decommissioning such temporary connectivity **shall** be included in the transition-in plan and they will be performed under the responsibility of the Contractor. Such connectivity services **shall not** be delivered over the public internet, but rather with private networks or point-to-point connections. The hardware, carrier and any other possible systems required **shall** be provided by the Contractor without exception. The temporary connections' **shall not** be a bottleneck constraining the ability of the Contractor to perform the transition-in project according to the model above and to meet the timeline of the milestones above. To the contrary, the Contractor **shall** choose the options that can ensure an optimal balance of time, cost and ECHA efforts whilst mitigating the risk of interruption of services.

In the transition project, under the overarching responsibility of the Contractor's project manager, ECHA will appoint a **team for coordination of the transition** who will have responsibility for:

- Coordinating the overall activity within ECHA, between different business and IT units. In particular, coordination with parallel relevant projects like the building project (ref. section 2.3 Elements for consideration)
- Resource provisioning. This entails ensuring appropriate availability of human resources from ECHA and said third parties to enable accomplishment of the transition activities.
- Communication and change management. This entails providing information to all audiences and stakeholders affected by the service, including users, business heads, IT and third parties.

The Contractor, ECHA and the Incumbents will establish a joint Project Board for the governance of the transition project. The Contractor **shall** be in charge of the secretariat of the Project Board.

ECHA does not envisage a piecemeal transition of individual services into the FMO outside of the transition project. However, it is possible that once M4 is achieved the milestone M3 is achieved by a staggered approach.

8.1.2 Transition plan

The transition plan is the key planning document for the transition from CMO to FMO services. The transition plan **shall** be created and updated by the Contractor. Project changes in the execution of the transition plan have to be agreed between the parties at project Board level. In any case the Contractor **shall** deliver at least the deliverables agreed as part of their offer.

The transition plan **shall** identify at least the following:

- Transition strategy
    - Requirements for exit tasks on the Incumbent(s)

    - Contribution expected of ECHA
    - Project management approach;
- Transition Work Breakdown Structure
- Transition timeline (including at least M1, M2, M3 and M4)
- Transition Cost Breakdown Structure and estimates
- Transition project organisation (roles and responsibilities of all parties)
- Migration (VMs and backups)
    - Approach
    - Timeline
- Transition of services to FMO
    - Technical aspects
    - Service management aspects
    - Administrative aspects
- SMP preparation and release
- Estimated efforts
    - required by ECHA
    - required by the Incumbents
    - required by the Contractor
- Knowledge transfer required
- Service transformations required
- Possible known service outages
- Acceptance testing (UAT) approach
- Impact to ECHA and third parties
- Risk analysis.

The transition plan **shall** have a related risk log that is continually updated and monitored by the Contractor.

8.1.3 Service model

The transition in project **shall** produce a service model document. This document is inherently different from service descriptions, as it is envisaged to be the cornerstone of the interaction between ECHA, ECHA's third parties and the Contractor.

The service model **shall** act as a manual for using the services and enable a party not familiar with the services to use them.

The service model **shall** include at least the following:

- Contractor account organisation
- Interfaces for service delivery to ECHA
- Interfaces and approaches for interaction with ECHA third parties.
- Processes
    - Incident Management
    - Security Management
    - Change Management and Service Request Fulfilment
    - Configuration Management
    - Problem Management
    - Capacity Management
    - Patch Management
    - User & Access Control management
    - Service provisioning
    - Business continuity
    - Disaster recovery
- Defined
    - Service Requests
    - Standard Changes
- Contact and escalation lists

8.1.4 User acceptance testing

User Acceptance Testing (UAT) for Transition in will be performed for M1, M2, M3 and M4.

The UAT of M4, and also in general, **shall** include at least testing of Service Requests, incidents and Standard Changes (ref. 6.3.9 Required Requests) against the service model.

The UAT of M1 **shall** include at least the migration of test VMs from the current infrastructure to the new infrastructure of this FWC. This is to ensure that the service is ready for production grade use and to ensure the workability of the migration strategy.

The UAT in general **shall** also include testing of Disaster Recovery coverage. Furthermore, backup and restore functionality **shall** be tested according to requirements in section 6.1.4 Backup and restore.

The UAT **shall** include performance testing on technical components in line with the Contractor's offer.

The Contractor **shall** together with ECHA create a UAT plan. For completion of UAT, the Contractor **shall** provide a UAT report supplemented with evidence that tests have been successfully completed.

8.2 Transition out

During the implementation of the FWC, the Contractor **shall** actively collaborate with other providers of comparable services designated by ECHA to ensure the smooth transitioning or interconnection of the services, to minimise costs and to guarantee the continuity of services for the Agency, especially when the FWC will be nearing its end. In this case, the Contractor **shall** provide termination assistance as requested and ordered by ECHA, irrespective of the reason for termination.

Towards the end of the FWC, ECHA will begin preparations for a full transition of all in-scope services to a future FWC (**transition out**). The Contractor **shall** be responsible to support ECHA in such preparations and of the execution of their part of the transition out, in good collaboration with the new contractor if this is the case.

The Contractor **shall** perform the transition out in a manner that maximises efficiency and minimizes downtime, risk, efforts and cost to ECHA.

The Contractor **shall** assist and contribute in all reasonable ways to guarantee the successful and smooth transition of required services to a new contractor, this can entail knowledge transfer and consultation.

The Contractor shall provide and migrate any information, documentation and other materials, generated for ECHA in the execution of this FWC, in particular in the fulfilment of the provisions and requirements set in section 9.4 Knowledge sharing, documentation management, ticket management, performance monitoring.

The Contractor **shall**, at the request of ECHA and in cooperation with ECHA, prepare, maintain, update, and deliver to ECHA – for approval – a **transition out plan** setting forth (in such detail as can reasonably be required) the measures, processes and procedures required to ensure a successful and smooth transition of the services.

Any changes to the technologies or services during the lifetime of the FWC **should not** negatively impact a smooth transition out.

9 Governance

Governance **shall** be articulated around specific roles and two levels of cooperation between the parties.

9.1 Roles

The Contractor **shall** appoint at least:

- A **Programme Manager**, to be the reference person for the interaction with ECHA on the entire scope of the service portfolio, the Contractor performance, the procurement and financial aspects.

- A **Service Delivery Manager (SDM) function**, responsible for fulfilling the requirements of the FWC and of the specific contracts in the regular provision of the services, including SLAs. The SDM function is the point of contact for ECHA in the day to day management of the service. It propagates the voice of the customer inside the Contractor's organisation. The SDM represents the point of contact for cooperation and is jointly (with ECHA) responsible for the integration and on-going development of processes with third parties, under the general coordination of ECHA.

- A **Chief System & Solution Architect (Technical Lead)**, responsible of following all the architecture aspects ensuring continuity of service and proper knowledge transfer to other experts or engineers, notably during transition and transformation projects. This role is used as an interface between ECHA and the Contractor to have technical discussions, service related planning and decision making easier. The Technical Lead **shall** familiarize himself with ECHA's environment, be able to see the big picture and know the interdependencies between services, environments and systems.

- A **Contract Security Manager**, responsible for all aspects of security related to this FWC. The Contract Security Manager is the point of contact for ECHA in the day to day management of security. It propagates the voice of the customer inside the Contractor's organisation;

ECHA will appoint:

- An **Outsourcing Service Manager**, to be the reference person for the interaction with the Contractor on the entire scope of the service portfolio, the Contractor performance, the procurement and financial aspects at FWC level. The programme manager **shall** have the authority to take decisions on all aspects of the FWC within the boundary of their delegations in ECHA;

- The **Executive Authority** for this FWC with delegations on financial matters;

- One or more **Contract Managers** for the Specific Contracts signed in the implementation of the FWC;

- One or more **Service Managers**, responsible of interfacing the SDM and integrating the services provided under this FWC with the other services of the organisation.

- One **ECHA Security Manager.**

9.2 Levels of cooperation

9.2.1 Steering Committee Level

The purpose of this level is to accompany the transition, supervise the transformations, monitor the regular performance in the delivery of the services, handle exceptions, and ensure continuous improvement.

The Committee permanent members:

- **ECHA:**
    - Executive authority
    - Outsourcing Service Manager
    - Service Owners, normally middle management
- **Contractor:**
    - Programme Manager
    - SDM

Regular participants, depending on the agenda: Contract Security Manager, ECHA Security Manager, Chief System & Solution Architect

Regular agenda points:

- Status of the portfolio (particularly SLAs status)
- Roadmap (including optimisation initiatives)
- Customer satisfaction analysis and service quality matters
- Status of security (at least quarterly)
- Financial matters

The Steering Committee meets at least monthly during transition in or out and at least quarterly thereafter.

The Contractor **shall** provide the secretariat for the Steering Committee and be responsible for: agenda preparation, preparation of the background material in their competence, drafting of the minutes within one week, following through the approval of the minutes by both parties.

ECHA commits to providing a response to the draft minutes within one week.

9.2.2 Operational level

The purpose of the operational governance is to enable both parties to handle changes, problems, issues and opportunities for improvement appropriately.

The SDM is regularly represented at the ECHA relevant Change Advisory Board(s) meetings, and partakes in change planning and coordination with ECHA third parties.

The SDM chairs regular service portfolio meetings with the ECHA Service owners, service managers and Outsourcing Service Manager to discuss the status of the portfolio, analyse issues, improvement possibilities and relevant incident reports. Such regular meeting is a key opportunity for communication and mutual understanding, ultimately alignment of expectations.

The SDM works with ECHA and the ECHA third parties to identify areas of improvement in the common processes.

Unless otherwise agreed, the SDM is responsible for the minutes of the meeting.

9.2.2.1 Security operational level

The ECHA Security Manager and the Contract Security Manager cooperate actively at this level.

The purpose is to:

- ensure regular monitoring of the status of security for the services in the scope of this FWC.
- actively propose security improvements and analyse proposals, follow-up status of the agreed security related improvements
- analyse potential risks and issues
- discuss on security related changes, occurred security incidents
- report regularly to the Steering Committee.

Unless otherwise agreed, the Contract Security Manager is responsible for the minutes of the meeting.

9.3 Working with third parties

The Contractor will operate in a multi-party environment. In the ECHA IT sourcing strategy software and application management services, and software development are outsourced. As an important part of the quality of the service, the Contractor **shall** be committed to acting independently in the delivery of the services by proper communication and collaboration with all such parties. ECHA **shall not** be expected either to play a mediation role in every discussion, ticket, email thread etc. or to be responsible of all communication between different parties.

The Contractor is expected to develop an understanding of the end-to-end processes linking the contribution of the different parties and to actively strive to maximise the added value of their contribution.

9.4 Knowledge sharing, documentation management, ticket management, performance monitoring

The Contractor **shall** populate a knowledge base with the content relevant to the management of the services in scope and the FWC governance.

Such content **shall** cover at least:

- Contact information, also in case of escalations and crisis
- Contractual documents
- Relevant technical documentation
- Supporting material for running the FWC governance
- Change management information

The Contractor and ECHA **shall** apply documentation control to the documents in the knowledge base, notably when subject to approval.

The knowledge base **shall** always be the single source of truth for its content. The content **should** be maintained up-to-date, and as an important part of a transition out at the end of the FWC **should** contain all the relevant content for this activity.

The Contractor **shall** be ready to provide a secured hosted solution and make it accessible to ECHA, if we so required, as part of the "governance services specific contract".

ECHA **may** also decide to offer an ECHA solution, either at the start of the implementation of this FWC or during its course, in which case the Contractor **shall** be ready to use such solution. Content migration services, if necessary, will be the object of a specific transformation contract.

The Contractor acknowledges that the content of the knowledge based created for the execution of this FWC is the property of ECHA. Pre-existing content shared with ECHA to the benefit of this FWC **shall** remain the property of the Contractor unless otherwise agreed by the parties.

The Contractor **shall** be ready to collaborate with the Incumbent(s) in the migration of content from the current knowledge base hosted by the Incumbent(s) during the transition-in phase.

The Contractor **shall** collaborate with ECHA to integrate the respective ticket management systems in the most efficient and effective manner for the parties. If needed, integration work (e.g. development of interfaces) besides configuration of existing tools, **shall** be chargeable and part of the transition-in contract.

The Contractor **should** offer a dashboard and user friendly access to an overall performance monitoring console to support the management of this FWC. Such performance monitoring console **should** cover elements such as:

- Status of SLA compliance
- Status of the on-going transformation projects
- Status of the rolling optimisation plan
- Status of security.

In their offer, the Contractor **should** target meaningful and compact information for middle to senior management regarding the overall performance of the portfolio of services and projects.

9.5 Customer satisfaction management and poor performance claim

Customer satisfaction **shall** be the core of assessing the performance of the Contractor on the entirety of the portfolio. Therefore, a customer satisfaction management process **shall** be put in place by both parties, according to the following requirements:

Plan

Customer satisfaction key measurements and related targets are agreed in the Steering Committee at the inception of this FWC; such measurement are as far as possible harmonised across the service portfolio and reflect the business value to ECHA of good performance in the delivery of the services

Do

The Contractor collects customer satisfaction data regularly (e.g. monthly) at operational level (including the security operational level) and at steering level (e.g. quarterly); ECHA commits to contributing as far as needed to such collection, timely and accurately (e.g. by responding to survey questions)

Check

After collection, the Contractor elaborates the data to express the status and the trends in a customer satisfaction status report that will be analysed together with ECHA at the appropriate governance level

Act

Depending on the reported status, corrective and preventive actions and related timelines **shall** be agreed at the appropriate level of governance. The Contractor **shall** present an action plan that **shall** be adopted and strictly monitored at the Steering Committee level.

Repeated failure to implement the action plan, defined as three consecutive "execution off-track" assessment outcome in the Steering Committee, can result in a justified "poor performance claim" on the Contractor, subject to the provisions of Art I.15.1

The precise customer satisfaction management process **shall** be defined in the “governance services specific contract” covering the start-up and the regular provision of the service.

9.6 Innovation

ECHA **may** launch an innovation procedure to introduce services and/or technologies in the FWC, in accordance with Art. I.5.4. of the draft framework contract.

In consultation with ECHA, the Contractor **shall** prepare an offer (technical and financial) based on the following elements:

The innovation **shall** re-use suitable service elements already foreseen in the FWC. For example, if the output of the innovative service is comparable or equivalent to the output of a foreseen service, such similarity **should** be leveraged and emphasised;

The daily fees used to cost the innovation, when referred to consultancy services, **should not** deviate from the ones offered for the consultancy services foreseen in this FWC unless duly justified by a well substantiated difference in the competences and by a market benchmark;

Any remaining gaps and mismatches **shall** be filled with reasonable and realistic estimates, preferably based on market benchmarks that the Contractor **shall** justify.

On positive assessment of the offer, ECHA can propose an amendment of this FWC to reflect the innovation.

Disagreements on innovation related issues **shall** be resolved via the governance mechanisms of the FWC at steering committee level.

10 Continuous optimisation and cost reduction over time

ECHA is striving for optimisation of services, solutions and costs. By managing this service portfolio the Contractor will be in a position to recommend and propose optimisations, ultimately leading to better services, better performance and reduction of cost.

Both parties can initiate optimisation actions; however, ECHA wants to create incentive in this regard.

The Contractor **shall** identify and collect "qualified" optimisation proposals and be responsible for a rolling optimisation plan to be updated at least once a year (in synchronisation with the planning cycle of ECHA) and discussed at the appropriate level of the FWC governance.

Examples of optimisations include, but are not limited to, the following:

- Continual efforts to automate changes, i.e. Normal Change to Standard Change and Standard Change to Service Request, to minimize effort spent on change management.
- ECHA usage and uptake of Contractor off-the-shelf solutions;
- Integration of IT Service Management systems;
- Integration of managed services automation tools, e.g. configuration automation, into Cloud management automation and orchestration;
- Usage of auto-scaling (e.g. vertical and horizontal) solutions for demand driven usage of services and invoicing.

A "qualified" optimisation proposal **shall** at least contain the following elements:

a) Definition of the optimisation target in a measurable manner

b) Justification

c) Impact analysis

d) High level estimation of the implementation cost

e) High level estimation of the benefits.

The Contractor **shall** elaborate the agreed optimisation proposals into an implementation plan as part of the governance.

Depending on the nature and size of the optimisation, the plan can become a transformation project and the subject of a specific contract.

It is ECHA's expectation that over time the cost for services will decrease. The driver behind ECHA's expectation is that the parties **shall** implement a rolling optimisation plan and the Contractor **shall** continuously work to automate service delivery.

Due to the investments into automation and optimisation, the regular services fees and usage of efforts **should** decrease.

From the second year until the end of the FWC (5th year), thanks to the aforementioned optimisation plan, ECHA expects to achieve up to 5% reduction of the annual cost, implemented through price revision of the offered prices. Further consolidated savings up to 2% are expected for the two additional years of extension. Part of the savings can be reinvested by ECHA in the rolling optimisation plan.

If the Contractor is unable to deliver savings according to these expectations, they **shall** submit a recovery plan.

11 SLA and pricing

The Contractor **shall** provide services to ECHA based on the FWC Price Catalogue following the model in this section.

As part of the financial proposal, the Contractor is required to provide the rates (in €) for this model.

During the execution of the FWC, these rates will be used to determine the rates at which the services are to be offered and procured via Specific Contracts.

These rates, multiplied by the estimated consumptions defined by ECHA (Price Model), are used as part of the Financial Award Criterion to determine the value of the financial offer of the Contractor.

11.1 Service Level Agreement

The Service Level Agreement (SLA) is divided into three categories:

1. Availability
2. Incidents
3. Requests

All three categories make reference to the Service Band of the service.

When a breach of an SLA is discovered, ECHA **shall** be immediately informed. The Contractor **shall** make efforts to automate the discovery of deviations from the SLA and escalation triggering as much as possible, as it is ECHA's experience that manual incident discovery and reporting can cause major inefficiencies and loss of trust between parties.

SLA breaches **shall** lead to automatic triggering of an alert to the appropriate responsible person at ECHA; in clear and indisputable cases, penalties **shall** automatically be addressed in the relevant invoices as soon as possible.

11.1.1 Service Bands

Service Bands at which the Contractor **shall** be able to deliver the respective service are defined below. Different price tags **may** be associated with different Service Bands.

Service Bands relate to weekdays and weekends, irrespective of national or pan-EU holidays. All times refer to the time-zone and possible daylight savings where ECHA premises are (currently Eastern European Time).

Table 14 Definition of Service Bands

Service Band	**9/5**	**12/5**	**24/5**	**24/7**
Service days	Mon – Fri	Mon – Fri	Mon – Fri	Mon – Sun
Service hours	08:00 - 17:00	08:00 - 20:00	00:00 - 24:00	00:00 - 24:00
Availability	98.0 %	99.0 %	99.5 %	99.8 %
RPO	Depends on backups	Depends on backups	~zero seconds	~zero seconds
Scheduled downtime: allowed time-band	Outside 12/5	Outside 12/5	Outside 24/5	Outside 24/5
Maximum allowed time for running on only one datacentre	N/A	N/A	48 hours	12 hours

Most of the services of the FWC are defined in a Service Band that defines Availability and the

Recover Point Objective (RPO) for the service. Such Service Bands can also be called “service hours”.

Availability is a measure of the extent to which the service is available to perform its tasks. At the level of specific contract, ECHA retains the right to decrease the requested availability for a specific service(s) (i.e. 'relax' the availability).

Availability **shall** be counted as an aggregation of time over the month within the period of the applicable Service Band. In other words, if there are periods of non-availability of the service outside of the hours of the Service Band, this **shall not** impact on the availability calculations made in the context of the contract SLA.

'Pre-agreed with ECHA' downtimes of the service during service hours (i.e. within the hours of the Service Band) due to Contractor maintenance activities, **shall** be excluded. Likewise, non-availability due to reasons beyond the responsibilities or scope of the Contractor **shall** be excluded.

The Contractor **shall** report availability based on the SLA but also actual availability including agreed service breaks.

Availability **shall** be measured based on automated, regular and frequent measurements to be agreed, implemented, taken and reported monthly by the Contractor. ECHA reserves the right to simultaneously monitor availability.

The table below depicts the Service Bands for the services of the FWC.

Table 15 Services and their defined Service Bands

Service	9/5	12/5	24/5	24/7
6.1 Cloud and Infrastructure Services				
6.1.1 Managed Datacentre				X
6.1.2 Managed ECHA LAN and WAN				X
6.1.3 Office automation				X
6.1.4 Backup and restore services				X
6.2 Service Management Portal				
6.2 Service Management Portal				X
6.3 Service management				
6.3.2 Service Desk		X		
Capacity to react to Major, Priority 1 incidents and security incident				X[7]
6.3.4 Event management	X	X	X	X
6.3.5 Incident management	X	X	X	X
6.3.6 Problem Management	X			

[7] Service Desk response limited to Major and P1 Incident Management.

Service	9/5	12/5	24/5	24/7
6.3.7 Service Request Fulfilment[8]		X[9]		X[10]
6.3.8 Change Management	X			
Change implementation				
6.3.8.1 Standard Change		X		
6.3.8.2 Normal Change (generally happens outside ECHA normal working hours)	X[11]	X[12]	X	X
6.3.8.3 Emergency Change				X
6.6 Security Services				
6.6.1 Vulnerability management service				X
6.6.2 Security monitoring				X
6.6.3 Security incident response service				X
Horizontal				
6.4 Consultancy services	N/A	N/A	N/A	N/A
6.5 Transformation services	N/A	N/A	N/A	N/A
9 Governance	N/A	N/A	N/A	N/A

11.1.2 Incident management

Incidents are measured for their Maximum Incident Response Time and Maximum Incident Resolution Time under the SLA.

11.1.2.1 Incident Response Time

Incident Response Time is the time elapsed, counted within the service hours of the chosen Service Band, between a. the moment that the Incident occurs and b. the moment that the Contractor communicates to ECHA the ticket number or other record has been logged and the Incident Management procedure has been triggered. The response **may** be an automated response. The response **shall** inform ECHA of the ticket or record number assigned to the Incident.

The time the Incident is detected can differ from the time the Incident occurs and ECHA will whenever possible use the moment the Incident occurs as the basis of the response time calculations.

The **Incident Response Time shall be <= Maximum Incident Response Time** described in the table below.

[8] Service Requests referred to in 6.3.9 Required Requests **shall** be available through the SMP, thus triggering a SR is 24/7. In this table we refer to the fulfilment of the request.
[9] If fulfilment requires manual intervention.
[10] If fulfilment is automated.
[11] Subject to impact of Change.
[12] Subject to impact of Change.

11.1.2.2 Incident Status Notification

The Contractor **shall** regularly notify ECHA of the status of the Incident. The notifications only need to occur within the service hours of the chosen Service Band.

11.1.2.3 Incident Resolution Time

Incident Resolution Time is the time elapsed, counted within the service hours of the chosen Service Band, between a. the moment that the Contractor responds to the Incident (informing ECHA of the ticket number), and b. the moment that the Contractor resolves the Incident.

The **Incident Resolution Time shall be <= Maximum Incident Resolution Time** described in the table below.

11.1.2.4 Timers

The Contractor **shall** use their best endeavours to resolve Incidents within the Maximum Incident Resolution Time. The Contractor **shall** monitor and measure Response and Resolution times, and report them back to ECHA, in particular highlighting breaches. For any SLA breach the Contractor **shall** draft a separate Incident report with root cause of the Incident and remedial actions to be taken to avoid such incidents in the future.

Upon request of ECHA the Contractor **shall** make available all reasonable material relating to the Incident handling, including activities and timings. Evidence can include amongst other things, evidence showing at what moment in time the Incident occurred, at what moment in time the Incident was detected (or the Contractor received the information from ECHA to inform that the Incident had occurred), and at what moment in time the Contractor notified to ECHA the ticket number.

Irrespective of the maximum resolution time described above, the Contractor **shall** use their best endeavours to resolve incidents of all priorities, sufficiently quickly to ensure the undesired impact of the Incident is kept to the minimum.

Table 16 Incident timers

Priority	**Maximum Incident Response Time**	**Status notification**	**Maximum Incident Resolution Time**
Priority 1 or "Major Incident"	15 minutes	Every 30 minutes during first 8 hours, thereafter every hour	2 hours
Priority 2	1 hour	Every 2 hours	4 hours
Priority 3	4 hours	Every 24 hours	24 hours

11.1.2.5 Incident Manager

At least for any Priority 1 Incident or Major Incident or any Incident breaching the Maximum Incident Resolution Time the Contractor **shall** appoint an Incident Manager to handle all communications towards ECHA and ECHA third parties.

11.1.3 Service and Change Requests

Service Requests are measured for their Maximum Request Response Time and Maximum Request Resolution Time under the SLA.

Standard Changes are measured for their Maximum Request Response Time and Maximum Request Resolution Time under the SLA.

As Normal and Emergency Changes are single instance changes and thus not easy to predict in advance, they are both are exempt from Maximum Request Resolution Time under the SLA.

11.1.3.1 Request Response Time

Request Response Time is the time elapsed, counted within the service hours of the chosen Service Band, between a. the moment the Contractor receives a Request and b. the moment the Contractor communicates to ECHA the ticket number or other record has been logged and the Request Fulfilment or Change Management procedure has been triggered. The response **may** be an automated response. The response **shall** inform ECHA of the ticket or record number assigned to the Request.

Request Response Time shall be <= Maximum Request Response Time as described in the table below.

11.1.3.2 Request Resolution Time

Request Resolution Time is the time elapsed, counted within the service hours of the chosen Service Band, between a. the moment that the Contractor responds to the Request (informing ECHA of the ticket or record number), and b. the moment that the Contractor resolves the Request.

Request Resolution Time shall be <= Maximum Request Resolution Time as described in the table below.

11.1.3.3 Timers

The Contractor **shall** use their best endeavours to resolve Requests within the Maximum Request Resolution Times. The Contractor **shall** monitor and measure Response and Resolution times, and report them back to ECHA, in particular highlighting breaches.

Upon request from ECHA the Contractor **shall** make available all reasonable material relating to the Service Request or Change implementation, including activities and timings. Evidence can include amongst other things, evidence showing at what moment in time did the Contractor receive the Request from ECHA, at what moment in time did the Contractor notify to ECHA the ticket number, and at what moment in time did the Request get resolved.

Table 17 Request timers

Request Type	Maximum Request Response Time	Maximum Request Resolution Time
Service Request (fulfilment automated)	15 minutes	2 hours (unless specifically agreed in the SR description)
Standard Change	4 hours	24 hours (unless specifically requested, or defined in the standard change description)
Normal Change	8 hours	Mutual agreement between ECHA and the Contractor. Normal Changes will not be measured for timeliness.
Emergency Change	30 minutes	Mutual agreement between ECHA and the Contractor. Emergency Changes will not be measured for timeliness.

11.1.4 Penalties

Penalties are divided into three categories:

1. Availability
2. Incidents
3. Service Requests and Changes.

11.1.4.1 Availability

ECHA **may**, depending upon the particular circumstances of breaches of availability targets, impose financial penalties related to a lack of availability as follows, where “u” is the observed non-availability in a month and “U” is the maximum allowed:

- where U< u ≤ (2*U): **10 %** of the relevant Service Fees
- where (2*U)< u ≤ (4*U): **20 %** of the relevant Service Fees
- Where u > (4*U): **30 %** of the relevant Service Fees

The **total ceiling** for penalties associated with availability for any specific monthly service **shall** thus not exceed 30% of the value of the monthly fee for services (defined by the applicable Service Band in the Price Catalogue).

If the clear cut case that an **incident affects the availability of only parts of the service** (without grounded dispute by ECHA) then the penalty will be, as far as possible, apportioned accordingly. It is expected that the main driver for measurement will be virtual machines affected and the services associated to them, within reason; in fact, the accuracy of the apportioning will depend on the accuracy of the association. The CMDB information available to the parties will be considered in determining the entity of the effects.

Important note: for a Major Incident, the penalty **shall** be used for the entire service. This it to avoid a situation where it becomes difficult, or even impossible, for the Contractor to calculate the penalties.

In the case of failure of a datacentre, the same formula above **shall** be applied to the maximum allowed time for running on one datacentre metric (ref. Table 14 Definition of Service Bands). In this case the penalties will be applied to the services which lost their failover capability.

11.1.4.2 Incidents

Where ECHA judges that the Response and/or Resolution Times consistently breaches the Maximum Incident Resolution and Response Time indicated in the Timers table, or when ECHA judges the actions performed by the Contractor to be insufficient, ECHA **shall** address this via the Governance (ref. section 9 Governance).

Without prejudice to ECHA’s other rights under the FWC, in case of consistent breaches or recurrences, ECHA reserves the right to suspend or cease requesting services from the Contractor and potentially request them from an alternate service provider.

Important note: Penalties for Incidents are applied to the Service Fee for the entire service. Penalties for Incidents are never applied to Effort Bands.

Penalties **shall** be applied to the breaches of the Maximum Incident Response Time. The penalties apply to the Service Fee (defined by the applicable Service Band) of the entire service for each Incident, as follows:

- Major Incident: 1.0 %

- P1 Incident: 0.5 %
- P2 Incident: 0.2 %
- P3 Incident: 0.1 %

Penalties **shall** also be applied to breaches of the Maximum Incident Resolution Time according to the calculation below.

A separate penalty assessment **shall** be made for each service, for each month of the service. For example, a penalty calculation would be made for a service for the month of July and a separate penalty calculation would be made for the service for the month of August.

For the service, the incidents **(except Priority 3)** that were resolved during any given month **shall** constitute the set of Incidents upon which the penalty for that month **shall** be calculated.

The number of incidents that were resolved during that month are called [Total number of incidents during month].

The penalty calculation is as follows:

For <u>each individual incident</u> for that month, the 'Lateness Ratio' i.e. 'actual implementation time' versus 'maximum allowed implementation time' is calculated as:

Lateness Ratio =

[(timestamp when incident was resolved) - (timestamp when incident occurred)] / [(Maximum Incident Response Time) + (Maximum Incident Resolution Time)]

In other words 'how long did it take' / 'how long is allowed in total'.

For example, if the Lateness Ratio is >1, then the resolution is behind schedule (late). If the Lateness Ratio is >=2, it means the resolution took twice as long (or more) as the maximum allowed time to get implemented.

From amongst the set of incidents participating in the penalty calculation for that month, did 10% or more of the incidents have a Lateness Ratio of >= 2?

In other words, is 100% * ([no. of incidents with Lateness Ratio **>= 2**] / [Total number of incidents during month]) greater than or equal to 10%?

1. If the answer is **yes**, 10% or more of incidents have a Lateness Ratio of **>= 2.00**, then a penalty **shall** apply equal to the financial value of **25 %** of the Service Fee applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Incidents.)

2. If the answer is **'no'**, then the next question is

   "did 10% or more of incidents have a Lateness Ratio of **>= 1.75**?"

   If the answer is **'yes'**, then a penalty **shall** apply equal to the financial value of **20 %** of the Service Fee applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Incidents.)

3. If the answer is **'no'**, then the next question is

   "did 10% or more of incidents have a Lateness Ratio of **>= 1.50**?"

   If the answer is **'yes'**, then a penalty **shall** apply equal to the financial value of **15 %** of the Service Fee applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Incidents.)

4. If the answer is **'no'**, then the next question is

   "did 10% or more of incidents have a Lateness Ratio of **>= 1.25**?"

   If the answer is **'yes'**, then a penalty **shall** apply equal to the financial value of **10 %** of the Service Fee applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Incidents.)

5. If the answer is **'no'**, then no financial penalty **shall** apply concerning the lateness of incident implementation.

Note that an artificial minimum value of 'Total number of incidents during month' is set to **10** (i.e. if in reality the number of Incidents for that month of service was lower, for the purpose of the penalty calculations the value of 'Total number of incidents during month = 10' will be used). This artificial minimum of 'Total number of incidents during month' is introduced to prevent the case where for a month when there is a low number of incidents, the lateness of a small number of requests would provoke a penalty.

The **total ceiling for penalties** associated with Incidents for any specific Service Fee **shall not** exceed **25 %** of the value of the of the Service Fee for the services (defined by the applicable Service Band price category in the Price Catalogue).

The Contractor **shall** prepare the draft penalty calculations, and ECHA **shall** accept or rework or request the Contractor to rework the calculations.

Important note: Any Incident erroneously marked resolved, and subsequently reopened, will be counted from Incident start time to resolution time.

11.1.4.3 Service and Change Requests

Where ECHA judges that the Response or Resolution times consistently breach the Maximum Response and/or Resolution Times indicated in the Timers table, or when ECHA judges the actions performed by the Contractor to be insufficient, ECHA **shall** address this via the Governance (ref. section 9 Governance).

Without prejudice to ECHA’s other rights under the FWC, in case of consistent breaches or recurrences, ECHA reserves the right to suspend or cease requesting services from the Contractor and request them from an alternate service provider.

Important note: Penalties for Service Requests are applied to the Service Fees for the entire service. Penalties for Changes are applied to Effort Bands of the service, unless specifically noted differently.

Penalties **shall** be applied to breaches of the Maximum Request Response Time. The penalties apply to the Service Fee of the **entire service** per Request (defined by the applicable Service Band), as follows:

- Service Request: 0.2 %
- Standard Change: 0.1 %
- Normal Change: 0.1 %
- Emergency Change: 0.5 %

Penalties **shall** also be applied to breaches of the Maximum Request Resolution Time according to the calculation below.

A separate penalty assessment **shall** be made for each service, for each month of the service. For example a penalty calculation would be made for a service for the month of July, and a separate penalty calculation would made for another service for month of August.

For the service, the Requests that were resolved during any given month **shall** constitute the set of Requests upon which the penalty for that month **shall** be calculated.

The number of Request that were resolved during that month are called [Total number of requests during month].

The penalty calculation is as follows:

For each individual request for that month, the 'Lateness Ratio' i.e. 'actual implementation time' versus 'maximum allowed implementation time' is calculated as:

Lateness Ratio =

[(timestamp when request was resolved) - (timestamp when request was received)] / [(Maximum Request Response Time) + (Maximum Request Resolution Time)]

In other words 'how long did it take' / 'how long is allowed in total'.

If the Lateness Ratio is >1, then the resolution is behind schedule (late). If the Lateness Ratio is >=2, it means the resolution took twice as long (or more) as the maximum allowed time to get implemented.

From amongst the set of Requests participating in the penalty calculation for that month, did 10% or more of the requests have a Lateness Ratio of >= 2?

In other words, is 100% * ([no. of requests with Lateness Ratio >= 2] / [Total number of requests during month]) greater than or equal to 10%?

1. If the answer is **'yes'**, 10% or more of requests have a Lateness Ratio of >= 2.00, then a penalty **shall** apply equal to the financial value of **25 %** of the Service Fee/Effort Band applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Requests.)

2. If the answer is **'no'**, then the next question is

   did 10% or more of requests have a Lateness Ratio of **>= 1.75?**"

   If the answer is **'yes'**, then a penalty **shall** apply equal to the financial value of **20 %** of the Service Fee/Effort Band applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Requests.)

3. If the answer is **'no'**, then the next question is

   "did 10% or more of requests have a Lateness Ratio of **>= 1.50?**"

   If the answer is **'yes'**, then a penalty **shall** apply equal to the financial value of **15 %** of the Service Fee/Effort Band applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Requests.)

4. If the answer is **'no'**, then the next question is

   "did 10% or more of requests have a Lateness Ratio of **>= 1.25**?"

   If the answer is **'yes'**, then a penalty **shall** apply equal to the financial value of **10 %** of the Service Fee/Effort Band applicable for the month for which the penalty is being calculated. (This is the end of the penalty calculation for Requests.)

5. If the answer is **'no'**, then no financial penalty **shall** apply concerning the lateness of request implementation.

Note that an artificial minimum value of 'Total number of requests during month' is set to **100** (i.e. if in reality the number of requests for that month of service was lower, for the purpose of the penalty calculations the value of 'Total number of requests during month = 100' will be used). This artificial minimum of 'Total number of requests during month' is introduced to prevent the case where for a month when there is a low number of requests, the lateness of a small number of requests would invoke a penalty.

Note that as per described above, the total ceiling for penalties associated with requests for any specific monthly service **shall not** exceed **25 %** of the value of the of the Service Fee/Effort Band for the services (defined by the applicable Service Band price category in the Price Catalogue).

The Contractor **shall** prepare the draft penalty calculations, and ECHA **shall** accept or rework or request the Contractor to rework the calculations.

11.1.4.4 Combined impacts and example

In the event that more than one category is affected at the same time, ECHA will not combine penalties but will apply the penalties for the category in which the negative financial impact has been the highest, per service.

This could happen when an Incident affects many systems at one time and the Contractor’s ability to respond to Service or Change Requests.

Example:

A hardware failure in the Cloud Services causes 62 out the 1 000 ECHA virtual machines to crash. The VMs fail to restart automatically.

The Contractor responds within the 15 minute response time to the Incident, but is unable to bring services back online. An Emergency Change is requested and the Contractor responds after 40 minutes. The Incident is closed after 5 hours and 15 minutes (Response Time + Resolution Time).

During the resolution of the Incident, ECHA has tried to provision 4 new virtual machines via two separate Service Requests. These have failed due to unknown causes, but perhaps related to the Incident.

Furthermore there are 11 Standard Changes for Backup and Restore that have not met their Maximum Resolution Time during the same month.

Finally, there have been 81 Service Requests that have met the requirements of the SLA. During the month there have been another P2 Incidents having affected 50 VMs resolved in 6 hours and one P3 affecting 48 VMs resolved in 29 hours after response. The Incident Response Times of the two incidents are two hours each.

Availability:

The service is in the 24/7 Service Band and can suffer an outage of approx. 1.44 hours (1 hours and 26 minutes).

- 62 VM P2 Incident
  - The 62 VMs represent 6.2 % of ECHA’s server farms, warranting a P2 Incident.
  - The outage is approx. 3.65 times the larger than the allowed, triggering a 20 % penalty for the Service Fee for the affected services for availability.
- 50 VM P2 Incident
  - The 50 VMs represent 5.0 % of ECHA’s server farms, warranting a P2 Incident.
  - The outage is approx. 4.16 times the larger than the allowed, triggering a 30 % penalty for the Service Fee for the affected services for availability.

- 48 VM P3 Incident
    - The 48 VMs represent 4.8 % of ECHA's server farms, warranting a P3 Incident.
    - The outage is approx. 20.14 times the larger than the allowed, triggering a 30 % penalty for the Service Fee for the affected services for availability.

<u>Incidents:</u>

The calculations are as follows:

- The Incident Response Time for the 50 VM P2 is 2 hours vs the 1 hour allowed, bearing a 0.2 % penalty.
- The Incident Response Time for the 48 VM P3 is 2 hours vs the 1 hour allowed, bearing a 0.1 % penalty.
- The amount of Incidents is 2 (2 x P2, **P3 discarded**), triggering the minimum of 10.
- 62 VM P2 Incident
    - 5.25 hours / (1 hours + 4 hours) = 1.05 Lateness Ratio
- 50 VM P2 Incident
    - (2.00 hours + 6.00 hours) / (1 hours + 4 hours) = 1.60 Lateness Ratio
- At least 10 % of the Incidents had a Lateness Ratio >=1.50 (but less than 1.75), triggering a 15 % penalty for the Service Fee for the service related to the breaching Incident(s).
    - In this case the 50 VM P2 Incident

<u>Requests:</u>

The calculations are as follows:

- The amount of requests is 95 (1 Emergency Change, 83 Service Requests, 11 Standard Changes), triggering the minimum of 100.
- Service Requests
    - As the Service Requests have failed, they have a potentially infinite Lateness Ratio, but for the sake of the example we will merely state that they are over 2.00.
    - 2 % of the Service Requests had a Lateness Ratio >=2.00, triggering no penalties for the Service Fee for the service related to the Service Requests.
- Standard Changes
    - For this example, we state that the 11 Standard Changes have a Lateness Ratio between 1.25 and 1.40.
    - 11 % of the Standard Changes are >=1.25, triggering a 10 % penalties for the Service Fee for the service related to the breaching Standard Changes.
- Normal Changes
    - None
- Emergency Changes

- As the Emergency Change did not meet the Maximum Response Time, a 0.50 % penalty is applied to the service affected.

The impacts would therefore be as below.

Table 18 Combined impacts example

Penalty type	Reference	Availability	Maximum Response Time	Maximum Resolution Time	Service
Availability	62 VM, P2 50 VM, P2 48 VM, P3	~~20.00 %~~ ~~30.00 %~~ ~~30.00 %~~	N/A	N/A	Cloud Services
Incidents		N/A	0.30 %	15.00 %	Cloud Services
Service Requests	None	N/A	~~0.00%~~	~~0.00 %~~	Cloud Services
Standard Changes	None	N/A	0.00 %	10.00 %	Backup and restore
Normal Changes	None	N/A	0.00 %	0.00%	None
Emergency Changes	62 VM, P2	N/A	~~0.50 %~~	~~0.00 %~~	Cloud Services

To be clear, the following penalties apply for the month:

- *Availability*
  - *Cloud Services, 62 VM P2: 20 % of 62 VMs / 1000 VMs = 1.24 %*
  - *Cloud Services, 50 VM P2: 30% of 50 VMs / 1000 VMs = 1.50 %*
  - *Cloud Services, 48 VM P4: 30 % of 48 VMs / 1000 VMs = 1.44 %*
  - *Total: 4.18 % of Cloud Services*
- Incidents
  - Maximum Incident Response Time
    - Cloud Services, (62 VM P2): 0.20 %
    - Cloud Services (48 VM P3): 0.10 %
  - Maximum Incident Resolution Time
    - Cloud Services, (50 VM P2): 15.00 %
  - **Total: 15.30 % of Cloud Services**
- Requests
  - *Maximum Request Response Time:*

        - *Cloud Services Emergency Change: 0.50 %*
    - Maximum Request Resolution Time
        - **Backup and Restore services: 10.00 %**
- **Total penalties:**
    - **Cloud Services: 15.30 % of Service Fees (Incidents)**
    - **Backup and restore services: 10.00 % of Effort Bands (Requests)**

11.2 Pricing

Pricing and payment for services will follow the following principles.

1. All services will be based on items in the Price Catalogue, unless otherwise agreed by both parties in writing.
2. ECHA will pay for services upon delivery and only after successful acceptance testing, when all requirements are fulfilled (in particular they are fully migrated to the FMO) and the SLA is in place.
3. Effort Bands require that the Contractor has submitted information to ECHA of the efforts performed in writing and agreement has been reached.

11.2.1 Price Catalogue

The pricing in the Price Catalogue will be articulated according to three categories:

- Service Fees
- Effort Bands
- Daily fees

The Contractor **may** quote separate prices for service Fees and Effort Bands depending on the defined Service Bands.

The Contractor **should** offer Service Fees **differentiating among Tenancy options** (ref. 6.1.1.1 Tenancy) whenever they can provide such options in the Price Catalogue.

11.2.2 Service Fees

The Service fees apply to on-going services in FMO.

ECHA **will start accepting Service Fees after the completion of the transition-in project** (ref. 8.1.1 Model for transition).

The services costed at monthly Service Fees **shall** have a fully linear pricing based on a unit price that does not change due to a changing volume of service, with the exception of the possible reduced price (ref. 11.2.2.1 Service Volumes and flexible capacity). Services based on services fees **shall** be scalable up and down without extra charge. Unless otherwise agreed in the specific contracts, the repeatable timespan for invoicing of Service Fees will be monthly. Regardless of the timespan used, the actual volume consumed at the end of the repeatable timespan will be used for invoicing.

The **Service Fee** for a service always **includes** the following **service management processes** (ref. 6.3 Service management):

- Set-up of the service

- Termination of the service
- Incident Management including related Emergency Changes
- The handling of the Service Requests defined in Section 6.3.9 Required Requests, as the Contractor **shall** utilise automation to the highest degree possible
- Problem Management
    - Problems **shall** be resolved according to agreement between ECHA and the Contractor. However, problem resolution **shall** always be included in the Service Fee.
- All monitoring activities and other required components to enable monitoring, e.g. infrastructure, licenses, etc.
- Coordination, collaboration, cooperation with ECHA third parties, in fulfilment of the requirement that the Contractor **shall** commit to integrating and collaborating with ECHA third parties in the management of the service, to the best of their capabilities.

The cost of the SMP **shall** be included in the Service Fees.

Any and all costs related to the hosting/housing of data-centre hardware at Contractor's DC's shall be included in the hosting Service Fee, e.g. suitable racks or rack-space, as well as any necessary services (e.g. physical installation; set-up fee). Hardware hosting fees **shall** also include the physical connectivity, i.e. material in terms of suitable copper and/or fibre-optic cables matching the relevant – e.g. IEEE – standard specifications and being compatible with physical-distance requirements, as well as associated labour (patching of cables, device-to-device and/or device-to-patch-panel, depending on the case).

Likewise, any and all costs related to running and operating of hardware in Contractor's datacentre facilities, including energy (electricity), suitable heating and/or cooling, and security **shall** be included in the hosting Service Fee. The pricing model underlying the FWC assumes that these costs are more or less and on average (across the whole range of systems) related to the size (i.e. height in rack-units) of the hardware to be hosted.

As laid down in 6.1.1.8 Remote Access, the Contractor **shall** take over the management of the current SSLVPN and two factor authentication solution, **based also on the current appliances that will be hosted in the Contractor's datacentres** (ref. 6.1.1.9 Datacentre hosting of ECHA owned hardware). Initially, ECHA will still own the physical appliances, the licences and maintenance contracts, the physical tokens, whereas the Contractor will be responsible for the managed services. During the implementation of the FWC ECHA can decide to **transform such infrastructure towards an as-a-service model** (according to which the Contractor will own any appliance, licence etc. as means to providing a service) through a transformation project; the scope of the managed services remaining the same. Therefore the Contractor **shall** provide a price offer for the managed services in the ECHA owned model and in the as-a-service model.

ECHA has set a **maximum Service Fee** for some items in the Price Catalogue. Those maximum Service Fees are based on ECHA's expected consumption of the different services and the budget availability of the Agency. ECHA expects the Contractor to price the services within the given maximum Service Fee.

11.2.2.1 Service Volumes and flexible capacity

The Contract **should** consider the current volumes as indicated in the CMO Annexes, particularly Annex 1: IT Infrastructure Architecture (CMO), as **baseline volumes** with regard to the volume that ECHA will initially order for the FMO services. Over time, such volumes can increase (the forecasted growth is indicated in the Price Model), decrease (the forecasted growth is indicated in the price model) or remain stable. Independently of the current ECHA forecasts, also due to the numerous areas of uncertainty for the ECHA IT in the period of validity of this FWC, **the Contractor should factor flexibility elements in their offer**, particularly in their technical and resource capacity.

The Contractor **may** for some services indicate a **minimum volume** of services that would be required to deliver the services at the Service Fee. However, ECHA does not necessarily commit to accepting the minimum volume of service. The minimum volume can never be above the initial volume of service to be migrated from CMO (when applicable and indicated in the CMO Annexes, particularly Annex 1: IT Infrastructure Architecture (CMO)) to FMO, but can be lower.

Despite any minimum volume, **the unit price shall remain the same for the volume of service inside and outside the minimum volume**.

Furthermore, for some services a **reduced price may** be set by the Contractor when volumes **cross a certain threshold** of service volume. The threshold **may** also be defined by the Contractor. To be noted, only the volume that has actually crossed the threshold will use the reduced price whereas the volumes beneath the threshold will use the original price.

11.2.3 Daily fees and Effort Bands

For service management processes not included in the Service Fee, for consultancy services or for projects (e.g. transformation projects), ECHA will order work that the Contractor **shall** cost according to daily fees and Effort Bands.

11.2.3.1 Daily fees

Daily fees are used to cost efforts of ordered consultancy services or to quote efforts in projects.

A Full Time Equivalent day (FTE) is 8 hours. One full year corresponds normally to an effective workload of 220 days.

The Agency **may** exceptionally also request the delivery of "on-call" (aka "stand-by-duty") intended to ensure the ability of a resource, i.e. to be reachable by phone – during the relevant period of time and to be present at the working place within 75 minutes of being alerted. Such "on-call" services are chargeable, the daily fee can increase by maximum 25% (during normal working days) or maximum 50% (during week-ends and ECHA holidays). The service **shall** be delivered by the same profile(s) providing the duties during normal working hours.

For off-site work, ECHA **may** ask for specific profiles.

If justified, ECHA can demand that the off-site resources follow a working schedule so that the time difference between the work hours at the place of performance and the ECHA normal working hours does not exceed two hours.

11.2.3.2 Effort Bands

Where applicable (e.g. the execution of Change[13] activities), ECHA will order work according to the following Effort Bands, per service. In this case, the Effort Band acts as a monthly budget envelope of person-days, available for the Contractor to use to perform the ordered work.

Table 19 Effort Bands definitions

Effort Band	**Cost driver**	**Description**
E1	<= 1 day / month	Covers up to 1 person-day per month of effort.
E3	<= 3 days / month	Covers up to 3 person-days per month of effort.
E5	<= 5 days / month	Covers up to 5 person-days per month of effort.

[13] Changes refer to changes requested by ECHA, and not to changes that arise from the Contractor running the service. For example, updating firmware on a switch is considered part of the service and not eligible to be invoiced via the Effort Band.

The Effort Bands can be valid in all Service Bands, and the Contractor will fill the price into the Price Catalogue as follows:

Table 20 Example of the Effort Bands in conjunction with Service Bands

Effort Band	**9/5**	**12/5**	**24/5**	**24/7**
E1	*price*	*price*	*price*	*price*
E3	*price*	*price*	*price*	*price*
E5	*price*	*price*	*price*	*price*

The Effort Band is irrespective of the profile(s) that are needed to perform the actions. For example, if ECHA purchases Effort Band "E3" (<= 3 days), this represents up to 3 person-days of work, irrespective of the Contractor profile(s) that is/are needed to perform the work. The Contractor is not required to restrict themselves to using the profiles listed in the section 6.4 Consultancy services.

A month represents a calendar month, irrespective of any local or pan-European holidays or other non-working days.

ECHA will typically consult with the Contractor when deciding on the most appropriate Effort Band so as to predict realistically the need. The Contractor **shall** carry out the duties required to provide the services regardless of the actual effort spent per month.

The Effort Band can be adjusted lower or higher depending on the average actual effort, previous agreement.

If the 'required' effort per month for the ordered work is consistently significantly less than the Effort Band initially ordered, ECHA reserves the right to decrease accordingly the Effort Band ordered for future months.

If the 'required' effort per month deployed by the Contractor is consistently significantly greater than the Effort Band ordered, and the Contractor can provide sound justification, ECHA reserves the right to increase the Effort Band ordered for future months. Sound justification **shall** include at least the following:

- Evidence that proper Problem Management is taking place to reduce the number of incidents
- Evidence that repetitive tasks have been analysed and automated to avoid manual labour, e.g. utilising Service Requests or Standard Changes
- Evidence that knowledge gained is resulting into efficiency gains.

For person-days that are required to carry out the work ordered by ECHA, occasionally exceed the available Effort Band for a specific month, within the financial capacity of the related Specific Contract, on agreement between the parties the Contractor **may** quote and be paid for additional ad-hoc efforts. Such efforts **shall** be quoted at the rate specified in the Price Catalogue for "E1" (<= 1 day), for the relevant Service Band for that month. More details **shall** be specified at the level of Specific Contract.

11.2.4 Separately billable services

11.2.4.1 Governance

ECHA acknowledges that, efficiently sustaining the governance model defined in Section 9 Governance, requires adequate resourcing, in quantity, level of seniority and level of authority in the Contractor's organisation. Therefore at the start of the implementation of this FWC, the parties will sign a "governance specific contract" covering the start-up and the regular provision of the service.

The Contractor will offer a monthly price for the Governance service as a percentage of the monthly financial volume of the Service Fees (ref. section 11.2.2 Service Fees) for the ongoing services consumed by ECHA (i.e. recurrent services, excluding consultancy and projects). The annual cost for ECHA is capped at 10% of the actual annual financial volume of the Service Fees for the ongoing services in any single year.

11.2.4.2 Transition out

The Contractor will offer a one-off price for the planning and execution of the transition out (ref. 8.2 Transition out). The transition out for ECHA is capped at 5% of the actual annual financial volume of the Service Fees (ref. section 11.2.2 Service Fees) for ongoing services (i.e. recurrent services, excluding Effort Bands, consultancy and projects) in the last full year of service before transition out.

11.2.4.3 Security Services

It is ECHA's understanding that the Security Services described in section 6.6 Security Services will have a cost driver relating to the amount of services that they are applied to. Therefore, the Contractor will offer a monthly fee for as a percentage of the monthly Service Fees (ref. section 11.2.2 Service Fees) for the ongoing services consumed by ECHA (i.e. recurrent services, excluding Effort Bands, consultancy and projects). The annual cost for ECHA is capped at 4 % of the actual annual financial volume of the Service Fees for the ongoing services in any single year.

11.2.5 Acceptance of Service Readiness and Periodic Review

To be seen as operational, all services will require formal acceptance of service readiness by ECHA. No invoicing for services can start before this acceptance has been achieved, regardless if the Contractor is already delivering some of the scope of the service.

The readiness criteria and the acceptance process will be defined at specific contract level.

The Contractor does not have the right to charge ECHA for services related to testing until the UAT (ref. section 8.1.4 User acceptance testing) has been successfully completed.

11.2.6 Transition-in project

Transition-in will be done in the form of a transition project as defined in section 8 Transition of services. Depending on the Contractor's proposal, it is possible that the Contractor's datacentres have to be temporarily connected to the Incumbent's datacentres for migration purposes during the Transition-in project. The costs related to commissioning, testing, using and decommissioning such temporary connectivity **shall** be included in the transition-in costs.

The transition-in cost for ECHA is capped at three months of the actual monthly financial volume of the Service Fees (ref. section 11.2.2 Service Fees) for ongoing services (i.e. recurrent services, excluding consultancy and projects) in FMO after completion of the project (ref. section 8.1.1 Model for transition).

The payment of the transition project will be incremental based on achievement of milestones as per the table below.

Table 21 Payment model for Transition-in project

Milestone	Payment (max. % of Transition-in cost)
M1: Readiness of Cloud infrastructure for migration of	10 %

Milestone	Payment (max. % of Transition-in cost)
services	
M2: Migration of services complete	20 %
M3: Managed services ready in the FMO	20 %
M4: SMP ready for use	20 %
Final balance: Completion of project, all milestones achieved, FMO fully operational	30 %
Total	**100 %**

11.2.7 Transformation services

Transformation services (as defined in section 6.5 Transformation services) are chargeable as projects. The Contractor **shall** cost efforts according to the pricing offered for consultancy profiles (ref. section 6.4 Consultancy services) in the Price Catalogue.

Costing of other means of delivery, such as licences, hardware, connectivity, **shall** be aligned with the basis for costing utilised in the Price Catalogue.

Transformation services will always be quoted according to the profiles in the FWC specification and the profile prices in the Price Catalogue.

Furthermore, the following volume discount table **shall** be applied to the price in the Price Catalogue:

Table 22 Transformation services volume discount table

Number of days	Discount (onsite)	Discount (offsite)
1 – 20	0%	0 %
21 – 100	10 %	15 %
100+	20 %	30 %

11.2.8 Invoicing and financial management

The SMP **shall** provide a billing and invoicing functionality.

The Contractor **shall** invoice based on the actual consumption of the in-scope services ordered via Specific Contracts. An up-to-date inventory of such services (on-going services) **should** be visible in the billing and involving area of the SMP. Pricing **shall** be based on the Price Catalogue.

Invoices **shall** be supported by reporting showing the basis for calculations and the actual calculation. This **shall** be available also on metadata tag level or consolidated into one bill.

The billing calculations underpinning the invoices **should** be to the extent possible automatic. Invoices and supporting information **shall** be electronic, **should** delivered via the SMP, and **should not** require delivery of paper of any kind or form, unless specifically requested by ECHA.

Upon request, the Contractor **should** be able to provide electronic exports of billing information, preferably in XML and Excel format.

The billing and invoicing area of the SMP **shall** contain a track record of all relevant financial events (e.g. signature of a contract, exception handling and historical view of the invoices)

ECHA accepts that financial documents and exchanges related to exceptions (e.g. credit notes, replies to requests for clarification etc.) will not be available via the SMP; however it **should** be possible to keep track of the related main events (e.g. credit note issued for a service) in the Billing and invoicing area of the SMP.

To ensure that the automation of the platform does not create overspending, the Contractor **should** be able to implement functionality for financial boxing of ECHA's in the SMP and provide an indicative financial quote in their offer.

If agreed, the implementation of financial boxing can be the subject of a transformation project.

Below is an example that would fulfil ECHA's needs. Please note that all figures are fictive.

Table 23 Example of a financial management hierarchy that would meet ECHA's needs

Tier	Explanation	Example
Tier 1: Framework Contract	This tier is not to exceed the threshold value at any time for any reason for the scope and validity time of the entire framework contract. The sum of the threshold values for tiers 2 – 4, whether past and present or future, are not to exceed the threshold value of this tier at any time for any reason. A Request that would breach the framework contract total budget is to be automatically denied and trigger immediate escalation by the Contractor.	Framework Contract ceiling 30 000 000 Million EUR
Tier 2: Framework Contract (timed)	This tier is not to exceed the threshold value in the defined time span (configurable, but mostly yearly) for the service scope of the entire FWC. The sum of threshold values for tiers 3 – 4, whether past and present or future, are not to exceed the threshold value of this tier during the defined time span. A Request that would breach the threshold taking into account all running services with projections until the end of the defined time span (configurable) is to be automatically denied and trigger immediate escalation by the Contractor. The projections are to be based on projections from tiers 3 – 4.	2020 infrastructure budget 3.92 Million EUR 01/01/2020 – 31/12/2020
Tier 3: Specific Contract (timed)	This tier is not to exceed the threshold value for any reason in the defined time span (configurable) for the scope of the entire Specific Contract. A Request that would breach the threshold taking into account all running services with projections until the end of the defined time span (configurable) is to be automatically denied and trigger immediate escalation by the Contractor. The projections, if not automated, could be based on a	Specific Contract 3 (Cloud Services) annual instalment 1.97 Million EUR 01/01/2020 – 31/12-2012

Tier	Explanation	Example
	monthly payment plan made by ECHA.	
Tier 4: Custom (timed)	Typically used for department, programme, workgroup or single user. This tier can optionally (configurable) be exceeded by a buffer (configurable) at any time with projections calculated until the end of the time period (configurable), as long as this does not cause a breach of higher tiers (1 – 3). However, automatic notifications are to be sent to a set of configurable users or parties that the budget has been exceeded. A Request that would breach the threshold (including the possible buffer) taking into account all running services with projections until the end of the defined time span (configurable) is to be automatically denied. The projections, if not automated, could be based on a monthly payment plan made by ECHA.	Management Information Systems Programme infrastructure 400 000 EUR 01/02/2020 – 31/01/2021

12 Acceptance procedure

The default acceptance procedure – i.e. unless otherwise agreed by the parties at the level of specific contract or otherwise specified in this document – is defined here. A project or service implementation will be deemed to be completed and accepted by ECHA once the acceptance criteria described below have been met:

1) All contractual deliverables have been completed by the Contractor.

2) The Contractor has successfully completed any required knowledge transfer, and ECHA has also provided all information which the Contractor requires in order to be able to start the delivery of services.

3) The Contractor indicates to the Agency the readiness for acceptance.

4) ECHA does not notify the Contractor in writing within 15 working days thereafter of any deficiencies. In order to enable the Contractor to take prompt remedial action such notice shall include a reasonably detailed specification as to the nature of the failure.

5) ECHA formally accepts in writing that all acceptance criteria have been met.

13 Annexes

- Annex 1: IT Infrastructure Architecture (CMO)
- Annex 2: Network Service Model (CMO)
- Annex 3: IT BCP - IT Continuity Technical Preparedness Plan (CMO)
- Annex 4: ICT Change Management (CMO)
- Annex 5: ECHA Indicative teleworking rules and requirements for IT hosting contractor

2982 # 14 Glossary

Abbreviation	Explanation
AD	Active Directory
AES	Advanced Encryption Standard
BC	Business Continuity
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
CI	Configuration Item
CMDB	Configuration Management Database
CMO	Current Mode of Operations
CPU	Central Processing Unit
DC	Datacentre
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DMZ	Demilitarized Zone
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DWDM	Dense Wavelength Division Multiplexing
ECHA	European Chemicals Agency
FMO	Future Mode of Operations
FWC	Framework Contract
GB	Gigabyte
GUI	Graphical User Interface
HTML	Hypertext Markup Language
IaaS	Infrastructure-as-a Service
IDS	Intrusion Detection System
IP	Internet Protocol
LAN	Local Area Network
MTA	Mail Transfer Agent
NOC	Network Operations Centre
NTP	Network Time Protocol
OSPF	Open Shortest Path First?
PDC/A	Incumbent's datacentre
PDC/B	Incumbent's datacentre
PKI	Public Key Infrastructure
RAM	Random Access Memory
RBAC	Role-based Access Control
RFC	Request for Change
RHEL	Red Hat Enterprise Linux
RPM	Revolutions Per Minute
RPO	Recovery Point Objective
RSA	Rivest–Shamir–Adleman
RTO	Recovery Time Objective
SAS	Serial Attached SCSI
SATA	Serial ATA
SDM	Service Delivery Manager

Abbreviation	Explanation
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMP	Service Management Portal
SR	Service Request
SSD	Solid-state drive
SSL	Secure Sockets Layer
SSO	Single Sign-On
TB	Terabyte
TCO	Total Cost of Ownership
TLS	Transport Layer Security
UAT	User Acceptance Testing
vCPU	Virtual CPU
VM	Virtual Machine
vRAM	Virtual RAM
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access II