Deliverable D6.1

First periodic report on operations

Responsible Partner:	MPG
Status-Version:	Final
Date:	22/04/2022
Distribution level (CO, PU):	Public

Project Number:	GA 101017207
Project Title:	DICE: Data infrastructure capacity for EOSC

Title of Deliverable:	First Periodic Report on Operations
Due Date of Delivery to the EC	31.03.2022
Actual Date of Delivery to the EC	22.04.2022

Work package responsible for the Deliverable:	WP6 – Federated Operations
Editor(s):	Reetz, J. - MPG
Contributor(s):	Testi, D. – CINECA Tonello, N. – BSC Weber, P. – KIT Kaila, U. – CSC
Reviewer(s):	Weber, P. - KIT
Recommended/mandatory readers:	WP1, WP3, WP7

Abstract:	The deliverable explains four main tasks of the DICE work package *Federated Service Management*: the general *operations coordination*, *helpdesk management*, *order management* and *information security*. It describes the activities and achievements of this work package within the first 15 months of the project.
Keyword List:	Operations, Helpdesk, Processes, ITSM
Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

Document Description

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	15.03.2022	First draft version	MPG
v0.2	09.04.2022	Comments received	MPG
v0.5	12.04.2022	Draft for internal review	CINECA, KIT, MPG
V1.0	22.04.2022	Final version	MPG

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

Table of Contents

List of Figures

List of Tables

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

Terms and abbreviations

ACCT	Accounting Tool
ARMT	Availability and Reliability Monitoring Tool
BSC	Barcelona Supercomputing Center - Centro Nacional de Supercomputacion
CHM	Change Management (SMS process)
CINECA	Cineca Consorzio Interunivasitario
CONFM	Configuration Management (SMS process)
CSC	CSC – Tieteen Tietotekniikan Keskus Oy
Customer	Organisation or part of an organisation that commissions a provider in order to receive one or more services and resources. A customer usually represents a number of users.
Data Project	Specifies the business case, the provided (data) service and resource, the customer, the provider, start and end date, the customer agreement between the provider and the customer.
DPMT	Data Project Management Tool
DoA	Description of Action
EC	European Commission
EOSC	European Open Science Cloud
EU	European Union
EUDAT ltd	EUDAT ltd
FitSM	Federated IT Service Management
FZJ	Forschungszentrum Juelich Gmbh
GA	Grant Agreement to the project
GRNET	National Infrastructures for research and technology
ISM	Information Security Management (SMS process)
ISRM	Incident & Service Request Management (SMS process)
KIT	Karlsruhe Institut für Technologie
MPG	Max Planck Gesellschaft zur Foerderung der Wissenschaften e.V.
PID	Persistent Identifier
Provider	Organisation or federation or part of an organisation or federation that manages and delivers services and resources to customers
SFRM	Supplier & Federation Member Relationship Management (SMS process)
SMS	Service Management System
SOCRM	Service Order and Customer Relationship Management (SMS process)
SPMT	Service Portfolio Management Tool
SRM	Service Reporting Management (SMS process)
SVMON	Service Version Monitoring tool
User	Individual that primarily benefits from and uses a service. User is authorised by the Customer and the Service Provider to access and use the service.
VA	Virtual Access
WP	Work Package

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

Executive Summary

The DICE work package WP6 *Federated Service Management* coordinates the operational environment and support the service reporting process for the DICE project that helps provisioning the services and resources via DICE based on the use of available and established tools and adapted processes that are or will connect to the EOSC platform.

The work package is employing EUDAT *operation tools* and *Service Management processes* for the coordination of collaborative operational activities such as order management, helpdesk and configuration management for the consortium. For keeping the task lean for DICE, the federated service management focuses on a subset of the originally 14 FitSM processes to support the consortium's delivery of services (capabilities) and resources (capacities) which is also important for DICE WP7. The service management is using operation tools and collaborative services that have been further developed and integrated via DICE WP3 with the EOSC platform.

The deliverable is explaining the four main tasks, general operations coordination, helpdesk management, order management and information security, and it is describing activities and achievements:

- supported organising the information about offers of DICE services and resources,
- improved descriptions of operational tools and central services relevant for operations,
- carried out webinars and individual tutorials for DICE providers on the usage of operational tools such as the Data Project Management Tool,
- reviewed and updated service management processes such as for
    - Service Order Management
    - Incident and Service Request Management
    - Supplier and Federation Member Relationship Management
    - Configuration Management
    - Change Management
    - Information Security Management,
- supervised the employment and use of the federation tools such as the Helpdesk, the AAI proxy B2ACCESS, the DPMT for order, configuration management and accounting, the Wiki, operational mailing lists, an instant messaging tool, and federation level security.

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

1 Introduction

1.1 About this deliverable

This deliverable reports the approach and the work done on federated service management within the DICE project over the last 15 months. The majority of DICE providers are EUDAT CDI partners. At the start of the project, it was agreed that the EUDAT service management system (i.e. the policies and procedures that are used by EUDAT) are employed as far as necessary and as far as possible also for the non-EUDAT providers. A similar agreement was reached with regard to the use of EUDAT's operational tools such as the EUDAT Helpdesk system, the Data Project Management Tool (DPMT) the Service Portfolio Management Tool (SPMT), the ARGO monitoring, the EUDAT accounting facility and few more. The federated service management via DICE WP6 has been recommended and was made available for all DICE providers. Not all the DICE installations mentioned in DICE WP7 and listed on Table 1 of the WP7 deliverable[1] have been comprehensively addressed so far, i.e. recorded via the EUDAT DPMT as a prerequisite for central monitoring and recording of accounting information.

The basic EUDAT operational environment for providers and customers of DICE services has been described in a series of deliverables of previous EUDAT projects[2] and especially the service management system (SMS) benefited from the SMS that was developed by the EOSC-hub project (2018-2021). It supports the provisioning of the DICE capacity (installations). Some of the operational tools have been further integrated with the EOSC platform as part of the WP3 activities (see also the WP3 deliverables D3.1 and D3.2).

The objectives of WP6, federated operations, are to

- coordinate the operations of the DICE providers following FitSM[3] principles and established processes and collaborate with the EOSC operations.
- support the service reporting process making use of the EUDAT resource registration and accounting facilities.
- provide DICE support using the CDI helpdesk system and collaborate with EOSC support instances.
- record and manage service orders, support the enabling of the services and maintain a good relationship with the customers and user groups to ensure that the active users are satisfied.
- coordinate an operational and infrastructure security for DICE on basis of EUDAT information security management procedures and policies, assess certain security aspects on DICE service topologies and collaborate with EOSC security activities.

1.2 Document structure

The structure of the document follows the breakdown of the work packages in to four tasks.

Section 2 presents some general aspects of the operation coordination with a focus on a. Supplier and Federation Member Relationship Management (SFRM), b. Service Level Management (SLM), c. Configuration Management (CONFM) and e. Change Management (CHM).

Section 0 deals with the helpdesk for DICE (Incident and Service Request Management) that is not only relevant for the support of customers, users and providers but also for receiving order requests.

[1] D7.1, p9-11
[2] e.g. EUDAT2020 D6.3 http://doi.org/10.23728/b2share.50eee85b6e724f1eb9c42a1bd92bec6e
[3] FitSM is a free and lightweight standards family for IT service management. http://www.fitsm.eu

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

Section 4 explains the important process of order and customer relationship management that has been implemented during the reporting period.

Section 0 highlights aspects of the information security management process and Section 6 presents the conclusion.

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

2 Operations coordination

2.1 Introduction

The coordination task of federated operations organised the IT service management processes and supported the 18 DICE providers (14 EUDAT partner) to use the EUDAT operational tools. The task

- helped organising the information about their provider's service offers that are provided as Virtual Access (VA) installations via WP7;
- organised information on the collaborative tools, and the improved the description of some operational tools, the Data Project Management Tool (DPMT) in particular;
- carried out webinars and individual tutorials for DICE providers on how to use the DPMT and individual tutorials with DICE partners.
- reviewed relevant service management processes;
- monitored the management of the operational tools and related central services such as the AAI proxy B2ACCESS in cooperation with WP3, the helpdesk system, the Data Project, service and resource registry (DPMT), the accounting tool, the Wiki with operational mailing lists, an instant messaging tool for operations (Mattermost), etc.;
- attended regular WP6-WP7 coordination meetings;
- setup of the Operational Advisory Board (OAB).

2.2 Service Management Processes and Tools

Table 1 presents the processes and related tools that are considered as relevant for the federated service management for DICE. The processes, borrowed from the concept of FitSM, and tools are described and maintained in the DICE project wiki space that is accessible for the providers.

The *Service Portfolio Management (SPM)* identifies and defines the high-level description of the offered kind of services, service options and resources and manages a portfolio of service offers that are presented, e.g., via the EOSC portal (https://eosc-portal.eu/services-resources). In principle, SPM addresses also the DICE-internal operational tools. The SPM was coordinated with and co-managed by the Service Order and Customer Relationship manager (section 4).

The *Service Level Management (SLM)* ensures the availability of relevant service levels agreements (SLAs) and operational level agreements (OLAs). DICE providers manage their SLAs individually while OLAs are relevant for the provisioning of the operational services (section 2.4).

The *Service Reporting Management (SRM)* is about defining and creating relevant service reports for the purpose of quality assurance. DICE applies this process to the monitoring of the availability and reliability of services (see also DICE D3.2 deliverable) and for collecting accounting information (DICE D7.1).

The *Information Security Management (ISM)* adds a coordinating security support function at the federation layer where IT-services are interdependent. In principle, every DICE provider must ensure that standards and best practices in IT security are fulfilled, taking national and European regulations into account (section 0).

The *Service Order and Customer Relationship Management (SOCRM)* records service orders and ensures that every order get its DICE provider assigned that fulfils the request - either immediately or after an enabling process of certain duration (section 4).

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

The *Supplier & Federation Member Relationship Management (SFRM)* records information about roles and contact about the DICE providers, and it maintains the relationship specifically to the operational contacts of these providers (section 2.3).

The *Incident & Service Request Management (ISRM)* provides the helpdesk and the support function for providers, customers, and users (section 0).

The *Configuration Management (CONFM)* collects a minimum amount of information about the projects, customers, providers, service instances provided, associated allocated resources and about the topology of composite services. It also comprises the directory of contacts and their roles in context of the various information items. All this information, the configuration items, is relevant for the helpdesk service, the central monitoring service, the accounting information collection process and for federated security management.

The *Change Management (CHM)* ensures that DICE providers and the operators of dependent services are informed in a timely manner about planned or already implemented relevant changes (section 2.6).

Table 1 Service Management Processes and Tools

SERVICE MANAGEMENT PROCESS	PROCESS TOOLS
Service Portfolio Management	SPMT
Service Level Management	SPMT, DPMT
Service Reporting Management	ARMT, DPMT, ACCT
Information Security Management	DPMT
Service Order and Customer Relationship Management	Helpdesk, DPMT
Supplier & Federation Member Relationship Management	DPMT
Incident & Service Request Mngmt	Helpdesk, DPMT
Configuration Management	DPMT
Change Management	Wiki, Jira, SVMON
Release and Deployment Management	DPMT, Jira, SVMON

WP6 uses mainly following operational tools:

- *Service Portfolio Management Tool* (SPMT, https://sp.eudat.eu, developed and operated by GRNET) that is used to record and manage the high-level descriptions of DICE services and resources (see also DICE WP3 deliverables D3.1 and D3.2). https://sp.eudat.eu/catalog/ publishes a catalogue services from that portfolio.
- *Data Project Management Tool* (DPMT, https://dp.eudat.eu, developed and operated by MPCDF) for recording and managing information about project requests, providers, customers, provided service instances, service components, allocated resources as well as about scheduled down times.
- Accounting tool (ACCT, https://accounting.eudat.eu, operated by MPCDF) used for collecting information about the allocated and used amount of resources.
- Availability and Reliability Monitoring Tool (ARMT, http://avail.eudat.eu, developed and operated by GRNET)

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

- Helpdesk system (http://helpdesk.eudat.eu, based on Request Tracker from Best Practical Solutions, operated by BSC)
- Wiki and Jira for DICE (based on Confluence from Atlassian, operated by CSC)
- Service Version Monitoring tool (SVMON, http://svmon.eudat.eu, developed and operated by KIT)
- Collaborative tools for DICE such as https://gitlab.eudat.eu and https://chat.eudat.eu, both operated by KIT.

In the following sections a few aspects from the most relevant processes are highlighted.

2.3 Supplier and Federation Member Relationship Management (SFRM)

The purpose of the *Supplier and Federation Member Relationship Management (SFRM)* in DICE is to

- register and maintain the information about the DICE providers with installations in a data base (the DPMT).
- ensure that there is a designated contact responsible for managing the relationship. This is typically the provider's operational contact. Contact addresses such as from the operational contact, a business contact, a support contact, and a security contact are recorded.
- assess regularly the validity of the information about the providers.
- regularly ask the providers to assess their engagement[4] keep their information up-to-date and to use the DPMT also to record any scheduled downtimes that might affect a provided DICE service.
- in order to allow self-management on the DPMT, new colleagues of DICE obtain specific privileges. Staff members who are leaving the consortium get any specific privileges removed.

The SFRM process is implemented. The monthly meeting with the providers takes place largely as part of the WP7 provider meeting.

2.4 Service Level Management (SLM)

The goal of the SLM process within DICE is to define, agree, offer and monitor service level agreements to the customers, and to allow the providers of central and operational services to gain credibility by signing an operational level agreement (OLAs).

The DPMT allows adding any standard or specific agreement (SLA or OLA) to a registered provider's offer. Service providers may specify own SLAs. A sample SLA is available as a template.

Every provider of central services, operational or collaborative services (section 2.2) shall sign an OLA.

Central services are the B2ACCESS proxy AAI service (FZJ), the B2DROP catch-all service (FZJ) and the catch-all B2SHARE repository (CSC).

These providers are also part of the EUDAT consortium and use the OLA from EUDAT. This OLA is in the process of being finalized but only a few providers have already signed the document.

[4] The DPMT offers a specific view for providers that displays specifically all the projects, service, resources that are specifically assigned to them ().

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

As an example, section 7.3 “Violations” of the present EUDAT OLA is presented in the following.

7.3 Violations

The Service Provider commits to inform operational coordinator if the Agreement is violated or violation is anticipated. The following rules are applying for communication in the event of the Agreement violation:

Target	Violation	Measures
Service Availability	Not meeting target level with more than 3% for 2 consecutive reporting periods (see 7.2)	• Service Provider will make an analysis report and propose corrective measures • Service Provider will inform the EUDAT Operational Coordinator
Service Desk Response Time	Not meeting target level in more than 10% of the requests issued to the service provider	• Service Provider will make an analysis report and propose corrective measures • Service Provider will inform the EUDAT Operational Coordinator
Maintenance	Maintenance window takes 1 working day longer than announced	• Service Provider will inform the customer as soon as possible after the estimated end time via Service Provider communication channels • Service Provider will update downtime information in DPMT • Service Provider will inform the EUDAT Operational Coordinator and provides updates every 24 hours thereafter • in case of severe delays, delays of more than 3 working days, Service Provider will draft a post mortem report and send it to the EUDAT Secretariat
Lost data	Expected data integrity issues and/or accidental data loss	• If this is being discovered after the backup retention period, User, Customer and EUDAT Operational Coordinator are being informed about this incident and draft a post mortem report and send it to the EUDAT Secretariat
Disaster	Long-term loss of access to service and/or data caused by a force majeure (see section 6)	• Service Provider will inform the customer as soon as possible via Partner communication channels • Service Provider will update downtime information in DPMT • Service Provider will provide updates every 24 hours thereafter • Service Provider will provide a post mortem report and send it to the EUDAT Secretariat
Order Request Response and Enabling Time	Not meeting target level in more than 10% of the requests issued to the service provider	• Service Provider will make an analysis report and propose corrective measures • Service Provider will inform the EUDAT Secretariat

In case of violating the service level targets specified in this Agreement for two consecutive quarters, it is requested to provide justifications and a plan for service enhancement. In case of no or not satisfactory justification, EUDAT Secretariat can suspend or remove the Service Provider from the CDI infrastructure.

Communication channels and contact addresses are defined in section 7.1.

The DICE project has received funding from the European Union’s Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

2.5 Configuration Management (CONFM)

The purpose of the configuration management is to provide and maintain a logical model of configuration items, their relationships and dependencies as far as relevant for a project. A minimal amount of information about the allocated resources, services and the topology of composed services is aggregated in the configuration management database (DPMT, http://dp.eudat.eu)[5].

Important information items are:

- *Data Project* - the specification of the business case and the provided service(s) and resource(s) that fulfil the customer's order, the customer, the (general) provider, start and end date, the "customer agreement" between the provider and all the necessary contact information.
- *Provider* – the organisation or federation, or part of both, that manages and delivers services and resources to the customer.
- *Customer* – the organisation or part of an organisation that commissions a provider to receive one or more services and resources. Important to note that the *customer* usually represents a number of *users*. Therefore, the DPMT is not directly managing the access for users to the resources that is the purpose of the AAI (i.e. B2ACCESS).
- *Registered Service* – the concrete instance of an abstract kind of service as it described in the SPMT. It is basically an aggregation of one or more service components provided as part of a *Data Project*.
- *Registered Service Component* - a multi-tenant (physical) instance, a component that can be employed by one or several *Registered Services*. The availability and reliability of these registered service components matter, and it is recorded by the ARGO availability and reliability monitoring service (DICE D3.2).
- *Registered Resource* - specifies a certain quota of a capacity with a defined characteristic assigned to a project and the associated customer. This resource can be a registered quota of storage or compute capacity. The resource usage is accounted per customer.

The configuration information is needed for or by the

- Helpdesk team → ISRM
- Monitoring of availability and reliability → SRM
- Accounting of the resource usage per project → SRM
- Security management (service topology) → ISM
- Order Management (registration of projects) → SOCRM
- Change Management (side effects of changes) → CHM

As a principle, the service order manager is registering the project and customer information while the (general) providers are managing the detailed information of the service and resource instances, supported and supervised by project enablers and the operations coordinator.

The process has two main policies and a number of procedures that, like other process definitions, are available on the SMS section of the DICE/EUDAT wiki. Figure 1 shows an excerpt from the list of CONFM procedures as an example.

[5] EUDAT D6.3, 2018, pp.32 http://doi.org/10.23728/b2share.50eee85b6e724f1eb9c42a1bd92bec6e

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

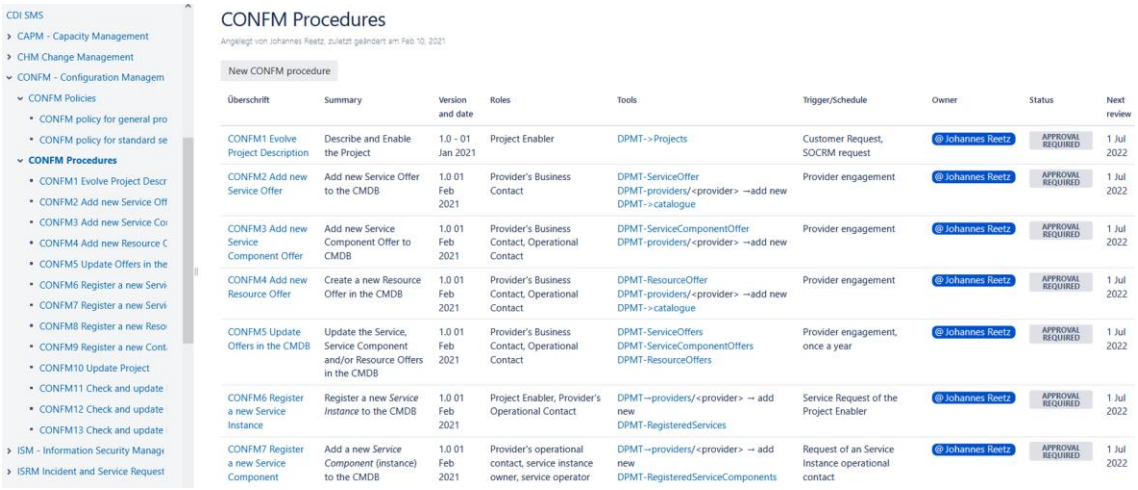

Figure 1 Excerpt from the list of CONFM procedures from the DICE Wiki

2.6 Change Management (CHM)

The goal of the Change Management is to ensure that the DICE providers are informed about planned changes (Change Requests), coordinate a process of commenting those Change Requests, and to trigger and synchronize the update of the configuration at the affected provider sites.

The CHM process has two policy documents defined, a *Risk Evaluation Policy* and *General CHM Policy Statements* that defines three kinds of changes.

Table 2 Matrix for evaluating the level of a CHM Risk

Likelihood	Impact			
	Minor	Moderate	Major	Catastrophic
Unlikely	Low	Low	Medium	Medium
Possible	Low	Medium	High	High
Likely	Medium	High	High	Extreme
Almost Certain	Medium	High	Extreme	Extreme

The risk level of a change (Table 2) such as for a design change of a service, for a configuration change of a production service instance or for the application of a security patch is evaluated by classifying the impact level of the change and by estimating the likelihood of the occurrence of that impact. As a principle, the information about the (initially) assessed risk level of a change has to be provided by the *Change Requester* him/herself when filling the *Request for Change* (RfC) form. Thus, the estimation of the risk of a change is based on the risk awareness, knowledge and expertise of the requester, i.e. often the implementer, of the change.

Currently there are three procedures in place – one for each CHM class (Figure 2).

The all changes are communicated to interested parties directly via Jira tickets or indirectly by notifying about the software updates via SVMON (the operational service for software version monitoring, see DICE D3.2 deliverable) and the Mattermost publication service (https://chat.eudat.eu). Many change requests are about autonomously implemented *standard*

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

changes without the need of specific coordination efforts and just requiring the notification about the change. DICE maintains a list of a number of known standard changes.

So far, DICE has coordinated just one *Non-Standard Change*, namely when the new version of the ARGO Monitoring Engine was put into operation in a new datacentre and several of the monitored DICE services had to be opened against new IP addresses and ports.

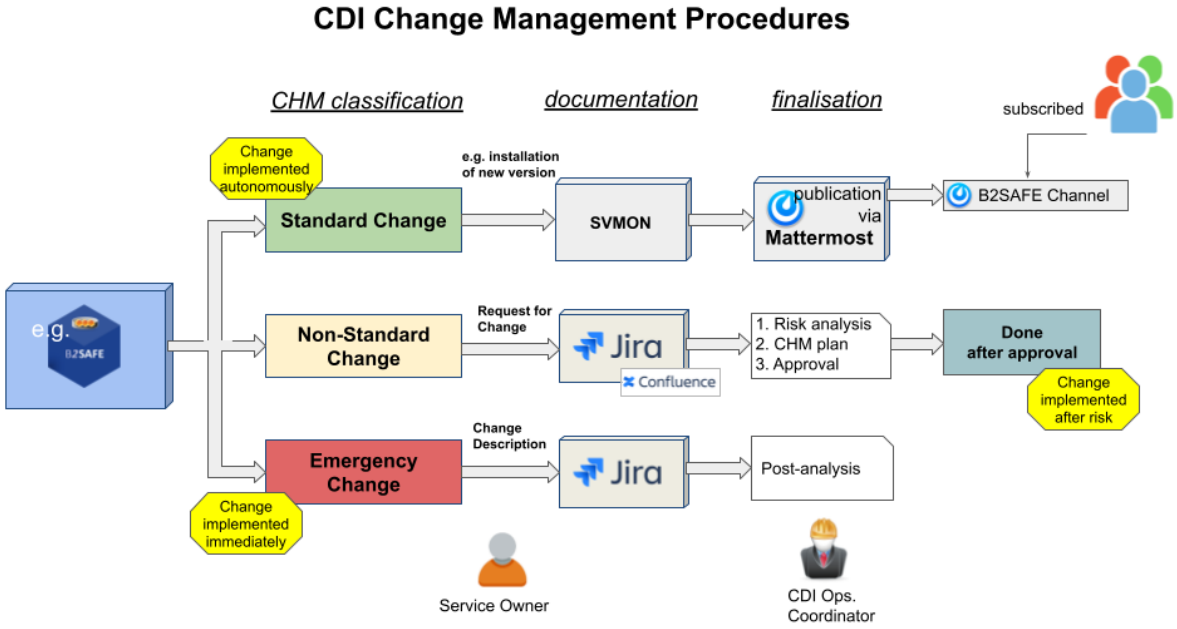

Figure 2 Change Management workflow: Standard Change, Non-Standard Change or Emergency Change

As an example, Figure 3 presents an overview about the different software versions for the B2SAFE service instances run by the DICE provider. SVMON is further developed via DICE WP3.

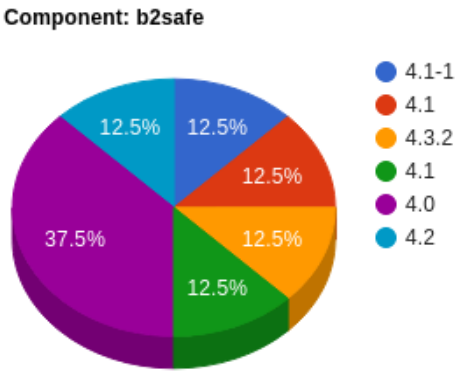

Figure 3 Example from the SVMON tool providing statistics about the distributed software B2SAFE.irods versions installed at the provider sites.

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

3 Incident and service request management (ISRM)

Incident and service request management provides the helpdesk service for customers, users and providers that follows certain rules.

The purpose of the Helpdesk task in DICE is

- to coordinate the support infrastructure for the DICE service providers and customers
- to operate and maintain a Helpdesk system, i.e. a ticketing system based on Request Tracker with interfaces to the support and contact form, and
- to provide specifically the 1st level support that is inspecting and forwarding incoming request to the adequate service expert teams and other support teams, e.g. those from the providers.

The helpdesk system is organised providing three support levels.

First level support: A dedicated First Level Support team is responsible for handling all incoming issue reports, support and contact requests which are normally received via the support and contact form. The 1st level support is the initial point of contact for stakeholders and customers of DICE, i.e. customers of existing or planned data projects, community and data managers and the users. The 1st level support provides basic information about the project, the services and how to use them. In addition, requests and issue reports are prioritized, classified, eventually clarified by contacting the requester and forwarded to the adequate 2nd level support teams. The 1st level support acts as a bridge to the 2nd level support by clarifying incoming requests which are too vague: standard questions are asked about more details if issue reports or requests are too unspecific, by that, requests are either filtered or enriched with further information before they are forwarded to the 2nd level support.

Second Level Support: Responsible for the Second Level Support are e.g. Data Project Enablers, Service Integrators, Product Owners, Service Area Managers, Provider Support contacts, and Service specialists, latter mainly from the provider sites. The 2nd level support provides detailed responses to requests and issue reports concerning specific services, the service catalogue, data projects, service design and feature requests. The 2nd level support is organized such that

- data project enablers and specialized DICE service integrators are responsible to response requests related to services or data projects, and that
- service providers are answering requests related to services and resources the machines that are hosting those services in their own domain.

When a request ticket has been forwarded from the 1st level support, the 2nd level support responds and starts interacting with the requester in order to solve the issue. It is also acting as a bridge to the 3rd level support, in particular if bugs and issues are reported which can only be solved on the level of service and software development.

Third Level Support: Responsible for the Third Level Support are the Service Area Managers and Service developers. The 3rd level support is handling bug and issue reports concerning the existing services, and they may record requirements for the developments of features and options for the DICE services. The 3rd level support is not necessarily responding to the original requester.

Three channels for reporting issues or making requests are offered: via webform, via email or directly on the helpdesk service (https://helpdesk.eudat.eu). The webform is made available via the EUDAT website (http://www.eudat.eu) and the EOSC portal (https://eosc-portal.eu). Request tickets can also be forwarded from the EOSC helpdesk system to the EUDAT helpdesk platform (deliverable DICE D3.2).

There are four kinds of ticket queues

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

- site queues for requests to be directed by the providers
- product queues for each of the DICE service
- functional queues for internal services such as accounting or new order requests
- project queues of specific projects or communities

Each queue has a group (team of experts) assigned and the helpdesk manager in its capacity as supervisor of the queues makes sure that at least one addressee, acting as queue manager, is assigned to a queue. This queue manager on the 2nd level is managing the team (queue watchers) and makes sure that the tickets are timely taken and processed.

Beside the daily operation of the Helpdesk system (https://helpdesk.eudat.eu) and the first level support activity the helpdesk team has

- reorganised the mentioned thematic queues of the Helpdesk system;
- revised the ISRM procedures and Helpdesk guidelines;
- implemented and monitored the measures to prevent or treat SPAM.
- Identified and coordinated the process activities in cooperation with SOCRM

The Helpdesk system, the main tool for managing all the requests and issue reports, is a Request Tracker (RT) Trouble Ticketing System (TTS). The configuration of the TTS, the setup of the queues and the escalation procedures, reflect the requirements from the different support levels, from the end users as well as from the project management that has to track the activities on service and project enabling.

Figure 4 is presenting the queues that received a fraction of the 320 tickets received during the reporting period. Beside the fact that almost 1/3 of the tickets are spam that was automatically and manually filtered out, the majority of the helpdesk requests are on services that are provided as self-service – probably because these services have the largest user base (B2SHARE, B2DROP and the generic B2ACCESS).

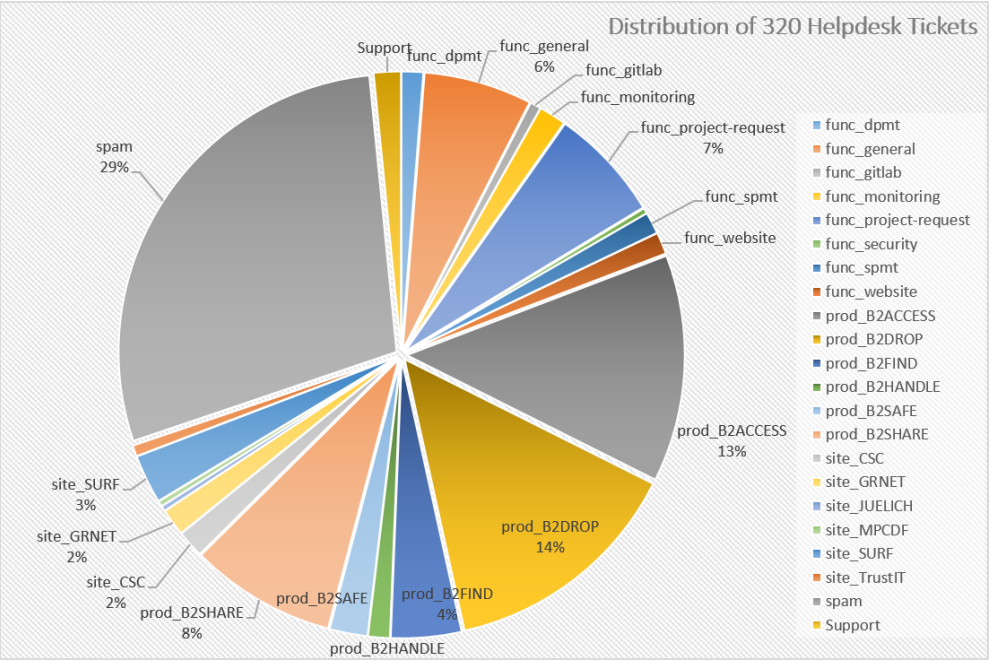

Figure 4 Distribution of the 320 tickets received since January 2021 over the queues.

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

4 Service order and customer relationship management (SOCRM)

Order management is an important operational task both for the efficient recording of requests for DICE services and resources and for their timely onward distribution to the appropriate providers, who promptly fulfil the requests as comprehensively as possible. The Service Order and Customer Relationship Management (SOCRM) process ensures that services are resourced as requested - either immediately or following a procedure that ensures the fulfilment of the request within a specified maximum timeframe. Good relationships with customers have been established and maintained using communication channels and tools such as the EOSC Service Order Management tool (SOMBO), the Helpdesk system and the DPMT for recording the customer requests, their feedback as well as to track the progress of providing services to the users:

- acting as a first contact point for incoming services requests
- processing the service requests efficiently
- forwarding the requests to the corresponding services providers
- tracking the timely provisioning of services
- maintaining a good relationship with customers and query user satisfaction

Beside the daily order management activities the team has

- further developed the order management workflow,
- provided in-depth customer support, helping customers for preparing order requests,
- supported service providers for the central registration of new orders into the DPMT,
- fostered the onboarding of DICE services (VA installations) into the EOSC portal,
- consolidated the service descriptions for the DICE services, in both the DICE catalogue and on the EOSC portal
  - updated general information and description of the services to include and improve features description
  - added and updated the description of service offers
  - added and update the description of service providers
  - reviewed the EOSC portal categories and suggested a better mapping to improve the findability of the services in the marketplace
- conducted a first DICE customer survey

Figure 5 shows the three different provisioning categories: *self-service*, *standard* and *customised*. While most demands fall into the category *self-service*, requests for larger capacities have been enabled in the *standard* cases within 2 and 10 days or, if customisations were necessary, with some enabling efforts on the customer and provider side.

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

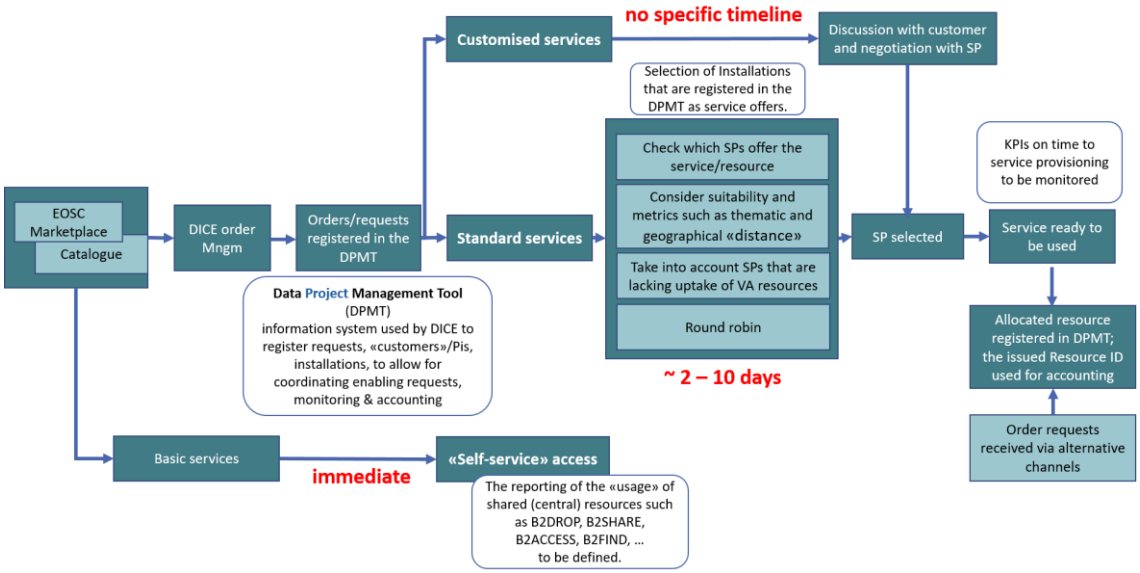

Figure 5 Order management with three different timelines for service and resource provisioning

At the end of the reporting period by 1st April 2022 there are

- 7 projects marked as being planned (for 3 of them a provider has not yet been selected),
- 6 projects are being enabled.

Two projects, namely the B2DROP catch-all project with the installation provided by FZJ and the generic B2SHARE repository project (CSC), make their installations available for self-service. This allows to reach out to a rather large number of users.

For 56 projects the services have been enabled in *standard* mode (2-10 days enabling time) and for 33 projects the services are or have been enabled in the *customised* mode.

Country	# Projects
Austria	1
Belgium	1
Czech Rep	6
Finland	1
France	4
Germany	8
Greece	3
Hungary	1
Iceland	1
Island	1
Italy	10
Lithuania	1
Norway	3
Poland	5
Serbia	1
Spain	7
Switzerland	1
Netherlands	3
Ukraine	1
UK	1
EU project	14
European	9

All Projects assigned to Providers

Provider	# All Projects	#Types of Provisioning
BSC	10	standard, customised
CESNET	3	customised
CINECA	10	standard, customised
CSC	9	**basic**, standard, customised
Cyl	1	standard
DATACITE	11	standard
DKRZ	19	customised
FZJ	8	**basic**, standard, customised
GRNET	7	standard
GWDG	2	standard
INFN	1	customised
MPG	2	standard
SURF	7	standard, customised
total	**90**	(planning, enabling, production)

Figure 6 Left: Customers with production DICE services by country. Right: DICE providers

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.

5 Information security management (ISM)

Information security management is about managing information security effectively through activities performed to deliver and manage services in such a way that the confidentiality, integrity and accessibility of relevant information assets are preserved.

The Information Security Management (ISM) task has monitored and reacted incidents that imply significant security risks for the federation of DICE (EUDAT) providers. The EUDAT CSIRT team (reaction team on known security incidents and vulnerability alerts led by the EUDAT security officer) were on stand-by for this purpose. Warnings about critical security vulnerabilities were submitted to the providers' security officers and in cases like the "Log4j" vulnerability alert, concerted risk analyses and countermeasures have helped mitigating the risks of a breach. As a rule, notifications were set up and triggered in the event of serious security incidents, if central services such as the wiki, the AAI proxy B2ACCESS or federation tools like the DPMT were affected. Fortunately there have been no major security incidents in the course of the present reporting period.

The EUDAT Security Policy and EUDAT CDI Acceptable Use Policy and the Conditions of Use have been reviewed and updated as well as the definitions of DICE (EUDAT) ISM Controls.

The EUDAT Security team members have regularly contributed in the work of EOSC Future Security team and participated in the regular coordination meetings.

The handling of the process for certificate renewal for IT services under the "eudat.eu" domain was updated and implemented by CSC.

6 Conclusions

This deliverable presents aspects of operations coordination in the DICE project at federation level, and it highlights employed service management processes that are roughly based on FitSM.

Helpdesk (ISRM) and Order Management (SOCRM) are fully implemented and operational, and the service management processes are defined. Many of these processes stem from best practices from EUDAT and from the EOSC-hub project. Many orders, support requests, services and resources are accordingly recorded and addressed by the operations team. However, the written documentation of these processes is still not complete - a prerequisite for an adequate assessment by the DICE Operations Advisory Board. The documentation should be completed in the following reporting period.

As pointed out, using the Federated Service Management within DICE WP6 is recommended for all DICE providers, but in some regards not mandatory particularly for those that are not members of the EUDAT Collaborative Data Infrastructure. For instance, although a large subset of DICE providers is using the DPMT to record and maintain project-related configuration information about own installations there are still configuration items to be properly recorded before the features of the federated operations become beneficial for all DICE installations, namely the central availability monitoring, accounting and service version monitoring. It is the plan of WP6 for the next period to improve the overall uptake of the operation tools. It is the plan to gain improvements with regard to the completeness of the maintained configuration information.

The DICE project has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 under Grant Agreement no. 101017207.