

# Eligibility Framework - Status and topics for STEPS

STEPS Tech Committee

4 Nov 2024

CERN IT Eligibility Framework team  
(Joint project FHR sector and IT)



# The Eligibility Framework (EF) project

- **Definition:**
  - A structured taxonomy and a framework for defining and applying "who can access what" resources.
- **Purpose:**
  - Ensuring appropriate and efficient allocation of resources while minimizing costs and reputational risks.
- **Key objectives:**
  - Policy Definition: Establish clear policies for resource access and usage.
  - Framework Setup: Develop and integrate a New Resource Portal to manage eligibility rules and lifecycle.
  - Resource Usage Monitoring: Track resource utilization to make informed decisions on policy adjustments, manage risks, and optimize costs.
- **Players:**
  - Main actors: FHR and IT
  - Stakeholders: the whole CERN

# EF - The Origin

- **The Eligibility Framework project started beginning of 2023,**
  - Green-light on policy and high level implementation plan at the CERN Extended Directorate meeting on the 30th of May 2023.
  - Acknowledged in ED meeting minutes: “some milestones and deliverables may need further discussion with technical experts on feasibility and implementation details”.
- **The project is progressing**
  - With delays in some of the areas wrt timeline defined ~2 years ago:
    - reasons discussed and understood
  - Updated deliverables organization and timeline
    - Discussed and agreed in FHR-IT Tech and Steering meetings
- **No showstoppers foreseen for the overall project**
  - But interesting challenges that will require iterations to be appropriately tackled.



## M1 [FHR+IT] - Computing Account Automatic Activation (C3A)

- Fully integrated.





## M2 [IT] - RUM (Resource Usage Monitoring)

- First version done. Results in 2024 March FHR-IT Tech. OK to re-run by end of 2024.



## M3 [IT] New Resource Portal

-  Work ongoing. First big service full integration: end of Q4 2024. Next service (Google) by end of Q1 2025.
-  Hackathon (beginning of 2025) under discussion to sprint the integration of services and validate the NRP backend API



## M4 [FHR] Admin e-guide and processes

- Draft available (next slide). No major issues. Will need a bit of work to set up the processes when NRP will be available. To be discussed in STEPS (today)



## M5 [CERN wide] Policy definition

- The “Eligibility Matrix”: first implementation done, next iterations in STEPS (today)

# Eligibility Matrix

admin eGuide  
MPA & MPE

admin eGuide  
Remote & contractors

admin eGuide  
retirees & others

Eligible		Limited = limited access controlled by egroups, or for a limited time period															
Not Eligible		MPEs & MPAs		Remote Participants			Contractors & Externals					Retirees		Other			
Eligible with Guarantor approval		MPEs + Trainees: (STAF, FELL, GRADS + Temp. Labour + EXTN RETC, MPAT: ADMI, APPR, DOCT, SUMM, TECH, TRNE)	Collaborators + Exchange Scientists (MPAC: COAS, EXAS, PJAS, USER + MPAC: CASS, GPRO, SASS, VIS)	EXTN PART, RETP	EXTN DIST	Future MPs (UOPR, FTMP)	Employees of CERN Contractors (computer users)	Employees of CERN Contractors (non- computer users)	EXTN Group A (GUID, ILOF, STAG, PROJ, EUPR, SCIE, COMT)	EXTN Group B (CONF, FORM, GACR)	EXTN Group C (ACCO, HOST, KIND, VISI, CLUB)	Retiree	Ex-Member of Personnel (Grace Period 2 months)	Alumni	Ex-Member of Personnel (non- contractors)	Ex-Member of Personnel (Externals + contractors)	Visitors
<b>Responsible body (who approves rules of eligibility)</b>		HR / IPT	HR / EP	EP	GTPA	HR/ Users Office	IPT Dept.	IPT Dept.	GTPA	GTPA, HR-LD (FORM), PF (GACR)	GTPA, HR-SA (KIND, CLUB), IPT (VISI)	PF	HR	IR	HR	GTPA + IPT	IR
<b>Guarantor (who approves requests) + Licence Manager</b>		Supervisor	Supervisor / Team Leader	Team Leader	CERN Guarantor	Future Supervisor	Technical Officer *	Technical Officer *	CERN Guarantor / Supervisor	CERN Guarantor	N/A	N/A	N/A	IR	N/A	N/A	N/A
<b>Population size JAN 2023</b>		3233	12913	7168	577	141	ca. 300	ca. 4270	697	61	606	ca. 3800		ca. 8000			
<b>Basic resources</b>				Visitors	Visitors	Visitors					Visitors		Visitors	Visitors	Visitors	Visitors	Visitors
Register device(s) on CERN network / connect to CERN wifi																	
Bulletin																	
Mattermost, Discourse																	
Security Services: firewall (PAN), mail quarantine (xorlabs)																	
Tax certificates, attestations, salary slips				If was MP	If was MP	If was MP	If was MP	If was MP	If was MP	If was MP	If was MP	Limited	If was MP	If was MP	If was MP	N/A	N/A
Be part of eGroups																	
Indico content (behind SSO)																	
Webcasts (behind SSO)												Limited					
Login to/Read Twiki, Drupal, Wordpress, CodiMD												Limited					
CERN websites (Alumni, ILOs, Pension Fund, CHIS...)												Limited					
CDS content (behind SSO)												Limited					
Mandatory online safety / security training courses																	
Official notifications + News																	
Phonebook																	
Personal home directory quota (CERNbox, Office A1 M365)																	
Central Compute Services (AFS, EOS, LXPLUS, LXBATC)																	
CERNPhone																	
Create egroups																	
EDH				?	?	?	?		?	?	?	Limited					
ESET Security software (CERN managed devices)						Limited	Limited					Limited					
ESET Security software (BOYD)																	
Other Learning courses				Limited	Limited	Limited	Limited	Limited	Limited					Limited			
<b>Controlled resources</b>		<b>In Portal?</b>															
Computing account / way to authenticate		N															
Service Now (be a supporter)		N															
Create Twiki, Drupal, Wordpress, CodiMD		Y															
Grid certificates		Y															
Java JDK JRE		Y															
Google Workspace																	
Overleaf, Gitlab, Atlassian, Zoom		Y															
Digital Library (ebooks + journals + ILS Library Catalogue)		Y															
Microsoft (Windows + Office A5 M365)		Y															
CAD/CAM & Engineering software		Y															
Create redirections (mail)		Y															
CERN redirection alias as connection string		N															
Mailbox + CERN email		Y															
Access to CERN resources portal?																	



# Eligibility Matrix - admin eGuide - draft for STEPS approval

## Eligibility - Members of the personnel, Temporary personnel and Externals RETC - Draft version

CATEGORY	MPEs / MPAs / TEMCs / EXTN RETC	
	HR / IPT ADMN, APPR, DOCT, SUMM, TECH, TRNE TEMC EXTN RETC	COAS, EXAS, PIAS, USER CASS, GPRO, SASS, VISC
Responsible body (who approves rules of eligibility)	HR / IPT	HR / EP
Supervisor / Guarantor (who approves requests) + Licence Manager	Supervisor	Supervisor / Team Leader
<b>BASIC RESOURCES</b>		
Register device(s) on CERN network / connect to CERN wifi Bulletin		
Mattermost, Discourse		
Security Services: firewall (PAN), mail quarantine (xorlabs)		
Tax certificates, attestations, salary slips		
Be part of eGroups		
Indico content (behind SSO)		
Webcasts (behind SSO)		
Login to/Read Twiki, Drupal, Wordpress, CodIMD		
CERN websites (Alumni, ILDs, Pension Fund, CHS...)		
CD5 content (behind SSO)		
Mandatory online safety / security training courses		
Official notifications + News		
Phonebook		
Personal home directory quota (CERNbox, Office A1 M365)		
Central Compute Services (AFS, EOS, LXPLUS, LXBATCH)		
CERNPhone		
Create egroups		
EDM		
ESET Security software (CERN managed devices)		
ESET Security software (BOYD)		
Other Learning courses		
<b>CONTROLLED RESOURCES</b>	In Portal?	
Computing account / way to authenticate	N	
Service Now (Be a supporter)	N	
Create Twiki, Drupal, Wordpress, CodIMD	Y	
Grid certificates	Y	
Java JDK .JRE	Y	
Google Workspace	Y	
Overleaf, Gitlab, Atlassian, Zoom	Y	
Digital Library (ebooks + journals + ILS Library Catalogue)	Y	
Microsoft (Windows + Office A5 M365)	Y	
CAD/CAM & Engineering software	Y	
Create redirections (mail)	Y	
CERN redirection alias as connection string	N	
Mailbox + CERN email	Y	
Access to CERN resources portal?	Y	
<b>Legend:</b>		
Eligible with supervisor / guarantor approval		
Not Eligible		

## Eligibility - Remote participants, Contractors and Externals - Draft version

CATEGORY	REMOTE PARTICIPANTS				CONTRACTORS AND EXTERNALS						
	EXTN PART, REIP	EXTN DST	Future MPN (UOPR, FTMP)	Employees of CERN Contractors (computer users)	Employees of CERN Contractors (non-computer users)	EXTN Group A: GIUD, ILOS, STAG, PROI, SUPR, SCIE, COMT	EXTN Group B: CONF, FORM, GACA	EXTN Group C: ACCO, HOPE, KINO, VISI, CLUB	EXTN Group D: GTPA, HR, SA (InvD, IPT (VIS))	EXTN Group E: GTPA, HR, SA (InvD, IPT (VIS))	EXTN Group F: GTPA, HR, SA (InvD, IPT (VIS))
Responsible body (who approves rules of eligibility)	EP	GTPA	HR / Users Office	IFT Dept.	IFT Dept.	GTPA	GTPA, HR, SA (InvD, IPT (VIS))	GTPA, HR, SA (InvD, IPT (VIS))	GTPA, HR, SA (InvD, IPT (VIS))	GTPA, HR, SA (InvD, IPT (VIS))	GTPA, HR, SA (InvD, IPT (VIS))
Supervisor / Guarantor (who approves requests) + Licence Manager	Team Leader	CERN Guarantor	Future Supervisor	Technical Office *	Technical Office *	CERN Guarantor / Supervisor	CERN Guarantor	CERN Guarantor	N/A	N/A	N/A
<b>BASIC RESOURCES</b>											
Register device(s) on CERN network / connect to CERN wifi Bulletin			Visitors						Visitors		
Mattermost, Discourse											
Security Services: firewall (PAN), mail quarantine (xorlabs)											
Tax certificates, attestations, salary slips				If was member of the personnel							
Be part of eGroups											
Indico content (behind SSO)											
Webcasts (behind SSO)											
Login to/Read Twiki, Drupal, Wordpress, CodIMD											
CERN websites (Alumni, ILDs, Pension Fund, CHS...)											
CD5 content (behind SSO)											
Mandatory online safety / security training courses											
Official notifications + News											
Phonebook											
Personal home directory quota (CERNbox, Office A1 M365)											Limited
Central Compute Services (AFS, EOS, LXPLUS, LXBATCH)											
CERNPhone											
Create egroups											
EDM											
ESET Security software (CERN managed devices)					Limited	Limited					
ESET Security software (BOYD)											Limited
Other Learning courses											
<b>CONTROLLED RESOURCES</b>	In Portal?										
Computing account / way to authenticate	N										
Service Now (Be a supporter)	N										
Create Twiki, Drupal, Wordpress, CodIMD	Y										
Grid certificates	Y										
Java JDK .JRE	Y										
Google Workspace	Y										
Overleaf, Gitlab, Atlassian, Zoom	Y										
Digital Library (ebooks + journals + ILS Library Catalogue)	Y										
Microsoft (Windows + Office A5 M365)	Y										
CAD/CAM & Engineering software	Y										
Create redirections (mail)	Y										
CERN redirection alias as connection string	N										
Mailbox + CERN email	Y										
Access to CERN resources portal?	Y										External
<b>Legend:</b>											
Eligible with supervisor / guarantor approval											
Not Eligible											

## Eligibility - Retirees and others - Draft version

CATEGORY	RETIRES		OTHER			
	Retiree	Ex-member of the personnel (since period 2 months)	Alumni	Ex-member of the personnel (non-contractors)	Ex-member of the personnel (externals + contractors)	Visitors
Responsible body (who approves rules of eligibility)	FF	HR	IR	HR	GTPA + IPT	IR
Supervisor / Guarantor (who approves requests) + Licence Manager	N/A	N/A	IR	N/A	N/A	N/A
<b>BASIC RESOURCES</b>						
Register device(s) on CERN network / connect to CERN wifi Bulletin						Visitors
Mattermost, Discourse						
Security Services: firewall (PAN), mail quarantine (xorlabs)						
Tax certificates, attestations, salary slips	Limited			If was member of the personnel		N/A
Be part of eGroups	Limited					
Indico content (behind SSO)	Limited					
Webcasts (behind SSO)	Limited					
Login to/Read Twiki, Drupal, Wordpress, CodIMD	Limited					
CERN websites (Alumni, ILDs, Pension Fund, CHS...)	Limited					
CD5 content (behind SSO)	Limited					
Mandatory online safety / security training courses	Limited					
Official notifications + News						
Phonebook						
Personal home directory quota (CERNbox, Office A1 M365)						
Central Compute Services (AFS, EOS, LXPLUS, LXBATCH)						
CERNPhone						
Create egroups	Limited					
EDM						
ESET Security software (CERN managed devices)						
ESET Security software (BOYD)						Limited
Other Learning courses						
<b>CONTROLLED RESOURCES</b>	In Portal?					
Computing account / way to authenticate	N					
Service Now (Be a supporter)	N					
Create Twiki, Drupal, Wordpress, CodIMD	Y					
Grid certificates	Y					
Java JDK .JRE	Y					
Google Workspace	Y					
Overleaf, Gitlab, Atlassian, Zoom	Y					
Digital Library (ebooks + journals + ILS Library Catalogue)	Y					
Microsoft (Windows + Office A5 M365)	Y					
CAD/CAM & Engineering software	Y					
Create redirections (mail)	Y					
CERN redirection alias as connection string	N					
Mailbox + CERN email	Y					
Access to CERN resources portal?	Y					
<b>Legend:</b>						
Eligible with supervisor / guarantor approval						
Not Eligible						



# Specific topics for STEPS

## 1. Draft admin eguide approval

- a. The matrix was approved in May2023 by the CERN Extended Directorate, the admin eGuide draft pages are just the matrix exposed in webpages.

## 2. Contact in case of requests for changes to the Eligibility Framework Matrix:

- a. we suggest is STEPS, i.e. we need to have some "contact us" in case of questions.

## 3. Eligibility Framework Matrix updates:

- a. we do not have big changes as of now to be suggested, one minor (next slide)

## 4. Guest accounts:

- a. they are not in the EFM
- b. we believe that unverified account should not be allowed to have "expensive" resources, expensive means anything that is more than some view on e.g. social, indico, etc.

## 5. Emeriti:

- a. Discussions are ongoing, from the Eligibility project point of view is OK if they have category of personnel (as it is proposed as of now), no issues foreseen.

## 6. Chargeback mechanism (once NRP is ready):

- a. we need to have a reasonable balance between creating one EDH doc for user for license (too many, more the cost than the gain!), and an "all-in", which would not allow us to be detailed enough and optimize costs while minimizing risks.
- b. We are thinking to setup a small TF to detail the process to be setup.

# Email - details

- In the present EFMMatrix we have:
  - “CERN redirections (mail)”: this relates to the capacity to get a CERN email address without a mailbox (with a redirection to an external email address)
  - “CERN redirection alias as connection string”: this is the possibility to connect to cloud services while being recognised as a CERN user; this means getting an @cern.ch login, but no email address behind.
  - “Mailbox + CERN email”: the “classic” one - the capacity to get a CERN email address with a mailbox
- It was noted by the experts that option “B” does not make much sense:
 

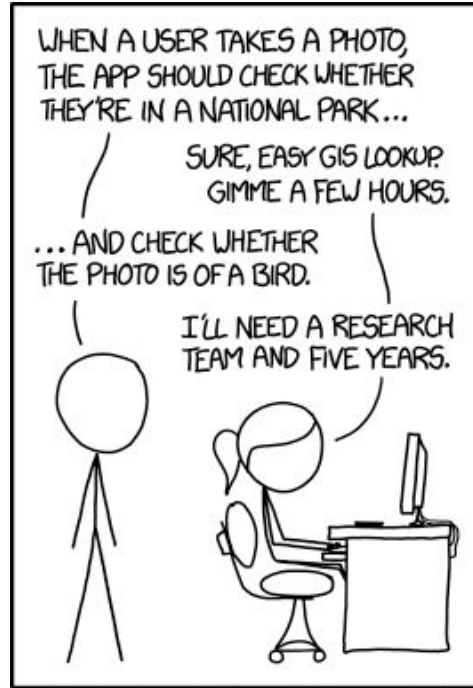
Cloud services do expect that the email address you enter as login can be used to validate the account, and/or simply send service-related information.
- We propose to merge A and B into a single “CERN email address without mailbox” line with the same colors as B except for the cells under “Remote Participants” which should be orange.

Eligible	Limited = limited access controlled by egroups, or for a limited time period															
Not Eligible																
Eligible with Guarantor approval																
Category	MPes & MPAs		Remote Participants			Contractors & Externals					Retirees	Other				
	MPes + Trainees: (STAF, FELL, GRADs + Temp. Labour + EXTN RETC, MPAt: ADMI, APPR, DOCT, SUMM, TECH, TRNE)	Collaborators + Exchange Scientists (MPAc: COAS, EXAS, PJAS, USER + MPAc: CASS, GPPO, SASS, VISC)	EXTN PART, RETP	EXTN DIST	Future MPes (UOPR, FTMP)	Employees of CERN Contractors (computer users)	Employees of CERN Contractors (non- computer users)	EXTN Group A (GUID, ILOF, STAG, PROJ, EUPR, SCIE, COMT)	EXTN Group B (CONF, FORM, GACR)	EXTN Group C (ACCO, HOST, KIND, VISI, CLUB)	Retiree	Ex-Member of Personnel (Grace Period 2 months)	Alumni	Ex-Member of Personnel (non- contractors)	Ex-Member of Personnel (Externals + contractors)	Visitors
Responsible body (who approves rules of eligibility)	HR / IPT	HR / EP	EP	GTPA	HR/ Users Office	IPT Dept.	IPT Dept.	GTPA	GTPA, HR-LD (FORM), PF (GACR)	GTPA, HR-SA (KIND, CLUB), IPT (VISI)	PF	HR	IR	HR	GTPA+ IPT	IR
Guarantor (who approves requests) + Licence Manager	Supervisor	Supervisor / Team Leader	Team Leader	CERN Guarantor	Future Supervisor	Technical Officer *	Technical Officer *	CERN Guarantor / Supervisor	CERN Guarantor	N/A	N/A	N/A	IR	N/A	N/A	N/A

Create redirections (mail)	Y															
CERN redirection alias as connection string	N															
Mailbox + CERN email	Y						External									



# Questions?



IN CS, IT CAN BE HARD TO EXPLAIN  
THE DIFFERENCE BETWEEN THE EASY  
AND THE VIRTUALLY IMPOSSIBLE.

# EXTRA

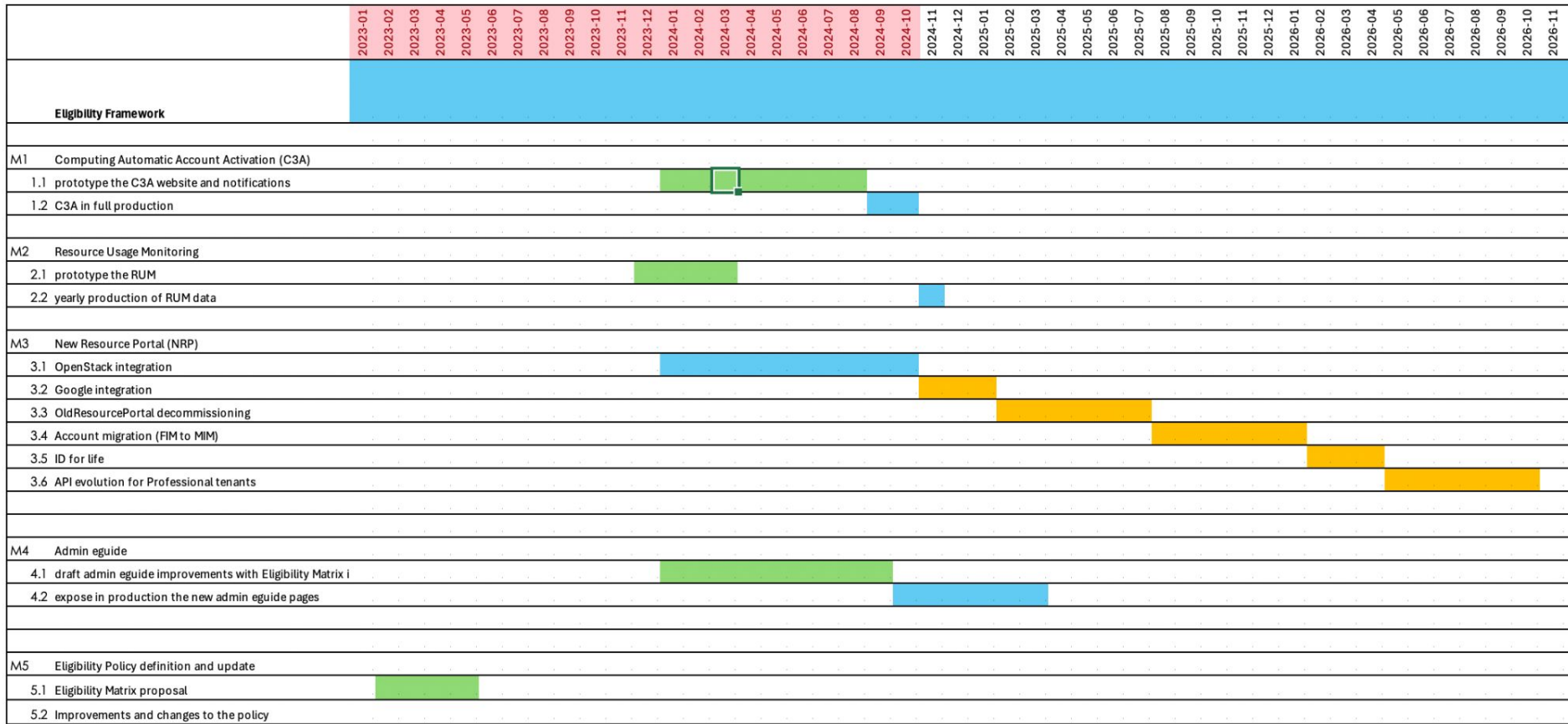


# Eligibility - Milestones and Deliverables

#	Name of Milestones and Deliverables	Status	To Be Reviewed By	CERN			STEP			Comments
				Start Date dd/mm/yyyy	End Date dd/mm/yyyy	Duration (months)	Start Date dd/mm/yyyy	End Date dd/mm/yyyy	Duration (months)	
	<b>Eligibility Framework</b>	<b>In Progress</b>	<b>ARB, FHR+IT</b>	<b>01.01.23</b>	<b>31.12.25</b>	<b>36</b>	<b>01.01.23</b>	<b>31.12.26</b>	<b>48</b>	severe underestimation of the complexity of the New Resource Portal
<b>M1</b>	<b>Computing Automatic Account Activation (C3A)</b>	<b>In Progress</b>								
1.1	prototype the C3A website and notifications	<b>Complete</b>	FHR+IT Tech and Steering	01.01.24	01.06.24	5	01.01.24	01.09.24	8	Several bugs discovered
1.2	C3A in full production	<b>In Progress</b>	FHR+IT Tech and Steering	01.09.24	01.10.24	1	01.09.24	01.11.24	2	Contractors and EXTN not yet fully informed
1.3										
<b>M2</b>	<b>Resource Usage Monitoring</b>	<b>In Progress</b>								
2.1	prototype the RUM	<b>Complete</b>	FHR+IT Tech and Steering	01.12.23	01.04.24	4				
2.2	yearly production of RUM data	<b>In Progress</b>	FHR+IT Tech and Steering	01.11.24	01.12.24	1				it requires logs from each relevant service
<b>M3</b>	<b>New Resource Portal (NRP)</b>	<b>In Progress</b>								
3.1	OpenStack integration	<b>In Progress</b>	IT Elig Team + ARB	01.01.24	01.04.24	3	01.01.24	01.11.24	10	
3.2	Google integration	<b>On Hold</b>	IT Elig Team + ARB	01.03.24	01.05.24	2	01.11.24	01.02.25	3	dependent on previous steps
3.3	OldResourcePortal decommissioning	<b>On Hold</b>	IT Elig Team + ARB	01.02.25	01.08.25	6				dependent on previous steps - will require Oracle and AFS experts
3.4	Account migration (FIM to MIM)	<b>On Hold</b>	IT Elig Team + ARB + FHR	01.08.25	01.02.26	6				dependent on previous steps
3.5	ID for life	<b>On Hold</b>	IT Elig Team + ARB + FHR	01.02.26	01.05.26	3				dependent on previous steps - can be fast once the migration to MIM is comp
3.6	API evolution for Professional tenants	<b>On Hold</b>	IT Elig Team + ARB	01.05.26	01.11.26	6				it could be done in parallel with the integration of services, but relies on the so
<b>M4</b>	<b>Admin eguide</b>	<b>In Progress</b>								
4.1	draft admin eguide improvements with Eligibility Matrix inf	<b>Complete</b>	FHR-IT	01.01.24	01.10.24	9				
4.2	expose in production the new admin eguide pages	<b>In Progress</b>	FHR-IT	01.10.24	01.04.25	6				it will take time to be able to have comments from the community
<b>M5</b>	<b>Eligibility Policy definition and update</b>	<b>Complete</b>								
5.1	Eligibility Matrix proposal	<b>Complete</b>	STEPS	01.01.23	01.06.23	5				agreed at ED May 2023
5.2	Improvements and changes to the policy	<b>On Hold</b>	STEPS							nothing critical to discuss with STEPS as of now. Emeriti are being discussed in

Status
Not Started
In Progress
Complete
On Hold

# Eligibility - Gantt chart



# Eligibility - Project Milestones Map: old → new

## High-level deliverables, responsibilities and timing \*

Theme	Deliverable	Responsible	Timing
Monitoring	Bi-annual report on computing resource usage for DHS	IT	Q3 2023
Access Control	Eligibility framework in place in eGroups and Admin eGuide	FAP-BC	By end 2023
Access Control	Initial request process for access to software + clean up of non-eligible access	IT	By end 2023
Access Control & Clean-Up	Day-to-day application of Eligibility Framework; Annual revision of exceptional accesses	Experiments & Departments	Ongoing from Q3 2023
Access Control	Computing accounts activated automatically **	IT	By end 2023
Clean-up + Findability	Email restriction for future Externals & Contractors + establish new resources portal	IT	By end Q1 2024
Clean-up	Registration & Termination tools to show eligibility criteria to individuals	FAP-BC	By end Q1 2024
Access Control	"ID for life"	IT	By end Q2 2024
Findability	Migration of resources from old portal(s) to new	IT	Rolling basis from Q2 2024 aft new resources portal is ready

\* Approved at E.D. on 30<sup>th</sup> May 2023  
 \*\* This bring resource savings in SCE in the scope of the CERN Welcome Centre

#	Name of Milestones and Deliverables	Status	To Be Reviewed By
	<b>Eligibility Framework</b>	<b>In Progress</b>	<b>ARB, FHR+IT</b>
<b>M1</b>	<b>Computing Automatic Account Activation (C3A)</b>	<b>In Progress</b>	
1.1	prototype the C3A website and notifications	<b>Complete</b>	FHR+IT Tech and Steering
1.2	C3A in full production	<b>In Progress</b>	FHR+IT Tech and Steering
1.3			
<b>M2</b>	<b>Resource Usage Monitoring</b>	<b>In Progress</b>	
2.1	prototype the RUM	<b>Complete</b>	FHR+IT Tech and Steering
2.2	yearly production of RUM data	<b>In Progress</b>	FHR+IT Tech and Steering
<b>M3</b>	<b>New Resource Portal (NRP)</b>	<b>In Progress</b>	
3.1	OpenStack integration	<b>In Progress</b>	IT Elig Team + ARB
3.2	Google integration	<b>On Hold</b>	IT Elig Team + ARB
3.3	OldResourcePortal decommissioning	<b>On Hold</b>	IT Elig Team + ARB
3.4	Account migration (FIM to MIM)	<b>On Hold</b>	IT Elig Team + ARB + FHR
3.5	ID for life	<b>On Hold</b>	IT Elig Team + ARB + FHR
3.6	API evolution for Professional tenants	<b>On Hold</b>	IT Elig Team + ARB
<b>M4</b>	<b>Admin eguide</b>	<b>In Progress</b>	
4.1	draft admin eguide improvements with Eligibility Matrix inf	<b>Complete</b>	FHR-IT
4.2	expose in production the new admin eguide pages	<b>In Progress</b>	FHR-IT
<b>M5</b>	<b>Eligibility Policy definition and update</b>	<b>Complete</b>	
5.1	Eligibility Matrix proposal	<b>Complete</b>	STEPS
5.2	Improvements and changes to the policy	<b>On Hold</b>	STEPS

# EXTRA

**Slides presented in previous meetings**



# The "New Resource Portal" (NRP)

IT Strategic Technical Delivery Forum  
(STDF) 11th September

- Service managing **resources lifecycle and eligibility**
  - Part of the authentication & authorization services
  - Includes the computing resources web application
- For service managers:
  - Define eligibility criteria
  - Manage **lifecycle** of computing resources
- For users:
  - View the services I can use
  - View and manage my resources

Not Eligible		Limited - Limited access controlled by groups, or for a limited time period															
Eligible with Quarantor approval		MPEs & MPA		Remote Participants				Contractors & External				Alumni		Other			
Category		MPEs + Trainees (CMF, FIEL, GACH + Terms, Labour + EXTN)	Collaborators + Exchange Scientists (MFA, COS, BSA, PIA, USER + MFA-CAS, OPER, SARC, VISO)	EXTN PART, BETP	EXTN DIST	Future MPE (UOPN, PTMP)	Employees of CERN Contractors (computer users)	Employees of CERN Contractors (non-computer users)	EXTN Group A (GJUS, ILOP, STAG, PICO, BUPR, SITE, COME)	EXTN Group B (CONV, FORM, GACH, CLUB)	EXTN Group C (ACCO, HOSZ, KING, VIO, CLUB)	Alumni	Ex-Member of Personnel (since Period 2 months)	Alumni	Ex-Member of Personnel (non-contractors)	Ex-Member of Personnel (External + contractors)	Visitors
Responsible body (who approves rules of eligibility)		HR / IT	HR / EP	EP	GTPA	HR Users Office	IPT Dept.	IPT Dept.	GTPA	GTPA, HR-GL (FORM), PF (GACH)	GTPA, HR-GL (KING, CLUB), IPT (VISO)	PF	HR	IR	HR	GTPA + IPT	IR
Quarantor (who approves requests) + License Manager		Supervisor	Supervisor / Team Leader	Team Leader	CERN Supervisor	Future Supervisor	Technical Officer +	Technical Officer +	CERN Supervisor	CERN Supervisor	N/A	N/A	N/A	IR	N/A	N/A	N/A
Population size JAN 2023	3239	1293	7168	577	141		ca. 300	ca. 420	61	606	ca. 3900						
Basic resources	Register devices on CERN network / connect to CERNs wifi			Visitors	Visitors	Visitors					Visitors		Visitors	Visitors	Visitors	Visitors	Visitors
Registration: Classroom	Security Services: Firewall (PAG), mail quarantine (varlab)																
Tax certificates, attestations, salary slips	As part of eReceipt																
Indico content (behind SSO)	Indico content (behind SSO)																
Login to Read Tools, Drupal, Wordpress, CodMD	CERN websites (Jkuam, LOS, Persion Fund, CHS...)																
CERN content (behind SSO)	Mandatory online safety / security training courses																
Official applications + News	Phonobook																
Personal home directory quota (CERNbus, Office All MSSES)	Central Compute Services (APS, EOS, LXR/LUS, URMATCH)																
CERNphone	Credit agencies																
EDH	EDS security software (CERN managed devices)																
EDS Security software (SDCI)	Other learning courses																
Controlled resources	Computing account / new to authenticate																
Service Now (Be a supporter)	Create Tools, Drupal, Wordpress, CodMD																
Grid certificates	Grid certificates																
Open Office	Google Workspace																
Overhead, Gantt, Atlasian, Zoom	Digital Library (books + journals + US Library Catalogue)																
Microsoft (Outlook + Office 45 MSSES)	GDCA/CA & Engineering software																
Create redirections (mail)	CERN redirection sites as connection string																
Mailbox + CERN email	Access to CERN resources portals?																







# Resources

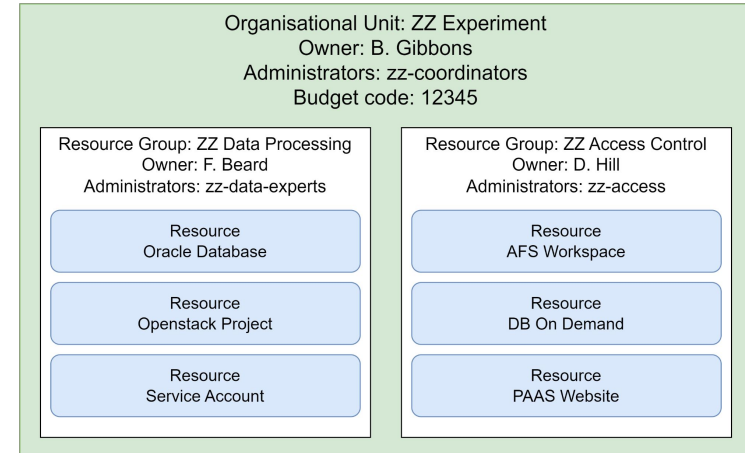
- **Resource:** element provided by a service for which we want to track lifecycle and ownership individually
- **Personal resource:** lifecycle bound to the owner
  - Not necessarily for personal usage. Example: mailbox or software license
  - Cannot be transferred to a new owner
- **Official resource:** lifecycle bound to a service or application
  - Currently owned by persons
  - In the new model, official resources should be assigned to **Resource Groups**

IT Strategic Technical Delivery Forum  
(STDF) 11th September

# Resource Groups (*blessed by ARB*)

- A **Resource Group (RG)** is a grouping of official resources
  - For a common operational purpose (service or application)
- A RG is owned by an **organisational unit** with budgetary responsibility
  - E.g. a CERN Department or an (official - graybook) experiment
- Users can manage resources in a RG if:
  - They are owners or administrators of the RG
  - They have the permissions required by the service
- Resources in a RG do not have a lifecycle
  - The RG does have lifecycle(more later)

*IT Strategic Technical Delivery Forum  
(STDF) 11th September*



# Resources lifecycle

- Each resource has a **state** that changes through its lifecycle
  - Model agreed with STDF 2023 Resource Lifecycle Working Group
  - IT services providing resources should follow this lifecycle model
- Lifecycle events are triggered by
  - Changes in the owner's eligibility status
  - Grace periods elapsing

IT Strategic Technical Delivery Forum  
(STDF) 11th September



# Lifecycle: personal resource

**Created\***: pending initialization

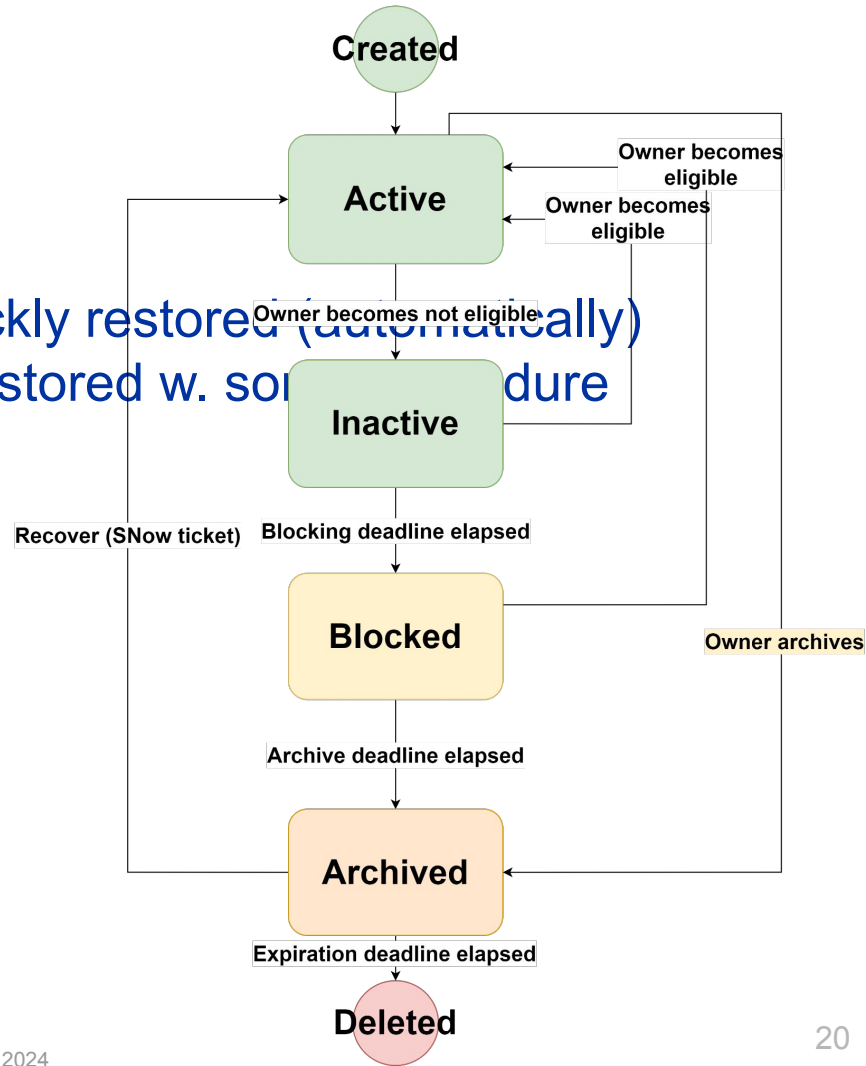
**Active, Inactive**: fully functional

**Blocked**: cannot be accessed; can be quickly restored (automatically)

**Archived\***: cannot be accessed; can be restored w. some procedure

**Deleted**: unrecoverable

\* = if the service needs or supports it



*IT Strategic Technical Delivery Forum (STDF) 11th September*

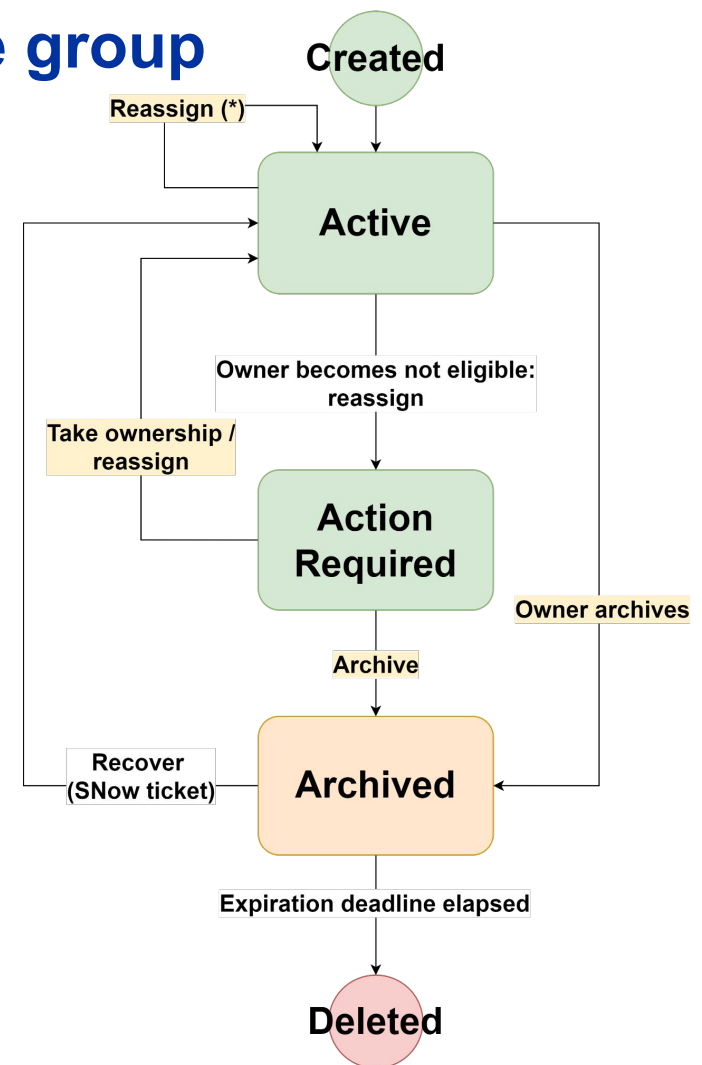


# Lifecycle: official resource / resource group

**Action Required:** fully functional

Owner becomes not eligible: reassign

- Resource => supervisor
- Resource group => Org Unit owner



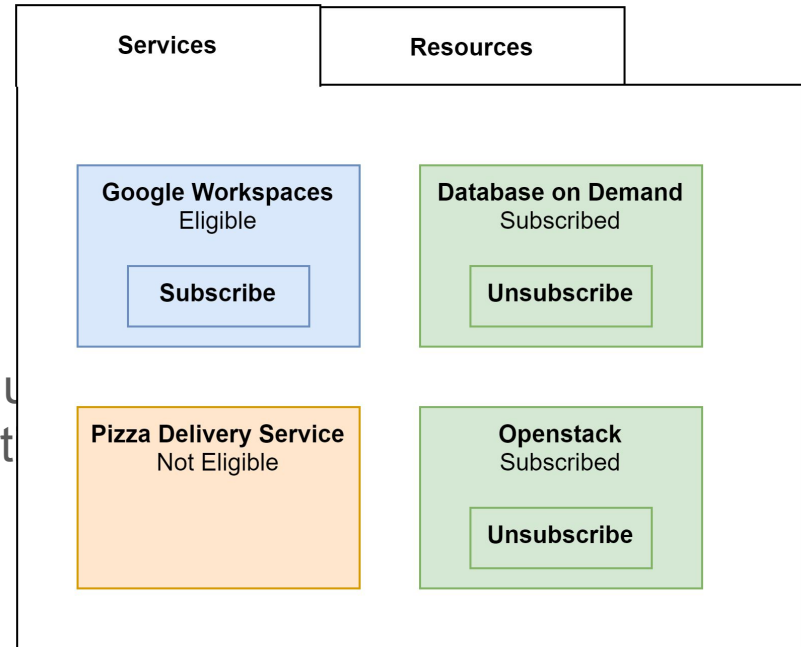
*IT Strategic Technical Delivery Forum  
(STDF) 11th September*



# Resources portal: Services view

IT Strategic Technical Delivery Forum  
(STDF) 11th September

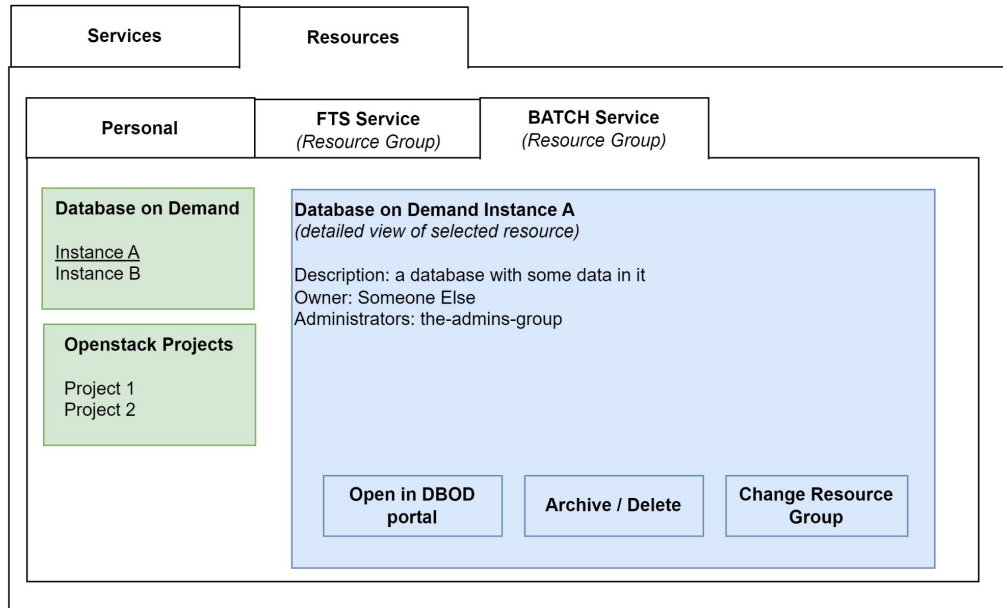
- See which services I can access
  - Eligible = I can subscribe if I want
  - Subscribed = I can use the service
  - Not eligible = I cannot subscribe
- **Subscribe or unsubscribe**
  - If the service allows it
  - If not, instructions on the procedure
- **Subscribed != I own resources**
  - "I'm a DBOD user" means that I can request a service, not necessarily that I own a part of it
  - For that, there is a dedicated view...



# Resources portal: Resources view

IT Strategic Technical Delivery Forum  
(STDF) 11th September

- View and manage the resources I own
  - My website, my secondary accounts...
- Resources belonging to my resource groups
  - I'm FTS and BATCH admin => see FTS and BATCH resources







# Integration - Community edition

IT Strategic Technical Delivery Forum  
(STDF) 11th September

- Roles (sets of groups) determine:
  - Who is eligible, i.e. can subscribe
  - Who is subscribed (optional: self-subscription group)
  - Who is denied access, overriding eligible / subscribed
- Automatic subscription: dynamic group mapped to "subscribed"
- On-demand subscription: static group mapped to "subscribed"
  - Group administrator approval = subscribe with guarantor
- Group membership restrictions can enforce validity of on-demand subscriptions
  - I subscribed to an opt-in group but I'm no longer eligible => the service will enforce the restriction automatically
- Get subscription to your service with a call to the REST API
  - No need to implement subscription logic on your side

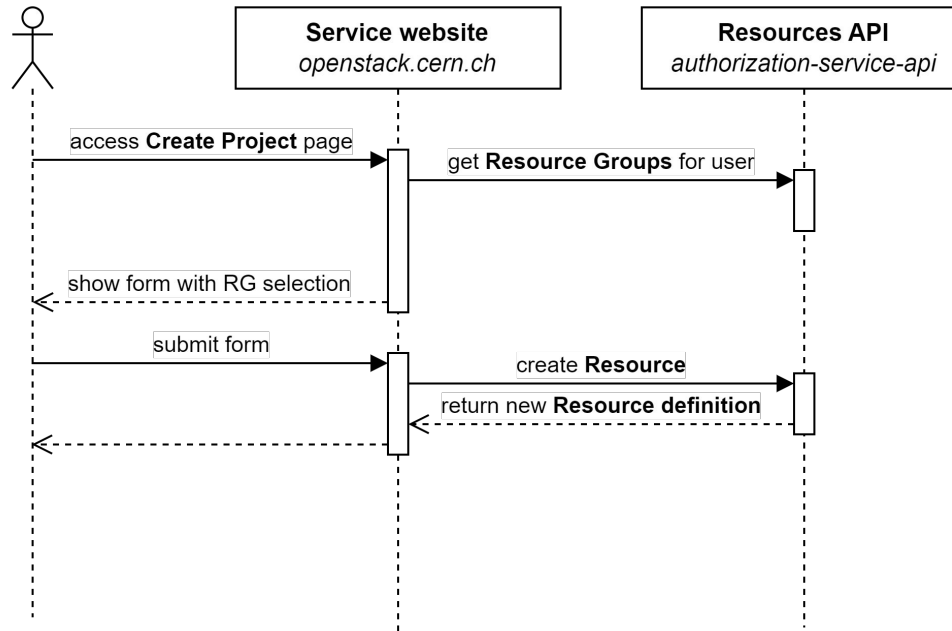
```
[  
  {  
    "identity": {  
      "upn": "slaurel",  
      "personId": 123456  
    },  
    "status": "eligible"  
  },  
  {  
    "identity": {  
      "upn": "ohardy",  
      "personId": 424242  
    },  
    "status": "subscribed"  
  }  
]
```

# Integration - Enterprise edition

IT Strategic Technical Delivery Forum  
(STDF) 11th September

- Resources managed on **your portal**

- All logic and functionality on resources portal would make it unmaintainable



# Integration - Enterprise edition

- Get resources state and ownership with a call to the REST API
- Implement the actual procedures for blocking, unblocking, archiving...
- Ownership and state changes enforced by Resources service
  - No need to implement lifecycle logic on your side

IT Strategic Technical Delivery Forum  
(STDF) 11th September

# The Old Resource Portal must die

- Old and new services running in parallel increase load on Authentication team
- Infrastructure running on old hardware
- Priority on the following services:
  - Services on the old infrastructure
  - Major infrastructure services (storage, compute)
  - Services in the “Controlled Resources” part of the eligibility matrix

IT Strategic Technical Delivery Forum  
(STDF) 11th September

# Services on old infrastructure

IT Strategic Technical Delivery Forum  
(STDF) 11th September

- Migrate service "as is" in a first step if necessary
  - Better integration and RG support can be achieved at later stages
- Enterprise model:
  - Oracle
  - AFS (lifecycle needed for Workspaces)
  - Openstack (integration ongoing)
- Community model:
  - Windows Terminal Server
  - Electronic Design Automation
  - WinCC-OA Scada (Pvss)
- Custom functionality in old portal:
  - Lxplus and Linux
- Informational / links only
  - EOS/CERNBox

# ARB review of Resource Portal

IT Strategic Technical Delivery Forum  
(STDF) 11th September

- ARB review of Resource Portal is ongoing
- Goal is to understand and clarify the interaction with all the services that make use of the RP
- And to introduce the Resource Ownership model
  - ..whereby standard “prod” resources are conceptually owned by a service rather than a person, via a Resource Groups
  - single place to update responsible person / admin group for everything in the RG
  - accounted for, because a Resource Group is owned by an Org Unit
  - compatible with external cloud provider resources



# What we need (would like!)

- Validation of the NRP [API](#) and [model](#) (still conceptual as of now) by the service experts (check if it's good enough)
- High-priority services (EF matrix Controlled Resources + Old Resource Portal critical + big infrastructure services):
  - Evaluate the integration effort needed to integrate the services in the NRP,
    - can the above be done by the POW?
  - Define a plan for the integration
    - For the TD workplan 2025

[IT Strategic Technical Delivery Forum \(STDF\) 11th September](#)

# New Resource Portal 1/3 - new features & improvements

- Implemented eligibility criteria for applications; service managers can
  - Define eligible / subscribed roles for their services
  - Get the list of subscribed users according to the defined criteria
- Users can see both resources they own and they are administrators of
- Easier API calls for integrated services
  - Return all basic relevant information in a single call (owner, administrators)
- Faster recursive group memberships API calls (relevant for eligibility status support)
- Reorganized the internal data structures for services and managed resources
  - Better support for the eligibility framework
- Update to .NET 6
  - minimize technical debt

IT Steering Committee 19 June 2024



# New Resource Portal 2/3 - current work

- Providing a state for resources
  - Following discussions with the Lifecycle Working Group
  - Will require reviewing several internal procedures (lifecycle)
- Completing integration with Openstack.
  - Still missing:
    - Resources state
    - Delegation features currently in old Resources portal (to be migrated to Openstack)
  - Estimate: end of 2024
- ARB review of resources and lifecycle
  - Questionnaire
- Reviewing the Service Desk portal
  - Improve users' support
  - Improve the Service Desk tools to manage the most common support tickets
  - Free up time for the team to work on other features

# New Resource Portal 3/3 - future developments

IT Steering Committee 19 June 2024

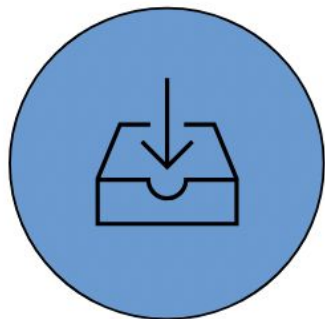
- Google Workspace integration
- Tenant-based resource ownership
  - Several open points in ARB recommendation
- Once the resources in the “old” portal have been migrated to the NRP:
  - Account management migration: accounts created and deleted by the new system, new portal for users and ServiceDesk migration to the new one.
  - Need migration from Microsoft Forefront Identity Manager (FIM, support stopped in 2016) to Microsoft Identity Manager (MIM)
- ID for life:
  - Related to the Account management migration.

# More (old) material - IT Steering Committee (Feb 2023)

## Eligibility Framework: IT Steering Committee in Feb 2023



Work in Progress



---

Computing accounts will be activated automatically and the resource portal will manage access to a set of high priority-controlled resources with corresponding consumption figures made available

---

# Eligibility Framework matrix

Eligible	Limited = limited access controlled by egroups, or for a limited time period															
Not Eligible																
Eligible with Guarantor approval																
Category	MPEs & MPAs		Remote Participants			Contractors & Externals					Retirees	Other				
	MPEs + Trainees: (STAF, FELL, GRADS + Temp, Labour + EXTN RETC, MPAT: ADMI, APPR, DOCT, SUMM, TECH, TRNE)	Collaborators + Exchange Scientists (MPA: COAS, EXAS, PIAS, USER + MPA: CASS, GPRO, SASS, VISI)	EXTN PART, RETP	EXTN DIST	Future MPs (UOPR, FTMP)	Employees of CERN Contractors (computer users)	Employees of CERN Contractors (non-computer users)	EXTN Group A (GUID, ILOF, STAG, PROJ, EUPR, SCIE, COMT)	EXTN Group B (CONF, FORM, GACR)	EXTN Group C (ACCO, HOST, KIND, VISI, CLUB)	Retiree	Ex-Member of Personnel (Grace Period 2 months)	Alumni	Ex-Member of Personnel (non-contractors)	Ex-Member of Personnel (Externals + contractors)	Visitors
Responsible body (who approves rules of eligibility)	HR / IPT	HR / EP	EP	GTPA	HR/ Users Office	IPT Dept.	IPT Dept.	GTPA	GTPA, HR-LD (FORM), PF (GACR)	GTPA, HR-SA (KIND, CLUB), IPT (VISI)	PF	HR	IR	HR	GTPA + IPT	IR
Guarantor (who approves requests) + Licence Manager	Supervisor	Supervisor / Team Leader	Team Leader	CERN Guarantor	Future Supervisor	Technical Officer *	Technical Officer *	CERN Guarantor / Supervisor	CERN Guarantor	N/A	N/A	N/A	IR	N/A	N/A	N/A
Population size JAN 2023	3233	12913	7168	577	141	ca. 300	ca. 4270	697	61	606	ca. 3800		ca. 8000			
Basic resources																
Register device(s) on CERN network / connect to CERN wifi	Green		Visitors	Visitors	Visitors	Green					Visitors	Visitors	Visitors	Visitors	Visitors	
Bulletin	Green															
Mattermost, Discourse	Green															
Security Services: firewall (PAN), mail quarantine (xorlabs)	Green															
Tax certificates, attestations, salary slips	Green		If was MP	If was MP	If was MP	If was MP	If was MP	If was MP	If was MP	If was MP	Limited	If was MP	If was MP	If was MP	N/A	N/A
Be part of eGroups	Green															
Indico content (behind SSO)	Green															
Webcasts (behind SSO)	Green															
Login to/Read Twiki, Drupal, Wordpress, CodiMD	Green															
CERN websites (Alumni, ILOs, Pension Fund, CHIS...)	Green															
CDS content (behind SSO)	Green															
Mandatory online safety / security training courses	Green															
Official notifications + News	Green															
Phonebook	Green															
Personal home directory quota (CERNbox, Office A1 M365)	Green															
Central Compute Services (AFS, EOS, LXPLUS, LXBATCH)	Green															
CERNPhone	Green															
Create egroups	Green		?	?	?	?	?	?	?	?	Limited	?	?	?	?	?
EDH	Green		?	?	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited
ESET Security software (CERN managed devices)	Green															
ESET Security software (BOYD)	Green															
Other Learning courses	Green		Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Limited
Controlled resources	In Portal?															
Computing account / way to authenticate	N	Green														
Service Now (be a supporter)	N	Green														
Create Twiki, Drupal, Wordpress, CodiMD	Y	Green														
Grid certificates	Y	Green														
Java JDK JRE	Y	Green														
Google Workspace	Y	Green														
Overleaf, Gitlab, Atlassian, Zoom	Y	Green														
Digital Library (ebooks + Journals + ILS Library Catalogue)	Y	Green														
Microsoft (Windows + Office A5 M365)	Y	Green														
CAD/CAM & Engineering software	Y	Green														
Create redirections (mail)	Y	Green														
CERN redirection alias as connection string	N	Green														
Mailbox + CERN email	Y	Green														
Access to CERN resources portal?	Y	Green														