

IFS Permissions Webinar

Webinar 10: Governance and Organizational Setup of Roles & Permissions

29 October 2026

Dr. Martin Brogli
Jafar Sabadia

Dr. Martin Brogli

CEO & Founder

Personal

Year of birth:	1965
Nationality:	Swiss/USA
Residence:	Hauptwil, Switzerland
Marital status:	Married, 5 children

Academic title

Dr. oec. HSG

Languages

German	mother tongue
English	mother tongue
French	business fluent

Expertise

Industries: machinery, engineering, building, pharma, chemicals and cosmetics

Services: Application strategies, implementation and change management

Education

University of St. Gallen, focus on business information management

Doctorate at the University of St. Gallen

Career

2 years Foundation for Information Management

7 years Helbling Management Consulting

2 years BSG Management Consulting

Founded 2BCS AG in October 2006



Jafar Sabadia

Senior Consultant



Personal

Year of birth:	1992
Nationality:	Swiss
Residence:	Cham, Switzerland
Marital status:	Married, 1 child

Academic title

M.A. Business Innovation HSG

Languages

German	mother tongue
English	mother tongue
Arabic	mother tongue
French	fluent

Expertise

Permissions management
Test management
ERP evaluations and implementation
IT-business-process optimization

Education

University of St. Gallen, Master in Business Innovation

Career

IT consulting at 2BCS since 2017
Work experience at misc. internet startups
1-year work experience in IT support

CERTIFIED
Project Manager
Business Software
CERTIFIED

2BCS and Purple Services

2BCS AG

- Consulting Company
- Focus on neutral ERP and evaluations and implementation support for SAP, Infor, IFS and D365
- 14 employees
- Cooperation with Trovarit, our common evaluation platform
- Founded in 2006
- In the Roles & Permissions area:
  - Concepts, audits, best practice, and hands-on support

Purple Services GmbH

- Software Company
- Focus on designing, selling, and supporting the IFS Permissions Manager Tool
- 2 part-time employees from 2BCS
- Cooperation with Trivo, a software company in Sri Lanka
- Founded in 2022
- In the Roles & Permissions area:
  - Subscription of IFS Permissions Manager and Onboarding
  - Conversion Services

Our Services in the IFS Roles & Permissions (R&P) Area

	Audit of R&P set-up	R&P Concept & Training & Templates	R&P Conversion 10 → Cloud	IFS Permissions Manager
Contents	Audit and recommendations to optimize your R&P concept, processes and set-up in IFS	Creation of an R&P concept and training based on client's situation and expectations	Semi-automatic conversion of R&P from IFS 10 to IFS Cloud incl. checks and corrections	The IFS Permissions Manager Tool including hosting and onboarding
Benefit	Best practice and proven improvement proposals	Efficient and correct start for your R&P concept, training and templates	Minimal effort and time needed to transform existing R&P into IFS Cloud R&P	The most effective way of managing IFS R&P incl. Reporting

What is the IFS Permissions Manager

The IPM is the most advanced Roles & Permissions tool which supports customers in their day-to-day access management activities, in reporting, and in transitioning to IFS Cloud

Technical background

- The IPM is a web-based tool that connects to a customer's IFS environment
- The tool is a front-end that presents and enables changes to the roles & permissions in IFS
- The IPM does not have its own data

Benefits

- Efficiency gains of 45% for routine tasks
- Acceleration of the initial set-up and testing due to templates
- Predefined reports for internal & external auditors
- Major reduction of effort when converting from IFS Apps 10 to IFS Cloud

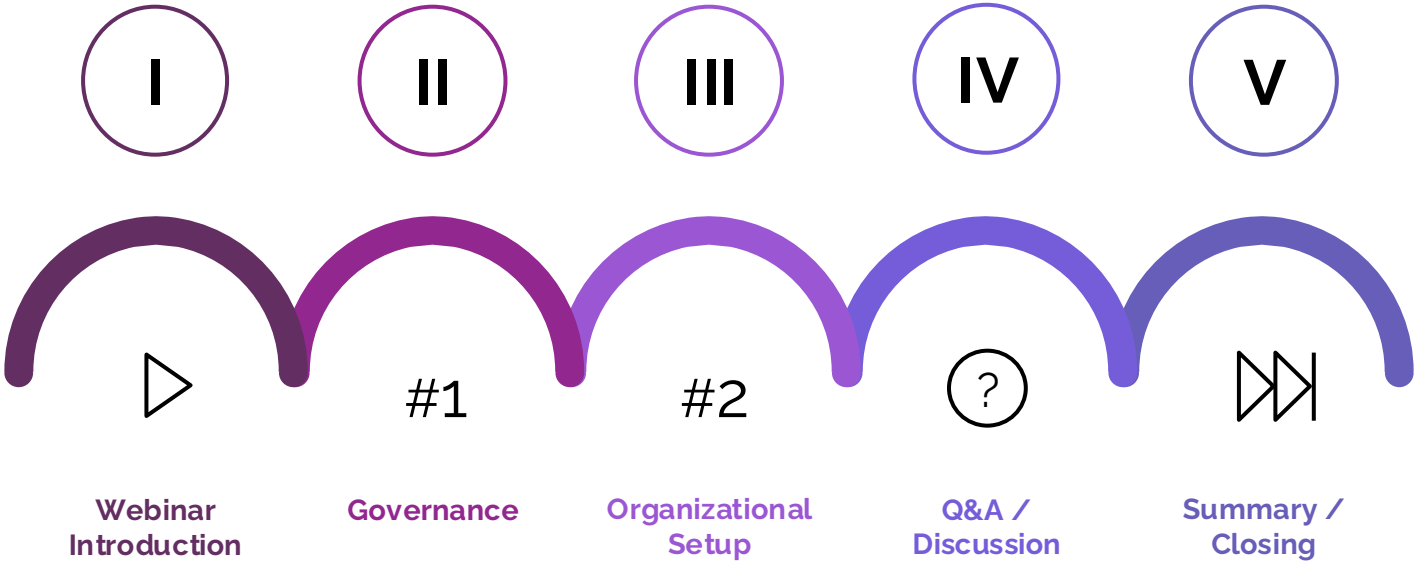
Use Cases

- Simplifies the day-to-day management of a company's IFS users, roles and permissions incl. reporting on access management
- Has best practice templates which ease the initial set-up of roles and permissions
- Can convert IFS Apps 10 to IFS Cloud roles and permissions

Services associated with IPM

- Technical set-up connecting tool to IFS
- Business training on method and best practice
- Hands-on support optimizing customers set-up
- Audit services
- Technical services completing the conversion
- Bi-monthly webinars and knowledge center

Agenda


I
II
III
IV
V
#1
#2
?
Webinar Introduction
Governance
Organizational Setup
Q&A / Discussion
Summary / Closing

Webinar Introduction

1

ONGOING WEBINAR SERIES

Centered around the topic of Roles and Permissions in IFS

2

CHALLENGING TOPIC

In our experience this is a topic that is difficult to execute in IFS and almost every customer is affected by it

3

OUR GOAL

Our goal is to share knowledge, build up a community and help people get in touch with each other

4

WEBINAR FORMAT

- Two topics presented by 2BCS / Purple Services
- Series now in its second year
- Q&A and discussion at the end

5

QUESTION MANAGEMENT

Submit questions anytime via the Q&A feature in Teams, we will address them during the Q&A section at the end

6

RECORDINGS

The webinar will be recorded and will be shared on the webinar website

Governance of Roles & Permissions

Topic 1

#	Topic
1	What the Standards Expect
2	Roles and Owners
3	Where IFS Makes It Harder
4	Running It in IFS



Access by Role, Least Privilege

The access each job needs is defined and documented, nothing more is granted (CIS Controls 6.8, NIST AC-6)



The Owner Approves, Someone Else Grants

Approval and implementation are separate, every grant is recorded (ISO/IEC 27002 5.18, NIST AC-2)



Access Follows the Person

Adjusted on a job change, removed on exit, temporary access expires (ISO/IEC 27002 5.18, NIST AC-2)



Reviewed Regularly

At least once a year, including separation of duties (CIS Controls 6.8, NIST AC-5, AC-6(7))

Sources: ISO/IEC 27001 and 27002:2022, NIST SP 800-53 Rev. 5, CIS Controls v8

1) Why It Breaks Down in Practice

The business knows what each job needs, IT knows how to grant it, and nobody connects the two

Copying a Colleague

Access is requested as "same as X", which copies everything X has accumulated over the years. A common route to privilege creep.

Nobody Can Explain a Grant

No owner and no documented purpose, so nobody dares to remove anything.

Movers Keep Old Access

The new role is added and the old one stays. Access grows with every job change.

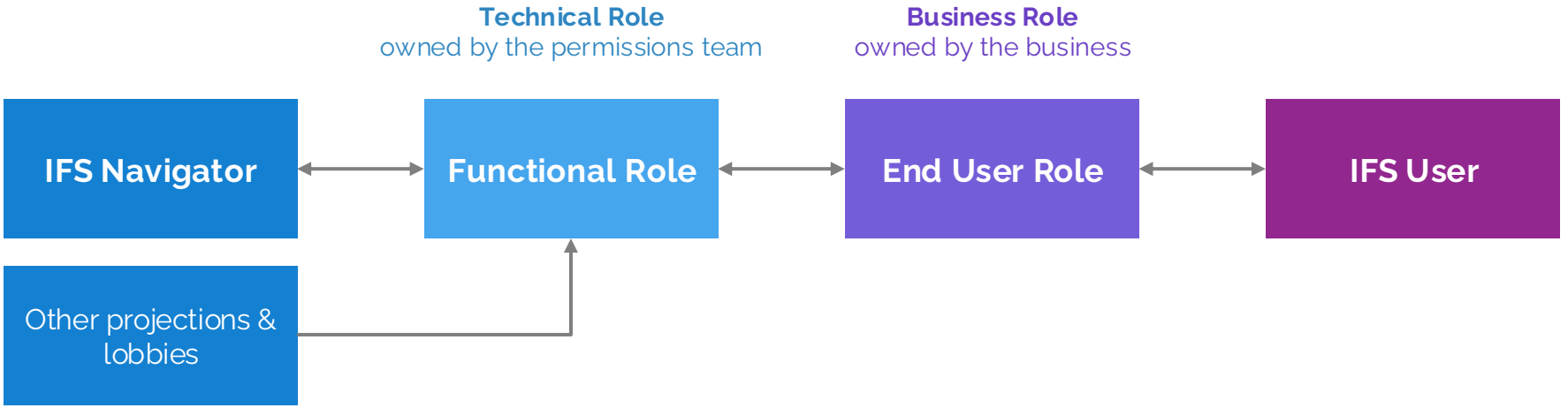
Signing Without Understanding

In IFS, approvers and reviewers are shown projections they cannot read, so they sign what they cannot assess.

Sources: ISACA Journal 2019, "Effective User Access Reviews" (movers keep access); tenfold, "Reference Users & Templates" (copying users)

2) Business Roles and Technical Roles

Identity governance tools separate business roles (what a job needs) from technical roles (bundles of system permissions). IFS has the same two layers.



Functional roles are the technical roles: building blocks around navigator areas, reused across jobs, maintained by the permissions team

End user roles are the business roles: one per job, owned and signed off by the business, reviewed by line managers

Sources: OpenText Identity Governance documentation (business roles); IFS Permission Set Overview (functional and end user roles). The owner per layer is our recommendation.

2) Who Does What

Activity	Role Owner (Business)	Line Manager	Permissions Team	Key User	Internal Audit
Define end user roles	A	C	R	C	I
Build functional roles			A/R	C	
Test and accept roles	A		C	R	
Request and approve access	R*	A/R	I	C	
Grant access in IFS		I	A/R		
Review who holds which role	C	A/R	C		I
Review what a role contains	A/R		C	C	I
Change or retire a role	A	I	R	C	I

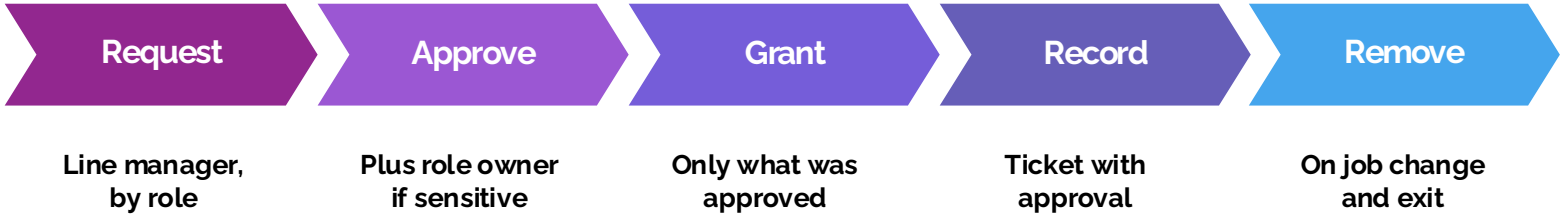
R = responsible, A = accountable, C = consulted, I = informed. * For sensitive roles. Separating approval from granting follows ISO/IEC 27002 5.18, business accountability for reviews follows ISACA (2019). The rest is our recommendation.

3) What the Standards Expect, and What IFS Gives You

The Standards Expect	IFS Cloud Gives You	What To Do
An owner approves each role	No owner field	Owner in the naming convention and Description, plus a register
Approval separate from granting	No request and approval process	Ticket tool. Grant only what was approved
Access follows job changes and exits	Grants never change on their own	One request removes and adds. End-date leavers
Temporary access expires	End date on the user only	Deputy roles, or a register with removal dates
Changes to roles are controlled	A change hits every holder at once	Impact check and role owner approval first
Only what the job needs	Granted per projection, unreadable for the business	Decide and review at navigator level
Review at least once a year	Reports, but no review campaigns	Run the yearly review outside IFS

Sources: ISO/IEC 27002:2022 5.18 (rows 1 to 3) and 8.32 (row 5); NIST SP 800-53 AC-2(2) (row 4) and AC-6 (row 6); CIS Controls v8 6.8 (row 7)

The same five steps for joiners, movers and leavers



1. **Request an end user role.** Never "same as colleague X"
2. **Approve twice where it matters.** The line manager confirms the need, the role owner confirms sensitive roles
3. **Grant exactly what was approved.** The permissions team never approves its own grants
4. **Keep the trail.** Every grant traces back to a request and its approval
5. **Remove in the same step.** A job change removes the old role in the same request. Leavers: end-date the user

Sources: ISO/IEC 27002 5.18 (authorization, separation of approval and implementation, records); NIST SP 800-53 AC-2 (approvals, transfers, terminations)

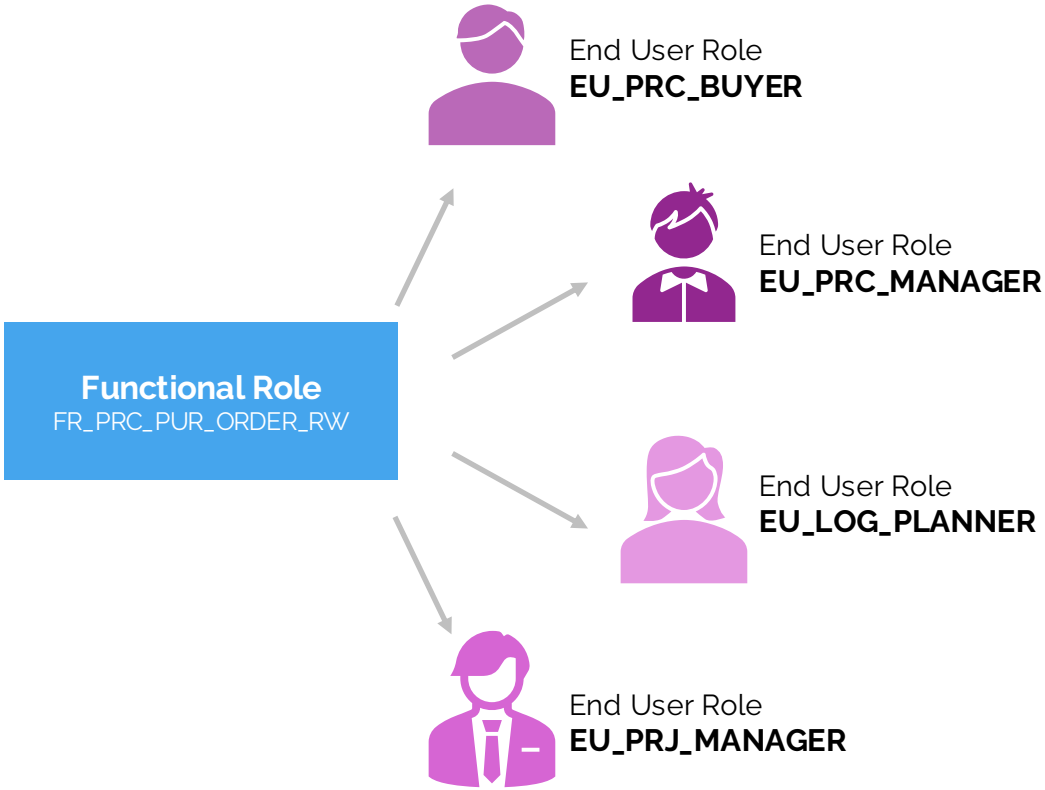
4) Temporary and Deputy Access

The standard: temporary access expires automatically (NIST SP 800-53 AC-2(2))

What IFS Supports	Temporary People	Temporary Rights	Yearly Review
An end date on the user account. No end date on a permission set grant, so a temporary grant stays until someone removes it.	Contractors and consultants: set the user's end date when the account is created.	Absence cover for existing users: a permanent, narrow deputy role, or a register with a removal date and a named person who removes the grant.	Temporary grants are checked again in the yearly review, together with everything else.

Every temporary grant needs a removal date: on the user account in IFS, or in a register for permission sets

4) Changing a Role: Check the Impact First



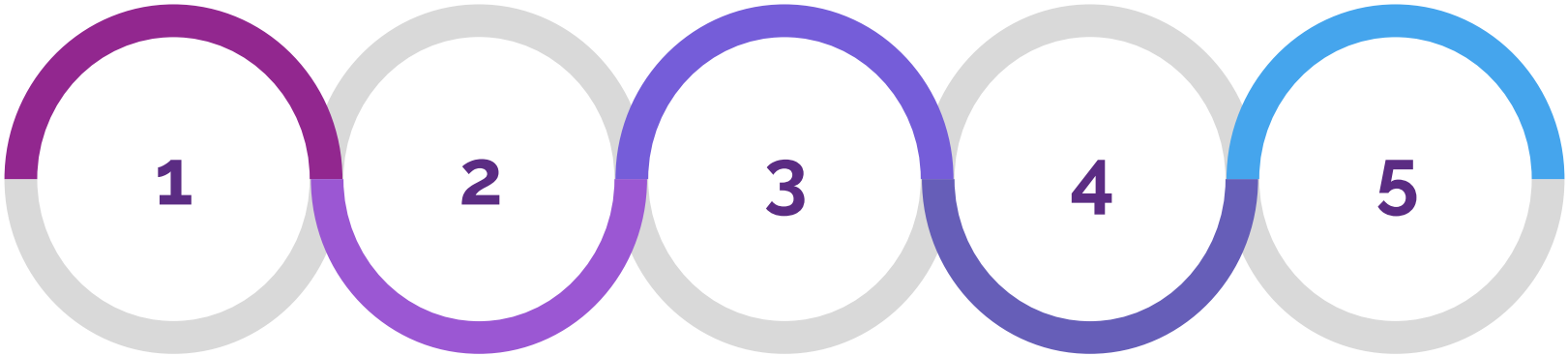
- A change to a functional role applies immediately to every end user role that contains it, and to every user holding one
- In a live environment with 400 functional roles, each one sits in two end user roles on average
- Before the change: list the affected roles and users, get each role owner's approval, build and test in CFG first

Rule for new projections: they go to the functional role that covers their navigator entry. The permissions team places the rest

Reuse measured in a live IFS Cloud environment with 400 functional roles and 60 end user roles. Role names are examples.

4) Reviewing Access Once a Year

At least once a year, and more often for sensitive roles (CIS Controls v8, 6.8)



Extract
Grant reports: who holds which role

Users
Line managers confirm their users' roles

Content
Role owners confirm role content at navigator level

Conflicts
SoD check with functional areas and conflicts

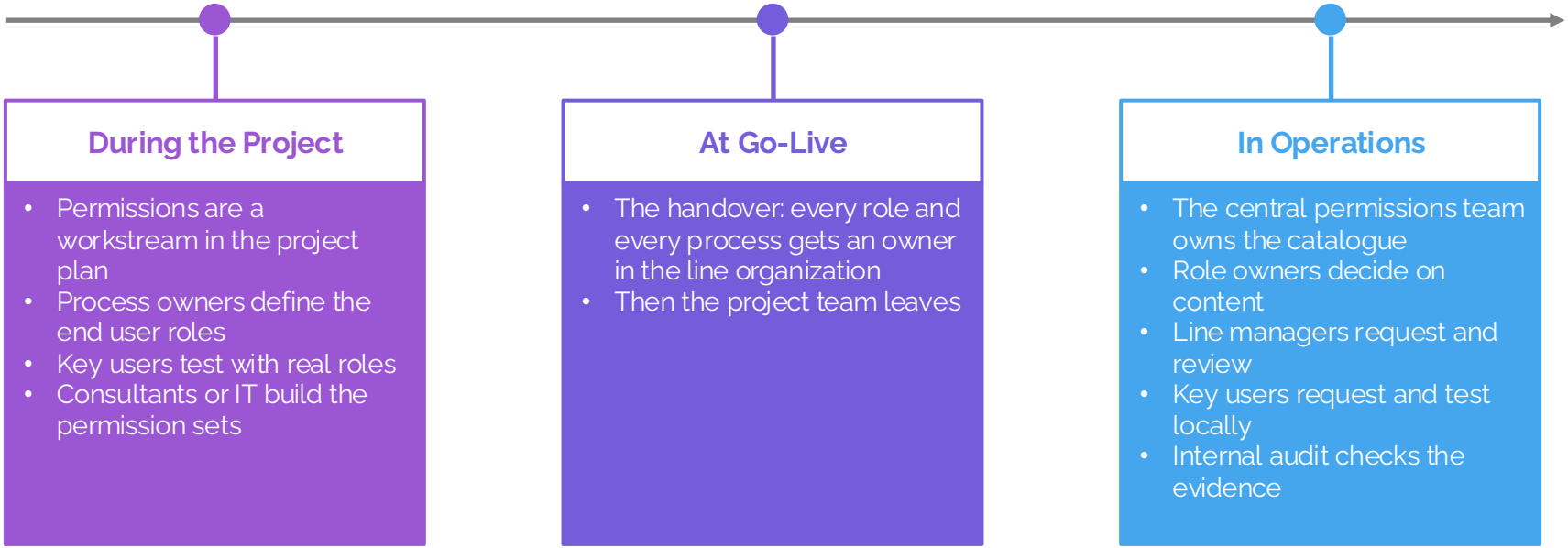
Remove and Record
Remove the rest, keep the signed results

Reviewers can only confirm what they can read: roles named after jobs, content at navigator level

Organizational Setup

Topic 2

Project Organization vs Line Organization



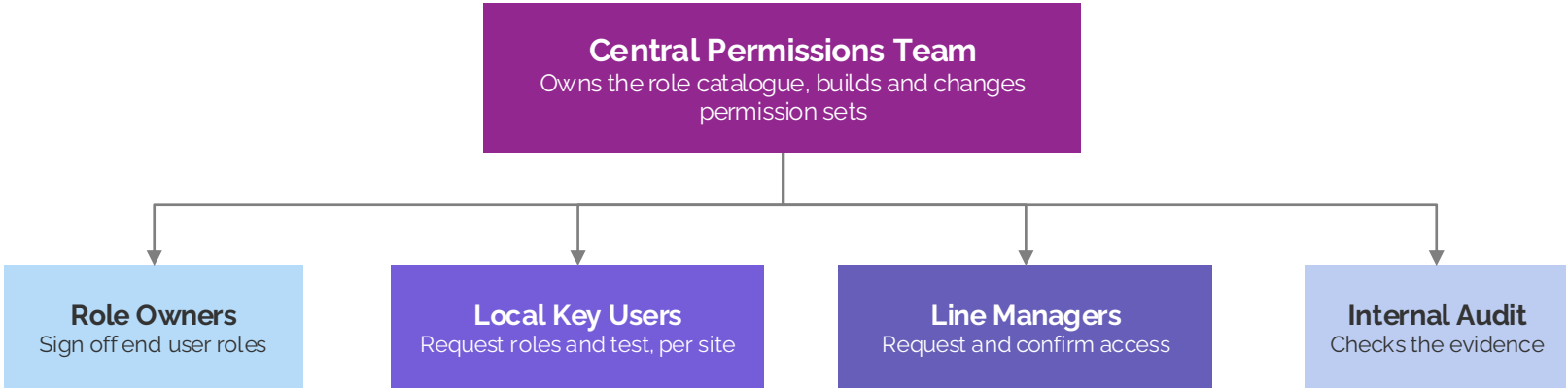
This session is about operations: who owns permissions after go-live

The Go-Live Handover: What Must Exist on Day One

Plan these as project deliverables, not as tasks for after go-live

- **An owner for every end user role,** recorded in a role register with purpose and approval date
- **The request process live** in the ticket tool, with the approval rules
- **A register for temporary grants,** with removal dates and a named person
- **A rule for new projections** from releases, service updates and deliveries
- **The first access review** in the calendar
- **A named permissions team,** with a deputy

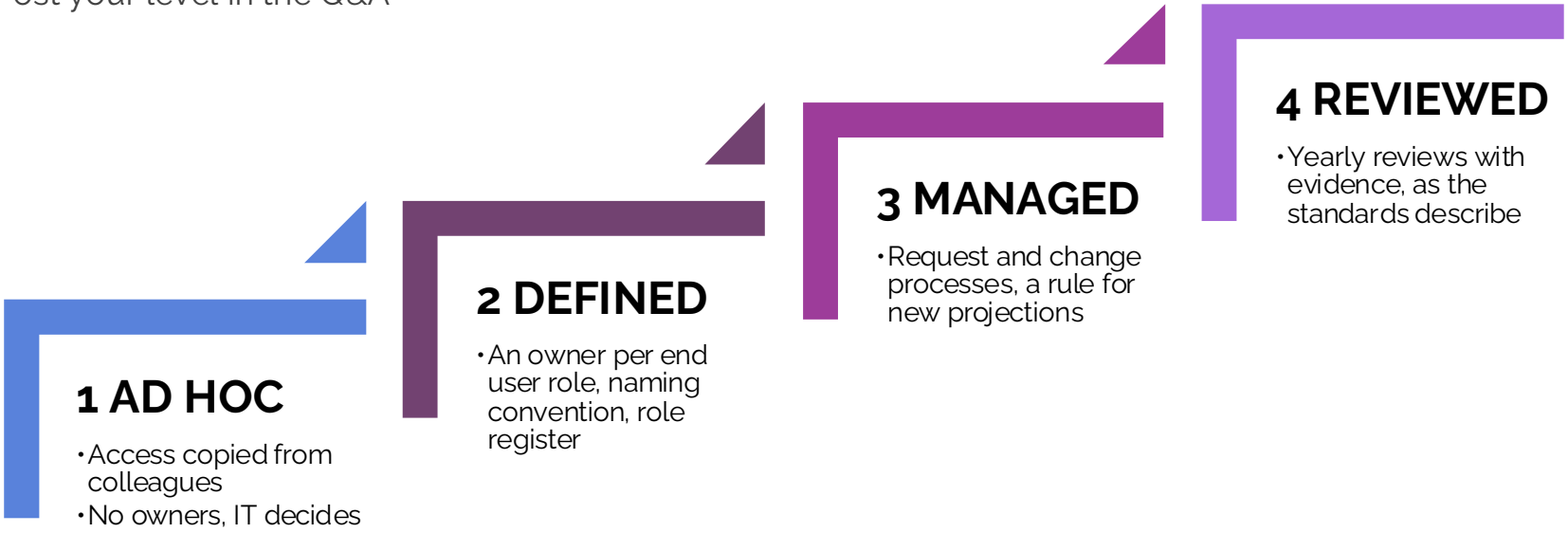
Central Catalogue, Local Key Users



- **One team owns the role catalogue.** Sites request roles, they do not build them
- **Key users are the local first contact.** They know the site's processes and people, request roles and test changes locally
- **Sites approve, the central team grants.** Approval and granting stay separate (ISO/IEC 27002 5.18)

Where are you today?

Post your level in the Q&A



Our model. Level 4 corresponds to the practices in ISO/IEC 27001/27002, NIST SP 800-53 and the CIS Controls.

Summary



The business owns end user roles, IT owns functional roles



Access is requested by role, never by copying a colleague



IFS has no end date on grants, so temporary access needs a register



Review access yearly, at the level the business can read

Q&A / Discussion

Summary / Closing

Summary / Closing

- We looked at what the standards expect from access governance, and where IFS makes it harder
- We covered business and technical roles with two owners, and who does what
- We covered requesting, changing and removing access, temporary access, and the yearly review in IFS
- We separated the project from operations, listed what must exist at go-live, and split central and local work
- The next webinar is on 17 December at the same time: IFS Cloud 26R2 Updates & Reporting with the IFS Permissions Manager
- We are always open for further topic suggestions – let us know!

THANK YOU

Martin Brogli
+41 79 355 85 16
martin.brogli@2bcs.ch

Jafar Sabadia
+41 78 767 53 66
jafar.sabadia@2bcs.ch

2BCS AG
Unterrietstrasse 2a
CH-8152 Glattbrugg
Switzerland

T +41 43 233 79 78
www.2bcs.ch

Purple Services GmbH
Untere Rebrainstrasse 7
CH-9213 Hauptwil
Switzerland

T +41 71 552 52 55
www.purple-services.ch

