ISSeG

EU-FP6 Project 026745

Overview

François Fluckiger

CERN

Integrated
Site
Security for
Grids

cern.ch/isseg

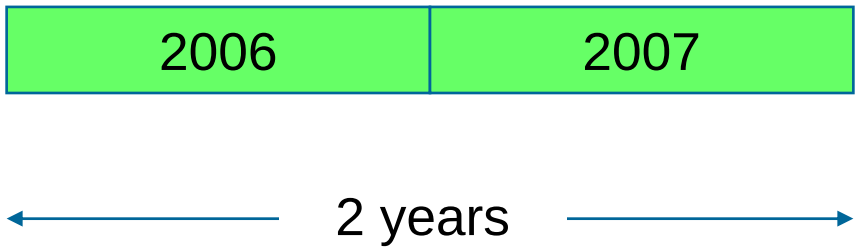
Information Society and Media

ISSeG Facts and Figures

- **Four Partners**
  - CERN (coordinator)
  - CCLRC, UK
  - FZK, Germany
  - CS-SI, France

- **Start: 01/02/06**

- **Two years project**



- **Budget: 1086 K€**

Integrated Site Security for Grids
cern.ch/isseg

Financial Summary: EC Contribution

Partners	EC Contribution	
	Total Activity (Direct + indirect cost)	Management (subcontracted audit)
CERN	**532 000**	**69 000**
CSSI	**180 000**	**2 000** (audit)
FZK	**200 000**	**3 000** (audit)
CLRC	**100 000**	

Integrated Site Security for Grids
cern.ch/isseg

Integrated Site Security for Grids

- **Overall aim**
  - *"Contribute to the consolidation of the European Grid infrastructure in the field of computer security"*
- **Focus**
  - **Site** Security to complement **Grid** security

Integrated Site Security for Grids
cern.ch/isseg

Origin of ISSeG

- **Summer 2004**
  - Initiative from W. von Rüden for an ***openlab*** project on Site Security
- **Fall 2004**
  - Discussion with industrial partners
- **March 2005**
  - Proposal submitted EU-FP6 ("*Specific Support Action*" Instrument)

Integrated Site Security for Grids
cern.ch/isseg

Integrated Site Security for Grids

- **Overall aim**
  - *"Contribute to the consolidation of the European Grid infrastructure in the field of computer security"*
- **Focus**
  - **Site** Security to complement **Grid** security
- **Project Objective:**
  a. **Create** expertise
  b. **Disseminate** expertise
- **Key concept**
  - **Integration** of all security components

Integrated Site Security for Grids
cern.ch/isseg

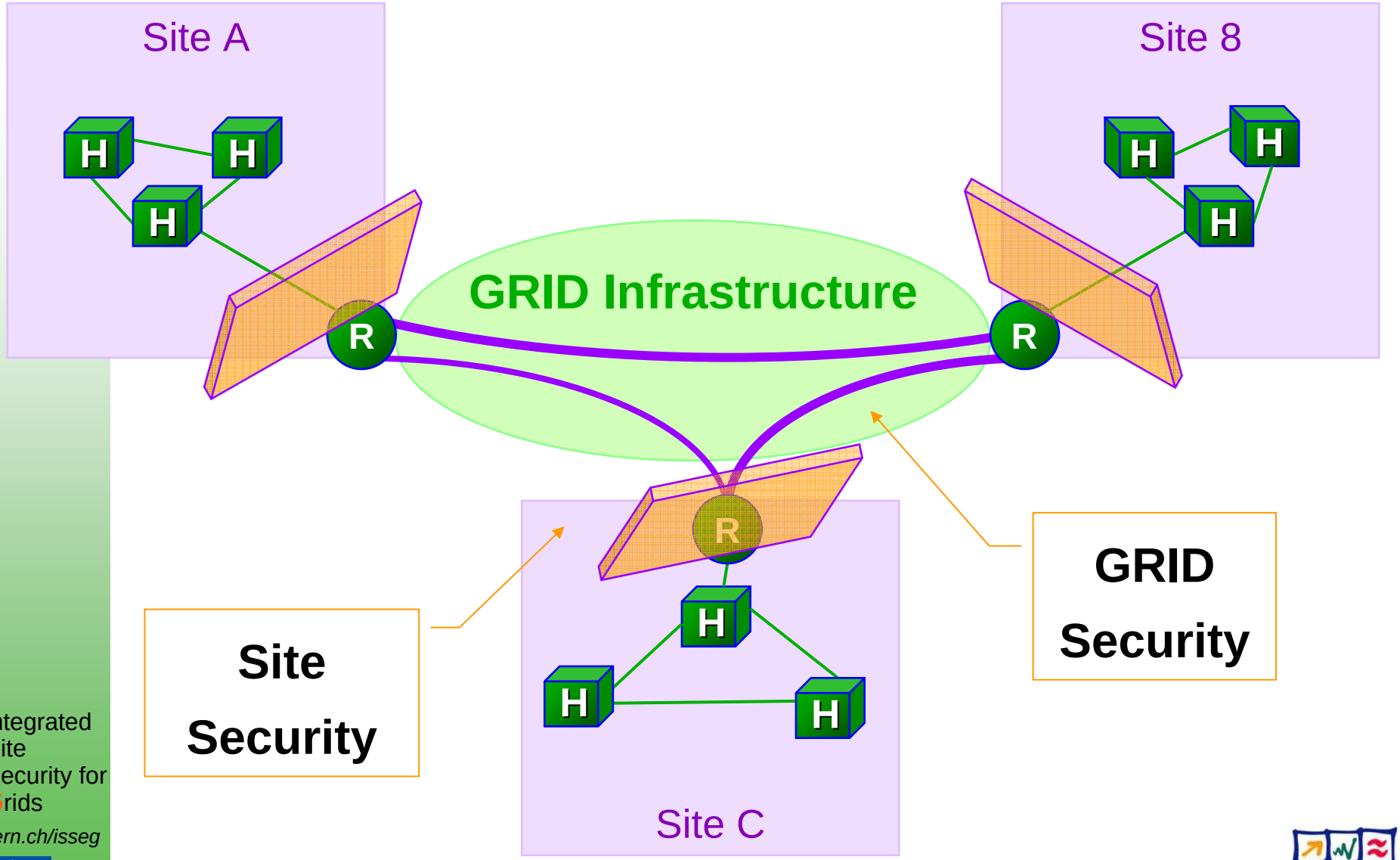
Site vs Grid Security

- **Grid** Security
  - Authentication / Authorization in VOs
  - Traveling Data integrity
  - Specific security incident

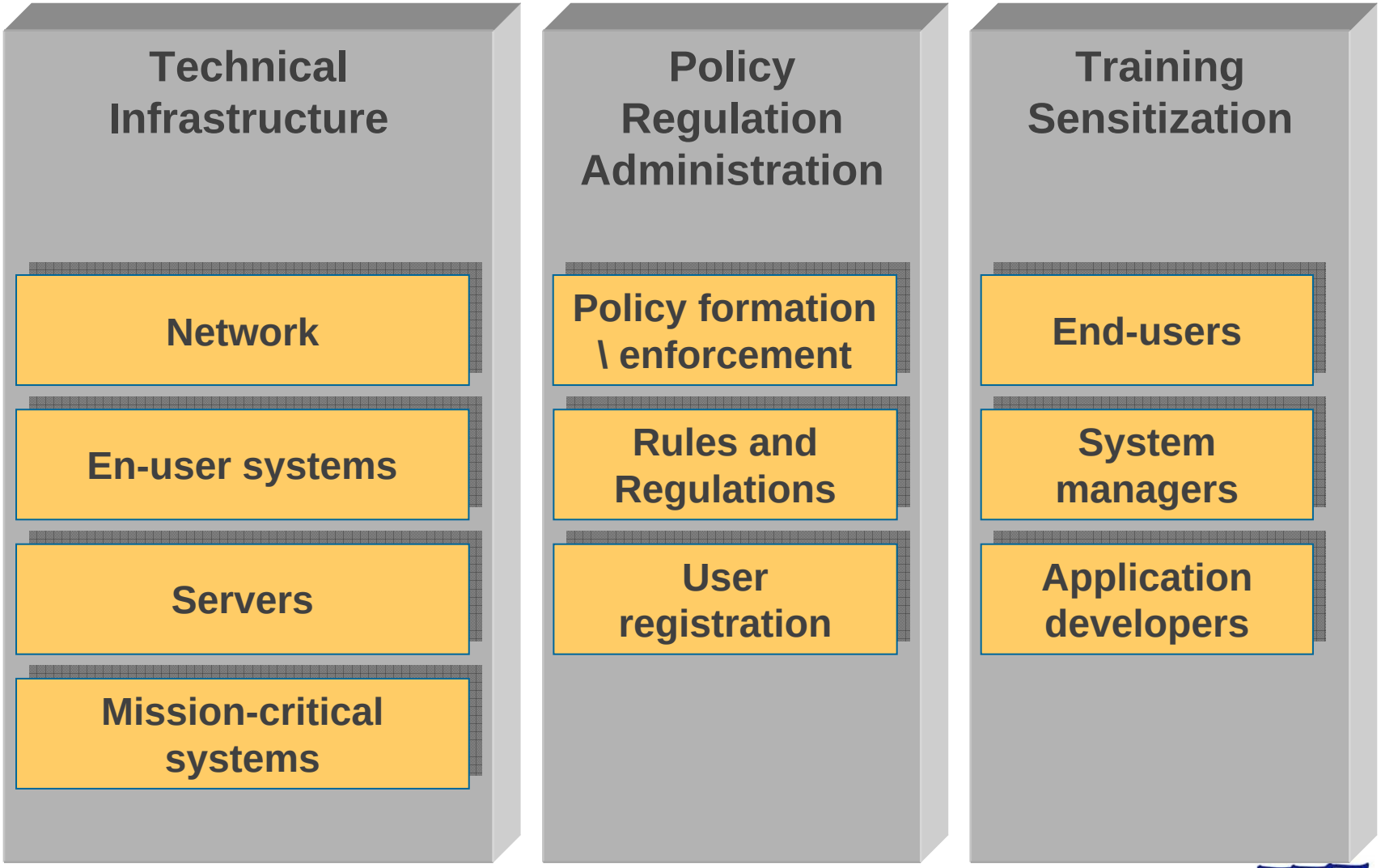
- **Site** Security
  - Technical Security
  - Policy, Regulation, Administration
  - Training and sensitization

Integrated Site Security for Grids
cern.ch/isseg

Site vs Grid Security



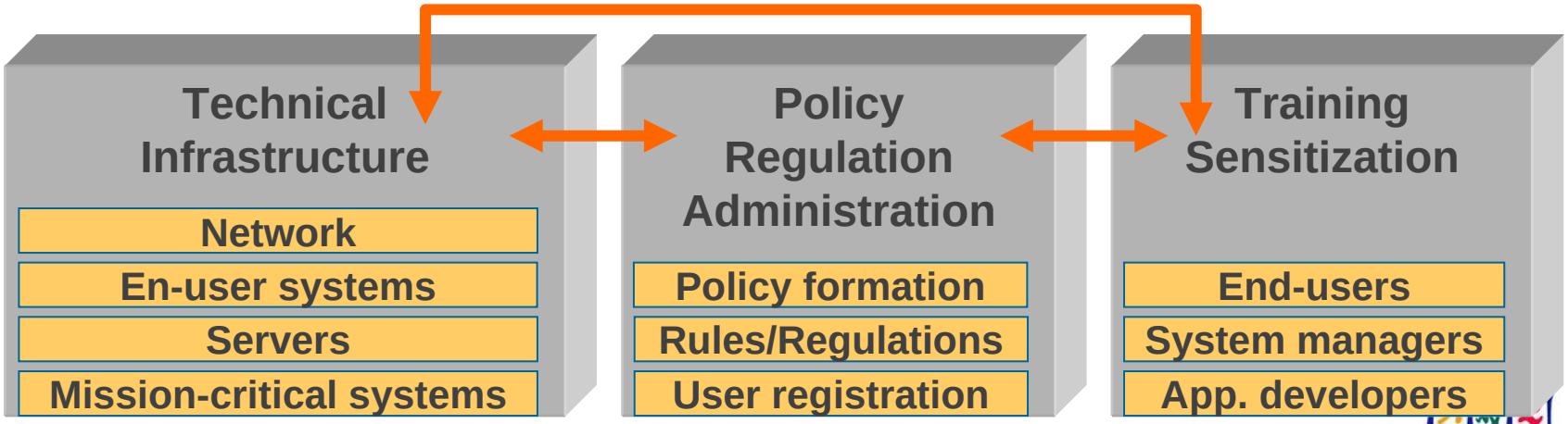
Integration: The Three Dimensions



Integrated Site Security for Grids
cern.ch/isseg

Integrated Approach

- *"Actions or decisions affecting one security component should be checked against other components likely to be affected, which in turn may have to be adapted"*
- *"Good synchronization necessary between changes affecting transversally multiple components"*
- **Examples of poor synchronization include:**
  - New anti-spam or virus detection measures translated with delay into end-user information / training material
  - New security policy published whilst technical components necessary to their enforcement are not yet fully operational



ISSeG Guiding principles

The **four** ISSeG **buzz words**

Site	ISSeG is not about GRID security
Integration	The concept we sold The genuine scientific dimension
Practical	Recommendations not-theoretical, based on practical deployments
Multi-disciplinary	Not only HEP

Integrated Site Security for Grids

cern.ch/isseg

A two stage process

1	**Creation of raw expertise via** ▪ Two-site real **deployment** ▪ Auditing	 ▪ **WP1** ▪ **WP2**

About "**Deployment** at CERN and FZK"

- In practice, improving site security:
  - A continuing process
  - Pre-dated ISSeG
- "Deployment" in more period during which actions are focussed

Integrated Site Security for Grids
cern.ch/isseg

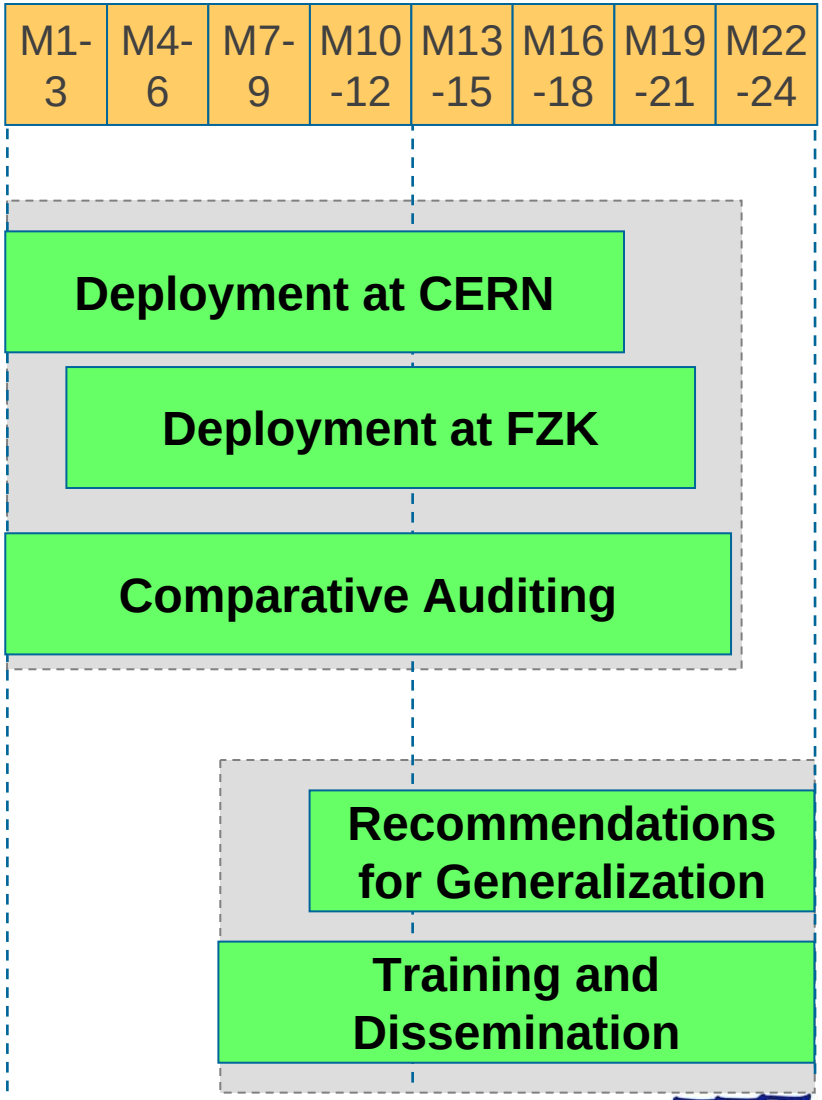
A two stage process

1	**Creation of raw expertise via** ▪ Two-site real deployment ▪ Auditing	 ▪ **WP1** ▪ **WP2**
2	**Translation into** ▪ Applicable recommendations ▪ Training	 ▪ **WP3** ▪ **WP4**

Integrated Site Security for Grids
cern.ch/isseg

ISSeG Methodology

- **Expertise Creation**
  - ISS deployment at CERN
  - ISS adaptation and export at FZK
  - Comparative auditing
- **Expertise Dissemination**
  - Recommendations for ISS generalization
  - Training and disseminations actions



Integrated Site Security for Grids
cern.ch/isseg

WP Lead Contractors

Activity	WP	Work package title	Lead	Start	End
Support	WP1	Deployment of Integrated Site Security at CERN and FZK	**CERN**	M00	M21
	WP2	Comparative auditing and analysis of site security	**CSSI**	M00	M22
	WP3	Recommendations for Integrated Site Security generalization	**FZK**	M09	M24
	WP4	Training and Expertise Dissemination	**CCLRC**	M06	M24
Management	WP5	Project Management	**CERN**	M00	M24

Integrated Site Security for Grids

cern.ch/isseg

Involvement of partners in WPs

- **All partners involved in all Activity WPs**

	CERN	CSSI	FZK	CCLRC	Total Activities
WP1 / Deployment	**98**	12	24	1	135
WP2 / Comparative Auditing	5	**12**	2	2	21
WP3 / Recommendations	3	1	**10**	1	15
WP4 / Training and Dissemination	5	1	3	**11**	20
Total 'specific activities'	111	26	39	15	191

- Effort in person.months, EU-funded and unfunded

Integrated Site Security for Grids
cern.ch/isseg

WP1.1: Deployment at CERN

T1.1.1 Articulation of the CERN ISS strategy

- CERN ISS strategy document (February 2006)

T1.1.2 Production of the implementation plan

- CERN ISS implementation plan document (March 2006)
- Public version (April 2006)

T1.1.3 Deployment and documentation of expertise 1

- Intermediate deployment report (October 2006)
- Public version (November 2006)

T1.1.4 Deployment and documentation of expertise 2

- Final deployment report (June 2007)
- Public version (July 2007)

Integrated Site Security for Grids

cern.ch/isseg

CERN Security Strategy

Defined by 5 Strategic directions:

S1 Centralise management of resources

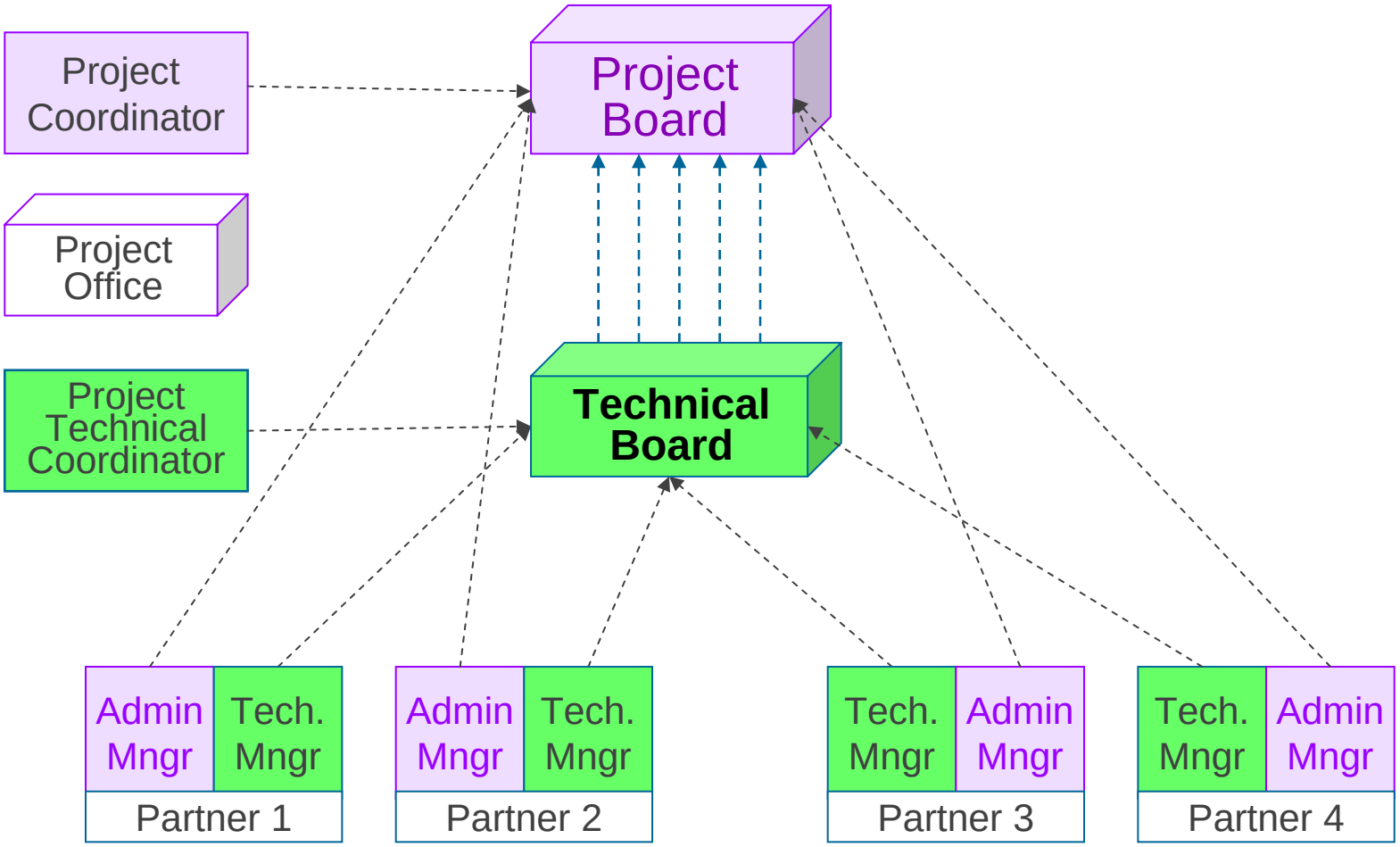
S2 Integrate management of resources via databases

S3 Enhance network connectivity management

S4 Integrate and evolve security mechanisms and tools

S5 Integrate Security Training, Best Practices and Administrative Procedures

Management Structure



Integrated Site Security for Grids
cern.ch/isseg

Information Society and Media

ISSeG Project Board members

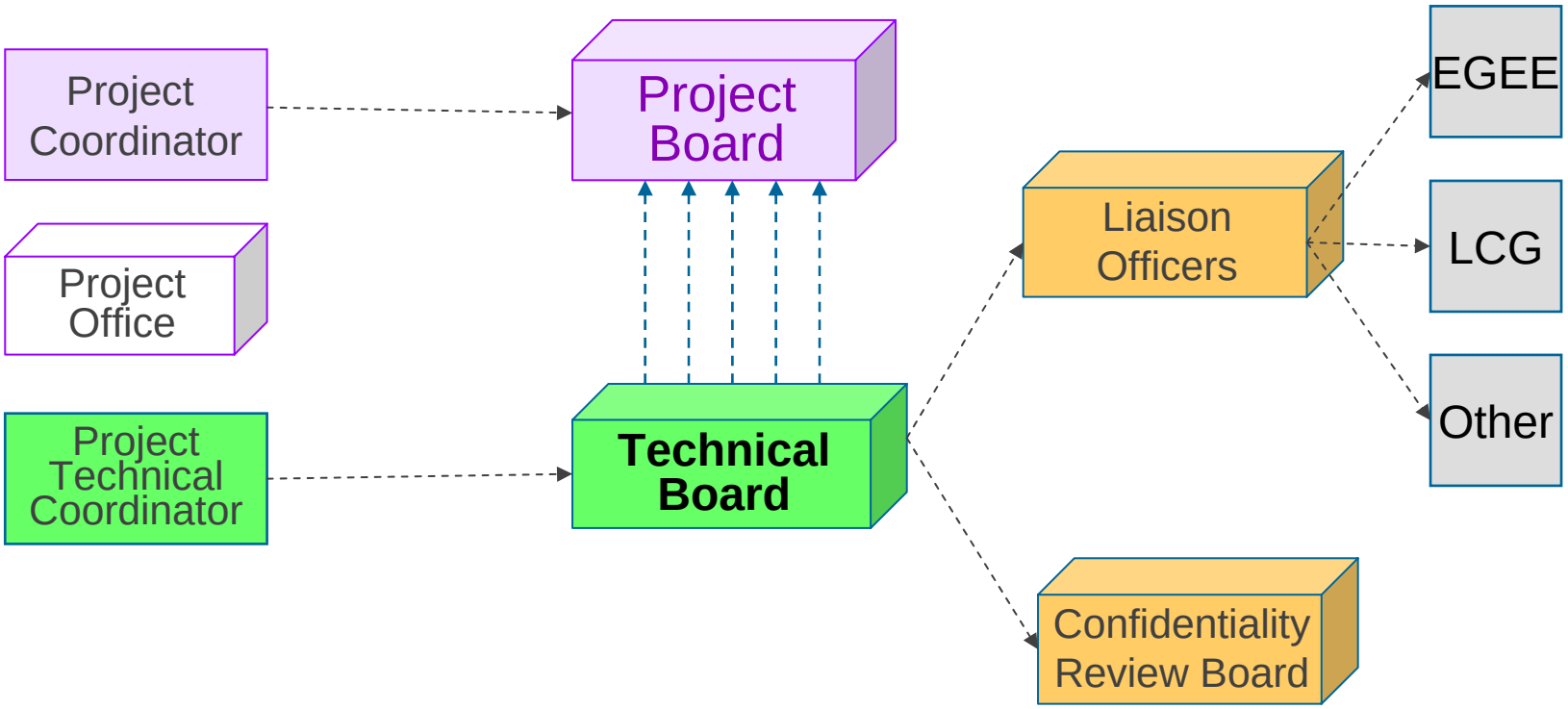
- Initial appointments

Partner representatives	Administrative Manager	Technical Manager
CERN	Frederic Hemmer	Lionel Cons
CS SI	Jean-François Musso	*tbc*
FZK	Ursula Epting	Bruno Hoeft / Ursula Epting
CCLRC	David Jackson	David Jackson

Project representatives	Project Coordinator	Project Technical Coordinator
CERN	Francois Fluckiger	Denise Heagerty

Integrated Site Security for Grids
cern.ch/isseg

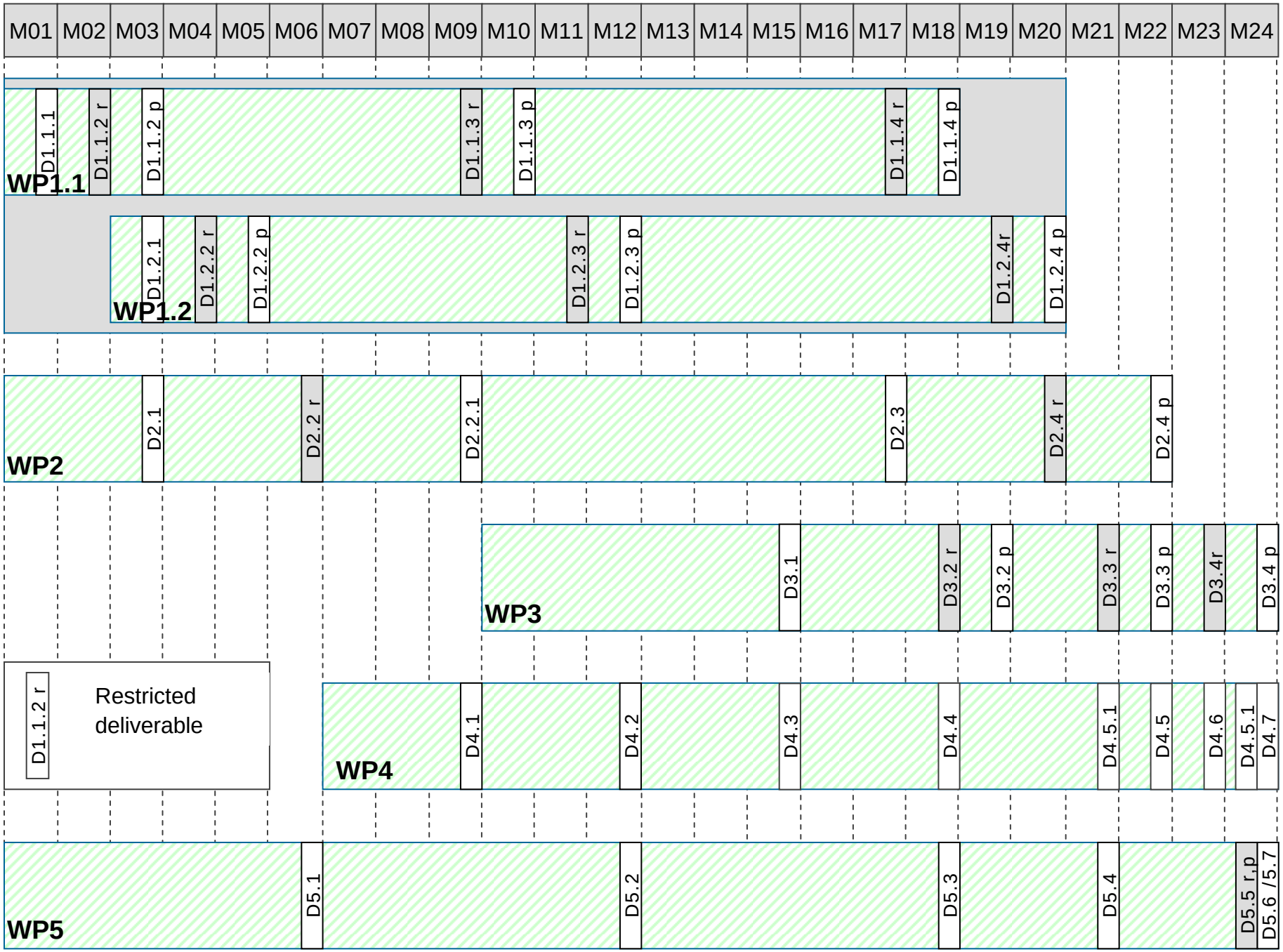
Management Structure

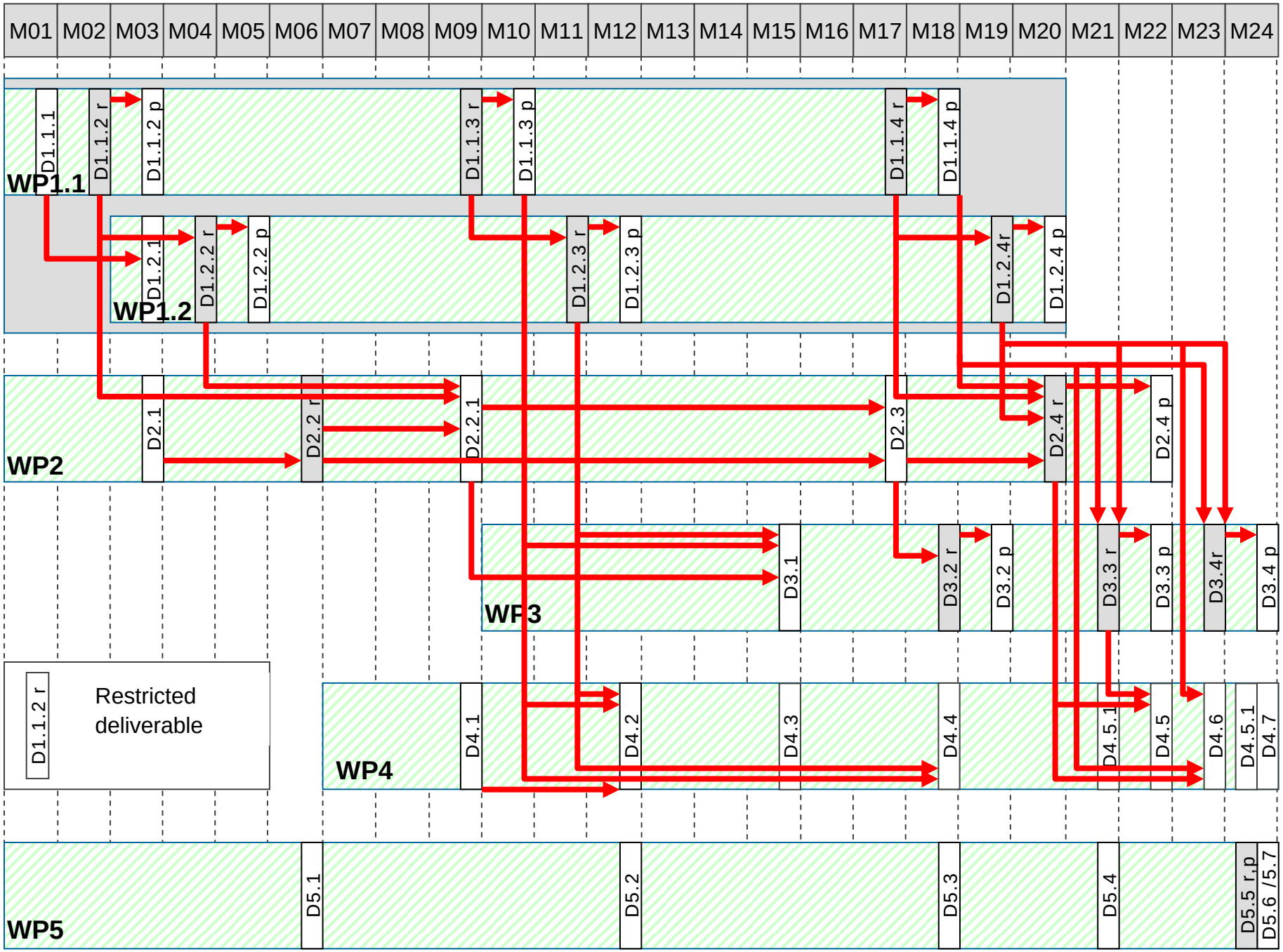


Integrated Site Security for Grids
cern.ch/isseg

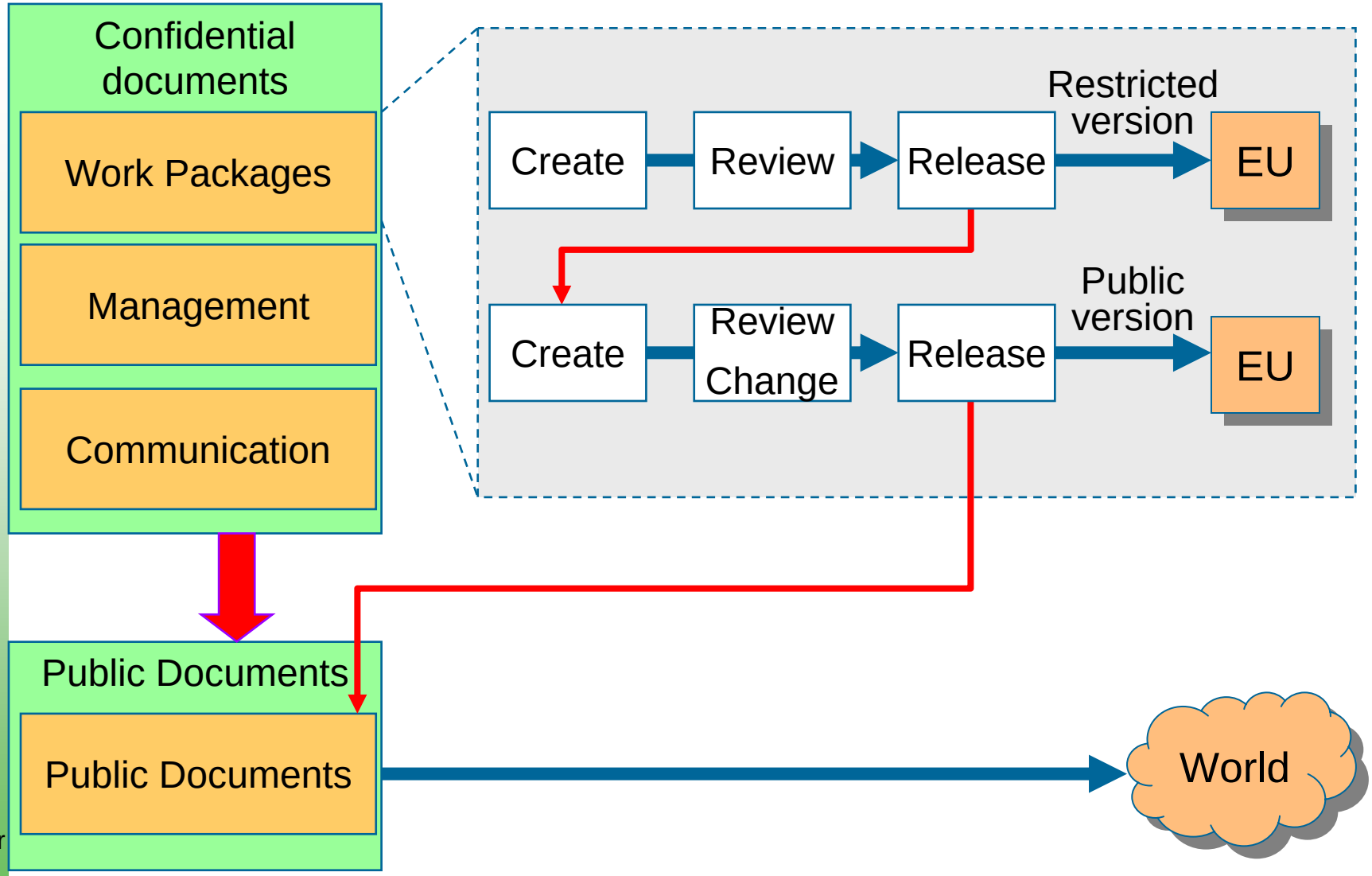
Restricted and Public Deliverables

- Most deliverables will have **two versions**
  - **Restricted**:
    - For EU and their designated reviewers
  - **Public**:
    - Delivered one month after the restricted version (usually, a stripped-down version)
- No public deliverable will be released without the agreement of the Confidentiality Board


M01
M02
M03
M04
M05
M06
M07
M08
M09
M10
M11
M12
M13
M14
M15
M16
M17
M18
M19
M20
M21
M22
M23
M24
WP1.1
D1.1.1
D1.1.2 r
D1.1.2 p
D1.1.3 r
D1.1.3 p
D1.1.4 r
D1.1.4 p
WP1.2
D1.2.1
D1.2.2 r
D1.2.2 p
D1.2.3 r
D1.2.3 p
D1.2.4r
D1.2.4 p
WP2
D2.1
D2.2 r
D2.2.1
D2.3
D2.4 r
D2.4 p
WP3
D3.1
D3.2 r
D3.2 p
D3.3 r
D3.3 p
D3.4r
D3.4 p
D1.1.2 r
Restricted deliverable
WP4
D4.1
D4.2
D4.3
D4.4
D4.5.1
D4.5
D4.6
D4.5.1
D4.7
WP5
D5.1
D5.2
D5.3
D5.4
D5.5 r,p
D5.6 /5.7

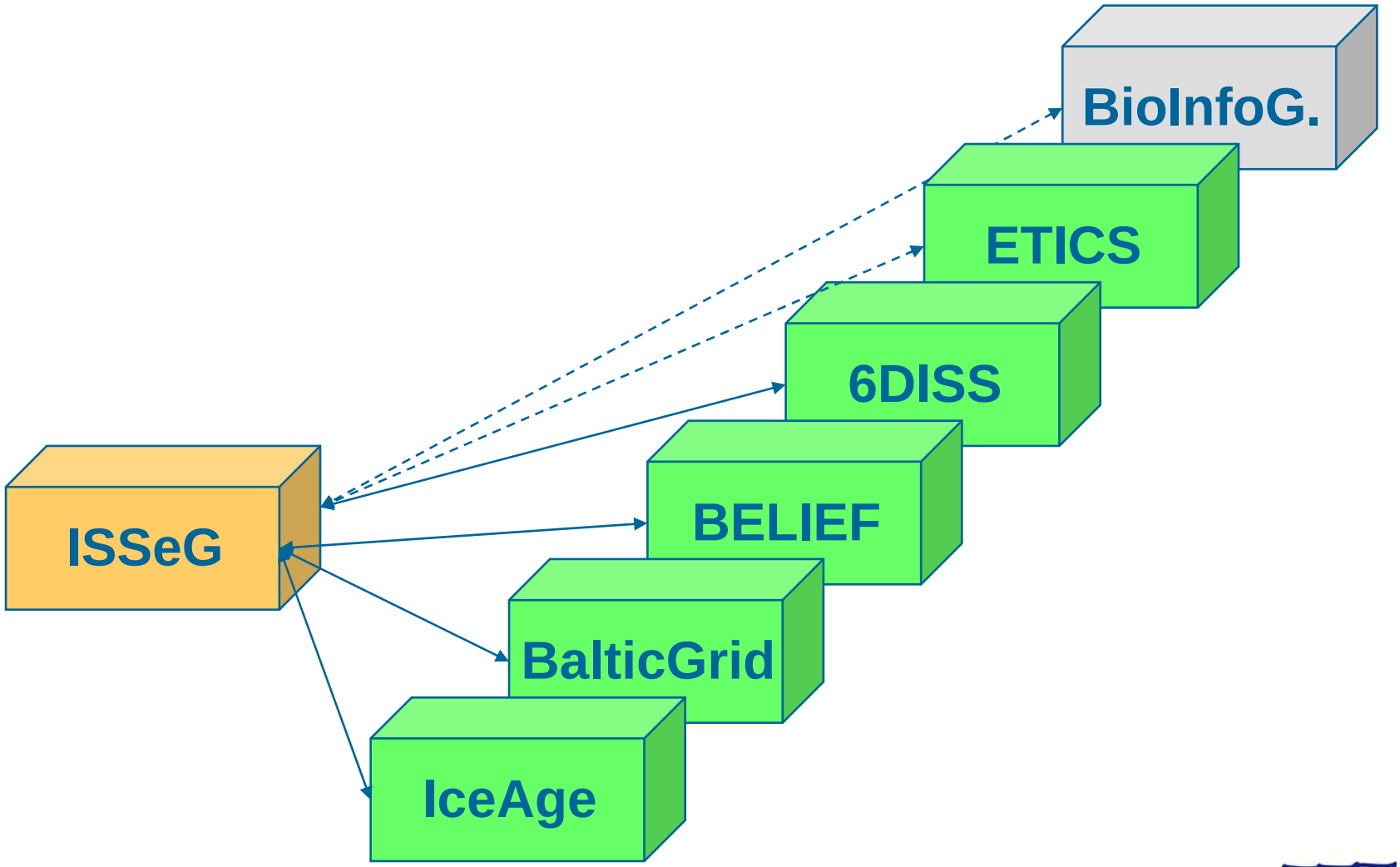

M01
M02
M03
M04
M05
M06
M07
M08
M09
M10
M11
M12
M13
M14
M15
M16
M17
M18
M19
M20
M21
M22
M23
M24
WP1.1
D1.1.1
D1.1.2 r
D1.1.2 p
D1.1.3 r
D1.1.3 p
D1.1.4 r
D1.1.4 p
WP1.2
D1.2.1
D1.2.2 r
D1.2.2 p
D1.2.3 r
D1.2.3 p
D1.2.4r
D1.2.4 p
WP2
D2.1
D2.2 r
D2.2.1
D2.3
D2.4 r
D2.4 p
WP3
D3.1
D3.2 r
D3.2 p
D3.3 r
D3.3 p
D3.4r
D3.4 p
WP4
D4.1
D4.2
D4.3
D4.4
D4.5.1
D4.5
D4.6
D4.5.1
D4.7
WP5
D5.1
D5.2
D5.3
D5.4
D5.5 r,p
D5.6 /5.7
D1.1.2 r
Restricted deliverable

Procedure for deliverables



Integrated Site Security for Grids
cern.ch/isseg

Synergies with other EU projects



Integrated Site Security for Grids
cern.ch/isseg

Criteria for success

We will be judged on our capability to

- Demonstrate we do not **duplicate EGEE's Job**
- Address also **non-HEP disciplines**
- Produce **quality** deliverables and dissemination material with **real substance**

Integrated Site Security for Grids

cern.ch/isseg

Criteria for progress

Description of qualitative and quantitative criteria and achievements to assess the progress of the project and measure its success	Date	Deliverable
Generalization of Central Management of on-site computers		
Generalize mechanisms for centrally managing on-site computers	M06	D1.1.3r D5.1
Increase the number of centrally managed computers at CERN beyond 5000	M06	D1.1.3r D5.1
Increase the number of centrally managed computers at FZK beyond 2000	M08	D1.2.3r D5.1
Automatic and customized configuration of on-site systems		
Put in place a pilot version of the system for centralized management of computers supporting customized configuration	M06	D1.1.3r D5.1
Test the pilot service over more than **50** computers at CERN	M06	D1.1.3r D5.1
Integration of computer account management facilities		
Put in place a system for synchronization and integration between computer accounts and personnel administrative data.	M06	D1.1.3r D5.1
As a measure of the usefulness and success of the system, detect at least **100** accounts to be closed due to policy violations at CERN	M06	D1.1.3r D5.1
As a measure of the usefulness and success of the system, detect at least **50** accounts to be closed due to policy violations at FZK	M08	D1.2.3r D5.1

Criteria for progress

Intrusion Detection		
Put in place a test Intrusion Detection System (IDS) by correlating host-based and network-based recorded data.	M12	D1.1.4p D5.2
Have deployed the test system on at least **6** host computers and **2** network devices at CERN.	M12	D1.1.4p D5.2
Protection of mission-critical systems		
Set up a Gateway system to access mission-critical devices (such a control systems).	M06	D1.1.3r D5.1
Provide access to mission-critical devices via a Gateway system to at least 50 users at CERN.	M06	D1.1.3r D5.1
Improvement of authentication mechanisms		
Evaluate comparatively alternatives for improving user authentication.	M12	D1.1.4p D1.2.4p D5.2
Having evaluated at least **3** differing technologies.	M12	D1.1.4p D1.2.4p D5.2
Improvement of user knowledge and awareness of computer security		
Create a quiz for evaluating and measuring the average knowledge of users on security principles, best practices, rules and policies.	M03	D5.1
Run the quiz at the beginning of the project at FZK, CCLRC and CERN and derive metrics on user awareness and knowledge of computer security.	M03	D5.1
Run the quiz at the end of the project at FZK, CCLRC and CERN. Analyze the results and compare them to those of the first evaluation.	M22	D5.5p

Criteria for progress

Dissemination via web site		
Release the first version of the education and dissemination web-site	M12	D4.2
Measure the achieved hit rate of the site after 3 months. Having attained at least **1000** hit after 3 months	M15	D5.3
Having attained at least **100** access of educational material after 3 months	M15	D5.3
Comparative auditing of security mechanisms		
Release first version of comparative auditing report	M06	D2.2r
Having identified and documented at least **20** security items significant for comparing auditing results.	M06	D2.2r D5.1
Recommendations for ISS generalization		
Release intermediate report on ISS generalization	M15	D3.1
Having drafted at least **5** recommendations in the intermediate report.	M15	D3.1 D5.5p
Dissemination beyond the audience of the project partners		
Having been invited by organizations or projects external to the consortium to give at least **10** public presentations on ISS	M24	D5.5p

- **The most difficult aspects**

  As perceived by the Project Coordinator

  - Involve **scientific disciplines** in requirements and dissemination
    (whom, how?)
  - Write clear, convincing, practical, useful **recommendations**
  - Meet our educational objectives (quantitative)

Beyond ISSeG

- ISSeG is a two-year project
- Too short to achieve **wide-scale ISS generalization**
- Sufficient to **create the conditions** for it
  - methods
  - recommendations
  - training

  all validated by the two deployments
- ISS generalization …

  … may be the subject of a **second phase**

Integrated Site Security for Grids
cern.ch/isseg