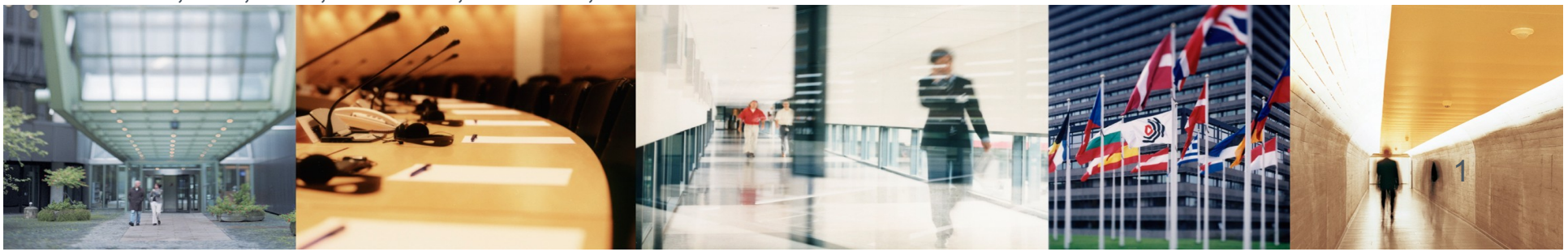
Europäisches Patentamt
European Patent Office
Office européen des brevets

IT Service Continuity Management

IT Service Continuity Components and Approach to the Test Activities

Roberto Giaffreda,
IT Service Continuity Manager
CISA, CISM, CISSP, ISO27001LA, BS25999LA, ITILv2

Pisa, 22 Maggio 2009



Agenda

- **The European Patent Office (EPO)**
  - **A Portrait (5 min)**
  - **EPO overview**

- IT Service Continuity framework
  - IT Organization and ITSC Methodology
  - IT Service Continuity vs. Business Continuity
  - IT Service Continuity Scenarios and Recovery Strategies

- IT Service Continuity Test
  - IT Continuous Availability Capability
    - Test Approach
    - IT Critical Perimeter
    - Benefits
  - IT Service Continuity Test Challenges

European Patent Office - a Portrait (5min)

Structure of the European Patent Organisation

European Patent Organisation

European Patent Office

The executive body

- responsible for examining European patent applications

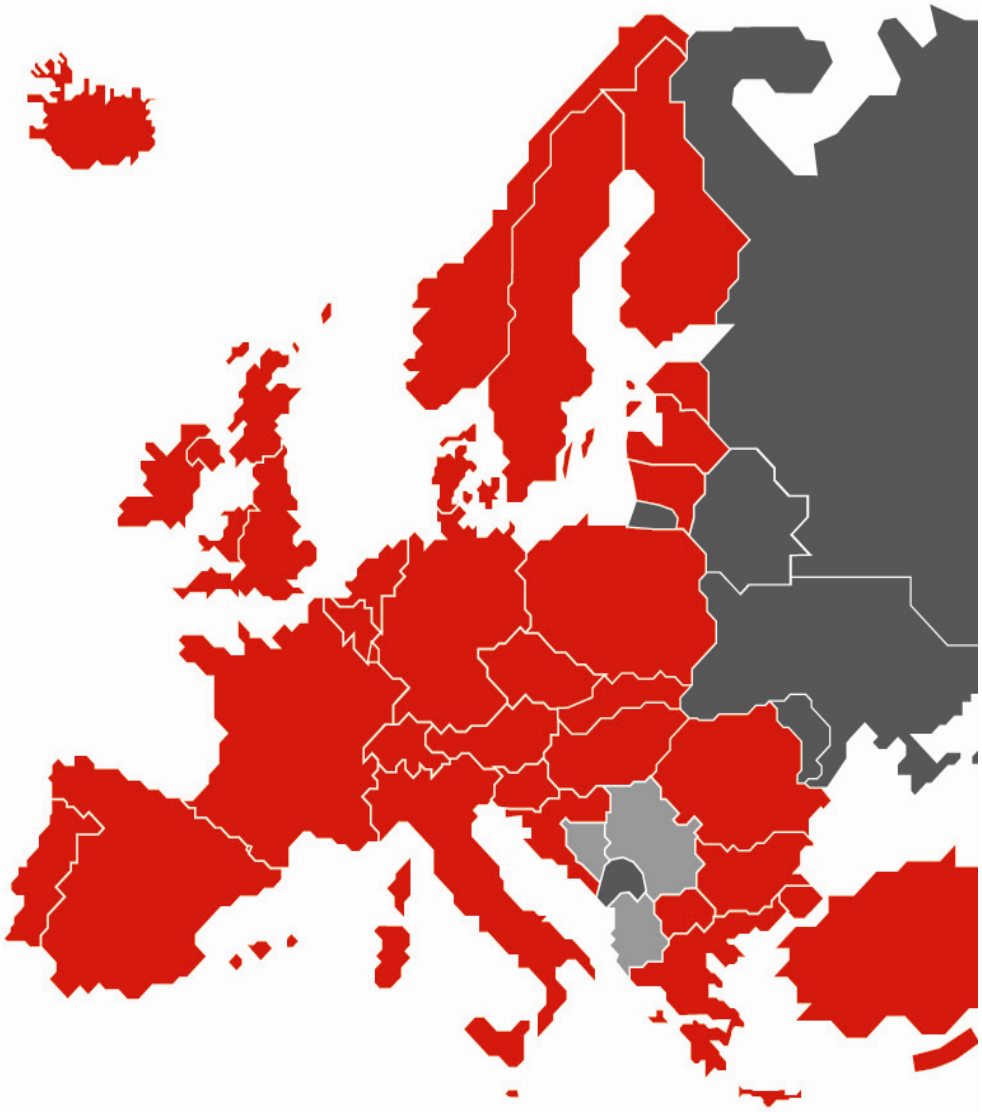
Administrative Council

The legislative body

- made up of delegates from the member states
- supervises the activities of the Office
- has a specific legislative function

38 member states

Austria • Belgium • Bulgaria • Croatia • Cyprus • Czech Republic • Denmark • Estonia • Finland • France • Germany • Greece • Hungary • Iceland • Ireland • Italy • Latvia • Liechtenstein • Lithuania •Luxembourg • Former Yugoslav Republic of Macedonia • Malta • Monaco • Netherlands • Norway • Poland • Portugal • Romania • Slovakia • Slovenia • Spain • Sweden • Switzerland • Turkey • United Kingdom



European patent applications and patents can also be extended at the applicant's request to the following states:

Albania • Bosnia-Herzegovina • Serbia

Status: Dec 2008

Autonomy

- Second largest intergovernmental institution in Europe
- Not an EU institution
- Self-financing, i.e. revenue from fees covers operating and capital expenditure

Number of staff

Around 60% are patent examiners

Überblick über den Personalbestand nach Dienstorten und Laufbahngruppen am 31. Dezember 2008[1]
Analysis of staff in post on 31 December 2008 by place of employment and grade[1]
Répartition des effectifs en poste au 31 décembre 2008 selon le lieu d'affectation et la catégorie[1]

			A	B	C	A+B+C
München	**Munich**	**Munich**				
Recherche, Prüfung, Einspruch	Search, Examination, Opposition	Recherche, Examen, Opposition	2211[2]	509	0	2720
Recht/Internationale Angelegenheiten	Legal/International Affairs	Questions juridiques/ Affaires internationales	78	69	0	147
Beschwerde (Vorsitzende/Mitglieder)	Appeals (chairmen/members)	Chambres de recours (présidents/membres)	152[3]	0	0	152
Beschwerde (Verwaltung)	Appeals (administration)	Chambres de recours (administration)	14	44	0	58
Informationsmanagement (IM)	Information Management (IM)	Gestion de l'information (IM)	47	42	0	89
Verwaltung	Administration	Administration	143	240	80	463
Zwischensumme	Sub-total	Total partiel	2645	904	80	3629
Den Haag	**The Hague**	**La Haye**				
Recherche, Prüfung, Einspruch	Search, Examination, Opposition	Recherche, Examen, Opposition	1657[2]	481	0	2138
Informationsmanagement (IM)	Information Management (IM)	Gestion de l'information (IM)	149	193	0	342
Verwaltung	Administration	Administration	33	113	33	179
Zwischensumme	Sub-total	Total partiel	1839	787	33	2659
Berlin	**Berlin**	**Berlin**				
Recherche, Prüfung, Einspruch	Search, Examination, Opposition	Recherche, Examen, Opposition	214[2]	46	1	261
Verwaltung	Administration	Administration	1	13	1	15
Zwischensumme	Sub-total	Total partiel	215	59	2	276
Wien	**Vienna**	**Vienne**				
Patentinformation	Patent Information	Information brevets	39	57	2	98
Verwaltung	Administration	Administration	2	15	2	19
Zwischensumme	Sub-total	Total partiel	41	72	4	117
Brüssel	**Brussels**	**Bruxelles**				
Verwaltung	Administration	Administration	1	3	0	4
Zwischensumme	Sub-total	Total partiel	1	3	0	4
Summe	**Total**	**Total**	**4741**	**1825**	**119**	**6685**

1 *Einschließlich der Beamten in unbezahltem Urlaub.*
2 *Diese Zahl umfasst sowohl Prüfer als auch Direktoren.*
3 *Diese Zahl umfasst die Vorsitzenden sowie die technischen und die juristischen Mitglieder der Beschwerdekammern.*

1 *Including employees on unpaid leave.*
2 *Includes management staff as well as examiners.*
3 *Includes chairmen and technical and legal members of the boards of appeal.*

1 *Agents en congé non rémunéré inclus.*
2 *Ces chiffres comprennent les cadres supérieurs et les examinateurs.*
3 *Ce chiffre comprend les présidents, ainsi que les membres techniciens et juristes des chambres de recours.*

Staff from 32 different countries

Nationalitäten- und Laufbahngruppenverteilung des Personals am 31. Dezember 2008
Analysis of staff in post on 31 December 2008 by grade and nationality
Répartition des effectifs en poste au 31 décembre 2008 selon le grade et la nationalité

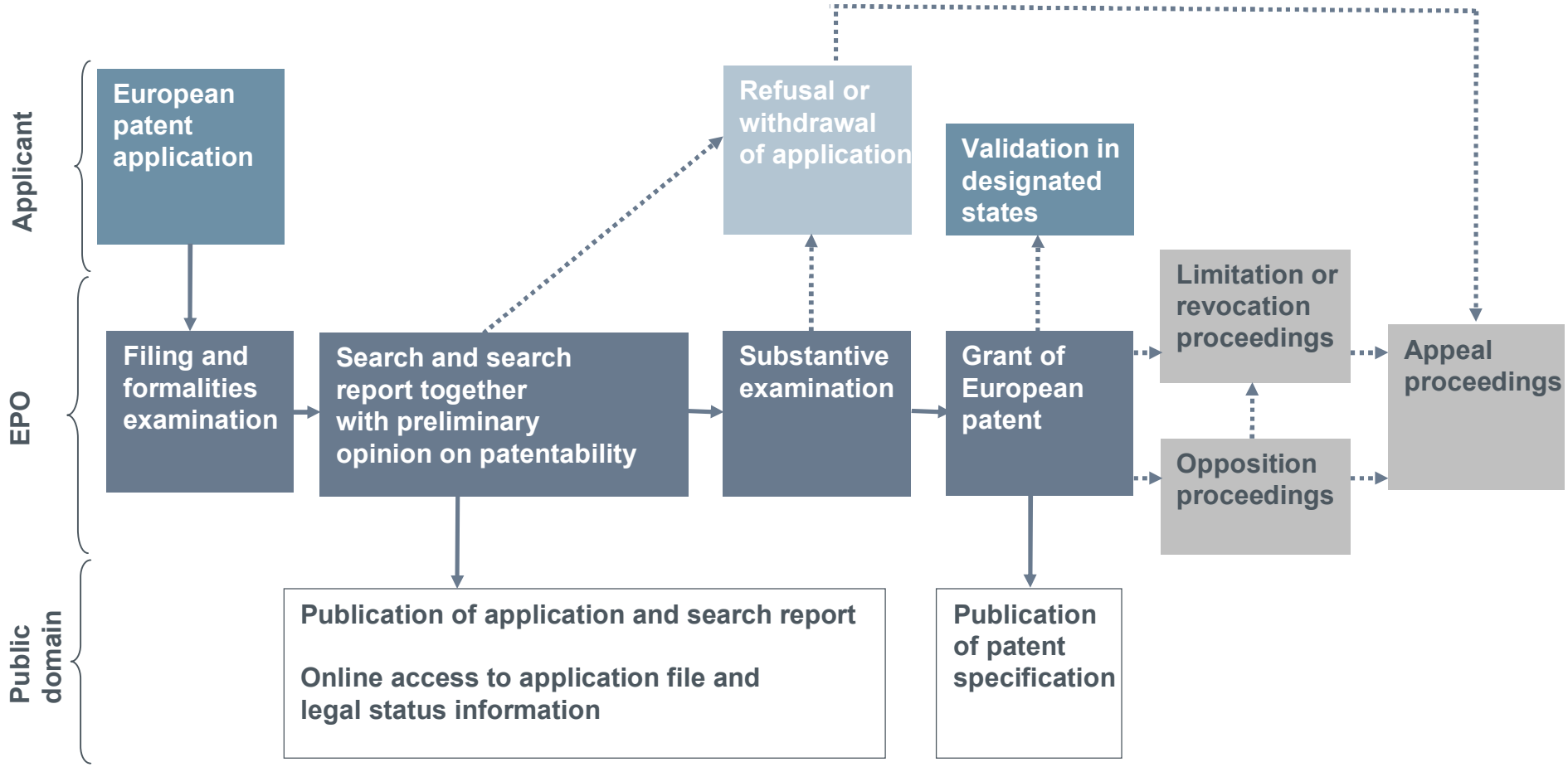
Land **Country** Pays				Laufbahngruppe A **A grade** Catégorie A		Laufbahngruppen B und C **B and C grades** Catégories B et C		Gesamtpersonalbestand **All staff** Ensemble des effectifs	
					%		%		%
AT	Österreich	Austria	Autriche	170	4	67	3	237	4
BE	Belgien	Belgium	Belgique	256	5	101	5	357	5
BG	Bulgarien	Bulgaria	Bulgarie	21	0	9	0	30	0
CH	Schweiz	Switzerland	Suisse	53	1	16	1	69	1
CY	Zypern	Cyprus	Chypre	5	0	3	0	8	0
CZ	Tschechische Republik	Czech Republic	République tchèque	15	0	5	0	20	0
DE	Deutschland	Germany	Allemagne	1263	27	544	28	1807	27
DK	Dänemark	Denmark	Danemark	52	1	22	1	74	1
EE	Estland	Estonia	Estonie	3	0	3	0	6	0
ES	Spanien	Spain	Espagne	344	7	82	4	426	6
FI	Finnland	Finland	Finlande	28	1	20	1	48	1
FR	Frankreich	France	France	880	19	310	16	1190	18
GB	Vereinigtes Königreich	United Kingdom	Royaume-Uni	358	8	156	8	514	8
GR	Griechenland	Greece	Grèce	134	3	26	1	160	2
HR	Kroatien	Croatia	Croatie	2	0	0	0	2	0
HU	Ungarn	Hungary	Hongrie	22	0	3	0	25	0
IE	Irland	Ireland	Irlande	49	1	33	2	82	1
IS	Island	Iceland	Islande	1	0	0	0	1	0
IT	Italien	Italy	Italie	389	8	108	6	497	7
LI	Liechtenstein	Liechtenstein	Liechtenstein	1	0	0	0	1	0
LT	Litauen	Lithuania	Lituanie	3	0	1	0	4	0
LU	Luxemburg	Luxembourg	Luxembourg	43	1	30	2	73	1
LV	Lettland	Latvia	Lettonie	4	0	0	0	4	0
MT	Malta	Malta	Malte	2	0	0	0	2	0
NL	Niederlande	Netherlands	Pays-Bas	294	6	324	17	618	9
PL	Polen	Poland	Pologne	45	1	11	1	56	1
PT	Portugal	Portugal	Portugal	71	1	14	1	85	1
RO	Rumänien	Romania	Roumanie	96	2	11	1	107	2
SE	Schweden	Sweden	Suède	100	2	24	1	124	2
SI	Slowenien	Slovenia	Slovénie	10	0	4	0	14	0
SK	Slowakei	Slovakia	Slovaquie	4	0	11	1	15	0
TR	Türkei	Turkey	Turquie	21	0	5	0	26	0
	Sonstige	Others	Divers	2	0	1	0	3	0
	Summe	**Total**	**Total**	**4741**	**100**	**1944**	**100**	**6685**	**100**

A Führungskräfte, Prüfer, Juristen, Verwaltungsräte und Übersetzer
B (Leitendes) Verwaltungspersonal
C Technisches und Hilfspersonal

A Managerial staff, examiners, lawyers, administrators and linguists
B Administrative and supervisory staff
C Technicians and service employees

A Managers, examinateurs, juristes, administrateurs et linguistes
B Agents administratifs et agents de maîtrise
C Agents techniques et agents de service

Overview of European patent grant procedure (I)



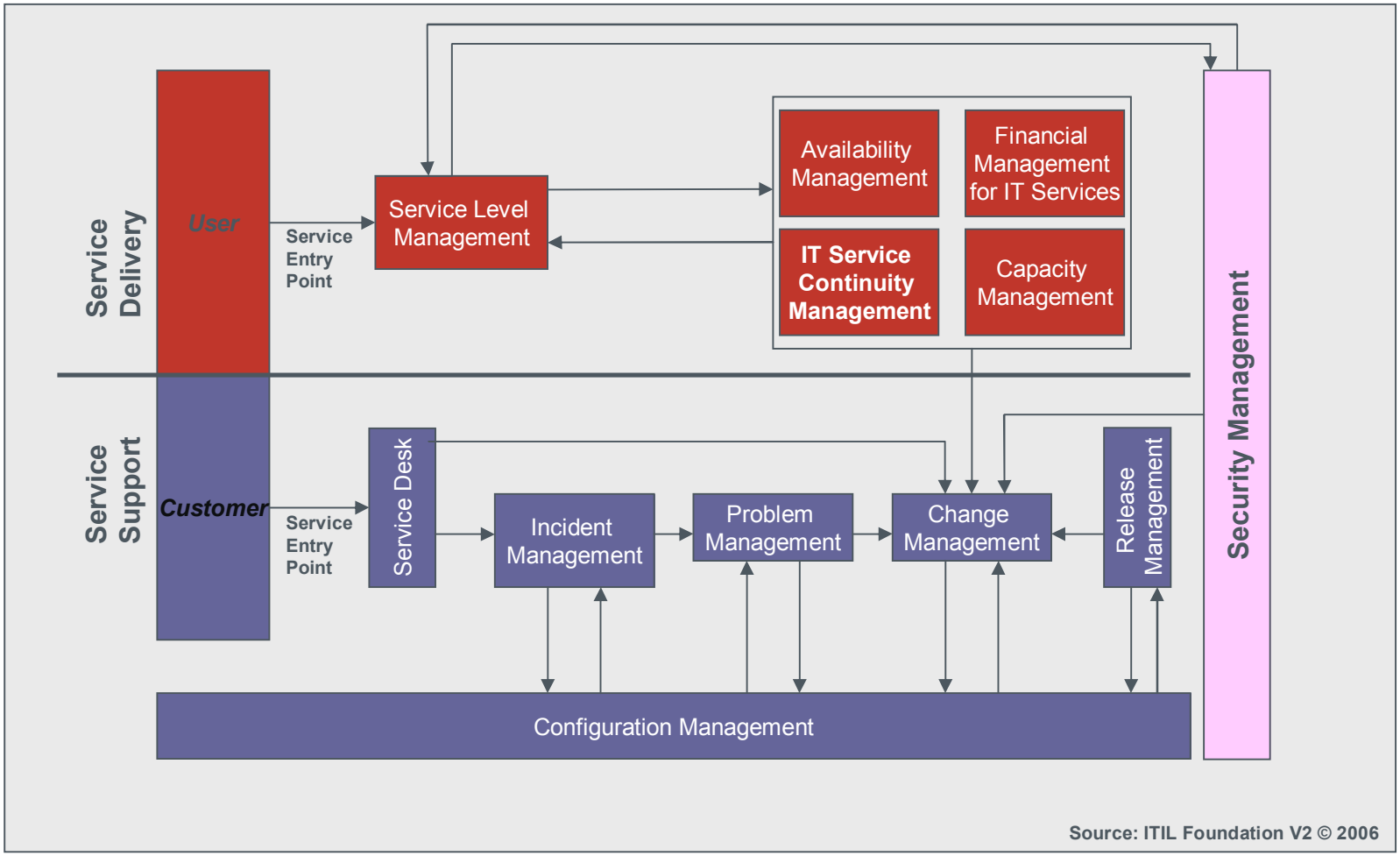
Agenda

- The European Patent Office (EPO)
  - A Portrait (5 min)
  - EPO overview

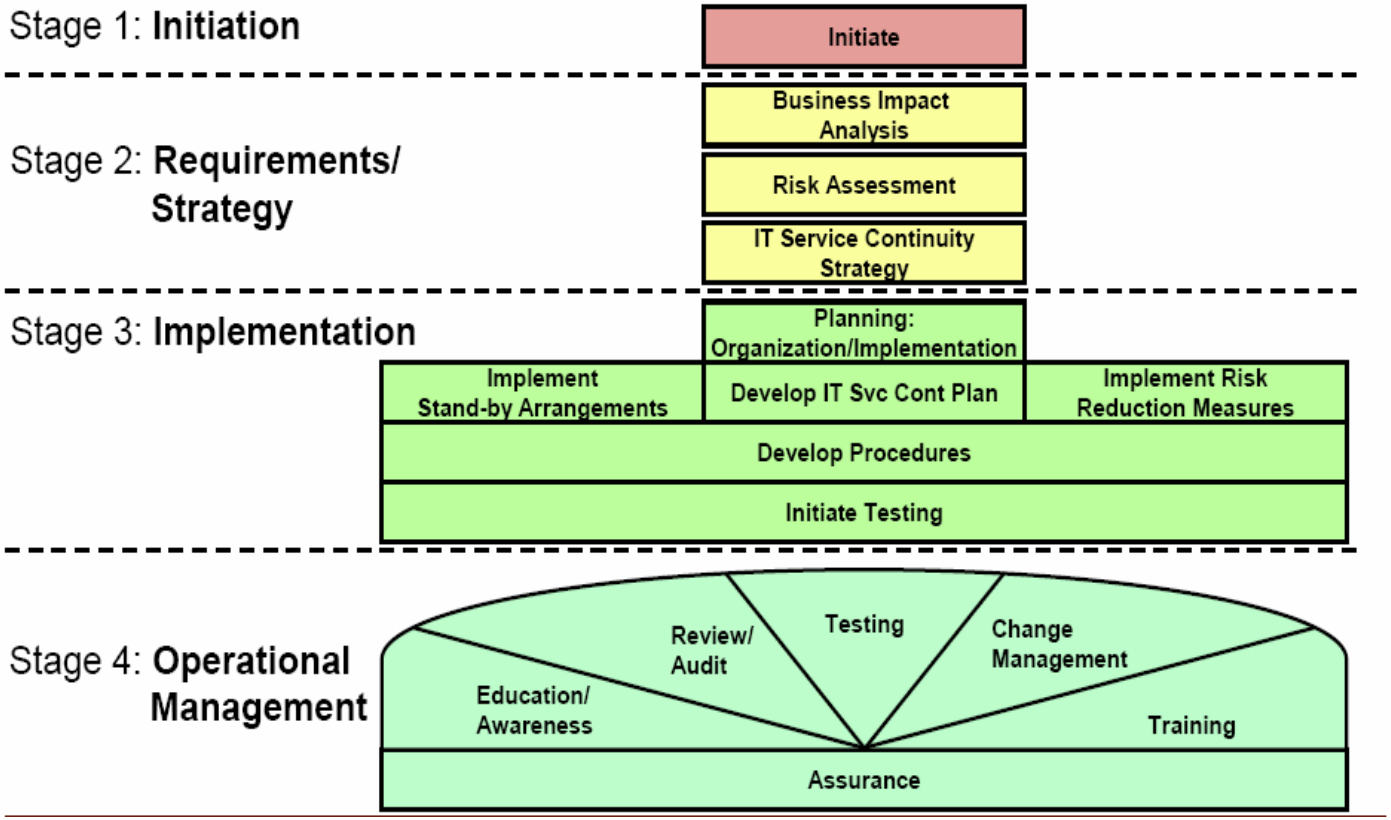
- **IT Service Continuity framework**
  - **IT Organization and ITSC Methodology**
  - **IT Service Continuity vs. Business Continuity**
  - **IT Service Continuity Scenarios and Recovery Strategies**

- IT Service Continuity Test
  - IT Continuous Availability Capability
    - Test Approach
    - IT Critical Perimeter
    - Benefits
  - IT Service Continuity Test Challenges

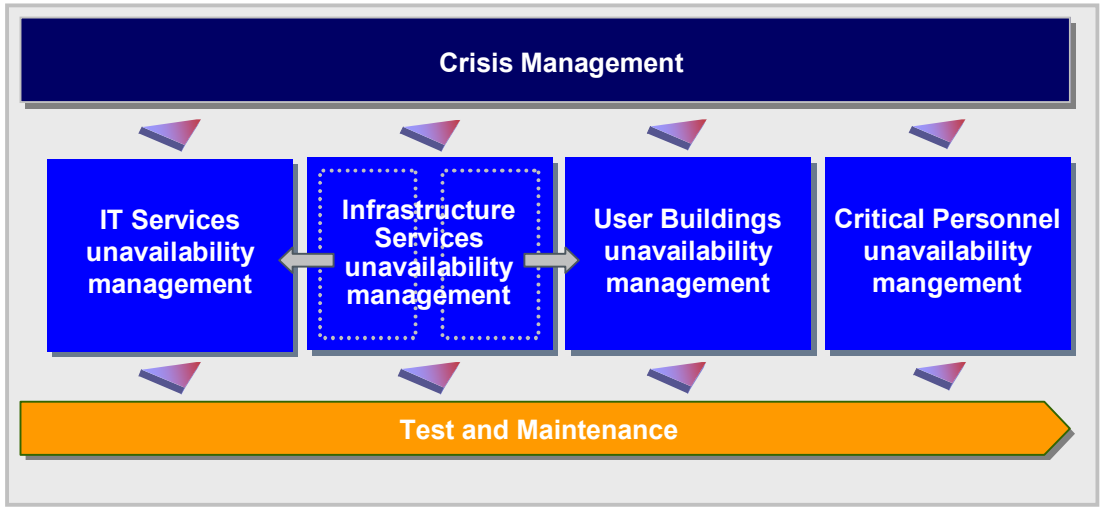
IT Organization - ITIL



IT Service Continuity - Methodology - ITIL



IT Service Continuity vs. Business Continuity



Example of Global Business Continuity Plan Framework

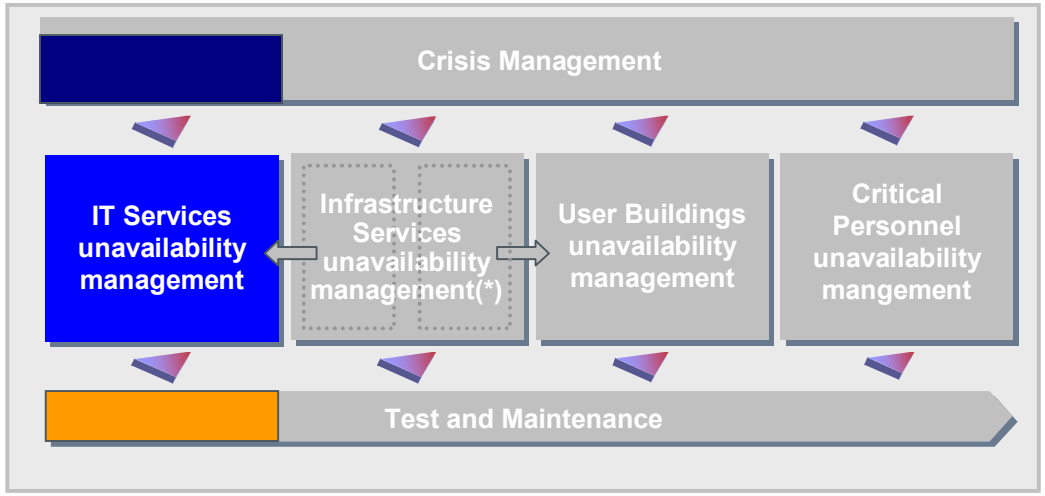
A Business Continuity Plan (BCP) is a documented collections of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable the organization to continue to deliver its **critical activities at an acceptable pre-defined level.**

In order to address a strategic solution for all the resources involved (i.e. people, premises,..) a Global BCP usually consists of a set of different plans (BCPs) that may be invoked in whole or part and at any stage of the response to crisis.

IT Service Continuity vs. Business Continuity

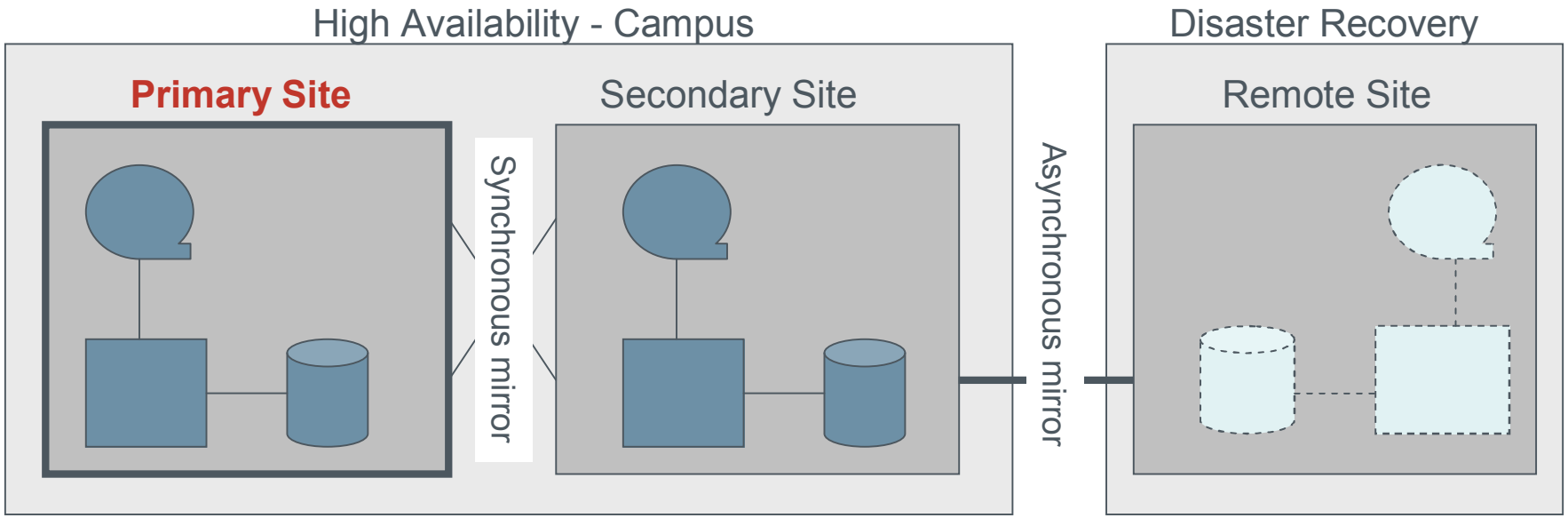
The Continuity Plan for the *IT Services unavailability* scenario is called **IT Service Continuity Plan.**

The main goal of this plan is to support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities (i.e. computer systems, network, application, data repositories) can be resumed within required, and agreed, business timescales (ref. ITIL v3).



Example of Global Business Continuity Plan Framework

IT Recovery Strategies

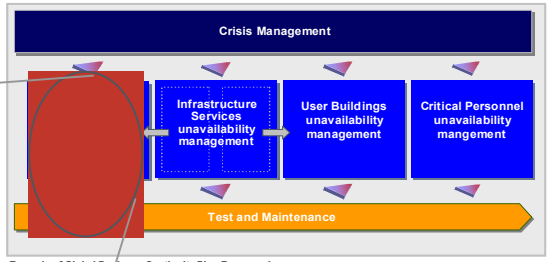


Campus: Technological and organisational solution that foresee a double localization of the IT Systems on **2 different sites always actives** (with synchronous data replication and application mirroring). Both sites are able to operate autonomously in case of unavailability of the other; this solution ensure the **high availability** of the IT Systems and the continuity of the vital and critical functions for the business.

DR: Technological and organisational solution that, within an acceptable time for the business (Recovery Time Objective), provide the necessary assets (hardware, software, data) in order to ensure the recovery of the IT Systems in the shortest possible time and with the less possible degradation. That solution foresee the activation of an **alternate and suitable site**, generally **another remote** site, to allow the recovery of the vital and critical functions for the business.

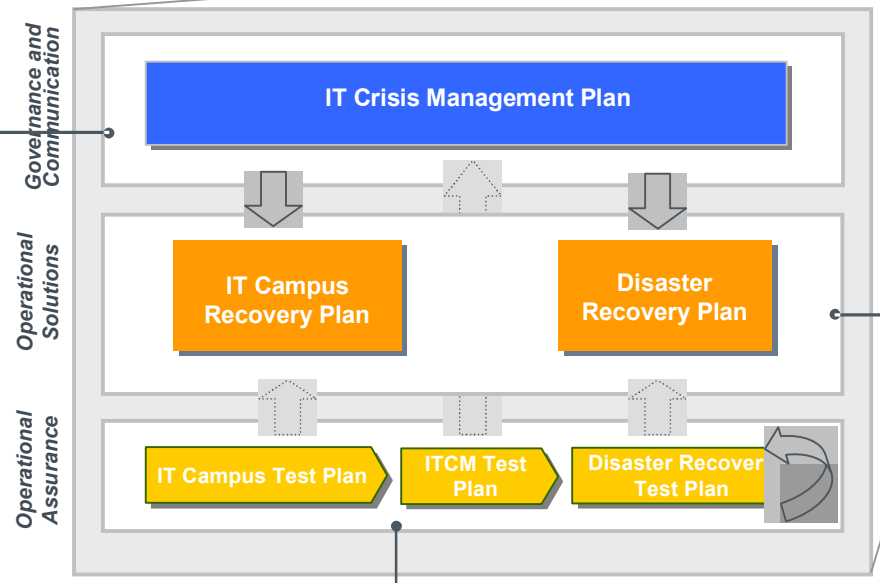
IT Service Continuity Plan Framework

Components



Example of Global Business Continuity Plan Framework

1st level: defines how to handle a crisis situation by the mean of a **Crisis Management Team** (CMT). The IT Crisis Management Plan describes the roles and responsibilities of the members of this team as well as the escalation procedure to activate it.

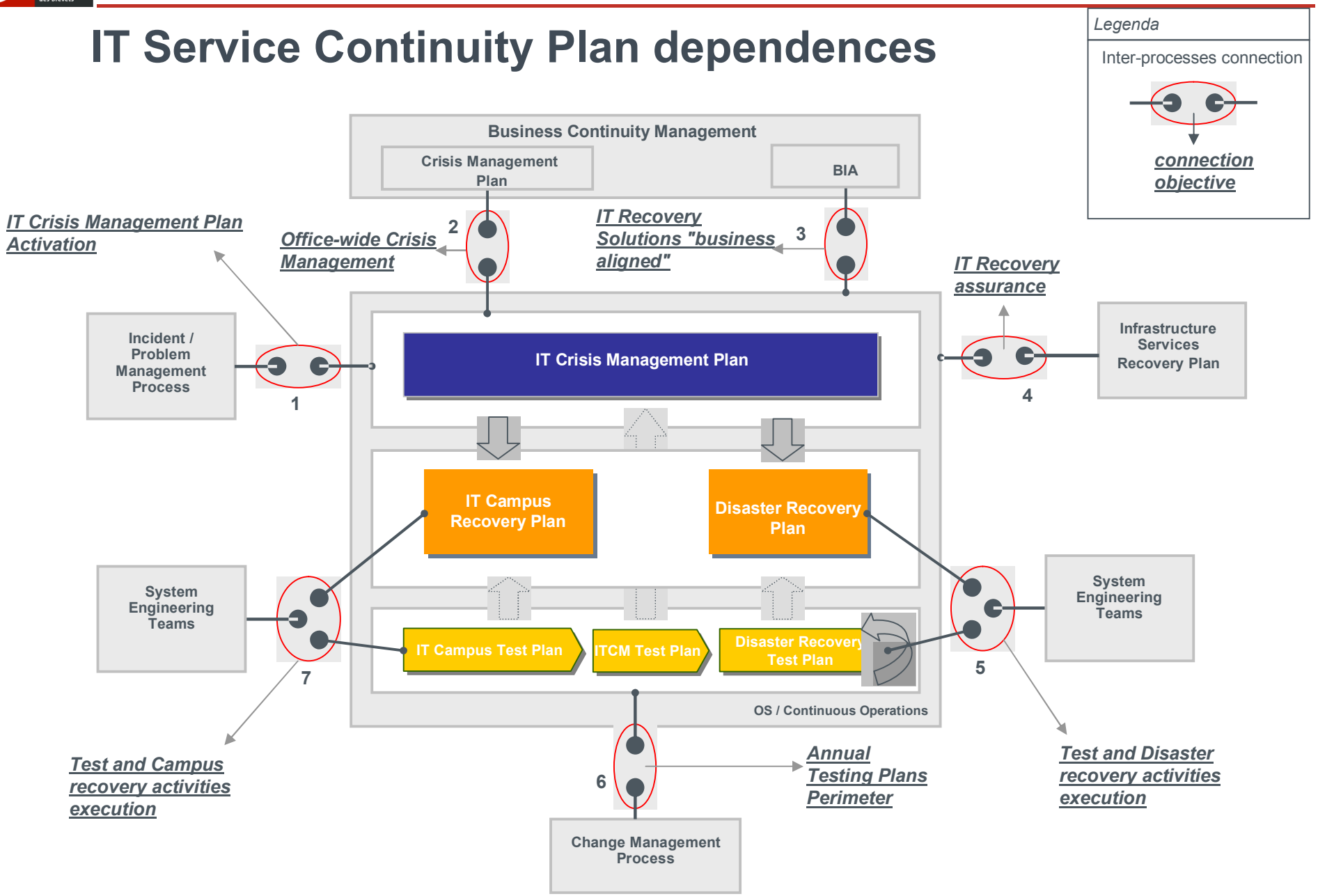


IT Service Continuity Plan

2nd level: 2 main scenarios have been identified. The technological and organisational solutions to resume the IT Services are:
1) the ***Campus Recovery Plan*** has the main objective to activate the secondary computer room in case of disruption at the primary computer room (*local disaster*);
2) the ***Disaster Recovery Plan*** consists of a set of predetermined actions to follow in order to relocate to a remote site only the IT systems and services in case of disastrous events impacting both computer rooms (*geographical disaster*).

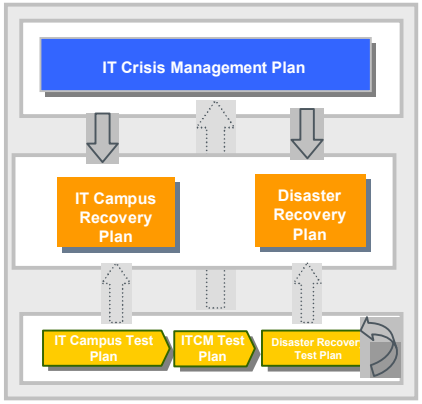
3rd level: prove the efficiency of the recovery solutions on the **IT critical perimeter** in terms of infrastructure and applications as well as organisational solutions. These formal test plans should be planned at least once a year and kept updated with the continuous infrastructure changes.

IT Service Continuity Plan dependences



IT Service Continuity Activities and Scenarios

Normality situation (Peace Time)



IT Service Continuity Plan

Governance and Communication

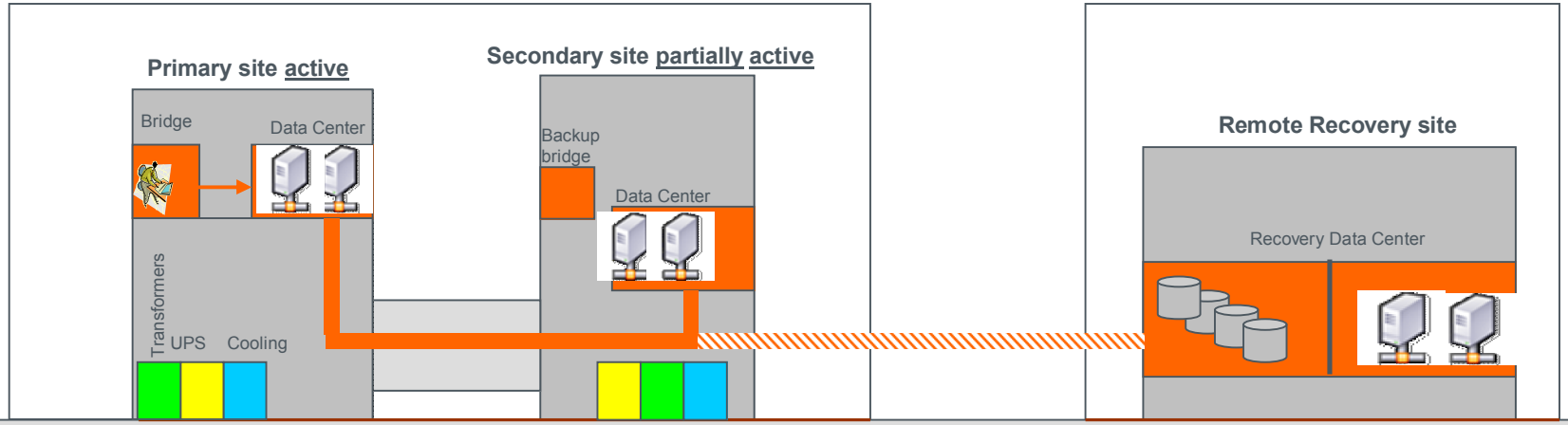
- IT Crisis Management Monitoring
- IT Crisis Management Awareness

Operational Solutions

- IT Campus Recovery Plan / Procedures documentation
- Disaster Recovery Plan / Procedures documentation

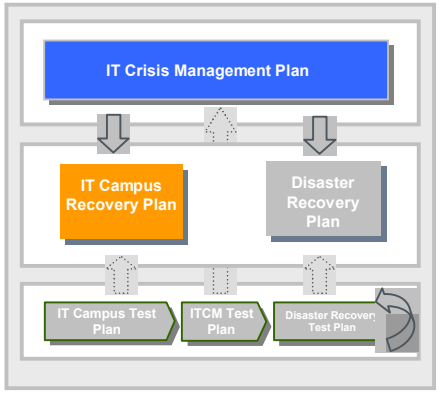
Operational Assurance

- High Availability Solutions Assessment and Test
- IT Crisis Management Plan Test (table top exercise)
- Disaster Recovery Test Plan



IT Service Continuity Activities and Scenarios

Emergency situation (War Time) - Scenario 1 - Local Disaster

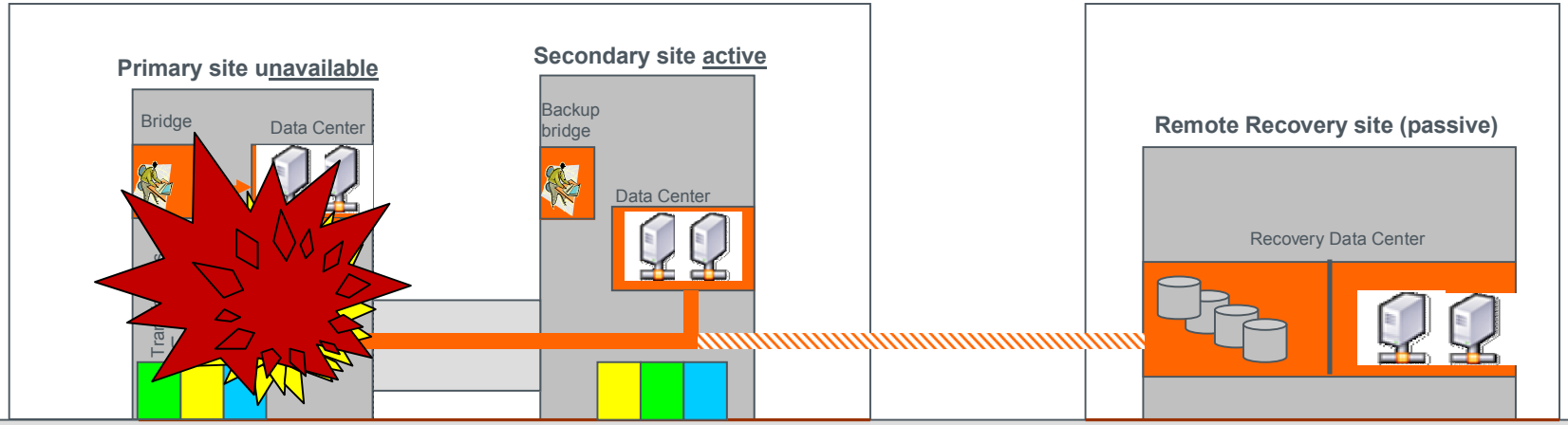


IT Service Continuity Plan

Governance and Communication - IT Crisis Management Team Activation

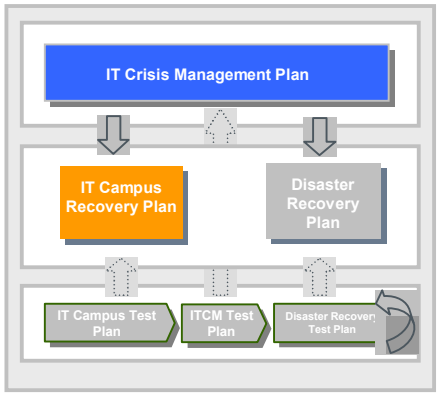
Operational Solutions - Eventual IT Campus Recovery Plan activation (Primary → Secondary)

Operational Assurance



IT Service Continuity Activities and Scenarios

Emergency situation (War Time) - Scenario 2 - Local Disaster

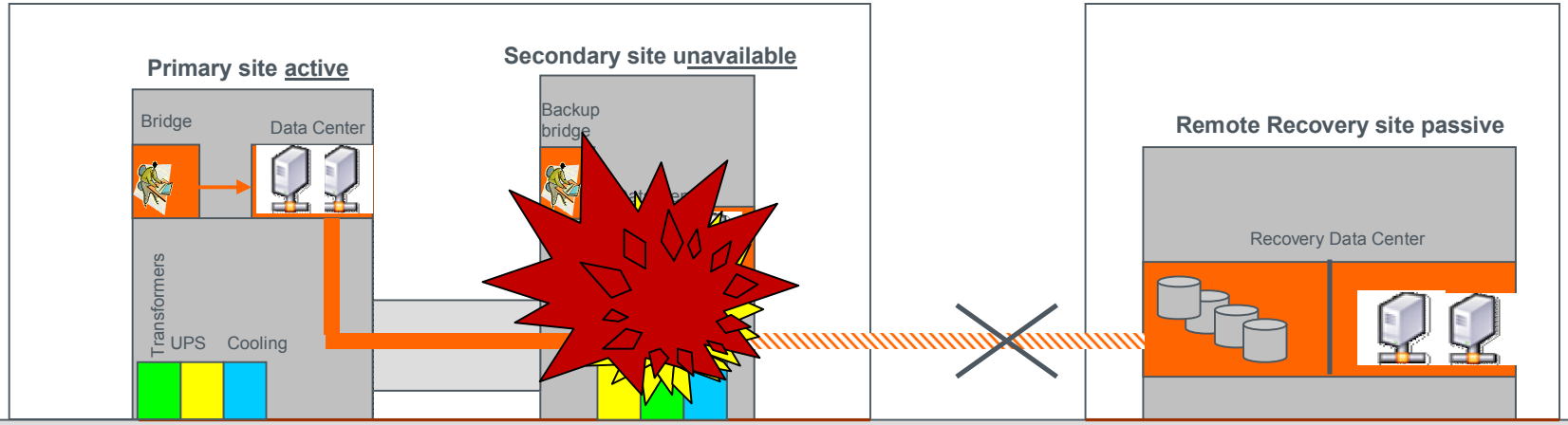


IT Service Continuity Plan

Governance and Communication - IT Crisis Management Team Activation

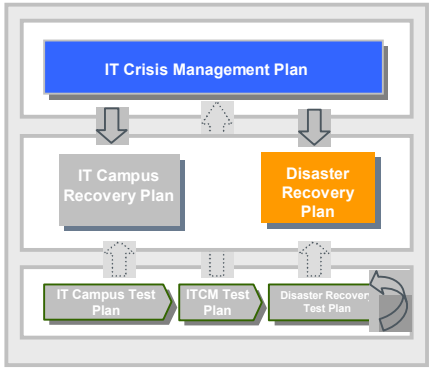
Operational Solutions - Eventual IT Campus Recovery Plan activation (Secondary→ Primary)

Operational Assurance



IT Service Continuity Activities and Scenarios

Emergency situation (War Time) - Scenario 3 - Geographic Disaster

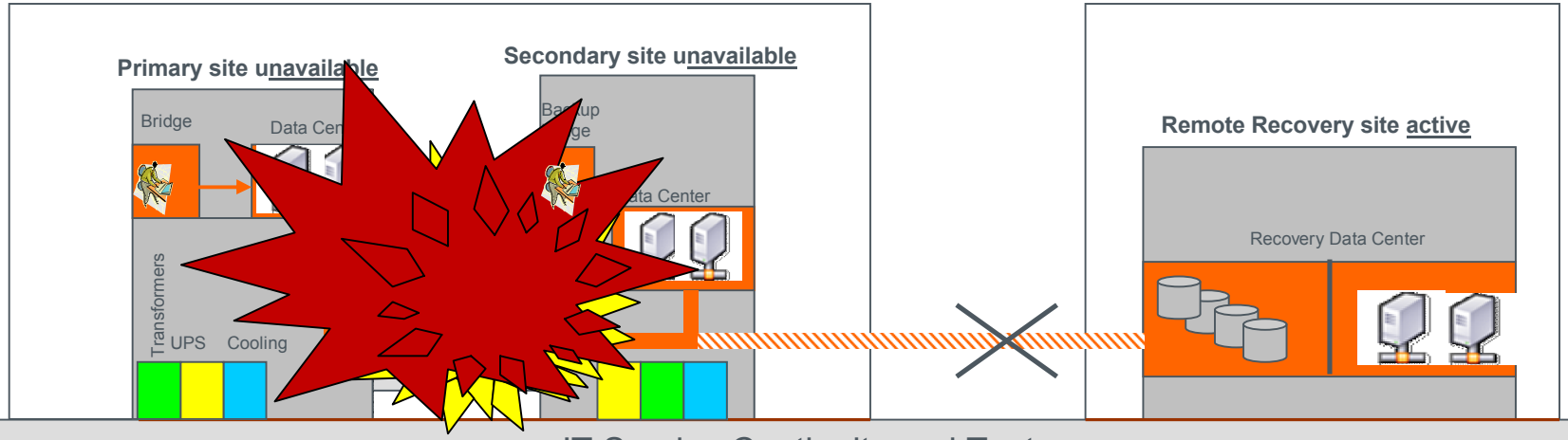


IT Service Continuity Plan

Governance and Communication - IT Crisis Management Team Activation

Operational Solutions - Eventual Disaster Recovery Plan activation (Secondary→ Primary)

Operational Assurance



Agenda

- The European Patent Office (EPO)
  - A Portrait (5 min)
  - EPO overview

- IT Service Continuity framework
  - IT Organization and ITSC Methodology
  - IT Service Continuity vs. Business Continuity
  - IT Service Continuity Scenarios and Recovery Strategies

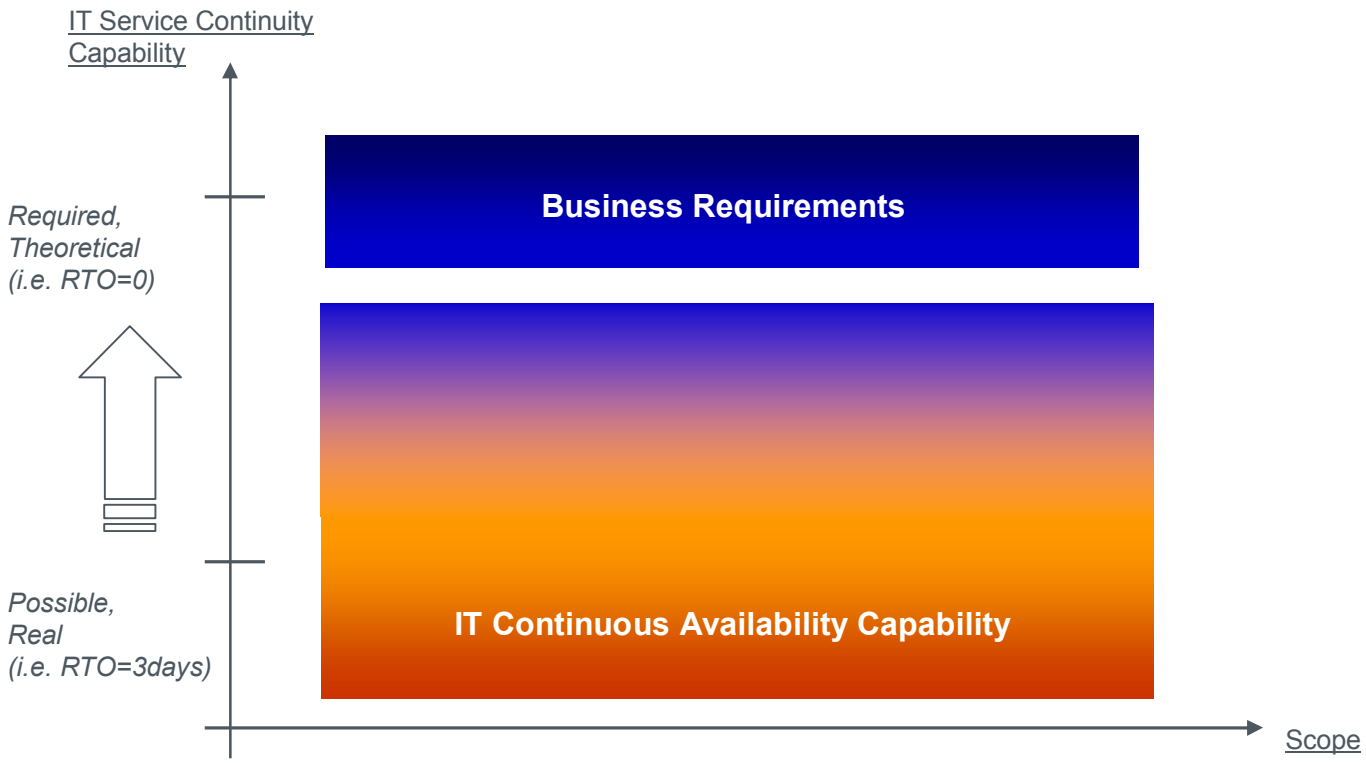
- **IT Service Continuity Test**
  - **IT Continuous Availability Capability**
    - **Test Approach**
    - **IT Critical Perimeter**
    - **Benefits**
  - **IT Service Continuity Test Challenges**

IT Service Continuity High Level Requirements

- Are the IT services able to switch and run (partially or in full) from another location if needed?
- If yes, how long does it take?
- If the IT Recovery Time has been estimated (and tested), is that acceptable?
- ...

IT Continuous Availability Capability

Requirements vs Capability



IT Continuous Availability Capability

Steps

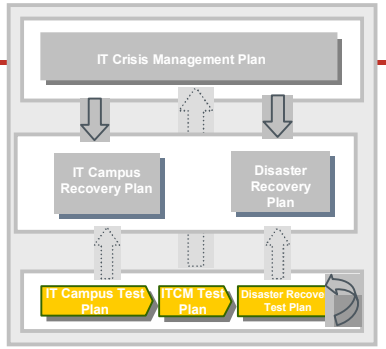
1. IT Critical Perimeter identification and agreement
   - List of Critical IT components and IT Services
   - List of Critical Applications (from BIA)

2. IT Critical Perimeter Continuous Availability Assessment
   - Description, Configuration, High Availability requirements, Failover Capability, Technology
   - Test Assessment
   - Test Plan (Component Tests)
   - Real RTO/RPO definition per component

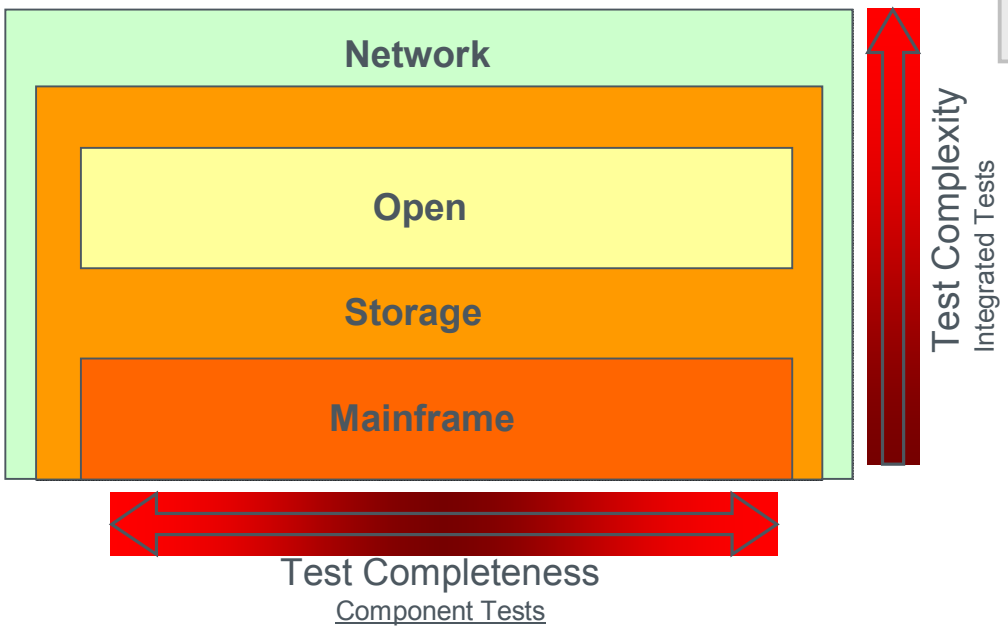
3. IT Recovery Plan
   - IT Critical Perimeter dependencies, priorities and order
   - Test Recovery Plan (Integrated Tests)
   - Real RTO/RPO definition for the IT Services

IT Continuous Availability Capability

Test Plan



IT Service Continuity Plan

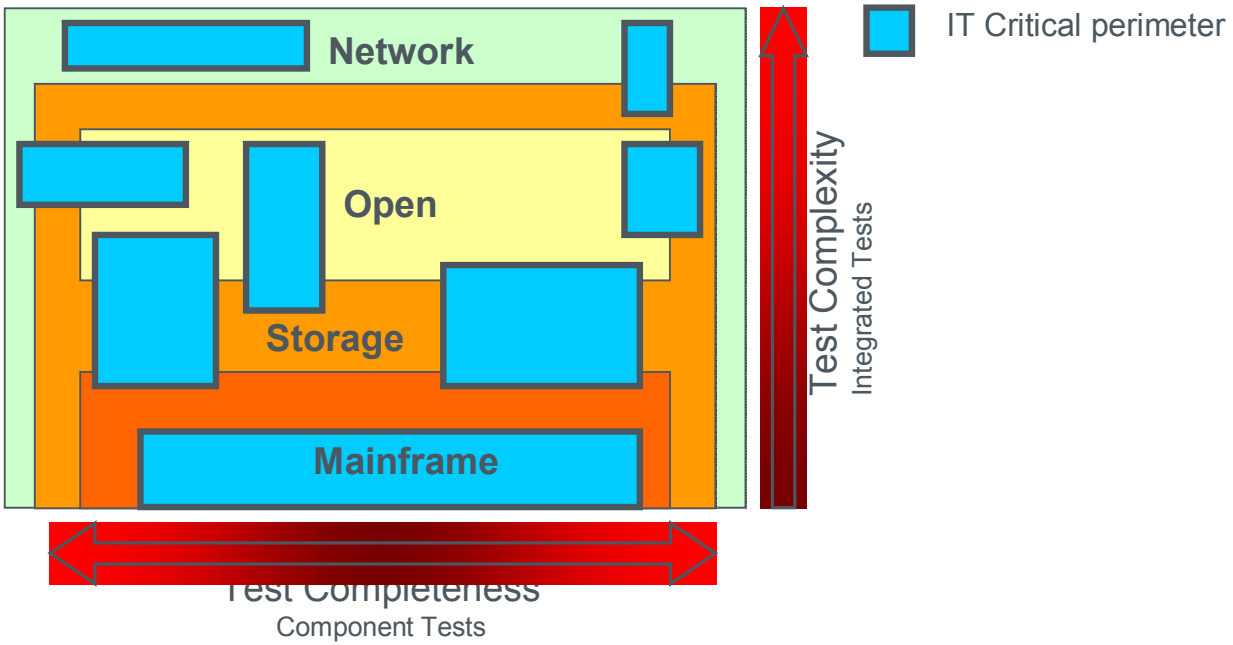


Testing the complete recovery of the IT services on a secondary mirrored site is a complex activity that needs to be approached at least through the execution of 2 levels of test:

- **Component** tests: homogeneous tests with the objective to assess and verify the ability to recover a single components of the Infrastructure.
- **Integrated** tests: intermediate objectives are to verify the ability to recover on the secondary/third site multiple components of the IT Infrastructure in the same time. The final objective is to test the ability to recover / switch the complete **IT critical perimeter** from the primary site on the secondary/third site.

IT Continuous Availability Capability

IT Critical Perimeter



The **IT Critical Perimeter** for each infrastructure layer shall to be identified and agreed with each IT teams.

The IT Critical Perimeter concept can be understood through 2 different perspectives:

- *High Availability* (business as usual): set of IT components and IT Services that failing will cause a wide negative impact on the Applications / Business services availability (i.e. DNS, LDAP,..)
- *IT Recovery Plan* (crisis situation): the first necessary layer of IT infrastructure and Services to recover before being able to resume any applications (i.e. authentication services, middle-tier,..).

IT Critical Perimeter

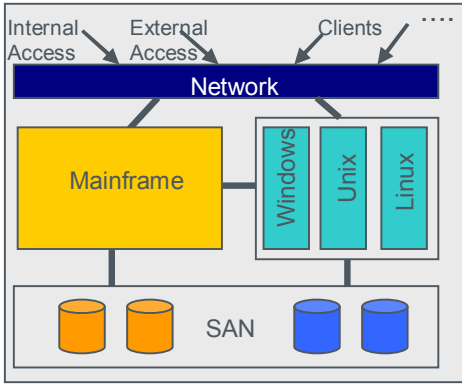
Main Benefits

- Cost-effective IT Services and not under- or over-invested through an understanding of internal and external dependencies within the infrastructure
- High Availability / Disaster Recovery investments and solutions aligned to the Business priorities
- Monitoring activities scope Business aligned
- Support the Incident / Problem Management / Crisis Management escalation process
- Prioritized and ordered IT Recovery Plans
- "IT Impact Analysis" supporting the Business Impact Analysis
- Gaps between Business requirements and Real Capability can be more easily identified and monitored
- IT maturity
- ....

IT Service Continuity Test Challenges

Human, Technology and Organizational factors

- Long term activity - no immediate results
- Missing Cross IT Vision
- Turnover rate
- Lack of Sensibility



- Continuous Changes
- Infrastructure complexity
- Vendors influence
- Technology obsolescence
- What is critical? IT Critical Perimeter identification
- IT Critical Perimeter maintenance

- Internal and External Business requirements definition and awareness
- Performance first, Resilience after
- Specific budget allocation and approval

Grazie per l'Attenzione

www.epo.org
info@epo.org
Tel. + 49 (0)89 2399 - 4636

Roberto Giaffreda