

Business Continuity & Disaster Recovery

Technology and Process

Alessio Di Benedetto
Presales Manager

Roma, 7th of May 2010

Objectives



The objective of this workshop is to provide:

- ➔ an overview of the EMC organization (roles and specialization)

- ➔ a brief introduction on the Business Continuity and Disaster Recovery subject matter.
 - ➔ What is Business Continuity / Disaster Recovery
 - ➔ Why Business Continuity / Disaster Recovery
 - ➔ Standard Methodology
 - ➔ Reference Technology
 - ➔ Process to be considered

EMC – Aligning, Innovating, Integrating



intelligent storage

Deep Integration

VM-Aware

Best In Class
Efficiency in
every dimension

Every Protocol

Every Scale

data protection

Deep Integration

Protect Files

Protect VMs

Protect Sites

Dedupe
Everywhere

resource management

Deep Integration

Service
Management

Operations
Intelligence

Automation and
Compliance

Discovery and
Mapping

information security

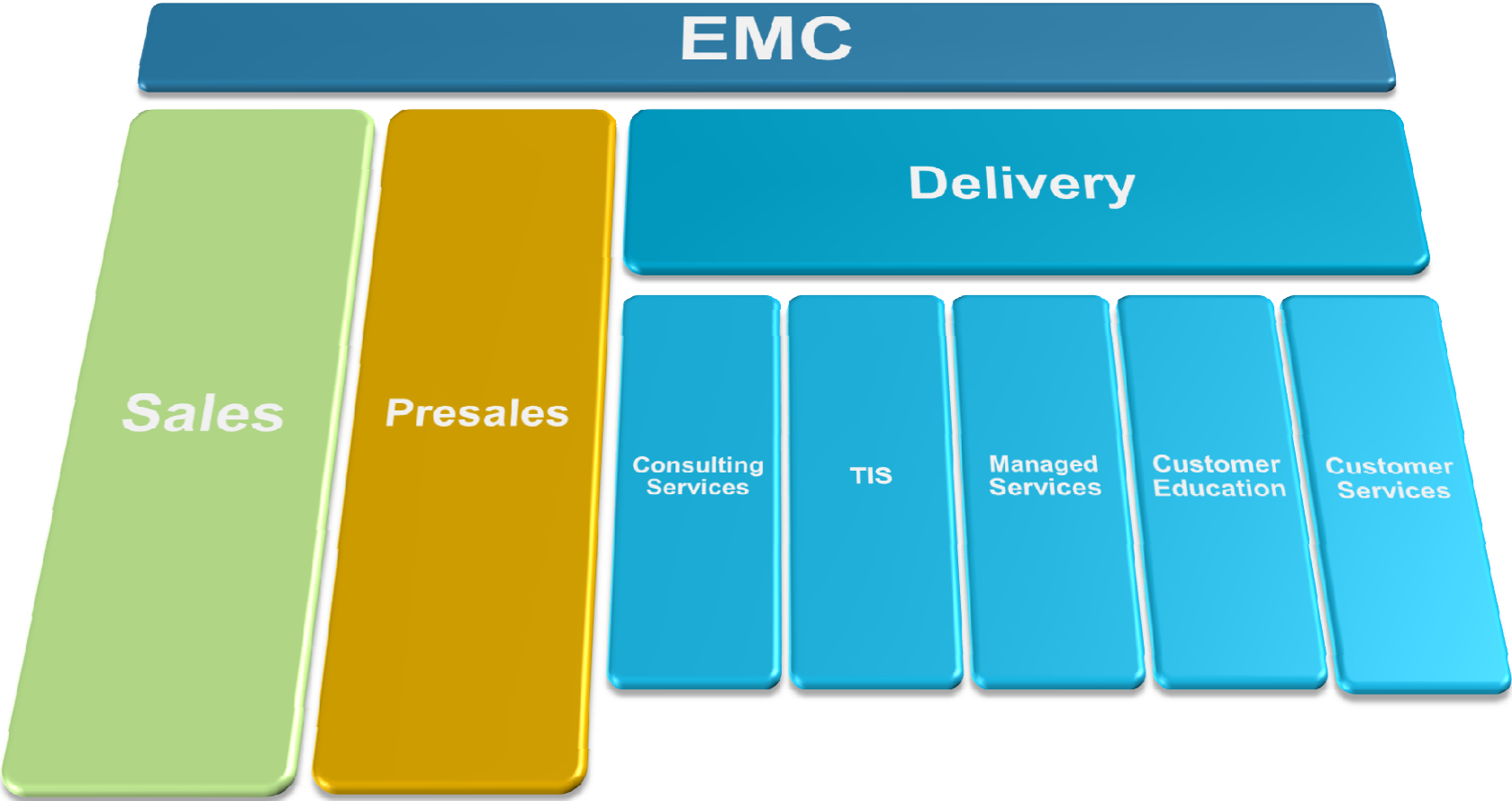
Deep Integration

Virtualize
Security

Secure
Virtualization

Leverage
Virtualization

EMC Italy Organization



➔ **What is BC/DR**

- ➔ Why Business Continuity / Disaster Recovery
- ➔ Standard Methodology
- ➔ Reference Technology
- ➔ Process to be considered

What is BC/DR



In case of disaster event a Company needs to consider:

- Loss of Human Resources (primary assets)
- Service Availability (revenue missing)
- Loss of Data (private or noticeable information)
- Economical Impact for Infrastructure (building and IT assets)

BC/DR definition



Business Continuity and Disaster Recovery is the whole activities to reduce damage to the Company Business due to the extended unavailability of Application or Data loss.

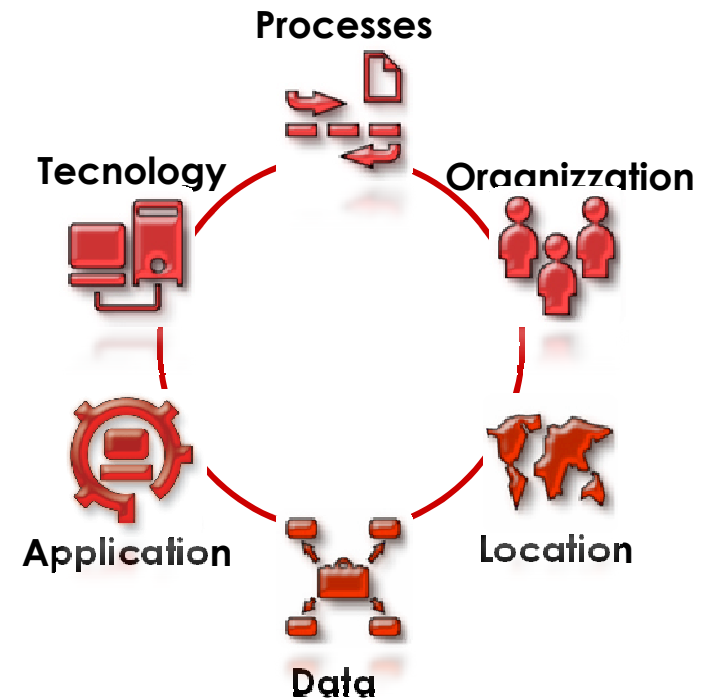
BC/DR consists of...

...**Technology and Process** to restore...

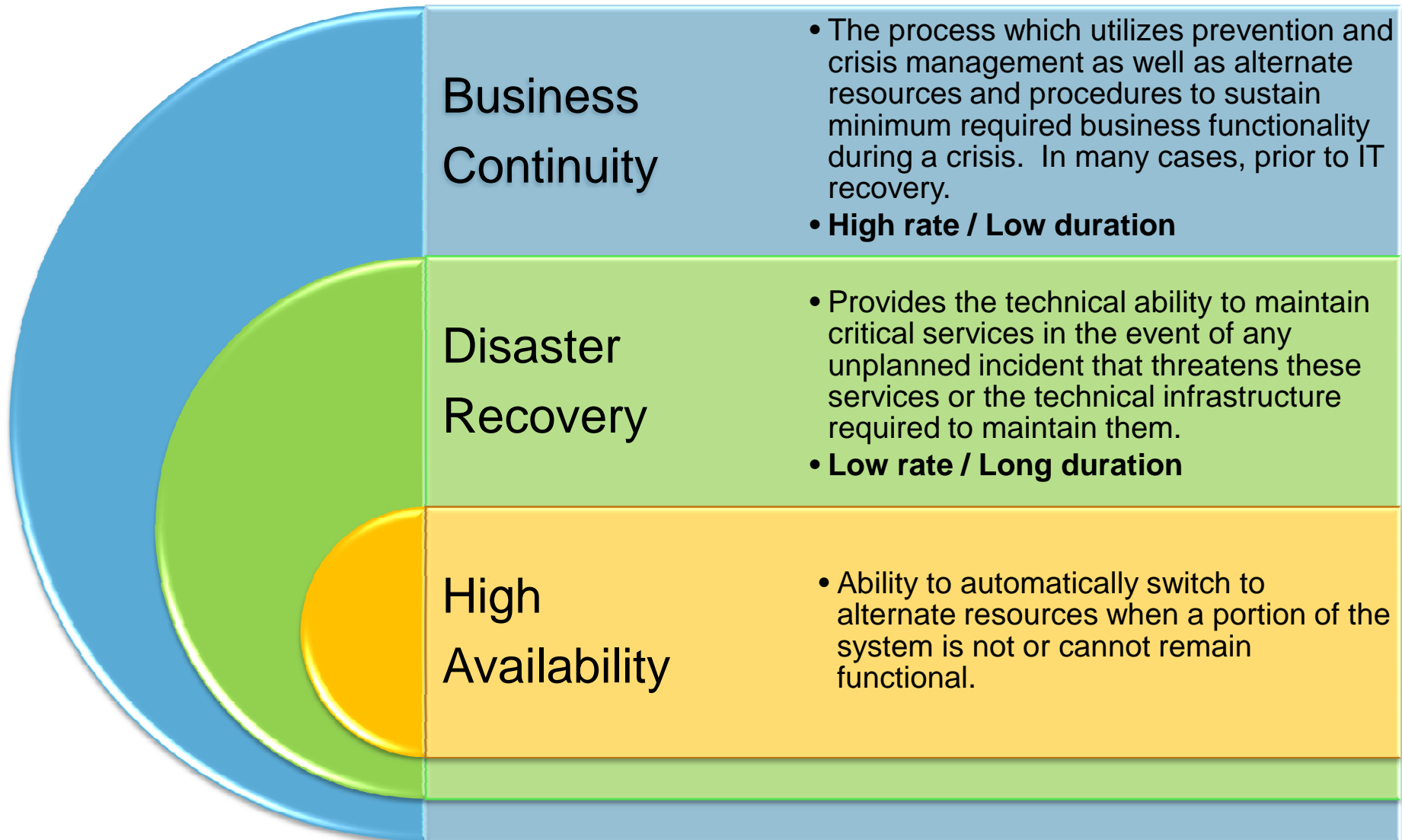
...**Application and Data** for the provisioning of...

...**Business Services** interrupted after a...

...serious Harmful Event (**Disaster**).



BC/DR definition



Agenda



→ What is BC/DR

→ **Why BC/DR**

→ Standard Methodology

→ Reference Technology

→ Process to be considered

Why BC/DR



70% of companies that suffer a major IT disaster without a valid recovery plan, fail within the next year. Of those that do survive, only 10% make a full recovery.

Gartner Group

A survey of 430 organisations revealed that 38% said application downtime costs them between £55,000 and £550,000 an hour, with 4% saying it was even more expensive than that.

Computer Weekly, 2004

- ➔ To minimize the interruption to critical business operations
- ➔ To limit the financial loss
- ➔ To avoid or minimize legal or regulatory problems
- ➔ To simplify the decision-making process during a stressful situation
- ➔ To provide for a controlled return to normal operations (fail-back)

Compelling Need for BC/DR



- In some industries, customers are insisting that their suppliers have viable Business Continuity Plans in place as a prerequisite to entering their Supply Chain
- Other industries (e.g. financial services) have regulatory demands that insist some level of Business Continuity is in place



Banca d'Italia defined “guidelines for operational continuity” for Italian Banks in order to identify actions and plans for DR implementation within 2006.

Basilea II is a regulation for international banking activities to promote suitability of the banks for credit risk and should be adopted within 2007.

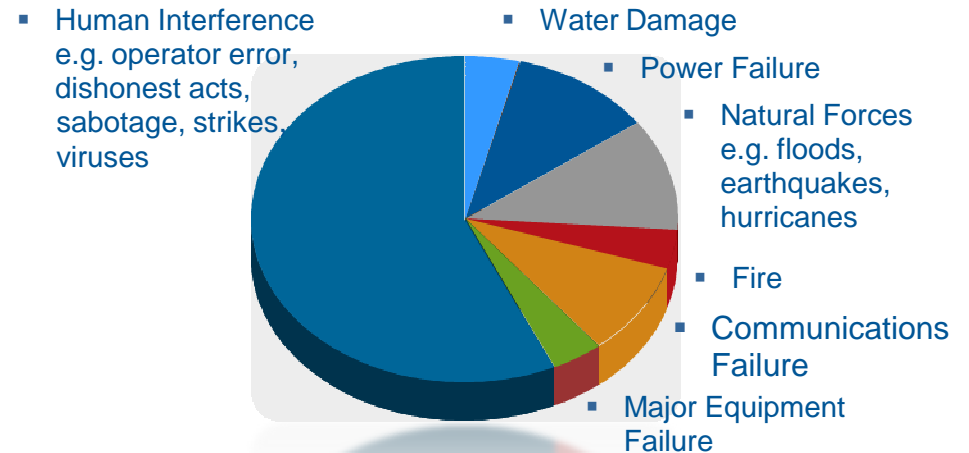
Residual Risk



BC/DR Management is concerned with managing risk to ensure that, at all times, an organisation can continue operating to a pre-determined minimum level.

- BC/DR Management objective is to minimize Operational Risk (financial, legal and reputation)
- Risk reduction through proper actions in order to minimize critical service interruption

Major Causes of Disruption



→ What is BC/DR

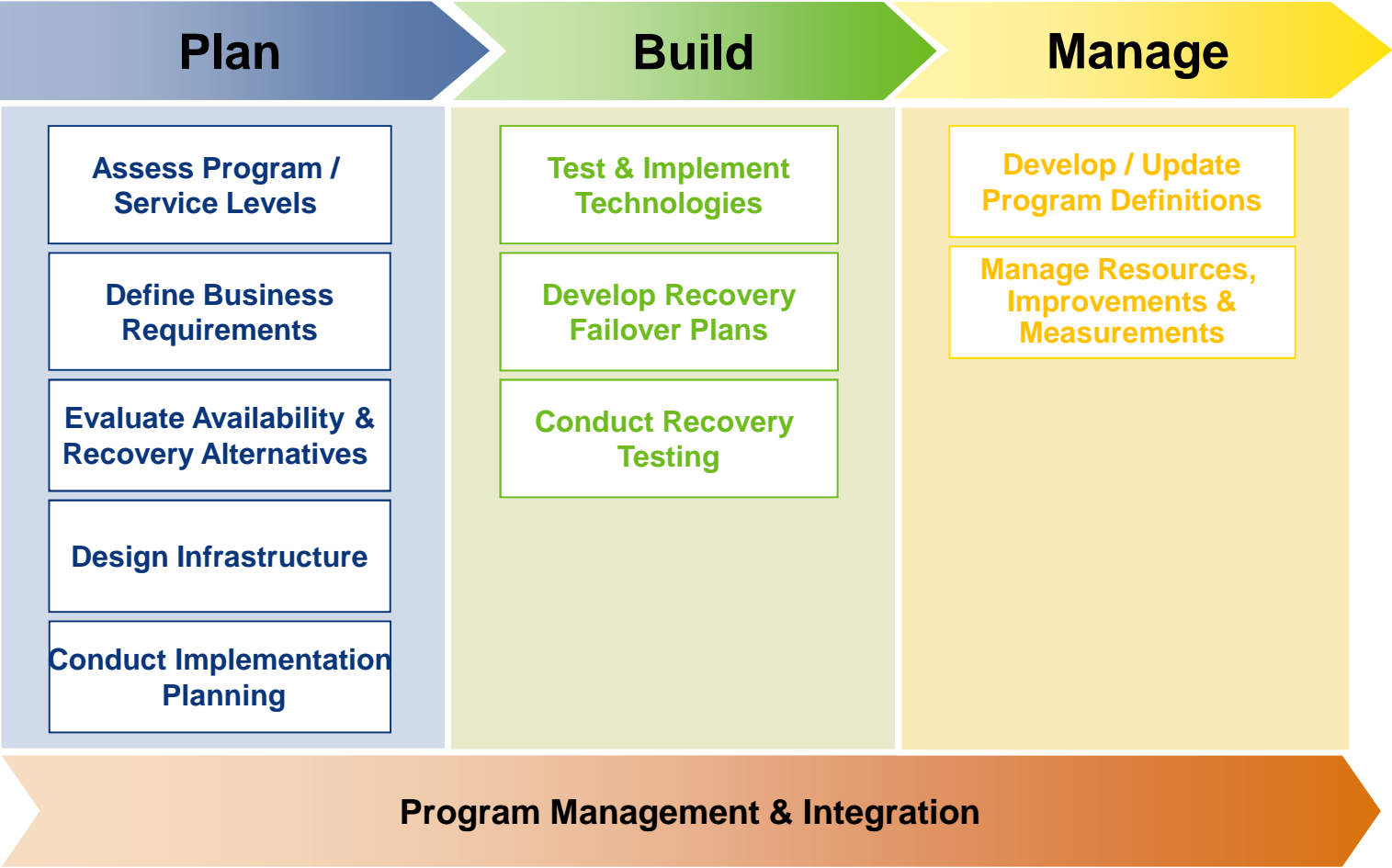
→ Why BC/DR

→ **Standard Methodology**

→ Reference Technology

→ Process to be considered

Methodology Framework

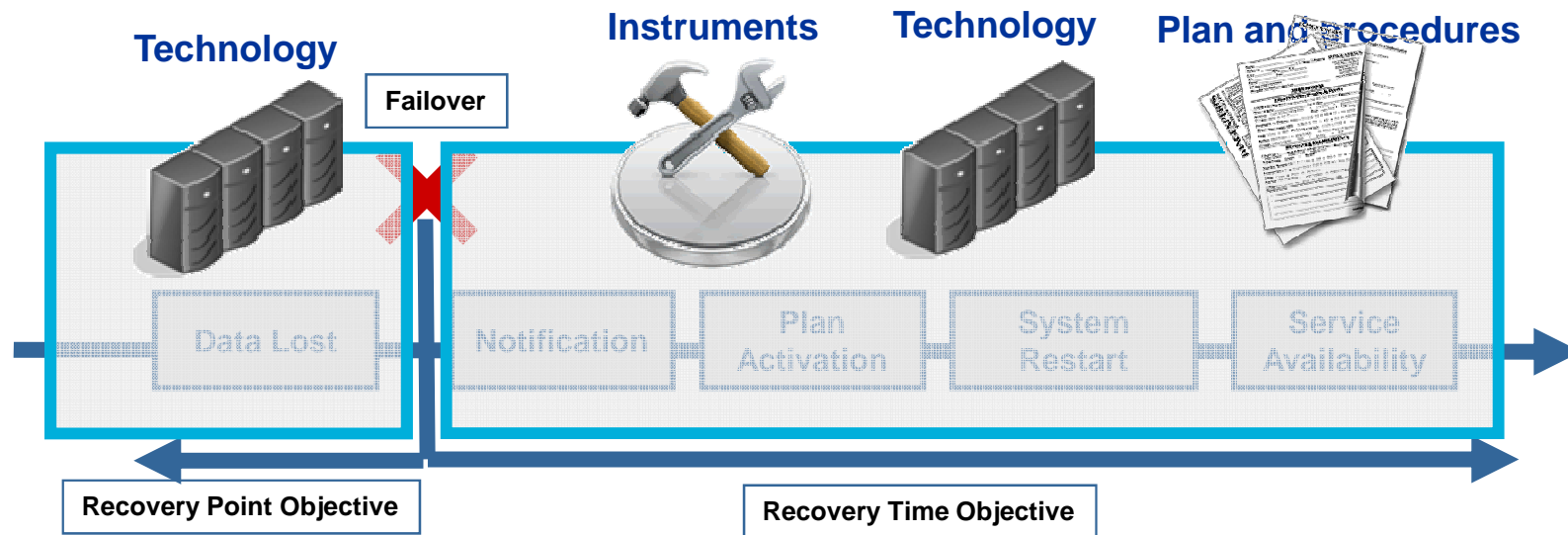


Key Performance Indicator

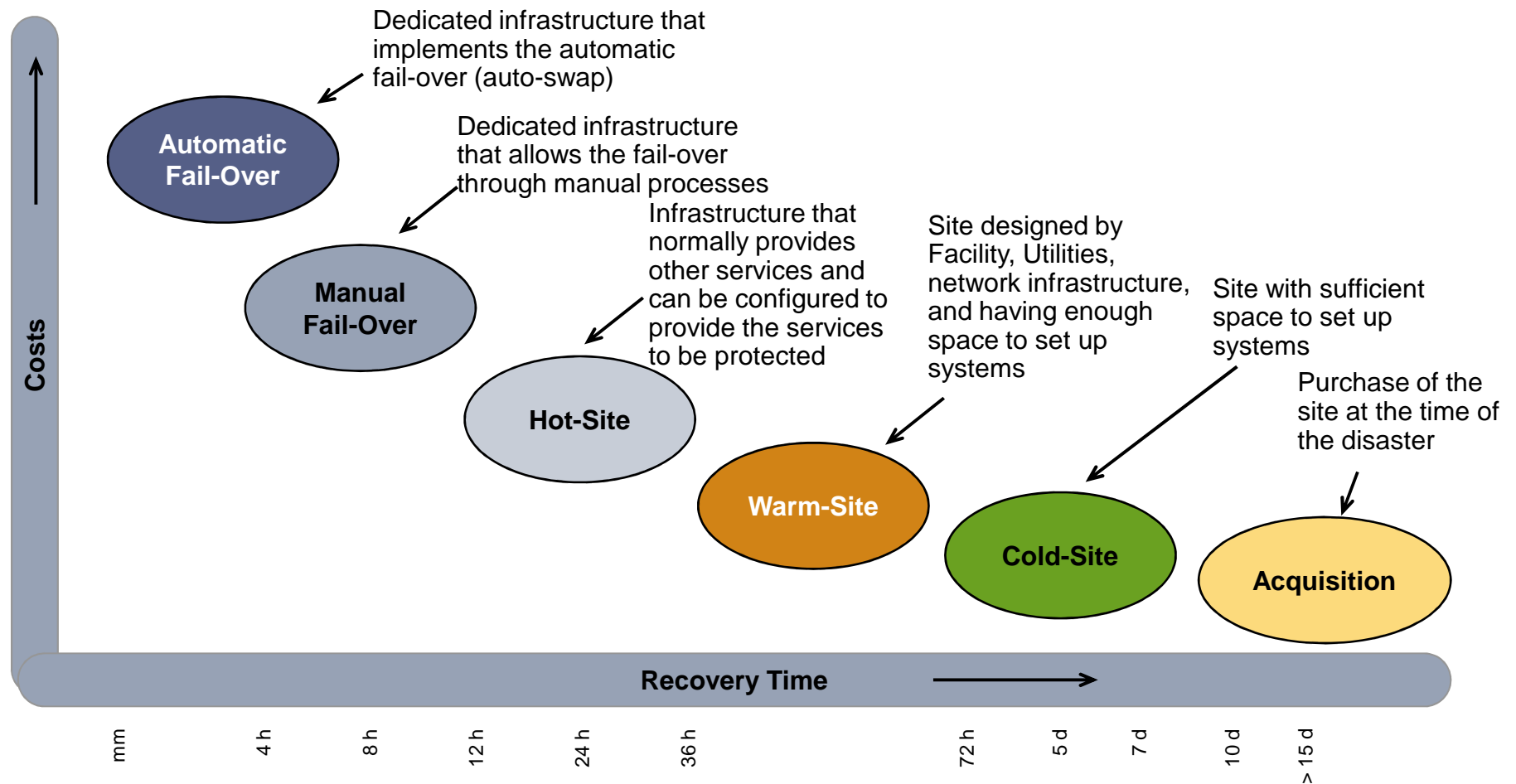


Business Requirements imply Technological Requirements:

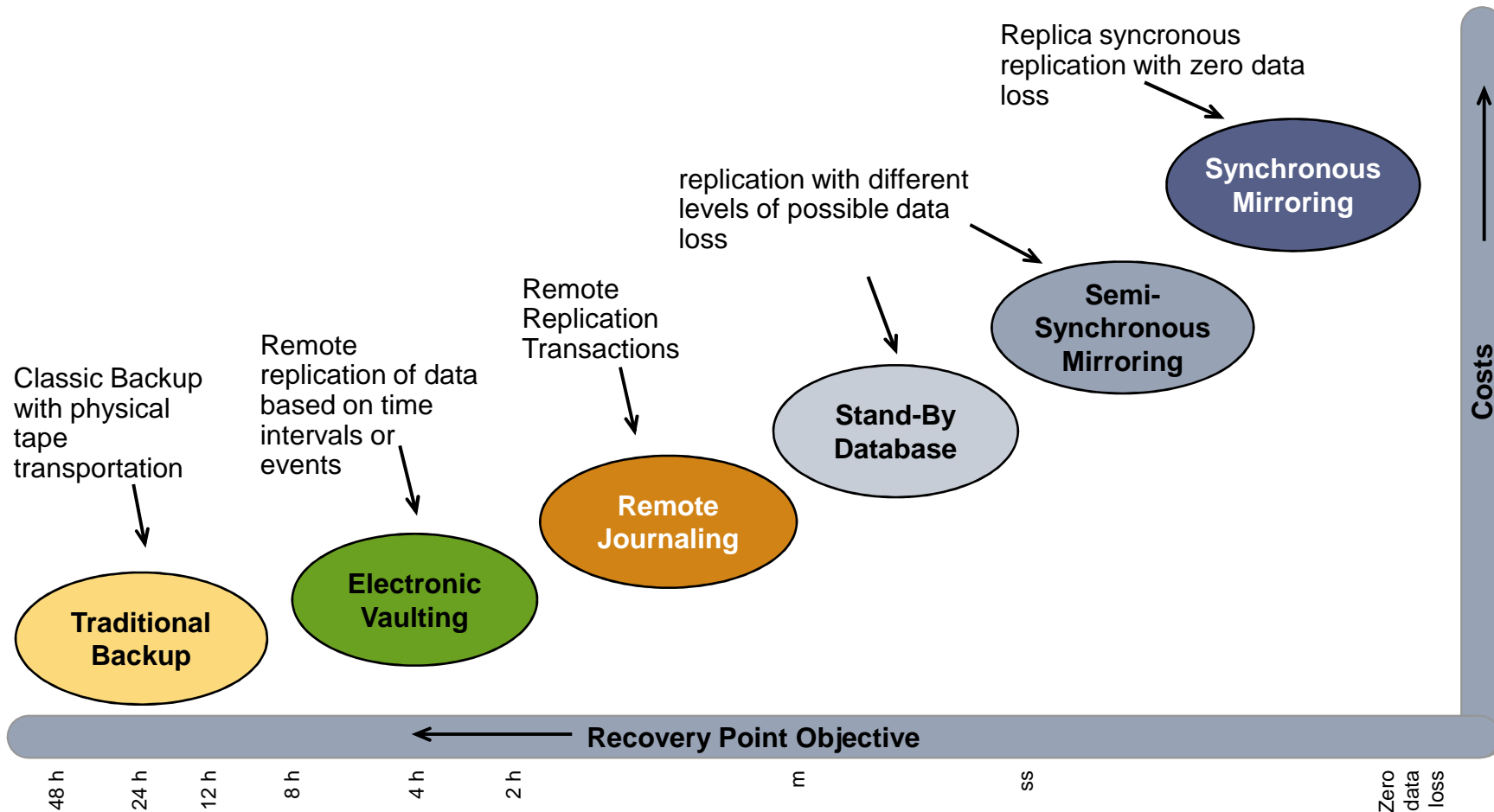
- **RTO** (Recovery Time Objective) = maximum acceptable time of systems unavailability after a disaster
- **RPO** (Recovery Point Objective) = maximum amount of data lost after a disaster



Different protection option considering Recovery Time Objective



Different protection option considering Recovery Point Objective

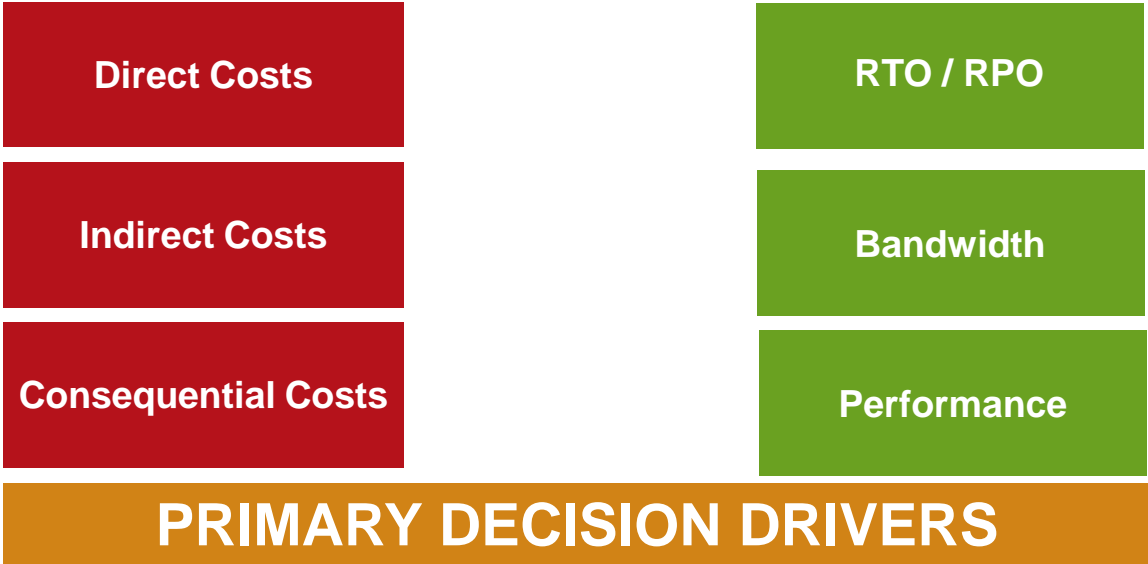


Decision Drivers to be considered



Down Time Costs

BC&DR Solution Costs



- What is BC/DR
- Why BC/DR
- Standard Methodology

→ **Reference Technology**

- Process to be considered

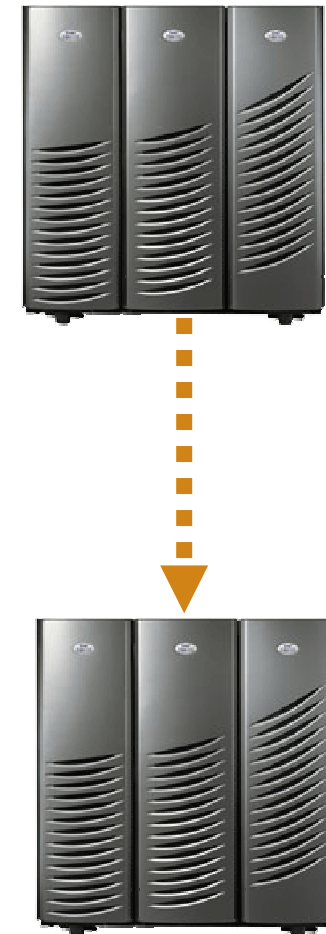
Techniques to reduce Service disruption risks



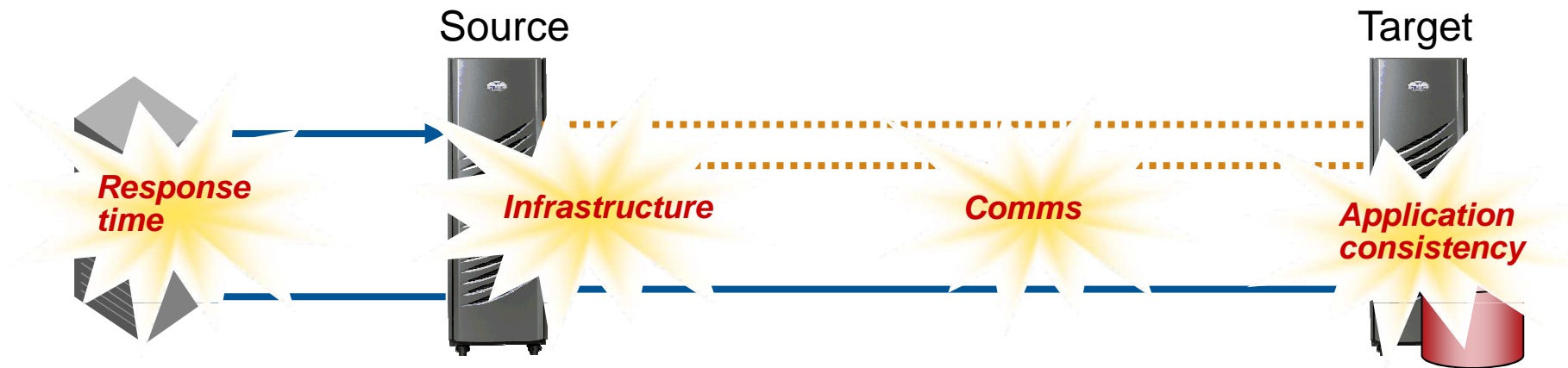
- Clustering
- Synchronous/Asynchronous Data Replication
- Virtualization
- Power Redundancy
- SAN access Redundancy
- ...

Synchronous/Asynchronous Data Replication

- Protect against local and regional site disruptions
- Provide near-instant recovery
- Migrate, consolidate or distribute data across storage platforms
- Enable non-stop operations



Remote Replication Pain Points



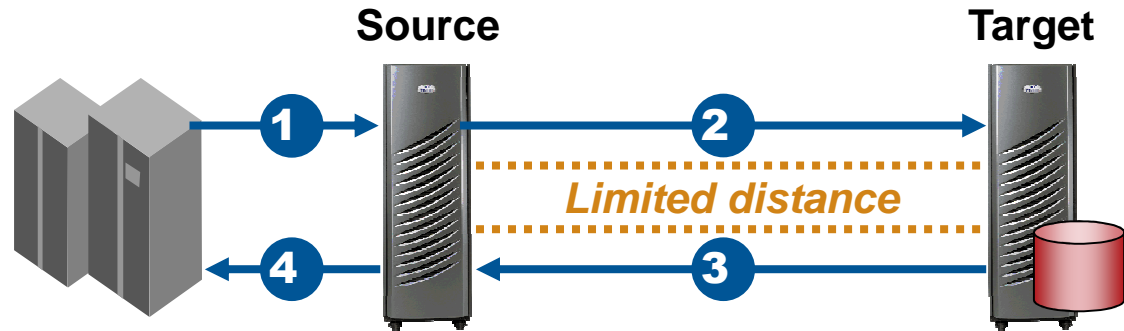
- **Response time**—Application impact of replication
- **Infrastructure**—Costs to enable solution
- **Communications**—Monthly line and bandwidth costs
- **Application consistency**—Application inter-dependency

Deployment Options to Fit Business Needs



Synchronous Replication

- No data exposure
- Some performance impact
- Limited distance



Asynchronous Replication

- Seconds of data exposure
- No performance impact
- Unlimited distance

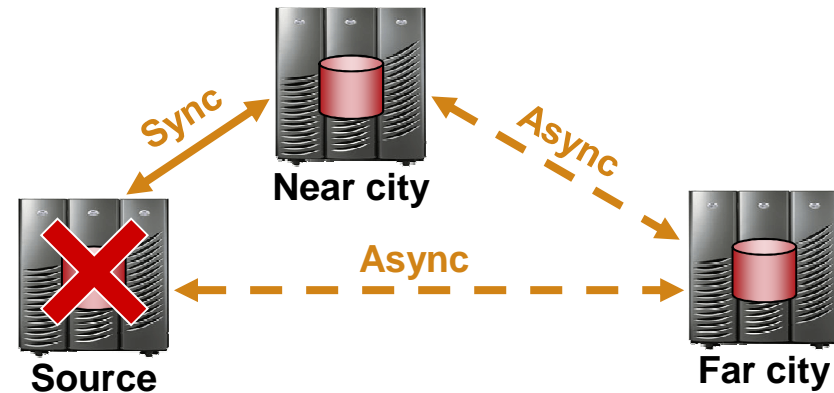


Deployment Options to Fit Business Needs



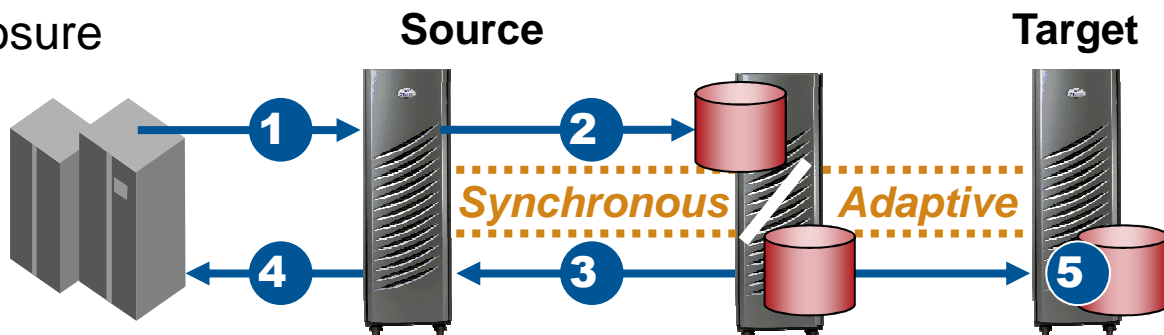
Multisite Replication

- No data loss on single point of failure
- Geographically dispersed protection
- Unlimited distance
- Ability to enable new Async between remote locations

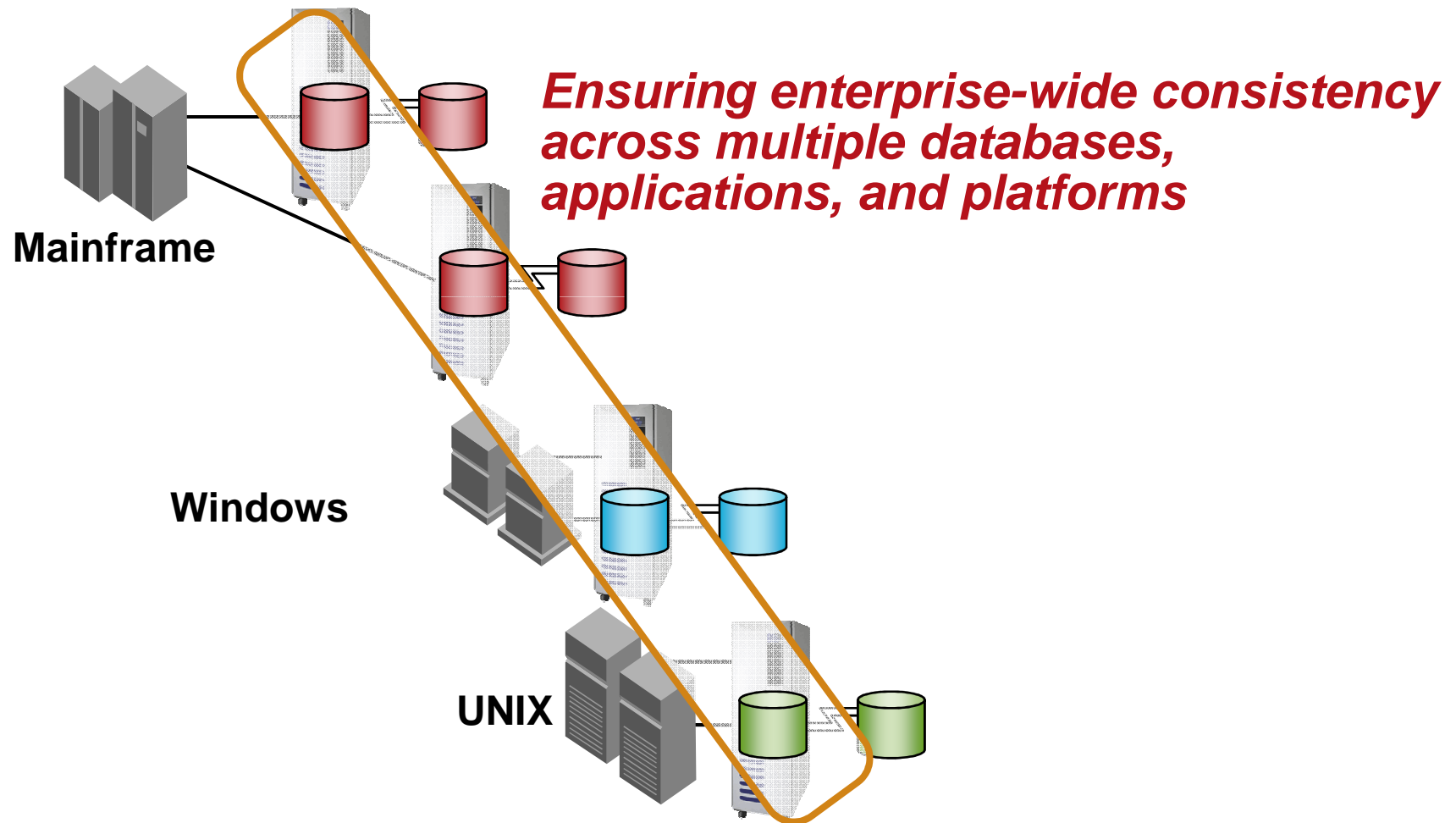


Multisite Replication

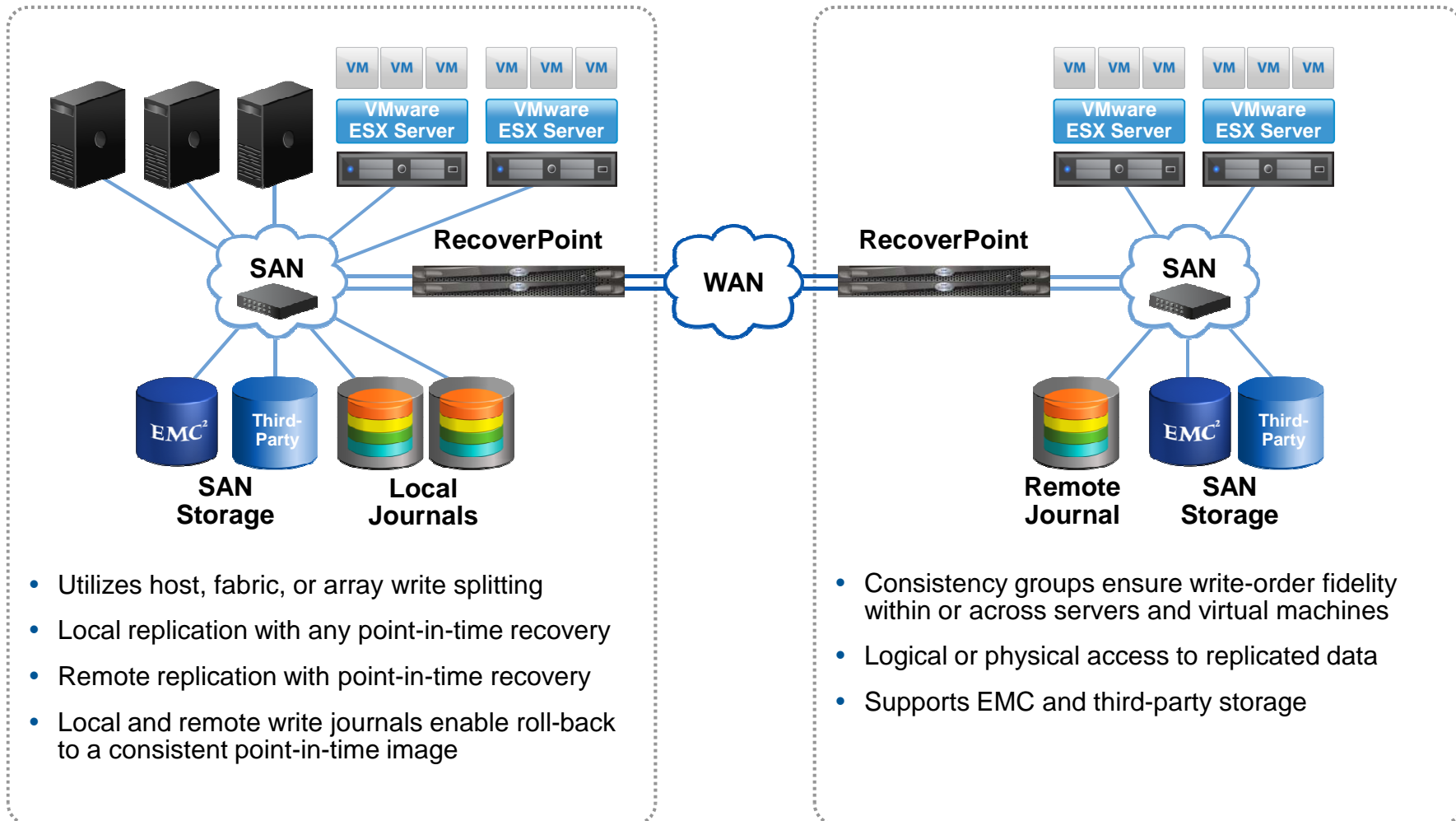
- Zero or hours of data exposure
- No performance impact
- Unlimited distance
- Requires BCVs



Achieving Enterprise-wide Consistency



Concurrent Local and Remote Data Protection



Agenda



- What is BC/DR
- Why BC/DR
- Standard Methodology
- Reference Technology

→ Process to be considered

- The **Business Continuity Management** is a strategic and tactical process that enables an organization to have an answer to any event and business interruption that may impact on business processes that contribute to "core business", ensuring a level of service minimum acceptable default.

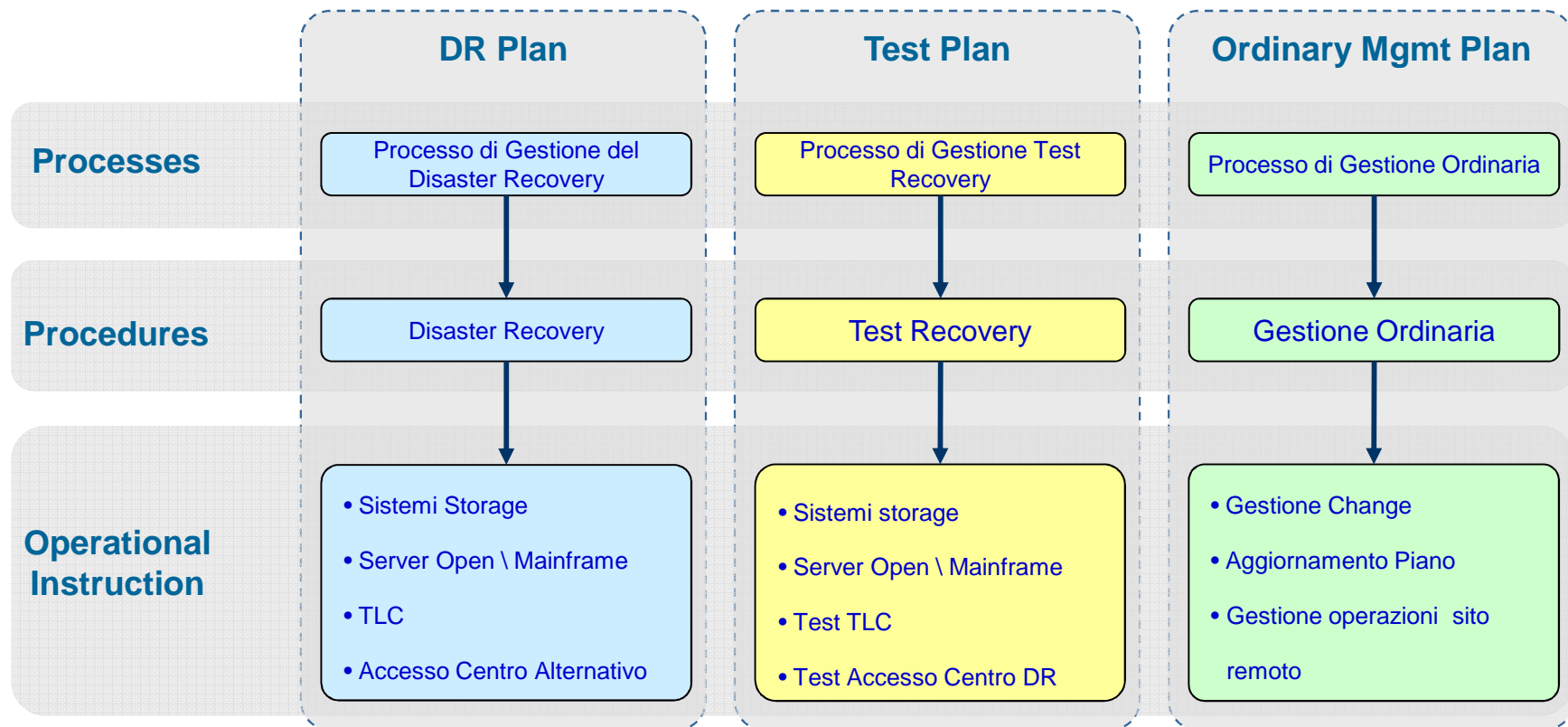


- **Disaster Recovery** is the set of processes and technologies capable of restoring systems, data and infrastructures necessary to service the core business in the face of serious emergencies (disasters).

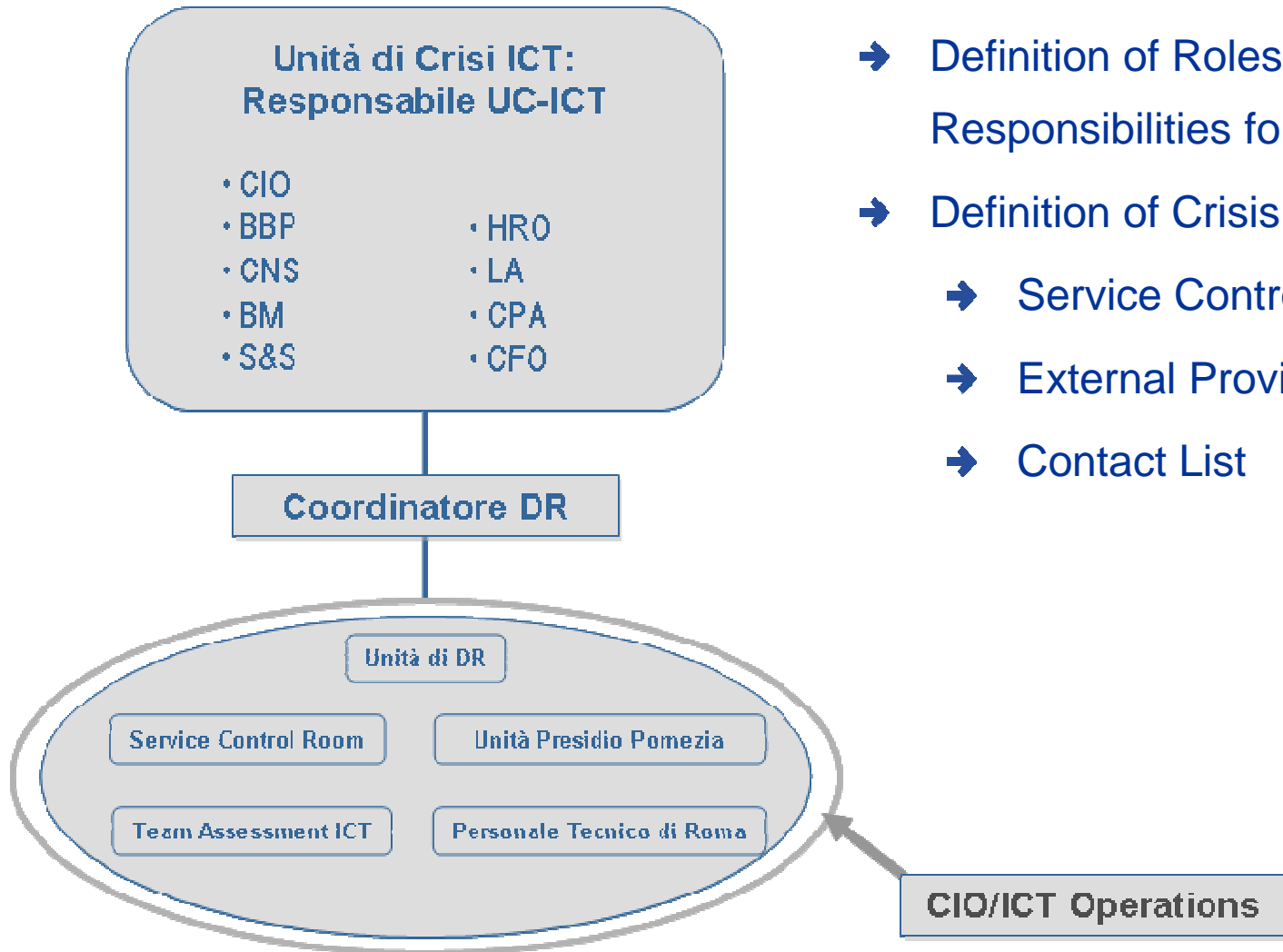
BCP Documentation



- ➔ DR Plan: management of real emergency situation
- ➔ Test Plan: periodical simulation of recovery
- ➔ Ordinary Management Plan: daily maintenance and solution check



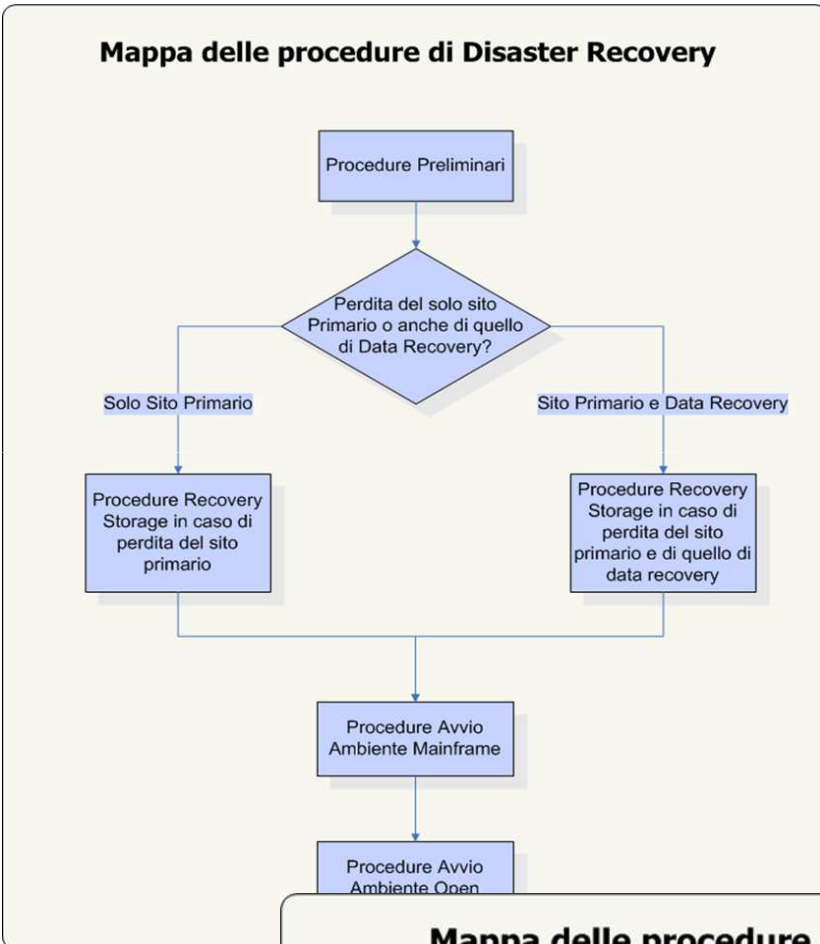
Example for Process



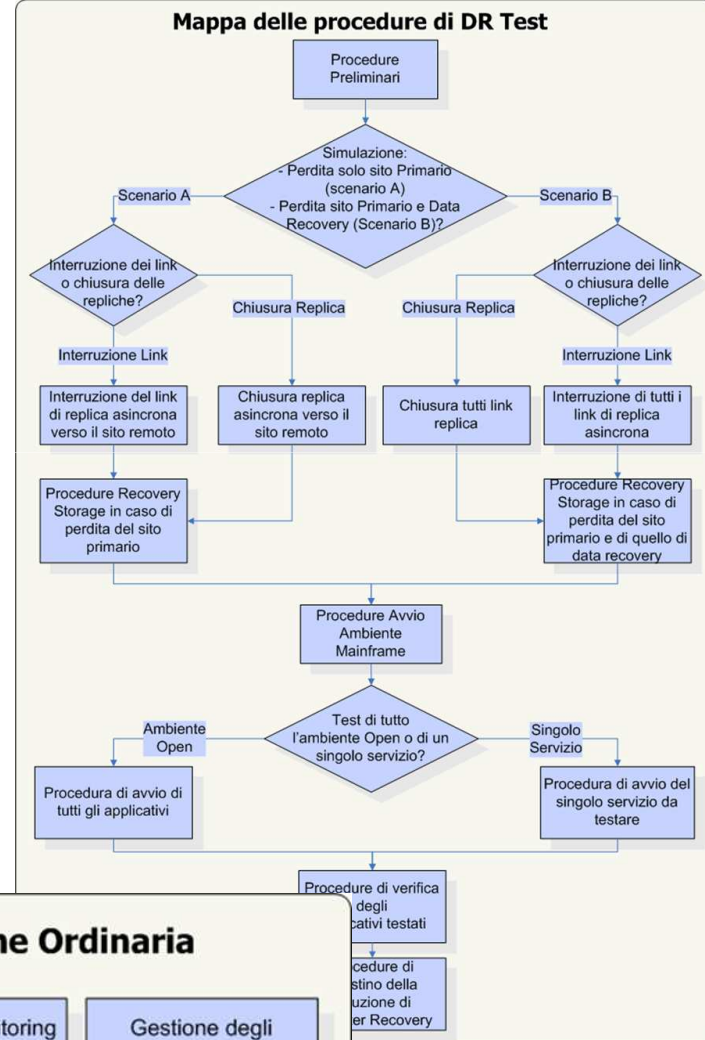
- ➔ Definition of Roles and Responsibilities for each activities
- ➔ Definition of Crisis Units
 - ➔ Service Control Room
 - ➔ External Providers
 - ➔ Contact List

Example for Procedures

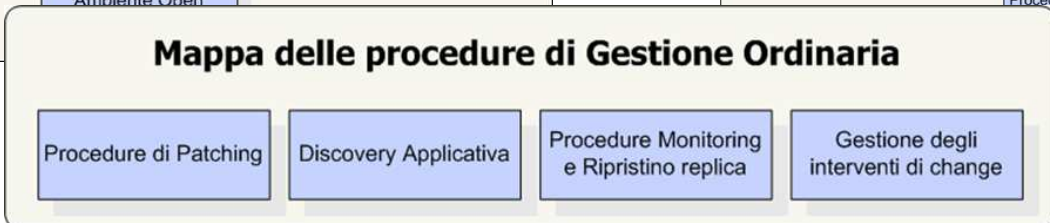
Mappe delle procedure di Disaster Recovery



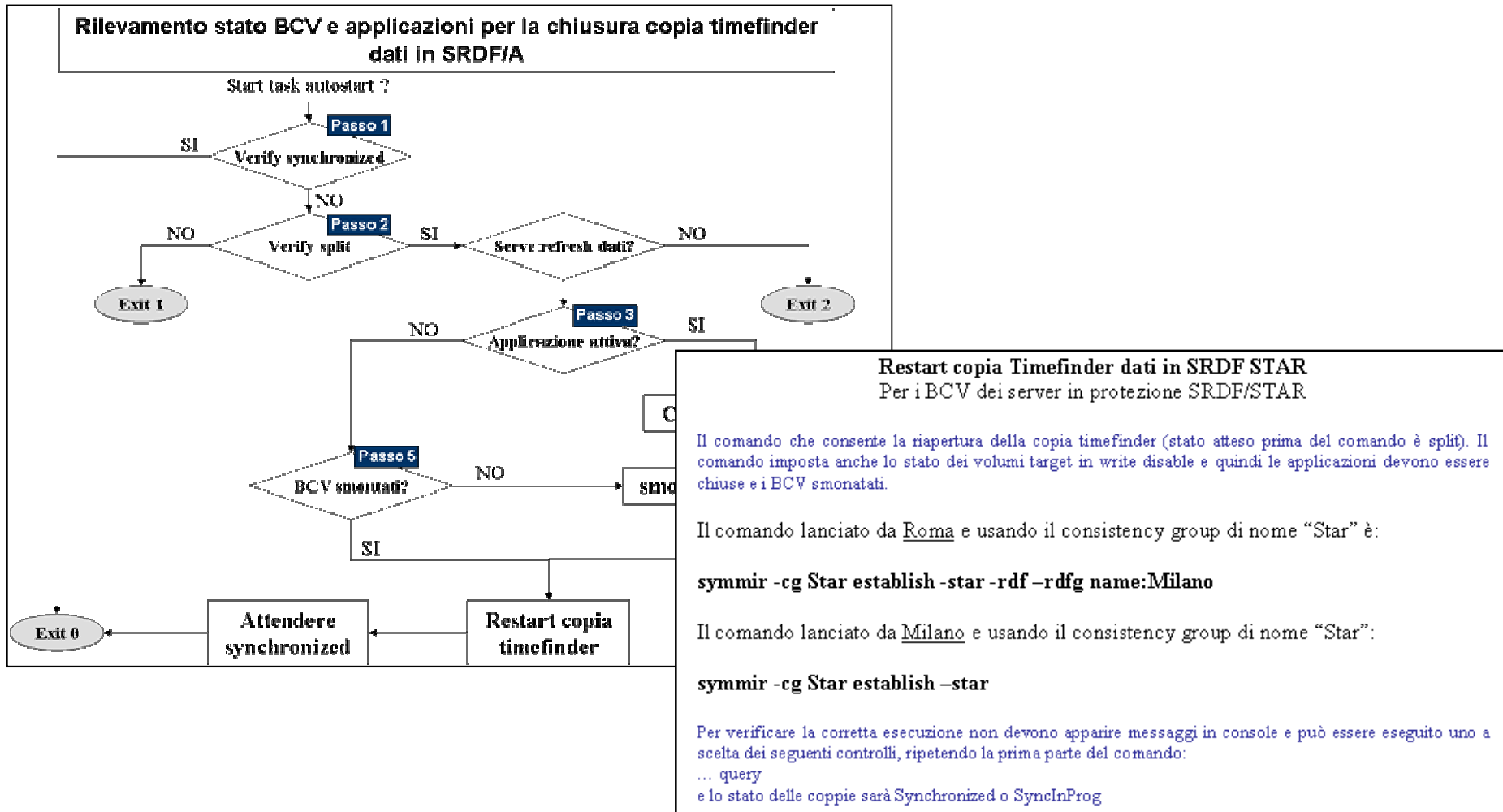
Mappe delle procedure di DR Test



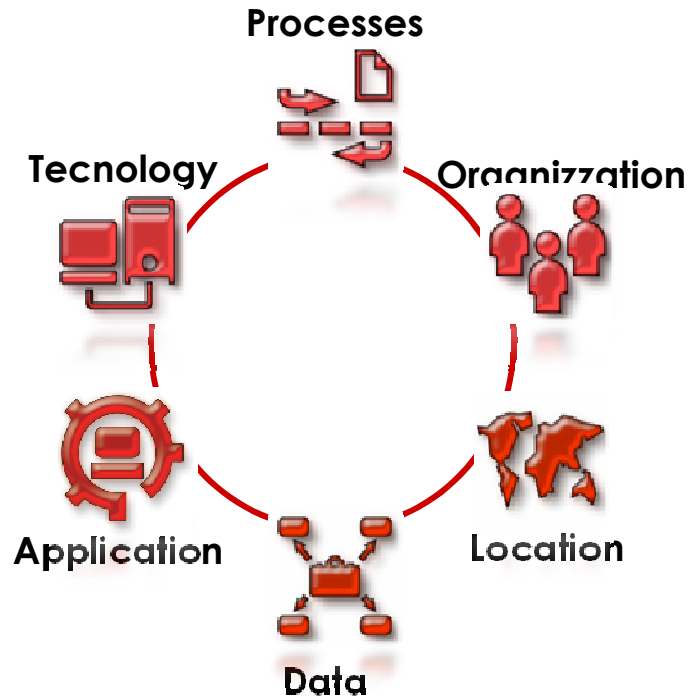
Mappe delle procedure di Gestione Ordinaria



Example for Operational Instructions



Summary



- Not “**una tantum**” but a continuous **Operational/ManagementProcess**
- It is not a **luxury** but a **need** for the Company

EMC²[®]

where information lives[®]