accenture

consulting | technology | outsourcing

Technology Consulting

Disaster Recovery Workshop – *Third Edition*

SECURITY
INFRASTRUCTURE
INFORMATION & DATA STRATEGY
social
big data
mobility
cloud
ENTERPRISE ARCHITECTURE & APPLICATION STRATEGY
IT STRATEGY

High performance. Delivered.

SAPIENZA
UNIVERSITÀ DI ROMA

Rome, 8th April 2013

Speaker: Attilio Di Lorenzo

Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

Accenture Portrait

Countries

120

Professionals

259.000

Dollars invested in Research & Development

400 million

High performance. Delivered.

Accenture is a global Management Consulting, Technology Services and Outsourcing Company, which combines in a unique way these specialized functional expertise with the experience and know-how of its professionals in different market sectors: Communications & High Tech, Financial Services, Products, Health & Public Service, Resources.

Knowledge, innovation and experience in Italy

Accenture is present in Italy since 1957, thanks to the efforts of a group of Italian entrepreneurs and managers, and relies on an international network for resources, skills and experience.

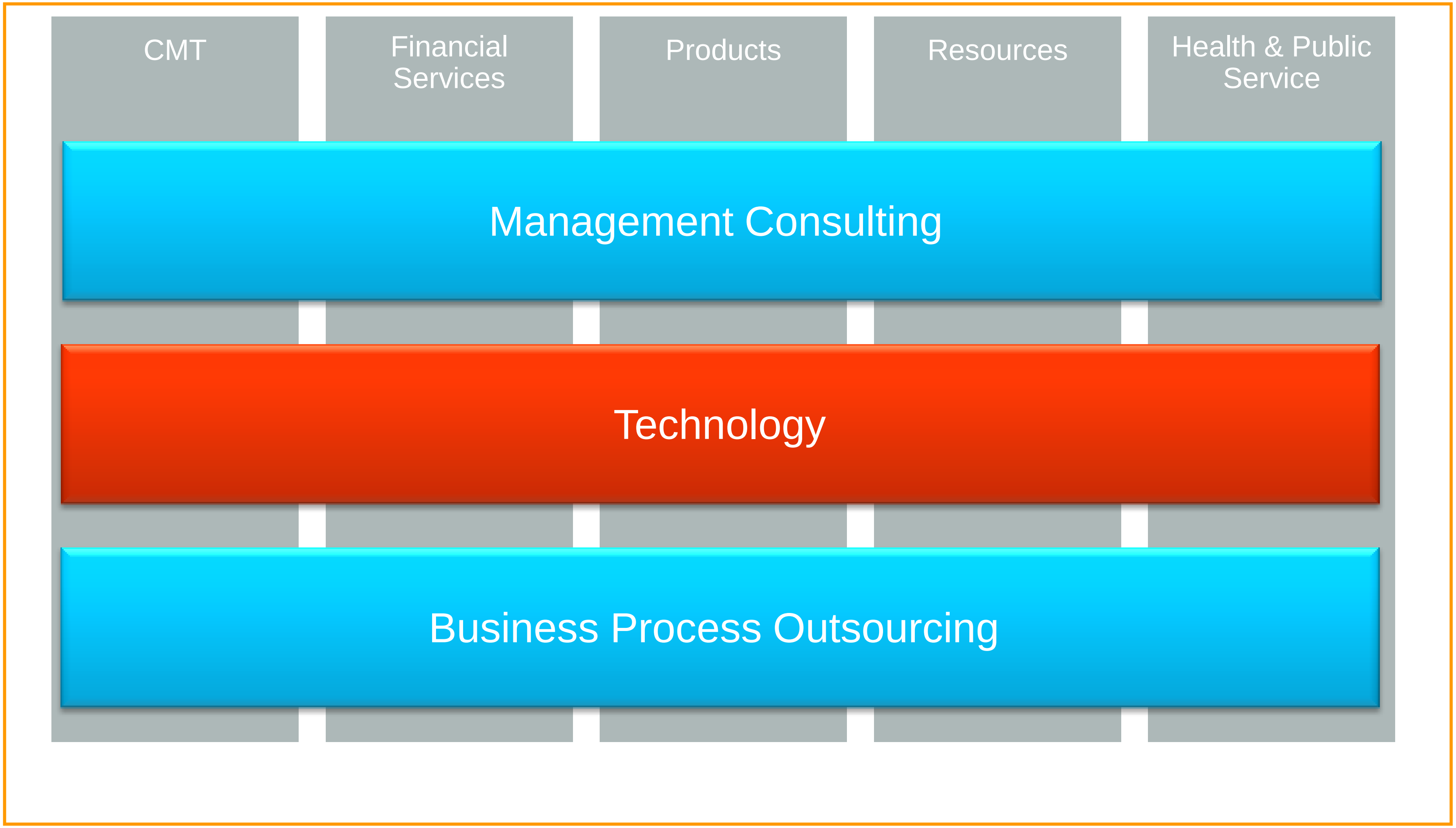
Today **Accenture** works in Italy for:

- **15** of the top 20 national financial groups
- the first **4** insurance companies
- **11** of the top 15 industrial groups

Accenture in fact funds service excellence to customers on the belief that the evolution of the organization is crucial to anticipate the needs of the market and be prepared to support change.

From September 2001 **Accenture Italia leads the IGEM Region**, a vast geographical area which includes Greece, Turkey, Middle East, Poland, Czech Republic, Slovakia, Hungary, Romania and Russia, accompanying the development through programs of transformation and innovation

Accenture Global Offering



CMT

Financial Services

Products

Resources

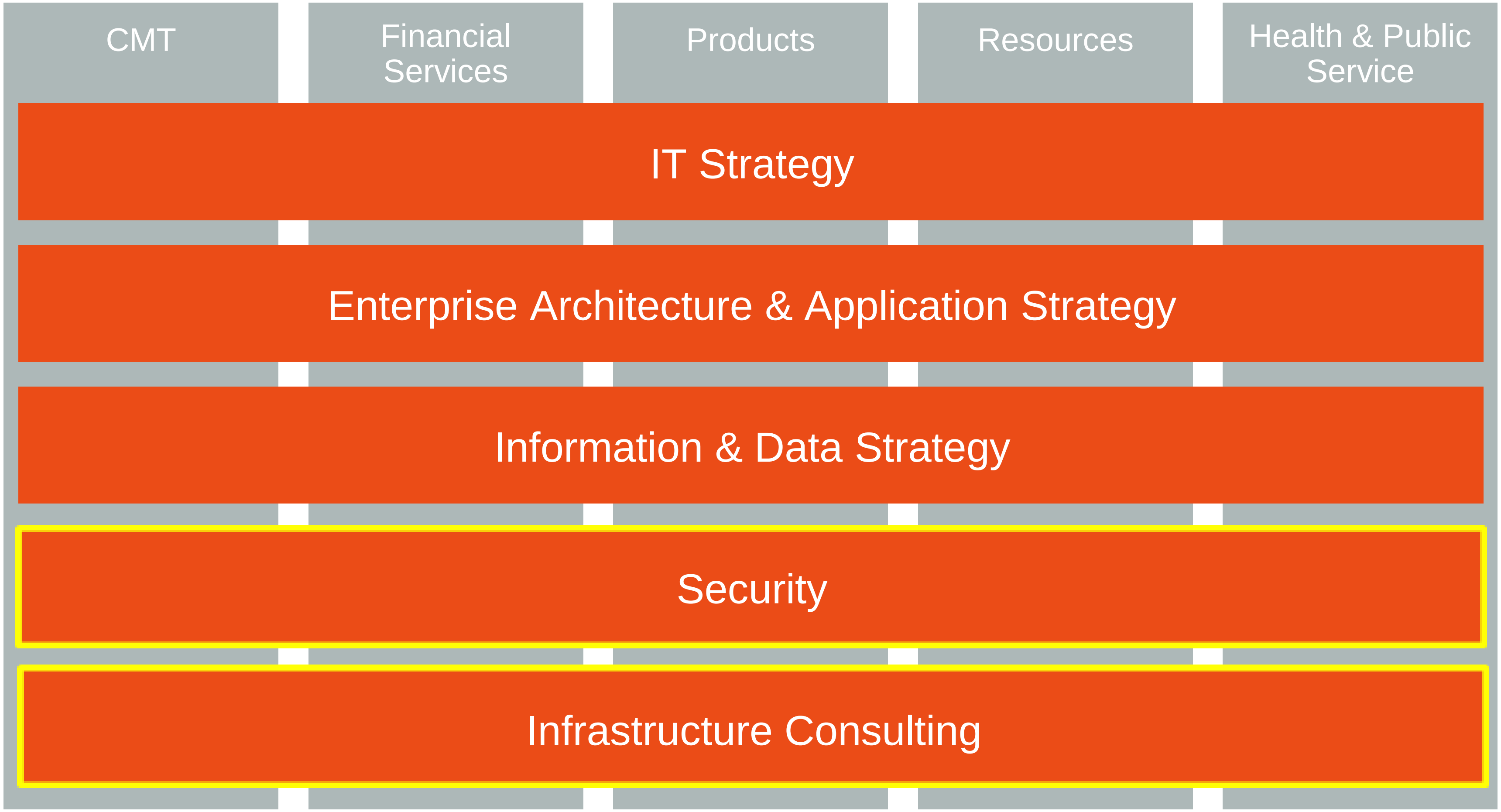
Health & Public Service

Management Consulting

Technology

Business Process Outsourcing

Our end-to-end portfolio of **Technology** services transforms IT and transforms how IT enables your business



CMT

Financial Services

Products

Resources

Health & Public Service

IT Strategy

Enterprise Architecture & Application Strategy

Information & Data Strategy

Security

Infrastructure Consulting

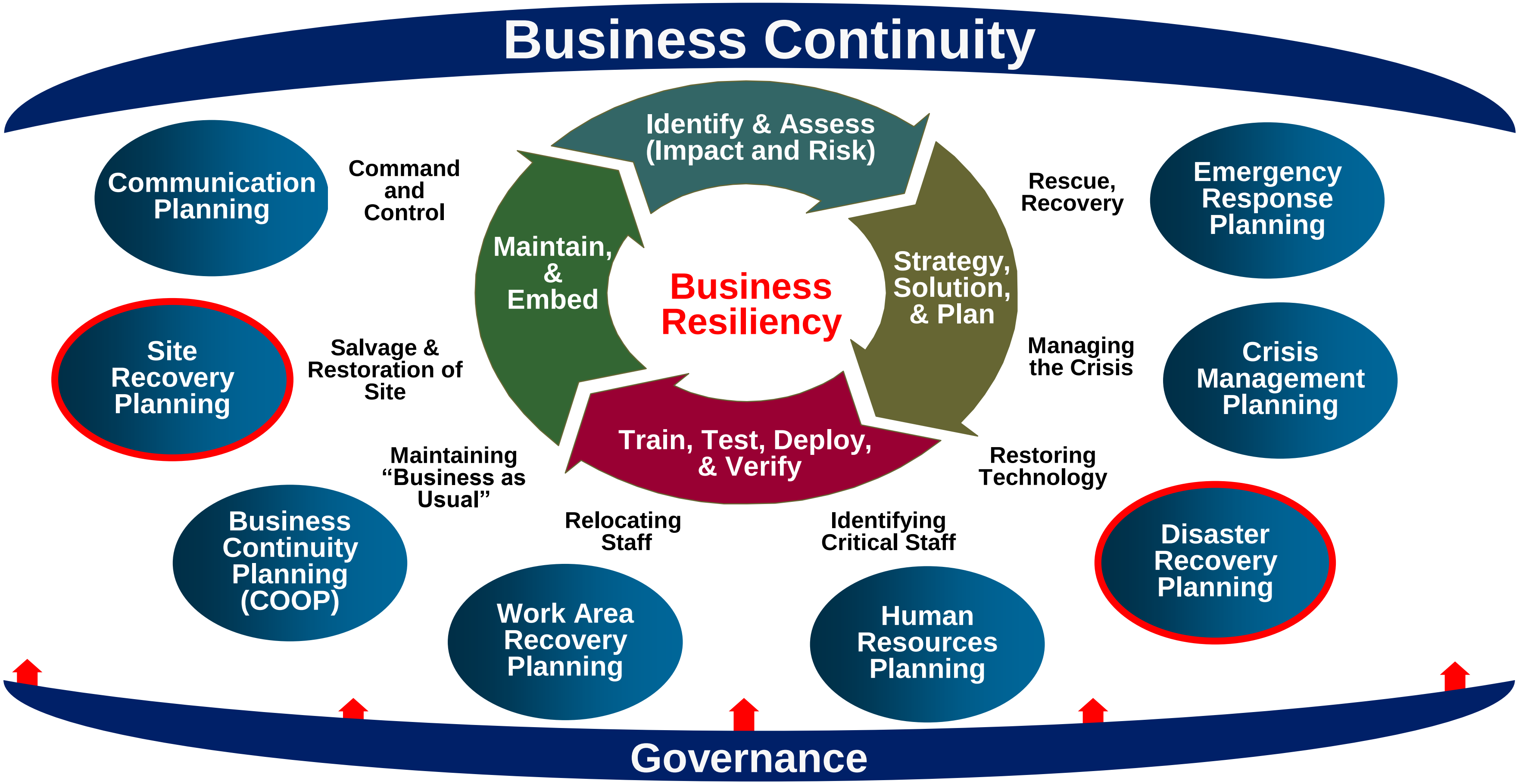
□ *Business Continuity e Disaster Recovery areas*

Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

BCDR program Approach

A strategy that meets the business objectives to continually assess and develop effective planning, testing, and recovery of critical services (People, Processes and Technology)


Business Continuity
Identify & Assess (Impact and Risk)
Strategy, Solution, & Plan
Train, Test, Deploy, & Verify
Maintain, & Embed
Business Resiliency
Communication Planning
Command and Control
Rescue, Recovery
Emergency Response Planning
Site Recovery Planning
Salvage & Restoration of Site
Managing the Crisis
Crisis Management Planning
Maintaining "Business as Usual"
Restoring Technology
Business Continuity Planning (COOP)
Relocating Staff
Identifying Critical Staff
Disaster Recovery Planning
Work Area Recovery Planning
Human Resources Planning
Governance

BC Procedures

Business Continuity procedures cover various aspects:

- **Business Recovery**: Recover critical business processes;
- **Business Contingency**: Procedures and workarounds in case of loss of an application (e.g. through manual processes);
- **Business Resumption**: Restart business as usual after a disruptive event.
- **Disaster Recovery**: Recover data and functionalities of critical computer applications;

This involves following Areas:

Information/Data

- Increased data availability
- Enhanced recovery times and storage management procedures
- Improved RPOs (Recovery Point Objectives)
- Enhanced transactional integrity
- Reduced potential for unauthorized/unplanned data loss
- “Critical” applications confirmed
- Application dependency map and its relationship to recovery is validated

Technology

- Smoother technology infrastructure recovery
- Appropriate RTOs
- Enhanced utilization of current technology infrastructure suites
- Identification of opportunities for potential technology refresh
- “Critical” processing platforms identified and quantified
- Technology rebuild matched to business restoration requirements

Telecommunications

- Increased network uptime capabilities
- Identification of network and continuity risks, as well as initiatives to fill identified gaps
- Assessment of current network capabilities and a determination of potential future needs
- Identification of Internet work-arounds for application access

Process

- Identification of processes truly needed in a disaster situation
- Functional process rebuild times established to guide technology recovery
- Process support requirements identified and quantified
- Third-party vendor recovery support requirements identified
- BCM integrated with change control, asset mgmt, help desk, etc.

People

- Identification of “critical” personnel for initial recovery activities
- Remote “work” capabilities identified
- Recovery team activities identified and integrated
- Declaration decision table developed
- Recovery plan maintenance plan developed and assigned across the organization

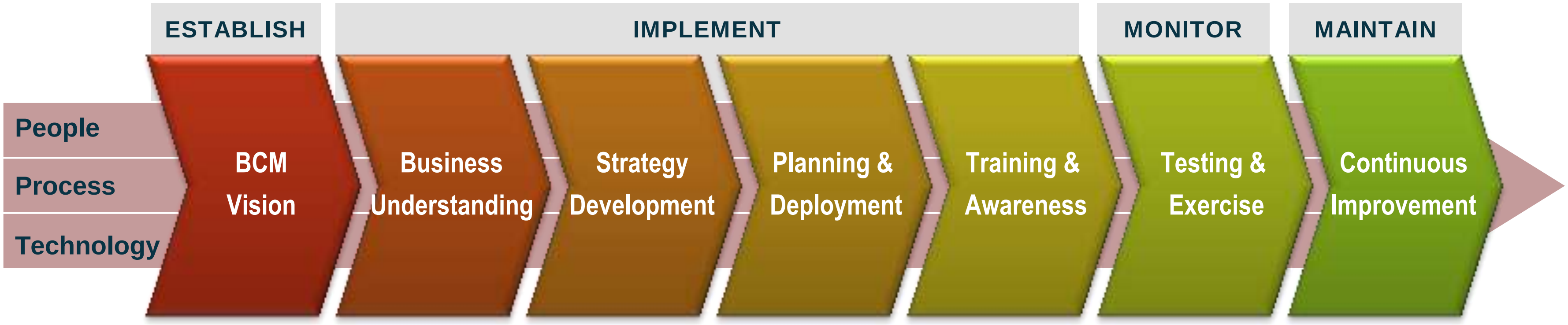
Facilities

- Operational and recovery gaps associated with current facilities are identified and quantified
- Data center ”tiering” is quantified and categorized
- Facility enhancement initiatives are identified
- Facility support drivers (i.e. MEP – mechanical (HVAC) , electrical and plumbing) gaps identified
- Facility recovery needs quantified

Accenture BC Methodology – Project Approach

Accenture's BCM Approach is designed to deliver the highest level of business value, and is aligned with industry standards. The methodology is iterative and repeatable.

Accenture BC Process



- **BCM Vision** and **Business Understanding** are phases where a Risk Assessment and Business Impact Analysis (BIA) are performed. These activities establish a baseline of business requirements from which future activities are aligned.
- **Strategy Development** and **Planning & Deployment** are the phases that will produce actionable plans in line with business requirements. In addition to creating documented plans, the capabilities needed to achieve those plans are procured.
- **Training & Awareness, Testing & Exercise,** and **Continuous Improvement** are ongoing activities to promote a continual state of preparedness to enable mitigation and recovery activities, if required. The opportunity to apply lessons learned into the process is another function of this phase.

Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

BC, DR and HA

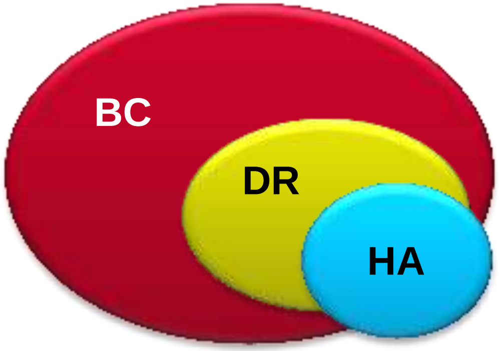
Business Continuity (BC) has historically been viewed as an Information Technology effort, with minimal input (or none at all) from Business Process owners. Recent events have proven this to be a defective planning model.

Minimizing Business Continuity risks requires thorough planning, using a Business Requirement-driven approach and a proven Business Continuity Planning methodology.

Business Continuity (BC): The process which utilizes prevention and crisis management as well as alternate resources and procedures to sustain minimum required business functionality during a crisis. In many cases, prior to IT recovery.

Disaster Recovery (DR) Provides the technical ability to maintain critical services in the event of any unplanned incident that threatens these services or the technical infrastructure required to maintain them.

High Availability (HA) Ability to automatically switch to alternate resources when a portion of the system is not or cannot remain functional.



Differences between BCP and DRP

Business Continuity Plan (BCP)	Disaster Recovery Plan (DRP)
• Focused on recovery of individual business processes, departments, functions, facilities, etc. *(revenue production and operational management)*	• Focused on recovery of enterprise information technology (IT) applications and supporting infrastructure *(support the business)*
• Recovery Time Objective (RTO) is typically measured in days or weeks … sometimes, months	• Recovery Time Objective (RTO) is typically measured in minutes or hours … sometimes, days
• Active business and IT participation	• Active IT participation with, normally, little to no business participation during an event
• Recovery addresses people, process and support technologies required to continue the business	• Recovery addresses enterprise data center/ computing, facility and support staff needs
• Continuity plans are usually by process, department, function and/or facility	• Recovery plans are usually by application suite, platform and/or data center facility

RTO and RPO Metrics

RPO

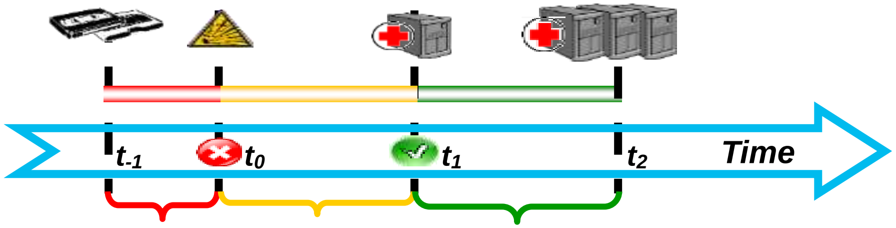
Maximum time accepted between last data backup on DR site and failure event. It consists in maximum time interval accepted for data loss.

RTO (min SLA)

Maximum time accepted for service recovery, starting from disaster declaration.

RTO (Normal Oper.)

Maximum time accepted for fixing infrastructure issue, and having back 100% of HW resources on DR site.



Interruption Window for Given Business Process

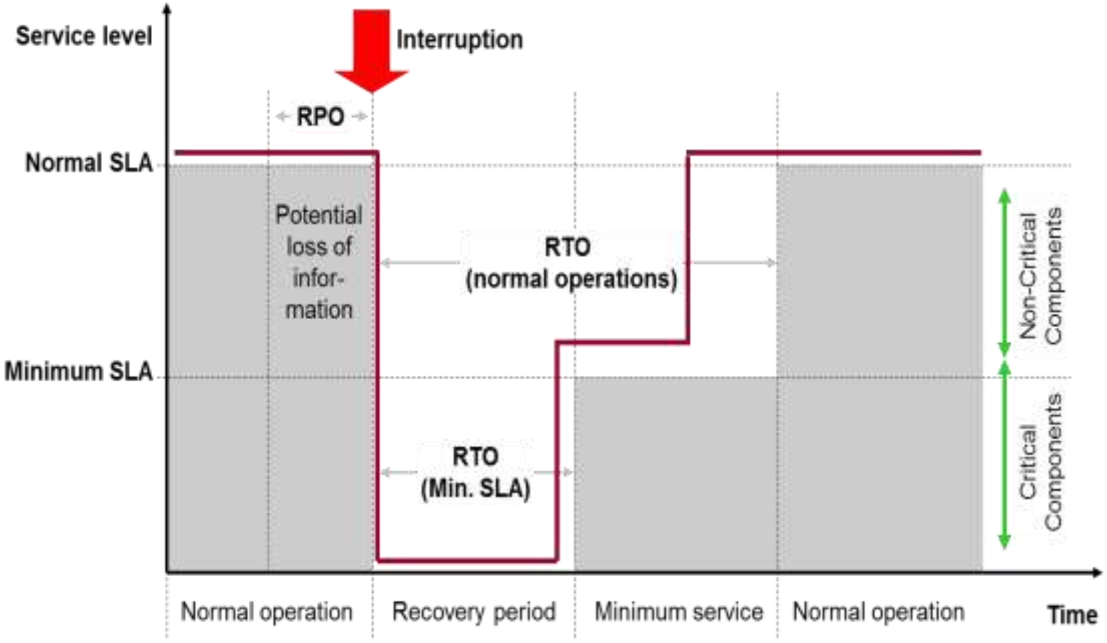


Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

Reality of Disasters

It’s not as impossible as it may seem…

Structural damages affecting immediate work areas and/or infrastructure (Level 2)

Natural disasters affecting a city or community (Level 3)

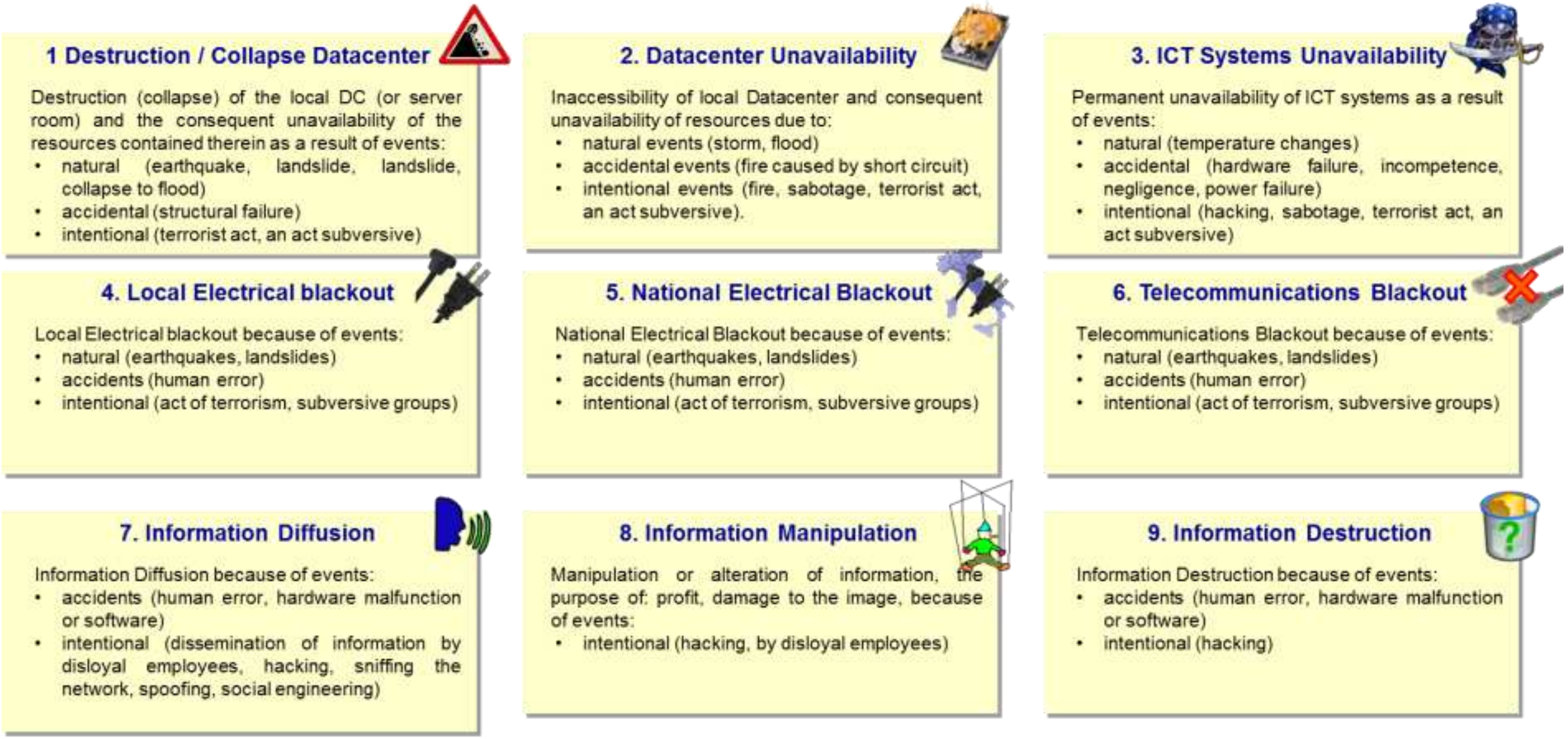
Socio-political unrest affecting certain parts or the whole country (Level 4)

Defining an IT disaster situation

- Disaster is any unplanned occurrence that substantially disrupts the operation of most or all the Applications and prevents users from performing their business functions.
- Many disasters (fire, plane crash, flood, earthquake, etc.) include physical damage and/or loss of the computer/networking hardware and/or IT personnel supporting the systems.
- Conditions that are not considered a disaster are: server failure, software issues, temporary network outage, bug on software, etc.
- The common thread is that the disaster is not a planned event (such as an upgrade) and gets in the way of the users performing the work they normally do with the application.
- In the case of background or utility applications that have no direct human users, a disaster prevents the company from enjoying the benefits of proper execution of all the applications.
- For example, these types of applications include the Internet transaction servers or fax servers. These supporting systems are critical to enable general processes to work. Furthermore, a disaster is something that does not commonly occur and for which extraordinary procedures are warranted.

Disaster Recovery Scenarios

The study of disaster recovery have been identified and proposed the following scenarios of disaster:



1 Destruction / Collapse Datacenter

Destruction (collapse) of the local DC (or server room) and the consequent unavailability of the resources contained therein as a result of events:

- natural (earthquake, landslide, landslide, collapse to flood)
- accidental (structural failure)
- intentional (terrorist act, an act subversive)

2. Datacenter Unavailability

Inaccessibility of local Datacenter and consequent unavailability of resources due to:

- natural events (storm, flood)
- accidental events (fire caused by short circuit)
- intentional events (fire, sabotage, terrorist act, an act subversive).

3. ICT Systems Unavailability

Permanent unavailability of ICT systems as a result of events:

- natural (temperature changes)
- accidental (hardware failure, incompetence, negligence, power failure)
- intentional (hacking, sabotage, terrorist act, an act subversive)

4. Local Electrical blackout

Local Electrical blackout because of events:

- natural (earthquakes, landslides)
- accidents (human error)
- intentional (act of terrorism, subversive groups)

5. National Electrical Blackout

National Electrical Blackout because of events:

- natural (earthquakes, landslides)
- accidents (human error)
- intentional (act of terrorism, subversive groups)

6. Telecommunications Blackout

Telecommunications Blackout because of events:

- natural (earthquakes, landslides)
- accidents (human error)
- intentional (act of terrorism, subversive groups)

7. Information Diffusion

Information Diffusion because of events:

- accidents (human error, hardware malfunction or software)
- intentional (dissemination of information by disloyal employees, hacking, sniffing the network, spoofing, social engineering)

8. Information Manipulation

Manipulation or alteration of information, the purpose of: profit, damage to the image, because of events:

- intentional (hacking, by disloyal employees)

9. Information Destruction

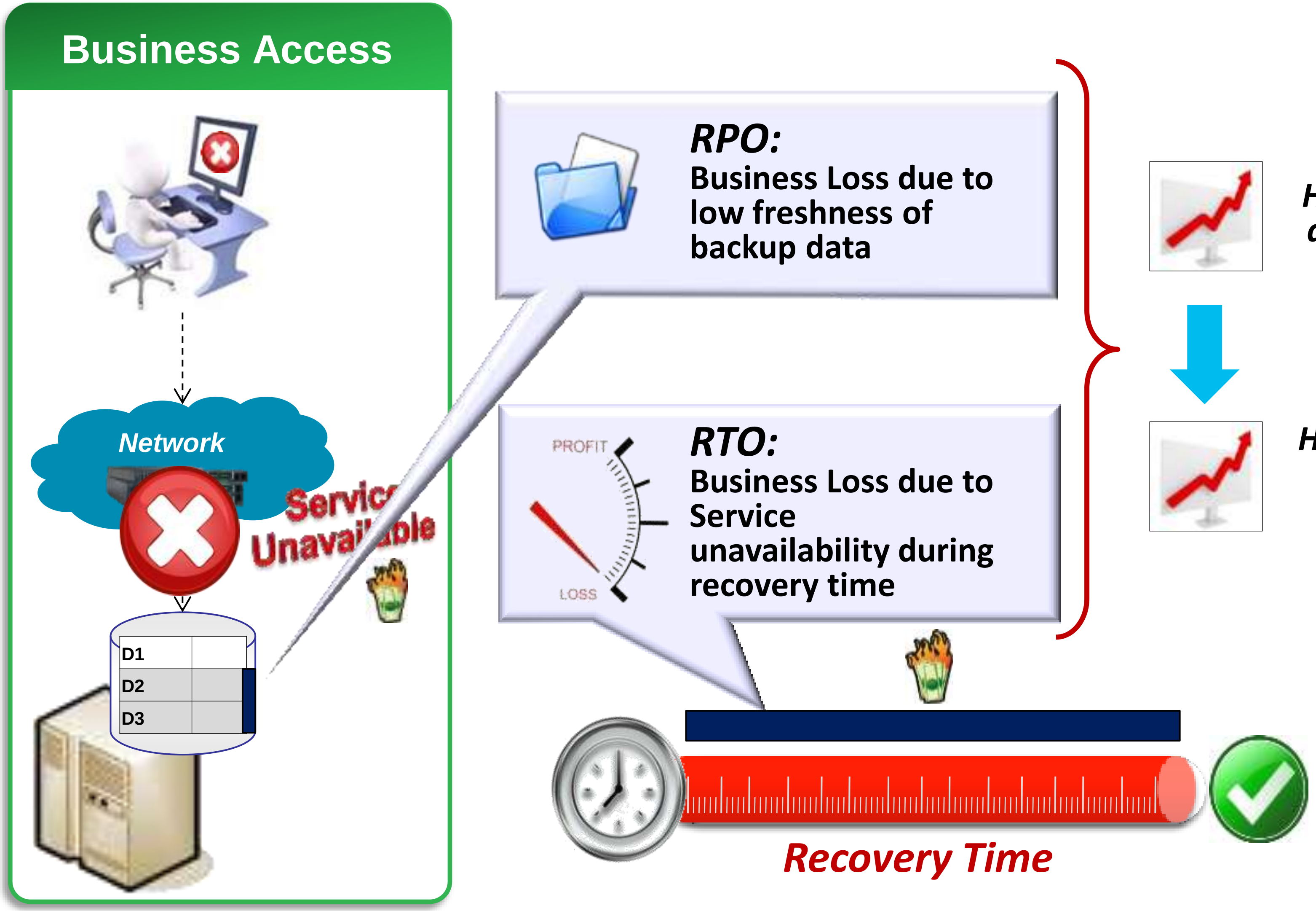
Information Destruction because of events:

- accidents (human error, hardware malfunction or software)
- intentional (hacking)

Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

Disaster from Business PoV



Business Access

RPO:
Business Loss due to low freshness of backup data

RTO:
Business Loss due to Service unavailability during recovery time

High RTO and RPO

High loss of Business revenue

Recovery Time

Disaster from IT PoV

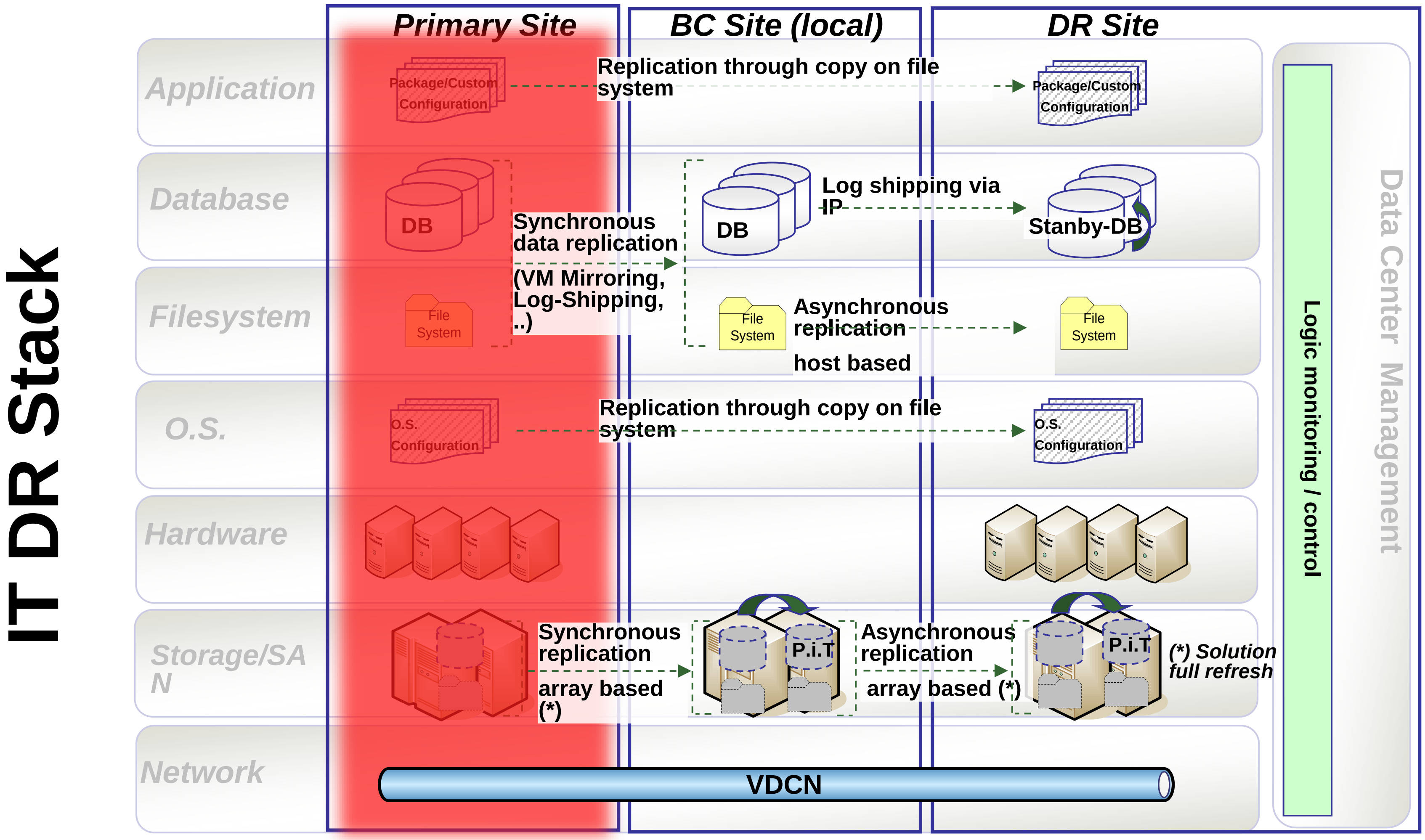
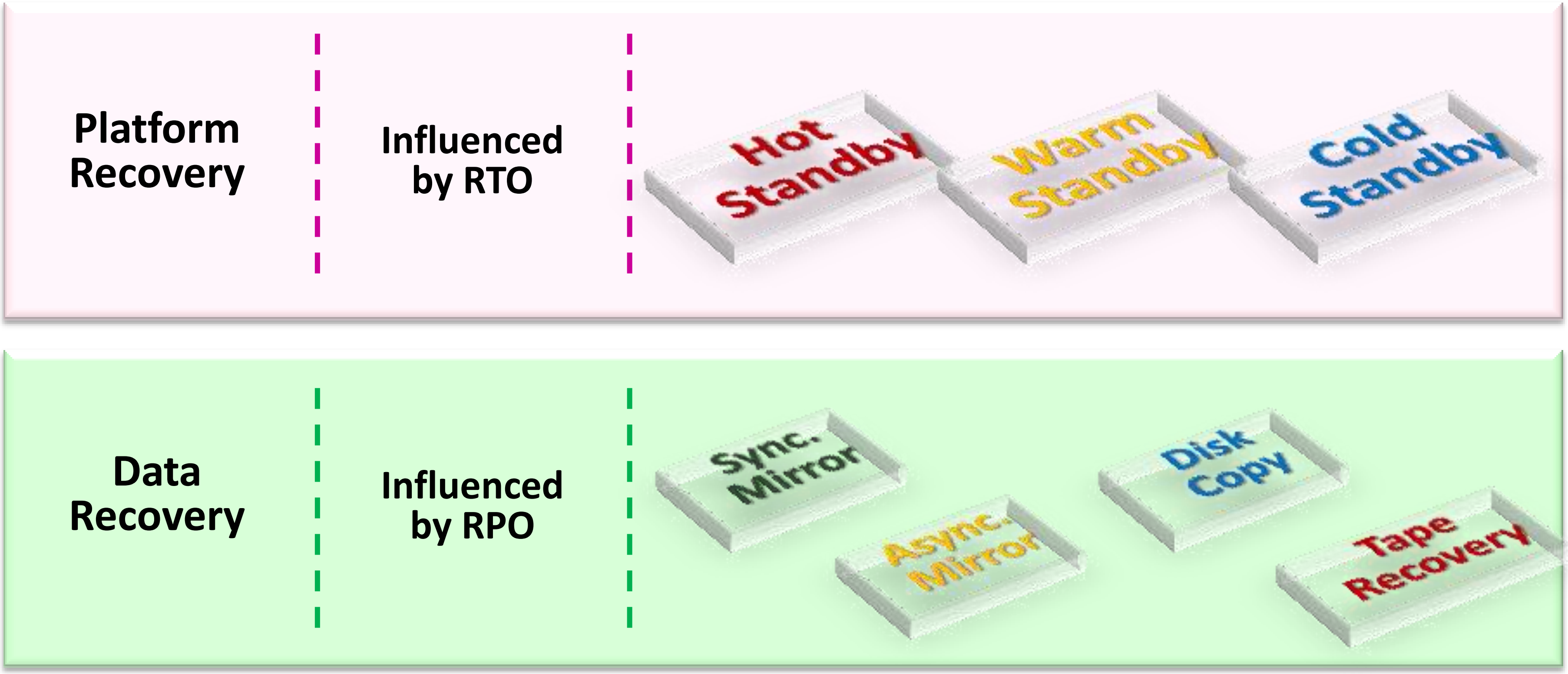


Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

RTO & RPO technological impacts

RTO and RPO parameters are used to evaluate possible disaster recovery solutions basing on two different dimensions: *Platform Recovery* and *Data Recovery*.



Platform Recovery

Influenced by RTO

Data Recovery

Influenced by RPO

Platform Recovery Strategies

Type	Description	Indicative RTO Coverage	Comment	Hardware Source
Hot Standby	Computer hardware that is pre-configured with software and business data in a way that is ready to accept the production load as soon as the primary server fails. The fail-over is typically through a stretched cluster or load-balancing	Minutes	This option requires high levels of operational attention because it is a fail over solution. The age of data is dependant on data restore method.	Dedicated
Warm Standby	Computer hardware that is pre-configured with software (or uses dynamic provisioning). Once a disaster occurs business data is restored, the network is switched to the backup site, and the server then accepts the production load.	Hours	This option has the resources required to recover the system available, but work is required to make them live.	Dedicated
Cold Standby **(incl. shared risk)**	Computer hardware that requires the necessary software and data to be built or restored before the system would be in a productive state.	Days	This option requires a rebuild of the system to recover at the alternate location .	Test / Development / Shared Risk
No DR Standby	No pre-built hardware for disaster recovery.	Weeks	This option should at least include DR procedures.	Procure on invocation

Data Recovery Strategies

Type	Description	Minimum RPO	Comment
Synchronous Disk Mirroring	Synchronous replication from one set of disks to another set of disks at an alternate location (often SAN based).	No Transactional Data Loss	High I/O applications limit the distance between primary and alternative data centres.
Asynchronous Disk Mirroring	Asynchronous replication from one set of disks to another set of disks at an alternate location (often SAN based).	Seconds or Minutes	Can run over very large distances but does not guarantee replication of transactional data.
Disk Copy **(Periodic Snapshot)**	Snapshot data replication technologies ensure point-in-time replication of data from one set of disks to another (often SAN based).	Hours (typically up to 24 hours)	Implementation may use synchronous or asynchronous mirroring but does not necessarily preserve write order during copy.
Tape Recovery (Regular Backup)	Regular backup from disk to tape followed by an off-siting process (either inline or duplication or manual transportation).	12 hours to many days	RPO depends on time from backup to off-siting.

Combing Platform and Data Strategies based on BIA results

Data Recovery Strategy

Platform Recovery Strategy

	RPO RTO	Synchronous Disk Mirroring	Asynchronous Disk Mirroring	Disk Copy	Tape Recovery
		Zero	Secs/Mins	Hours	12 Hours to Many Days
Hot Standby	Minutes	✓	✓	✓	🟦
Warm Standby	Hours	✓	✓	✓	✓
Cold Standby	Days	✓	✓	✓	✓
No DR Standby	Weeks	🟦	🟦	🟦	✓

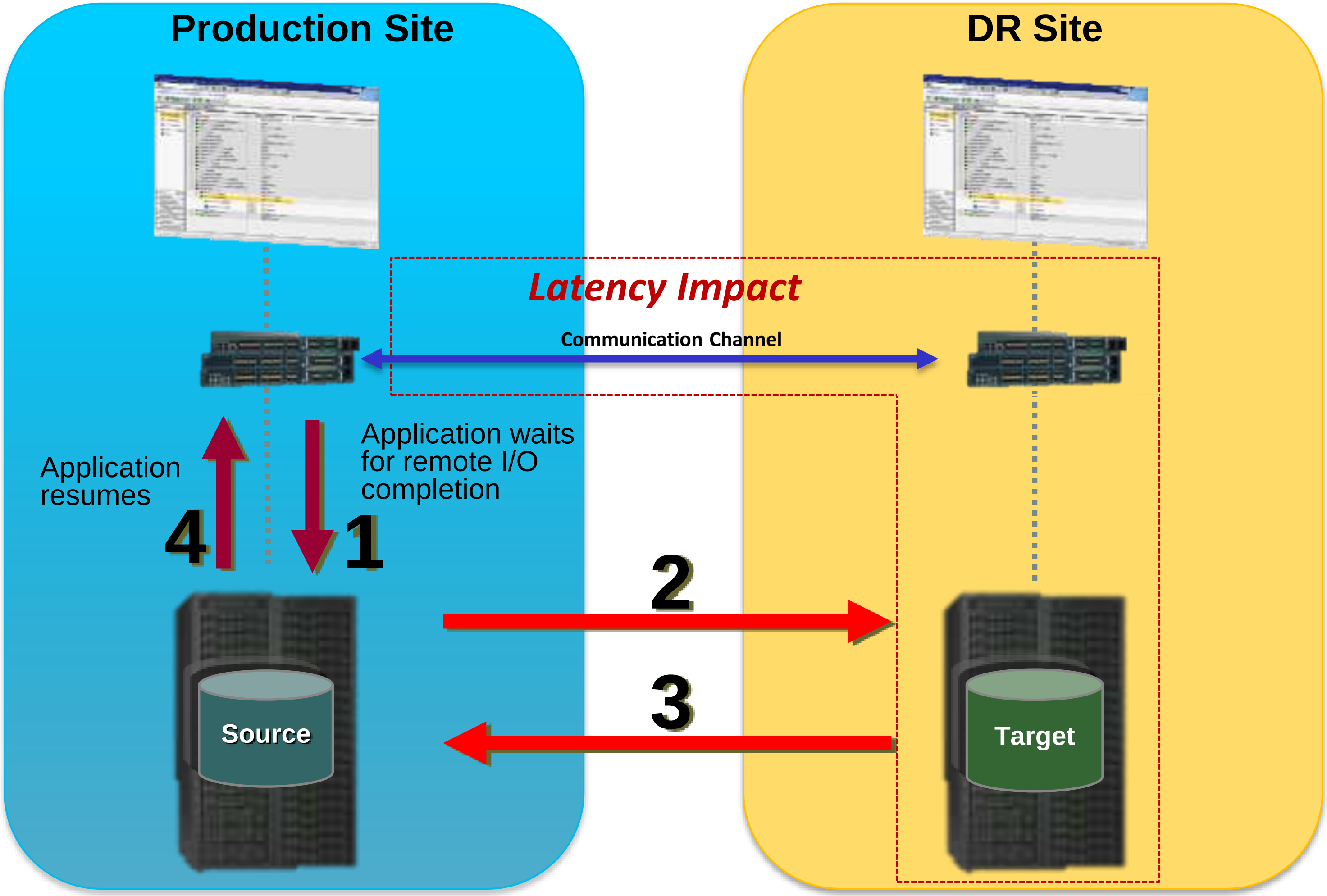
Key: 🟦 Not applicable ✓ Option available

Table of Contents

- Accenture Technology Consulting
- Accenture Methodologies and Framework
- Business Continuity and Disaster Recovery (Key Concept)
- Disaster classification
- Disaster Recovery from IT PoV
- Disaster Recovery Strategies
- Data Replication Technologies
- Disaster Recovery in the Cloud context
- DR Implementation Scenarios (Example)
- Appendix

Data Replication Technologies – Synchronous Data Replication

Synchronous Data Replication



Data Replication Technologies – Asynchronous Data Replication

Asynchronous Data Replication

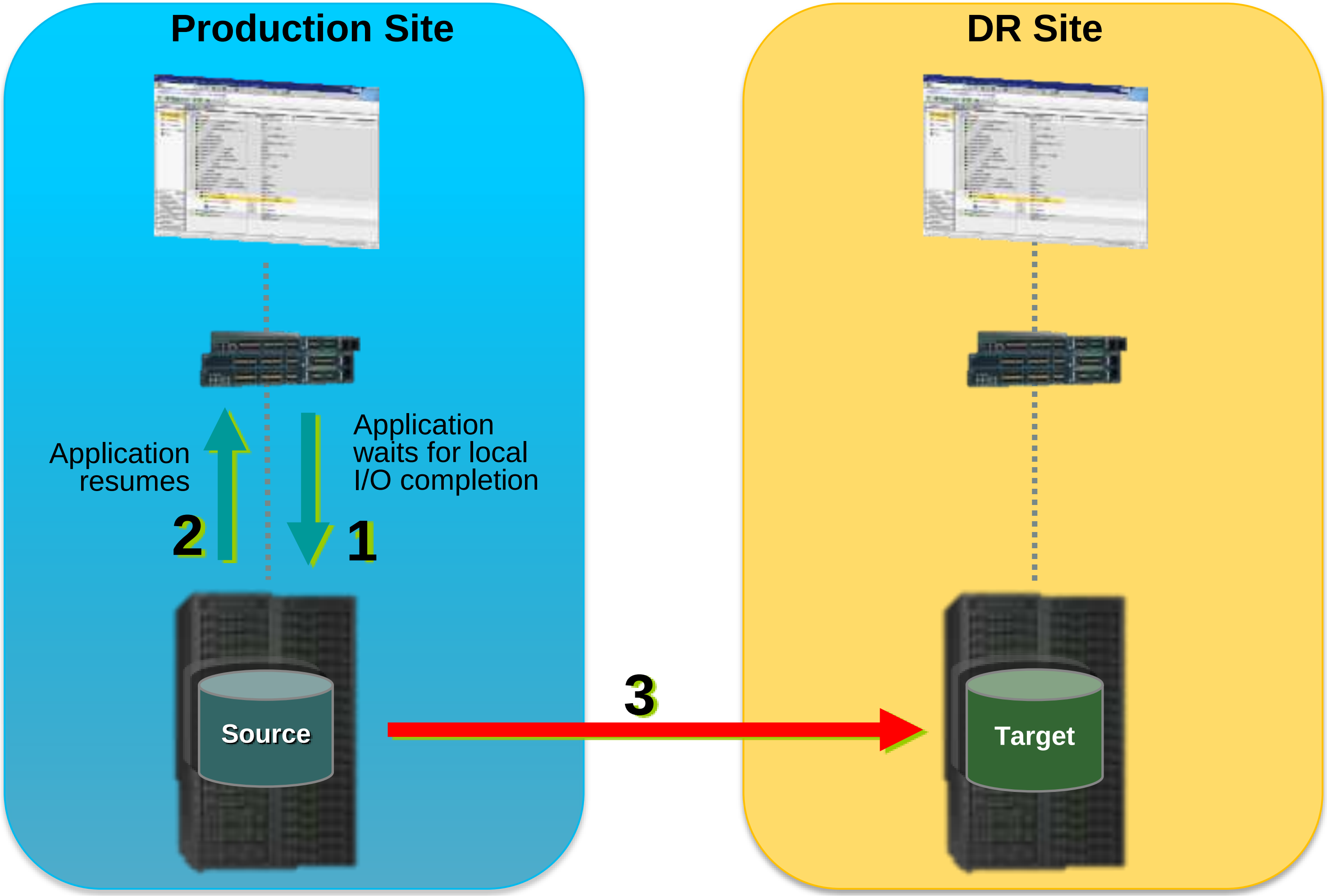
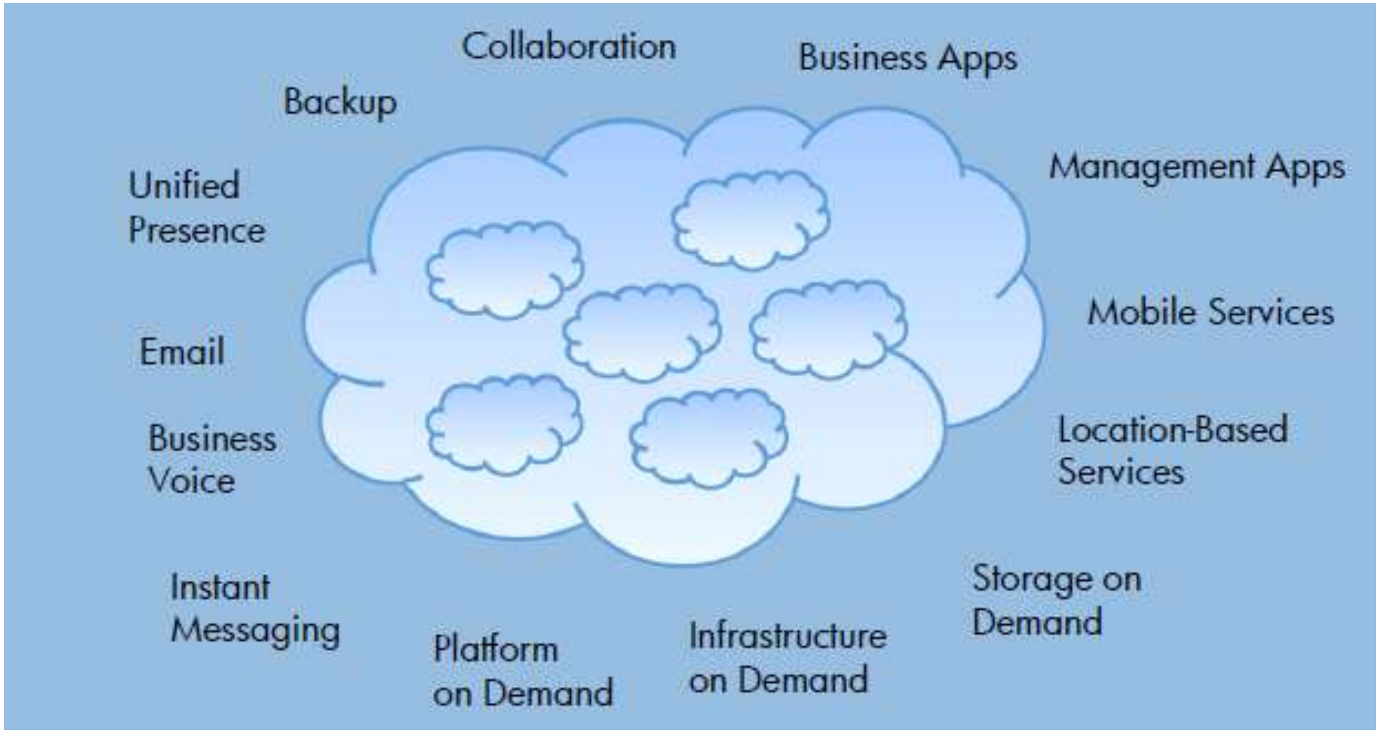


Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

What is Cloud Computing?

*“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”**

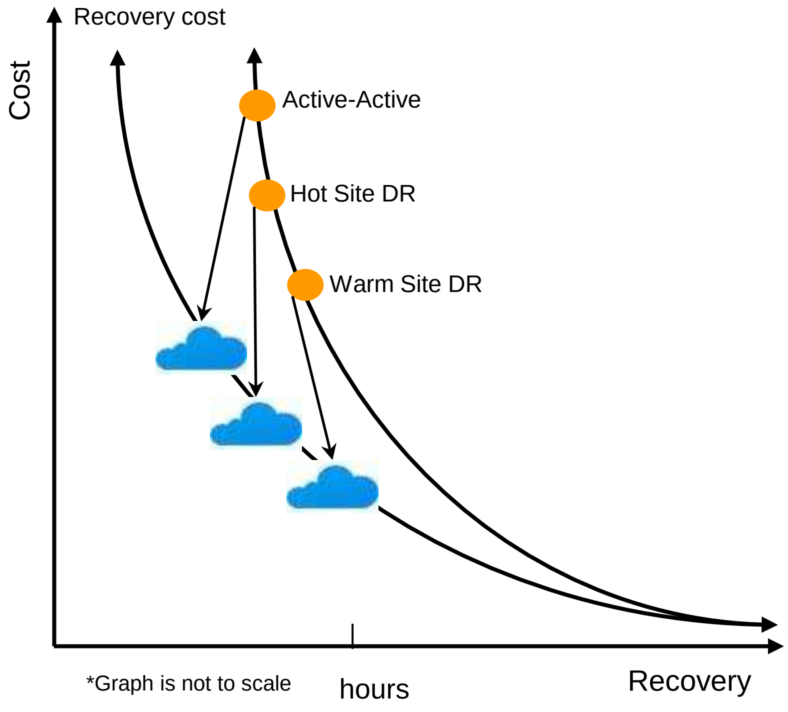


*National Institute of Standards and Technology, USA

Cloud DR as a service

Migrating entire IT operations or DR solutions only to cloud, and replication or movement of data to cloud brings significant cost savings and lowering of recovery times.

- Can shrink and grow in response to demand. ' Replication Mode' requires fewer resources and incurs low cost. When a business disruption occurs, the system enters 'Failover Mode', which requires more resources that scale smoothly without requiring large upfront investments.
- Cloud Computing eliminates hardware unification between primary datacenter and the cloud.
- Cloud servers start-up can be easily automated and managed.



Cloud BCDR Approach

New storage and backup functionality provided by the Cloud provide a way to have a remote copy of data outside the Primary Datacenter.

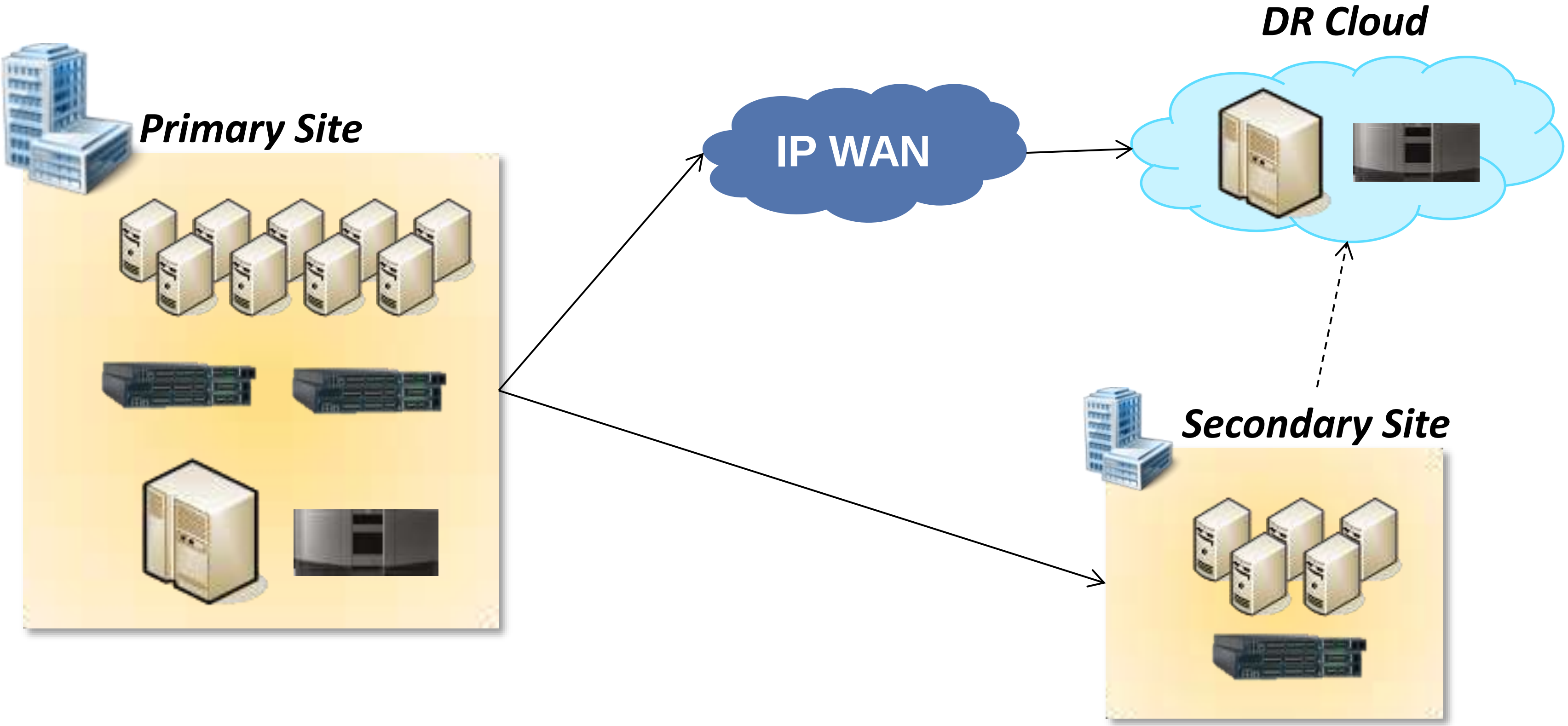
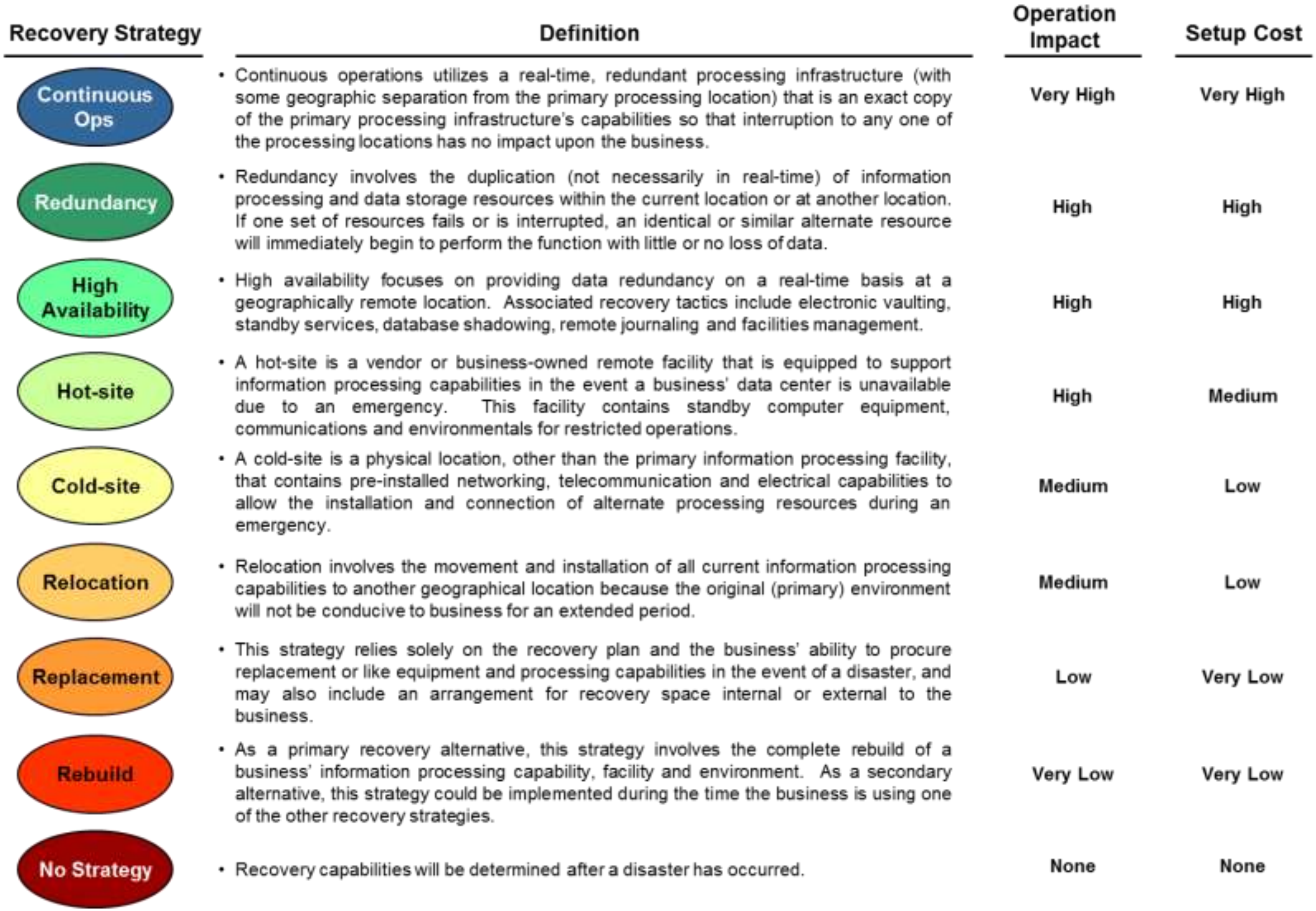


Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

Selecting DR Strategy…



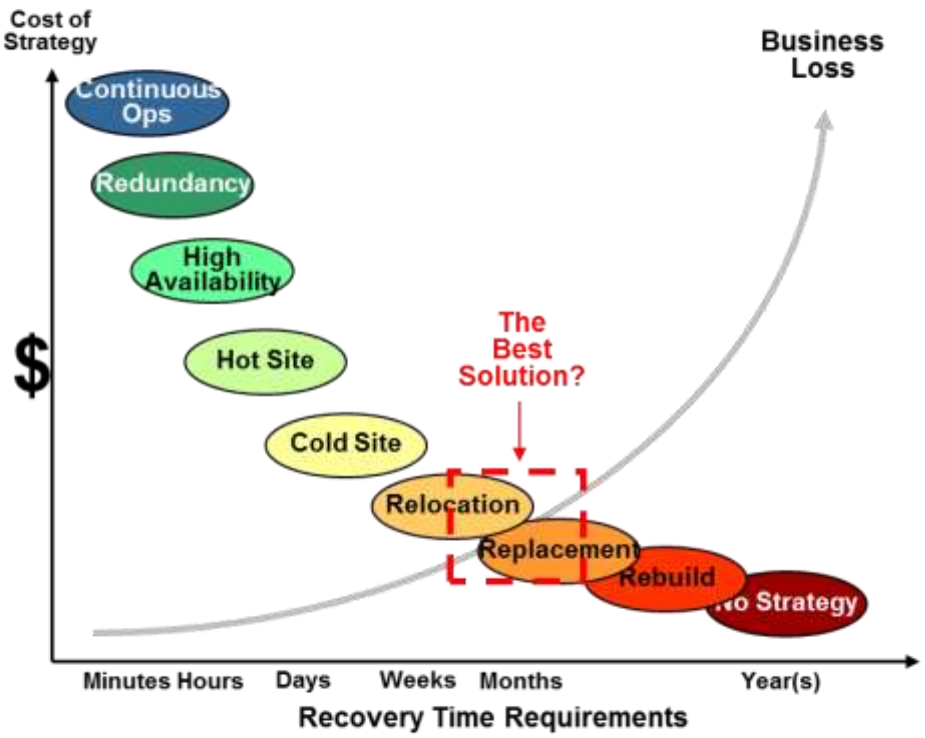
Recovery Strategy	Definition	Operation Impact	Setup Cost
Continuous Ops	• Continuous operations utilizes a real-time, redundant processing infrastructure (with some geographic separation from the primary processing location) that is an exact copy of the primary processing infrastructure's capabilities so that interruption to any one of the processing locations has no impact upon the business.	Very High	Very High
Redundancy	• Redundancy involves the duplication (not necessarily in real-time) of information processing and data storage resources within the current location or at another location. If one set of resources fails or is interrupted, an identical or similar alternate resource will immediately begin to perform the function with little or no loss of data.	High	High
High Availability	• High availability focuses on providing data redundancy on a real-time basis at a geographically remote location. Associated recovery tactics include electronic vaulting, standby services, database shadowing, remote journaling and facilities management.	High	High
Hot-site	• A hot-site is a vendor or business-owned remote facility that is equipped to support information processing capabilities in the event a business' data center is unavailable due to an emergency. This facility contains standby computer equipment, communications and environmentals for restricted operations.	High	Medium
Cold-site	• A cold-site is a physical location, other than the primary information processing facility, that contains pre-installed networking, telecommunication and electrical capabilities to allow the installation and connection of alternate processing resources during an emergency.	Medium	Low
Relocation	• Relocation involves the movement and installation of all current information processing capabilities to another geographical location because the original (primary) environment will not be conducive to business for an extended period.	Medium	Low
Replacement	• This strategy relies solely on the recovery plan and the business' ability to procure replacement or like equipment and processing capabilities in the event of a disaster, and may also include an arrangement for recovery space internal or external to the business.	Low	Very Low
Rebuild	• As a primary recovery alternative, this strategy involves the complete rebuild of a business' information processing capability, facility and environment. As a secondary alternative, this strategy could be implemented during the time the business is using one of the other recovery strategies.	Very Low	Very Low
No Strategy	• Recovery capabilities will be determined after a disaster has occurred.	None	None

… the tradeoff between time and money

Selecting the most appropriate recovery strategy for mission critical operations and applications involves the tradeoff between time and money.

- The speed at which business operations can be recovered, either in-house or with an external third-party, is directly related to the willingness to allocate resources to a specific recovery strategy.
- A particular recovery strategy should be selected based upon business needs, not solely on technical and/or equipment manufacturers' capabilities or third-party hot-site vendor's desires.
- The point at which the Business Loss and Recovery Strategy Cost lines intersect may not be the most prudent overall recovery strategy (i.e., the mathematical result is not always the best answer) as there may be multiple recovery tactics and strategies that are integrated within a recovery solution.
- Supporting the chosen strategy must come with an understanding of which resource will be traded off…time or money.

Business Recovery Strategies versus Business Loss over Time*

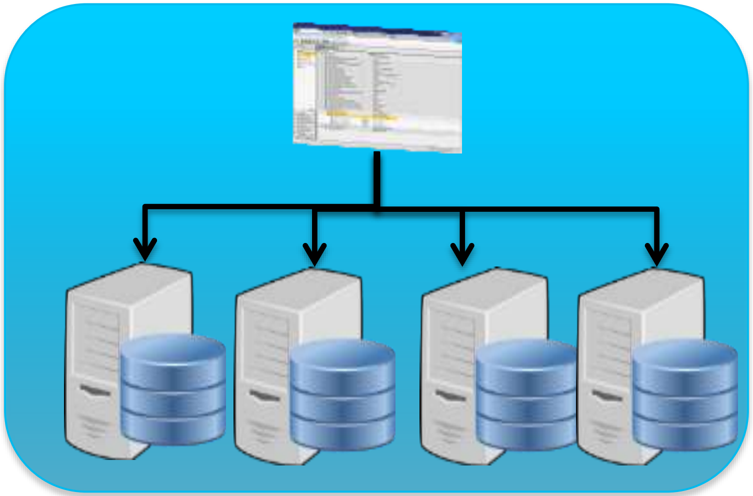


*Graph is not to scale and for discussion purposes only

DR Strategy – Exercise (1/2)

On *Primary Datacenter* we have this scenario:

- Average I/O rate of 100 Mb/s
- Hourly Data written Peak: 150GB
- 2 TB of storage for Data
- 4 server with each:
  - 2 CPUs @ 3.00 GHz
  - 4 GB RAM



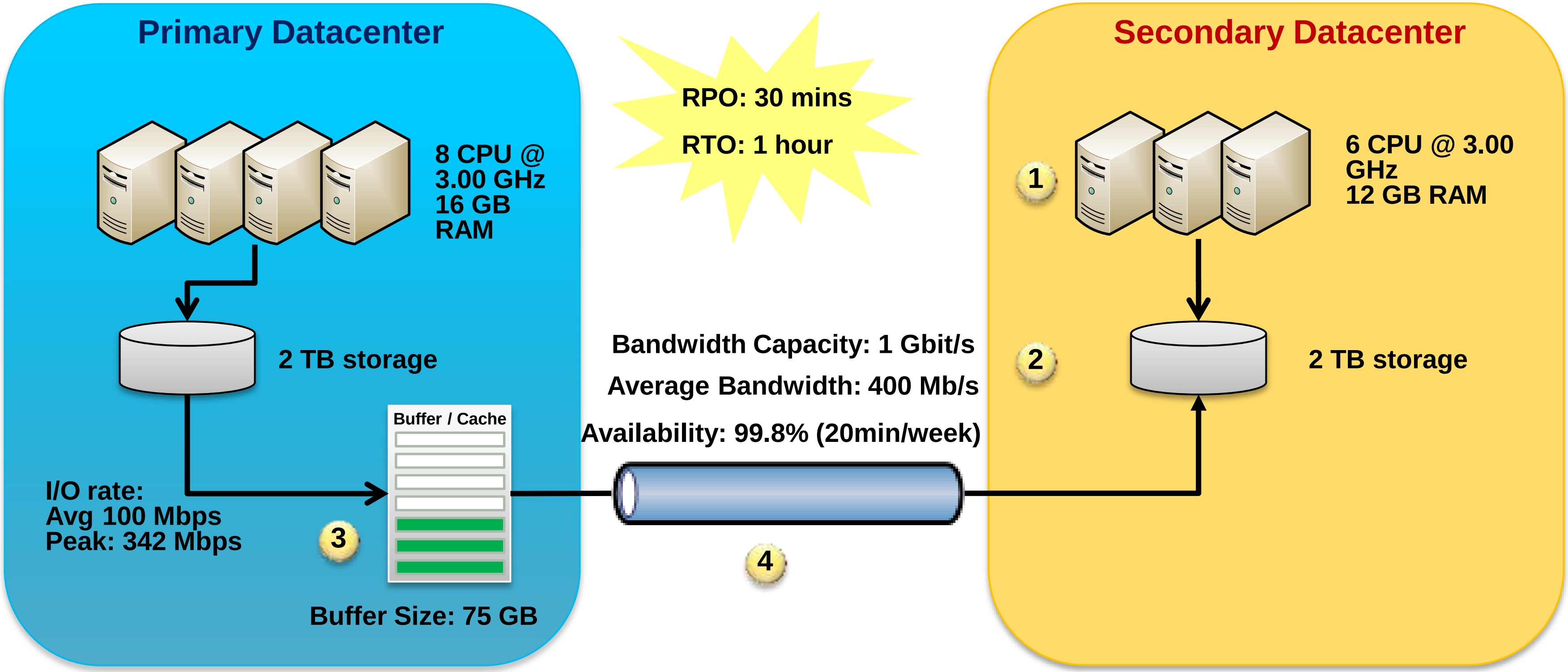
Recovery Requirements:

- RTO = 1 hour
- RPO = 30 minutes
- On *Secondary Datacenter* is admitted a degradation of performance of 25%
- We assume Array-Based technology for data replication

How to size the Secondary Datacenter’s infrastructure components (server, storage and network channel) in order to meet the Recovery Requirements?

DR Strategy – Exercise (2/2)

A possibile solution:

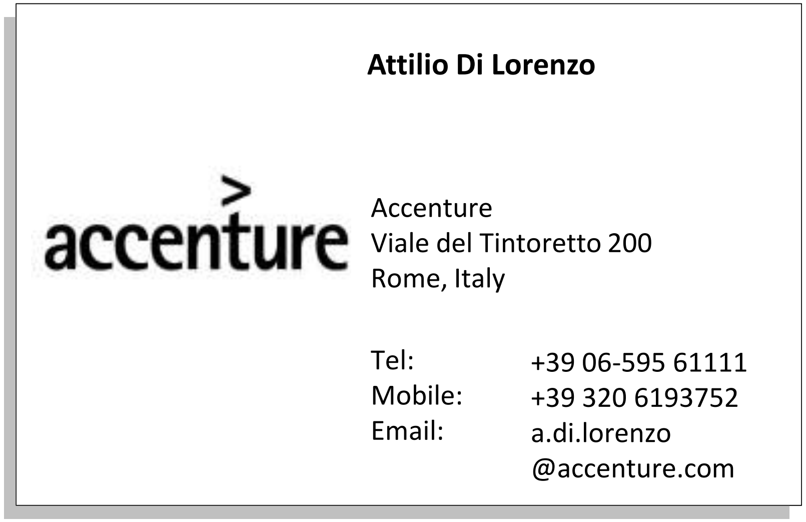


It's all we need for the Disaster Recovery Solution? *…Not yet!*

We need to define and test the recovery procedure to restore all the components (server, network, data, …) within the defined RTO.

Questions & Answers

Accenture Contacts



Attilio Di Lorenzo

Accenture
Viale del Tintoretto 200
Rome, Italy

Tel:	+39 06-595 61111
Mobile:	+39 320 6193752
Email:	a.di.lorenzo @accenture.com

Table of Contents

- **Accenture Technology Consulting**
- **Accenture Methodologies and Framework**
- **Business Continuity and Disaster Recovery (Key Concept)**
- **Disaster classification**
- **Disaster Recovery from IT PoV**
- **Disaster Recovery Strategies**
- **Data Replication Technologies**
- **Disaster Recovery in the Cloud context**
- **DR Implementation Scenarios (Example)**
- **Appendix**

“Generally Accepted Standards” and “Best Practices” for BCM

- CoBiT Framework for Assessing IT Controls (www.isaca.org) - the IT Governance Institute provides a guidance publication on IT governance, security and assurance: Control Objectives for Information Technology (CoBIT), third edition (2000). CoBIT is internationally accepted as good practice for control over IT and related risks (See Domain: *Deliver and Support* , Process: *Ensure Continuous Service* in the CoBIT framework)

- National Institute of Standards and Technology (NIST) Special Publication 800-34 (www.nist.gov) has produced a Contingency Planning Guide for Information Technology Systems, which sets fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans. Used by Federal departments and agencies.

- ISO 17799 (www.iso-17799.com): The information security standard of the International Standards Organization (ISO). ISO 17799 has an entire section entitled Business Continuity Management wherein testing, maintaining, and reassessing the plan are called for directly.

- British Standards Institute (www.bsiglobal.com) - The BSI has released a Publicly Available Specification, PAS56, which sets out a high-level process for implementing BCM within an organization. This is currently being developed into a full British Standard and in time will likely evolve into an ISO standard.

“Generally Accepted Standards” and “Best Practices” for BCM

- Business Continuity Institute (www.thebci.org) - The BCI has developed its "Business Continuity Management - Good Practice Guidelines." The BCI works closely with the BSI in the development of a BCM Standard, and these guidelines represent the latest thinking. Their website offers free downloads of Good Practice Guidelines. The BCI also provides certification with a number of different levels available (e.g. Member, Fellow, etc.) Basic certification is via references from previous BCM projects, with the higher levels requiring certification interviews. Membership of the BCI is more commonplace in Europe than the US.

- DRI International (www.drii.org) - The DRII's "Professional Practices for Business Continuity Planners" sets out a seven-step model for Business Continuity. DRII also provide certification of Business Continuity professionals through an extensive training and examination program. Whilst currently predominantly US-based, DRII is making in-roads in Europe with professionals who are looking for an exam-based certification, although some clients are sceptical that these exams are often at the end of paid-for training courses.

- IT Infrastructure Library (www.itil.co.uk) - ITIL is possibly the most widely accepted approach to IT Service Management, and includes an extensive process concerning "IT Service Continuity Management." Whilst this may sound IT-focused, much of the process focuses on "The Business Continuity Lifecycle" and covers many of the elements addressed by the Accenture BCM Methods. This is particularly useful when working at clients who have implemented or are in the process of implementing ITIL processes.

U.S. Federal Government Certification & Accreditation (C&A) Methodologies

There are generally three methodologies used for C & A initiatives:

DITSCAP is an acronym for Defense Information Technology Systems Certification and Accreditation Process. It is based on a publication known as Defense Information Systems Certification and Accreditation regulation Department of Defense (DoD) 5200.40. DITSCAP is typically used only for defense agencies, although civilian agencies may opt to apply DITSCAP principles to their own customized C&A process.

NIACAP stands for National Information Assurance Certification and Accreditation Process. It is based on a process published by the National Security Telecommunications and Information System Security Instruction known as NSTISSI No. 1000.

NIST is the National Institute of Standards and Technology, and its C&A methodology is described in a document known as Special Publication 800-37. While many civilian agencies have traditionally used either the NIACAP or NIST methodologies, the current trend is that most agencies are moving away from NIACAP to embrace the new NIST methodology.

Disclaimer

This document and the information contained herein are proprietary to Accenture. This document, either in whole or in part, may not be reproduced in any form or by any means without Accenture's prior written permission. Any third-party names, trademarks and copyrights contained in this document are the property of their respective owners.