09 Overview of Business Continuity Solutions

www.huawei.com

HUAWEI

Foreword

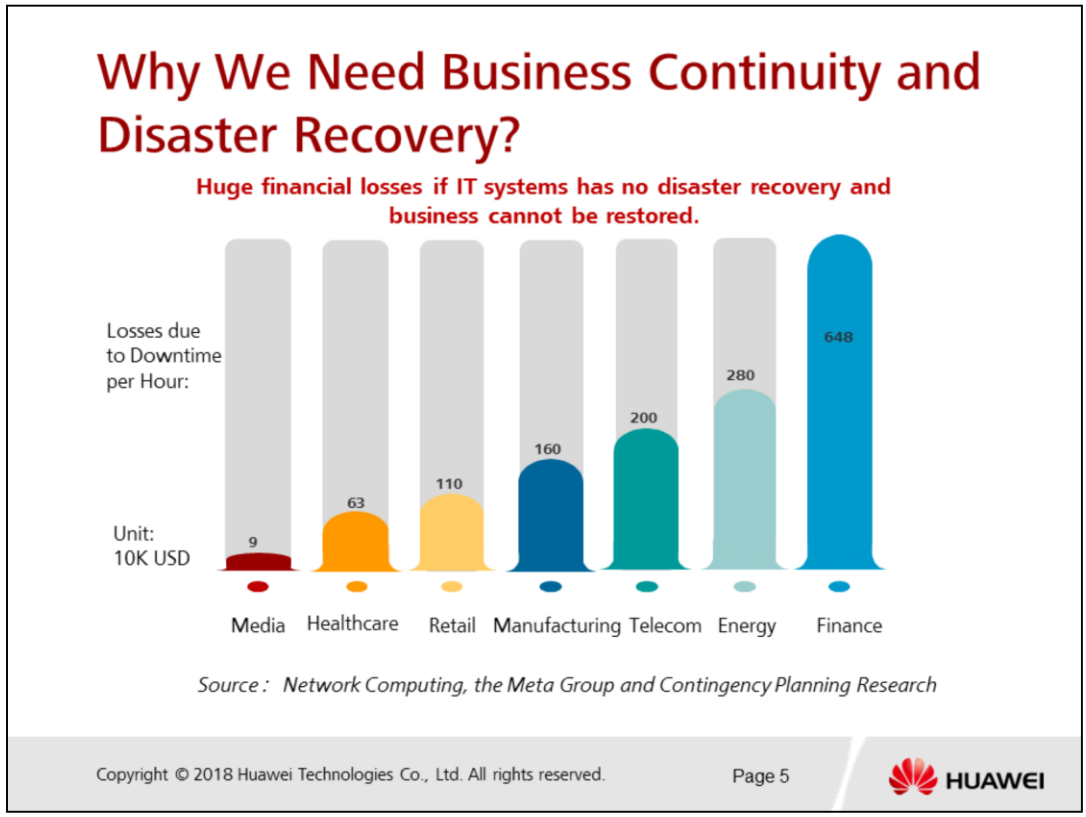
- This module introduces:
  - The importance and challenges faced by business continuity.
  - The definition and measuring standards of business continuity.
  - The types of business continuity solutions.
  - The panorama of Huawei Disaster Recovery solutions.

Objectives

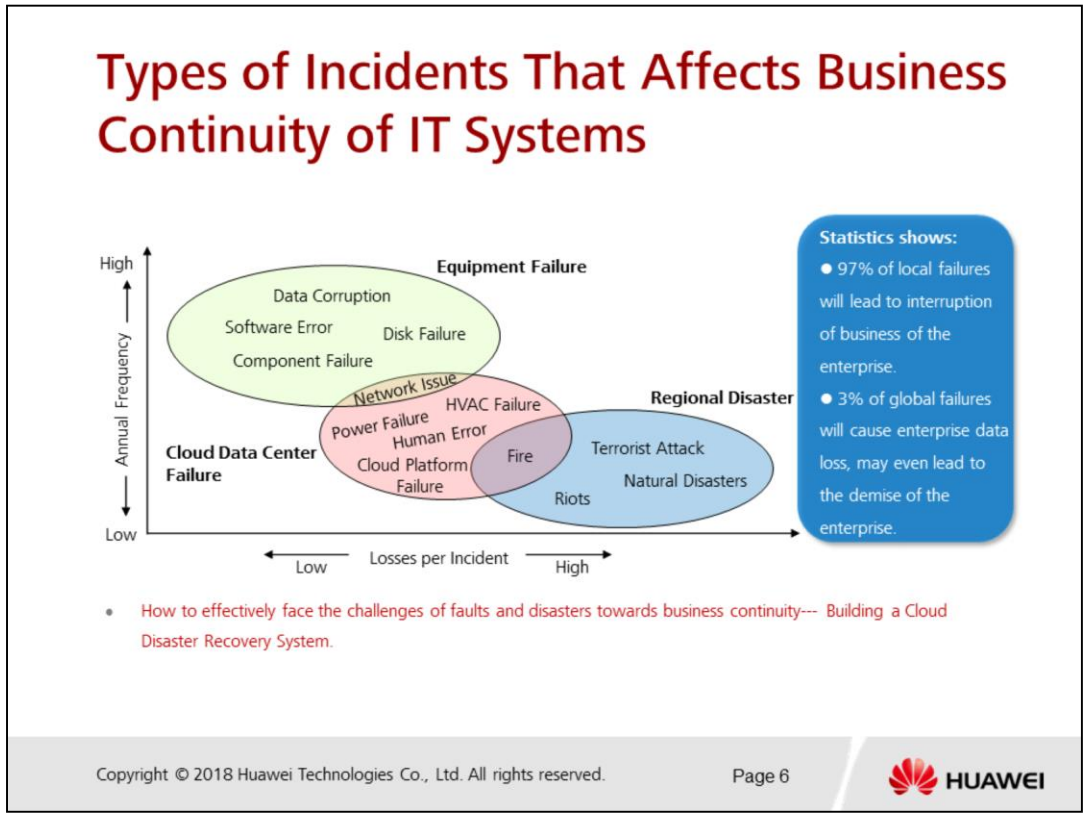
- Upon completion of this module, you will be able to:
  - Understand the importance and the challenges faced by business continuity.
  - Understand the definition of business continuity, standards and the relationship between the costs and risks in ensuring business continuity.
  - Understand the common solutions for business continuity.
  - Understand the panorama of Huawei business continuity solutions.

Contents

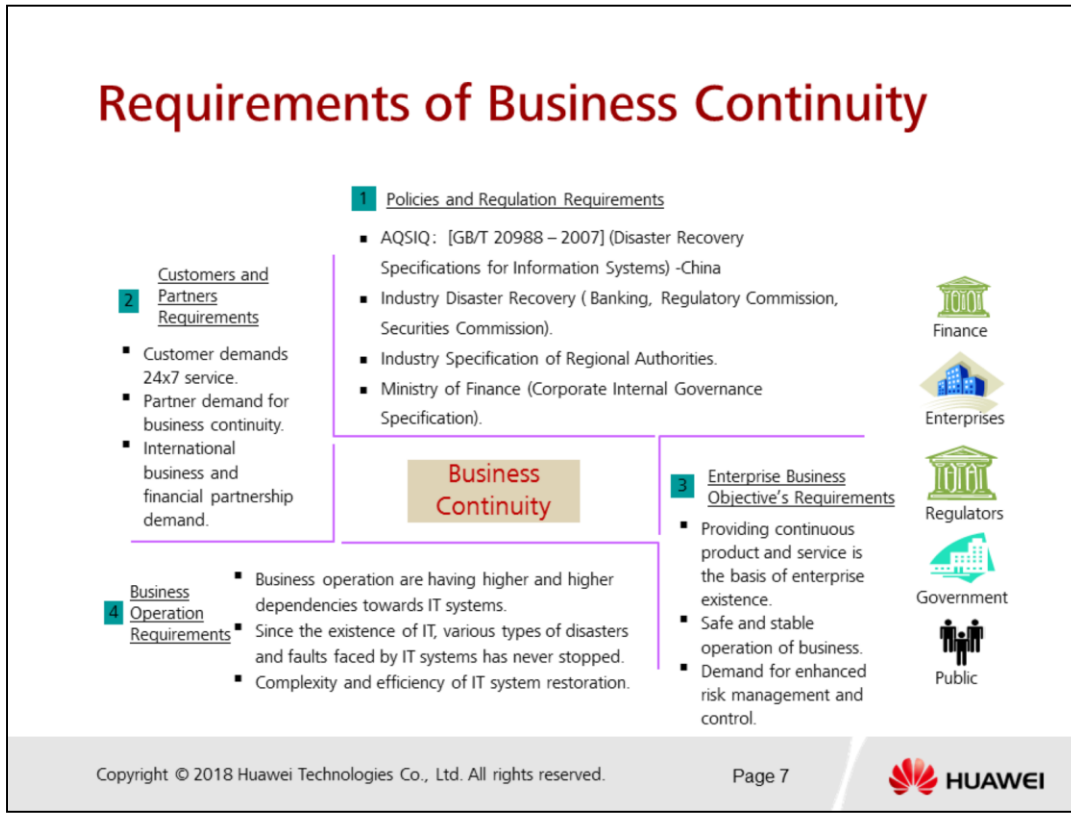
- Disasters are frequent, and able to destroy the important assets such as physical infrastructure, key personnel, information system, and key business data, which directly threatens the continuity and operation of businesses. Do you already have a plan and ready to face disasters now?
- Enterprises need to prepare for everything from natural disasters to cyber-attacks with disaster recovery plans that detail a process to resume mission-critical functions quickly and without major losses in revenues or business operations.



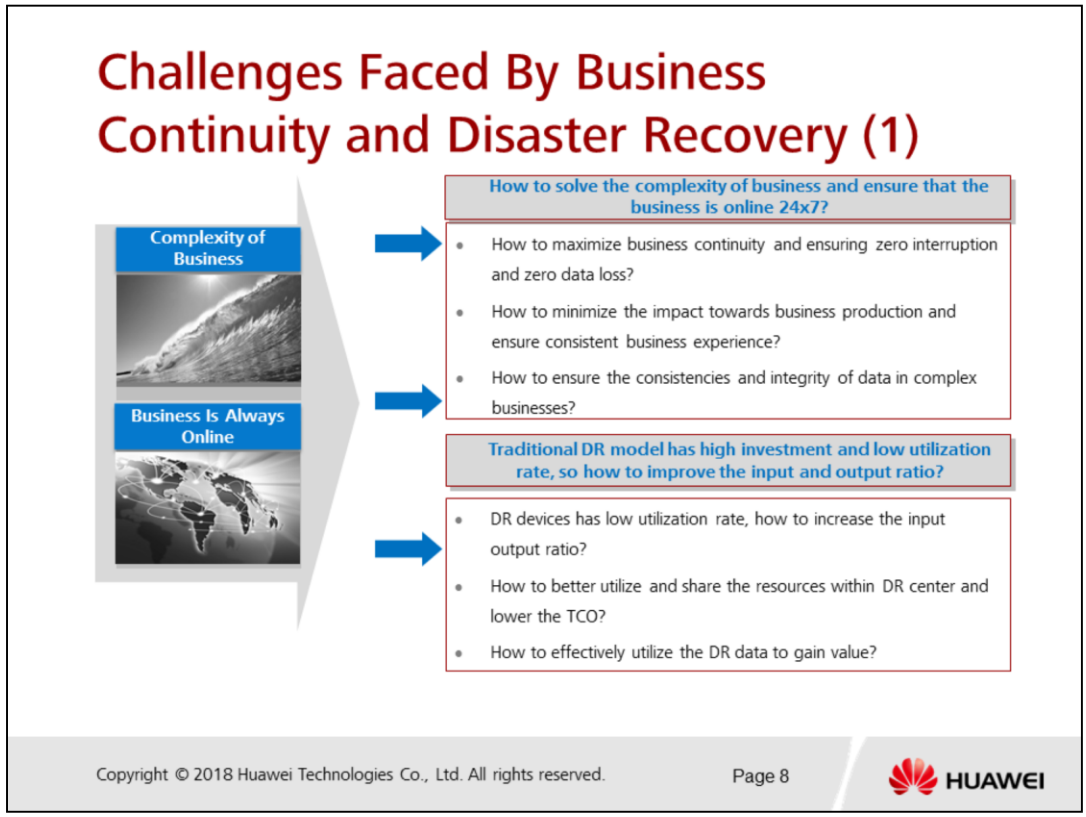
- From traditional data centers to cloud environments, business downtime will bring great financial losses and affect the reputation of the company. Customers has the demand for business continuity and data protection at any given time.
- Some government has regulated laws to build IT disaster recovery systems, such as:
  - Government regulations to require Telecom service providers to have compulsory disaster recovery systems to protect user data, and the RTO (Recovery Time Objective) must be lower than 1 hour. -Columbia
  - Government has published official documents on 2 occasions to emphasize the importance of disaster recovery and backup, and also a guide on disaster recovery, which has stressed the importance of disaster recovery, backup and restoration in the aspects of laws and regulations. -China
- Enterprises without a proper disaster recovery plan face the risks of potential financial losses and affect their reputation in the event of a disaster. No business is invulnerable to IT disasters, but speedy recovery due to a well-crafted IT disaster recovery plan is expected by today's ever-demanding customers. Too many businesses fail because they were ill prepared for an IT disaster.



- Equipment level failures refers to disk failure, failure of components in storage device or breakdown of the whole storage system.
- Data center level failure refers to incidents such as long power outage of data center, HVAC (Heat, Ventilation, and Air Conditioning) failure in the data center, or a fire that caused the collapse of the whole business system.
- Regional disasters refers to floods, earthquakes, or any major disasters that happen in the region, that cause the collapse of the whole IT system within the region which may cause permanent data loss within the data center.
- In order to prevent different types of errors, faults, failures and disasters, we need to implement different types of disaster recovery solutions. For example, to face equipment level failures, we could implement high availability disaster recovery solution locally. To face data center level disasters, we can implement a same city disaster recovery center. Additionally, to face regional disasters, we can build a remote region disaster recovery center.
- As the disaster level is different, there is no one size fit all solution for disaster recovery, we must first understand the customer requirements in terms of the expectation on the disaster recovery solution and build a disaster recovery solution that meets all the needs and expectations of the customer.



- The diagram above shows the requirement of business continuity from 4 different aspects which are from policies and regulations, customers and partners, business operation and business objectives.
- AQSIQ refers to The General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, which is a ministerial department of China, that serves as a regulator for quality and standards. In many countries, there are similar departments or regulatory bodies that specifies the standards and set the regulation for enterprises to implement a certain level of business continuity plan based on their sectors or industries.
- The public, government, regulators, enterprises and financial sector also plays a part in demanding business continuity plan to ensure smooth operation of the industries and businesses that are critical for the society. For example, government enforce policies so that key services to the public such as hospitals need implement a certain level of business continuity or disaster recovery plan, so that the public will not face the risk of not having proper healthcare in the event of a disaster.



- Business continuity management (BCM) is a holistic process to ensure uninterrupted availability of all key business resources required to support critical business activities, whether manual or IT-enabled, in the event of business disruption. Business continuity planning (BCP) involves planning and procedural aspects, encompassing emergency response, crisis communications, business continuity and disaster recovery. Disaster recovery planning (DRP) is the technical component of BCP and focuses on the continuity of information and communication technology systems that support business functions.
- During the process of planning for business continuity or even managing a current business continuity plan, there are a lot of considerations to be made as shown on the diagram above. The key idea is to build and manage a business continuity solution that balances the investment cost and meets all the requirement expected. During BCP, it is best to consider all the factors involved and implement a solution that fits your current needs with some rooms for expansion as the business grows.

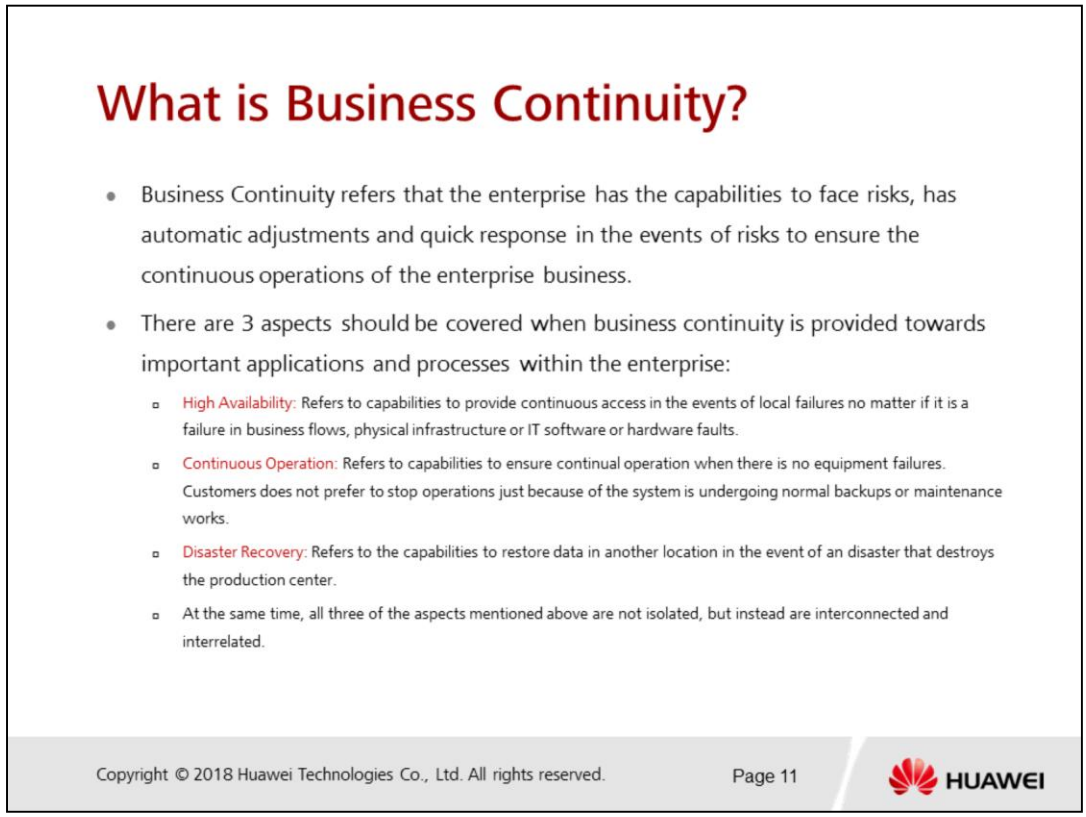
Challenges Faced By Business Continuity and Disaster Recovery (2)

How to simplify the DR system building, wide management areas, and high difficulties of DR ?

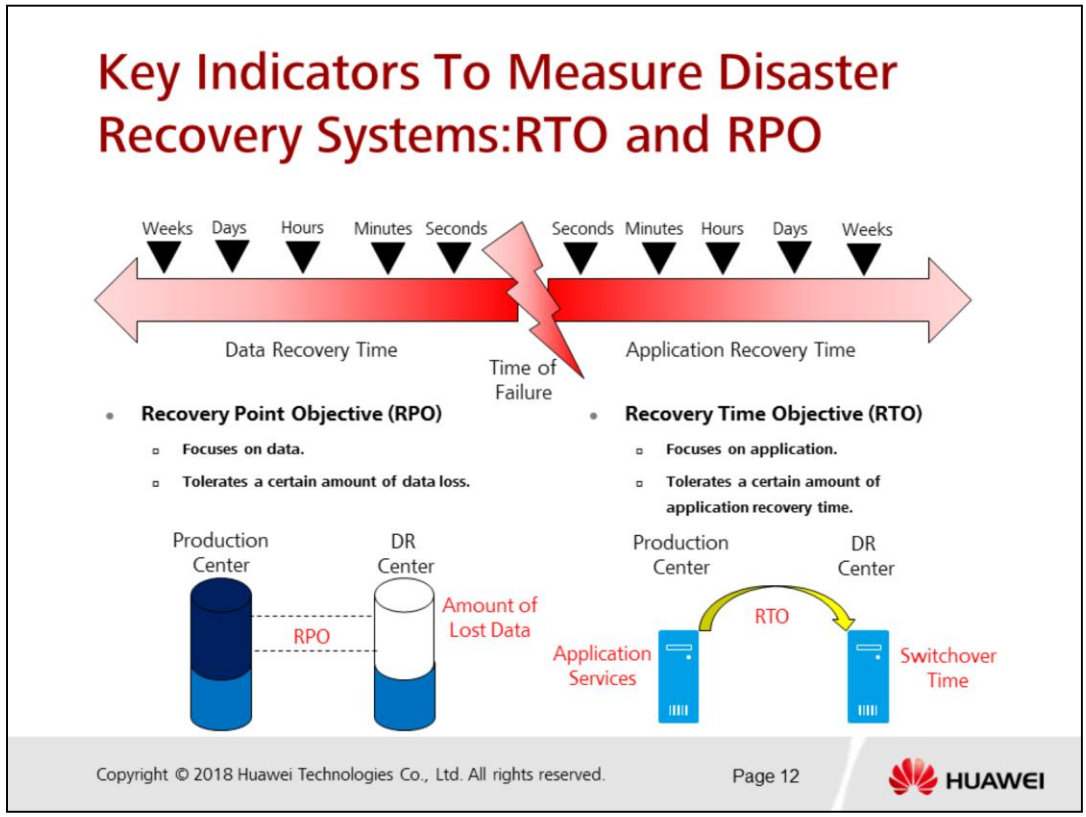
- How to effectively complete DR operations with limited manpower to ensure enterprise business continuity?
- How to simplify, and complete the building of DR system that meet the requirements quickly when it consist of a series of steps such as business analysis, risk analysis, solution design, implementation, walkthroughs and process flows.

HUAWEI

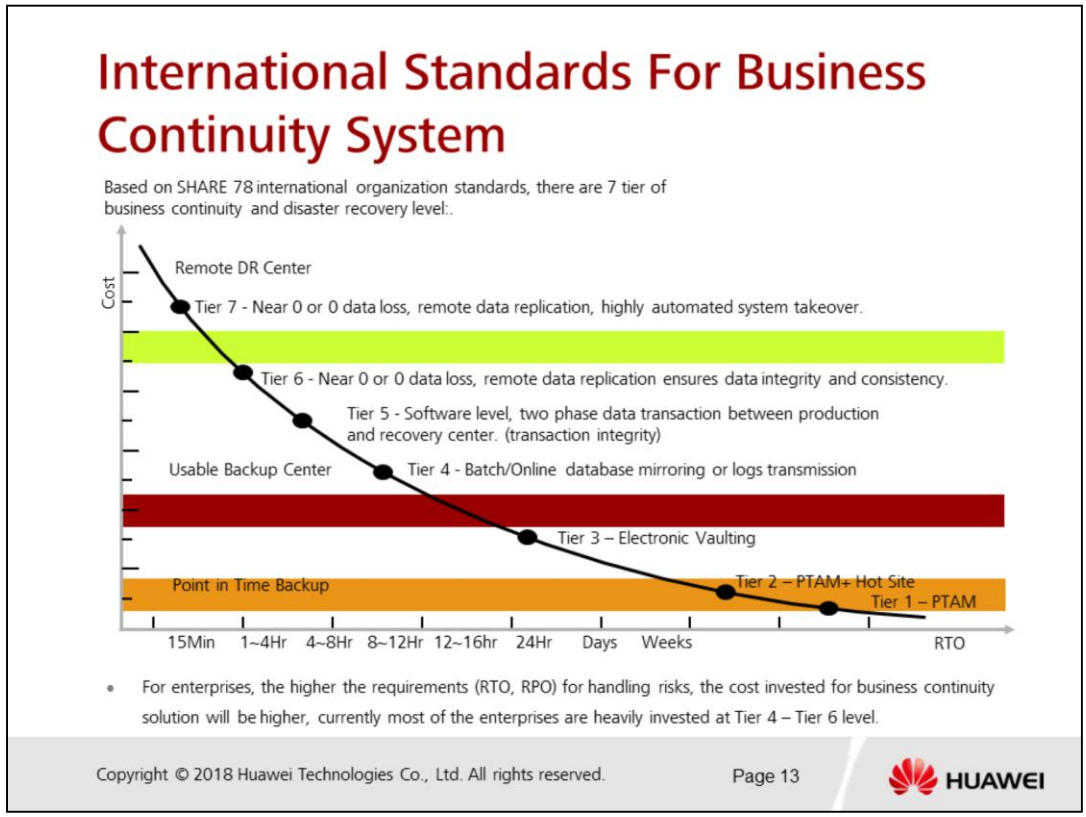
Contents



- Business continuity management originated in the disaster recovery planning of 1970s. At that era, disaster recovery activities are managed by data processing managers. During that time, if there is a major fault or crisis, downtime is calculated by days and not hours. Financial organization, such as banks and insurance companies largely choose to store backup tapes in another location away from the main data center. Recovery activities are usually caused by fire, flood, typhoon or other physical damages.
- By the 1980s, there are already a lot of commercial disaster recovery center that provides computing service on shared devices but they mainly focus on IT disaster recovery. By the 1990s, IT industry had a huge revolution, and disaster recovery plan developed into business continuity plan.
- Disaster recovery (DR) involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity.



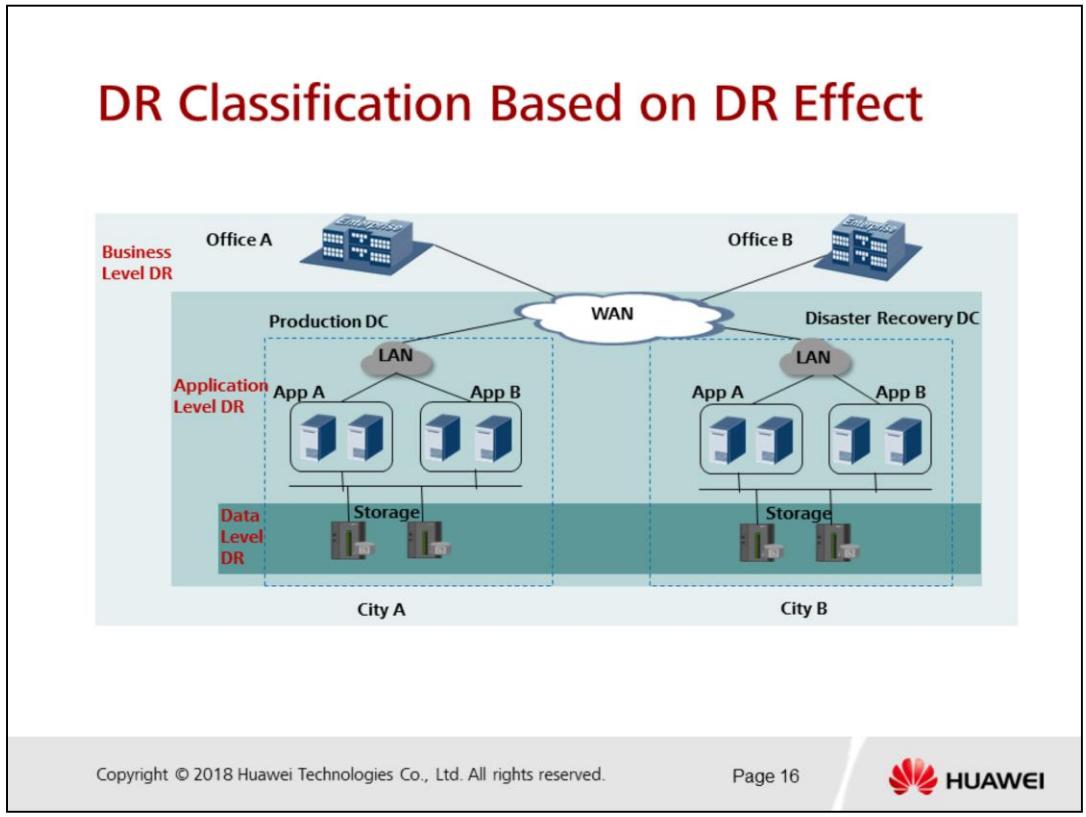
- RTO (Recovery Time Objective) refers to the time required for the information system or business function to recover from a breakdown after a disaster occurred. The smaller the value, means that the smaller the service interruption time.
- RPO (Recovery Point Objective) refers to a point in time where systems and data are restored after a disaster has occurred. The smaller the value means that the lesser the amount of data is lost.
- How to set the RTO indicator for active-standby system switchover ?
    - RTO is the requirement for the disaster recovery switching time for business systems, it is mainly derived from the business impact analysis. From the perspective of DR system design, the switchover time of the current DR system need to be considered from the overall application system as a whole including storage, database, and application in the aspect of time required for them to takeover services, and not only considered from the aspect of storage layer.
- In another sense, RPO limits how far to roll back in time, and defines the maximum allowable amount of lost data measured in time from a failure occurrence to the last valid backup. RTO is related to downtime and represents how long it takes to restore from the incident until normal operations are available to users.



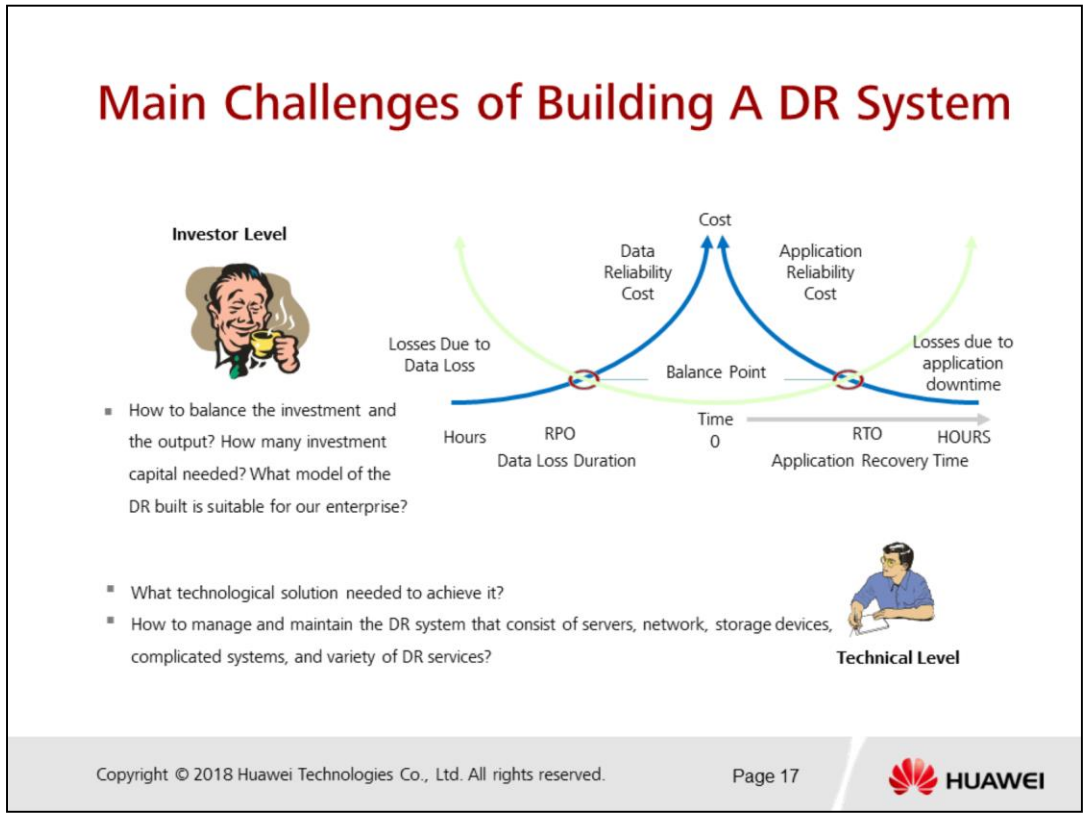
- PTAM (Pickup Truck Access Method) refers to the method of transporting backups between production and off site storage facility using pickup trucks.
- The 7 tiers of Disaster Recovery:
  - Tier 1: Data Backup with No Hot Site. Regular backups are transported to offsite storage facilities. No backup system or infrastructure to restore system in the event of disaster.
  - Tier 2: Data Backup with Hot Site. Regular backup combined with offsite facility and infrastructure to restore system in the event of a disaster.
  - Tier 3: Electronic Vaulting. It is build on top of Tier 2 functionality. Data is electronically vaulted which is more current than via PTAM. As a result, less data recreation or loss when a disaster occurs. The facilities for providing Electronic Remote Vaulting consists of high-speed communication circuits, some form of channel extension equipment and either physical or a virtual tape library and an automated tape library at the remote site.

- Tier 4: Point in Time Copies. Tier 4 solutions begin to incorporate more disk based solutions. Several hours of data loss is still possible, but it is easier to make such point-in-time (PiT) copies with greater frequency than tape backups even when electronically vaulted. Systems can be restored within a day using DR solutions of this tier. Applications that are developed also takes into considerations factors such as data replication, low RTO and snapshots.
- Tier 5: Transaction Integrity. It builds on top of Tier 4 but also adds the functionality of maintaining the state of data, ensuring data is updated in both local and remote databases. Only when data is updated in both local and remote database, then only the transaction is considered successful. Production and backup center is connected via high speed broadband, and the key data and application is running concurrently on both locations.
- Tier 6: Zero or Near Zero Data Loss. Tier 6 business continuity solutions maintain the highest levels of data currency. They are used by businesses with little or no tolerance for data loss and who need to restore data to applications rapidly. These solutions have no dependence on the applications or applications staffs to provide data consistency.
- Tier 7: Highly Automated Business Integrated Solution. Tier 7 solutions include all the major components being used for a Tier 6 solution with the additional integration of automation. This allows a Tier 7 solution to ensure consistency of data above that which is granted by Tier 6 solutions. Additionally, recovery of the applications is automated, allowing for restoration of systems and applications much faster and more reliably than would be possible through manual business continuity procedures.

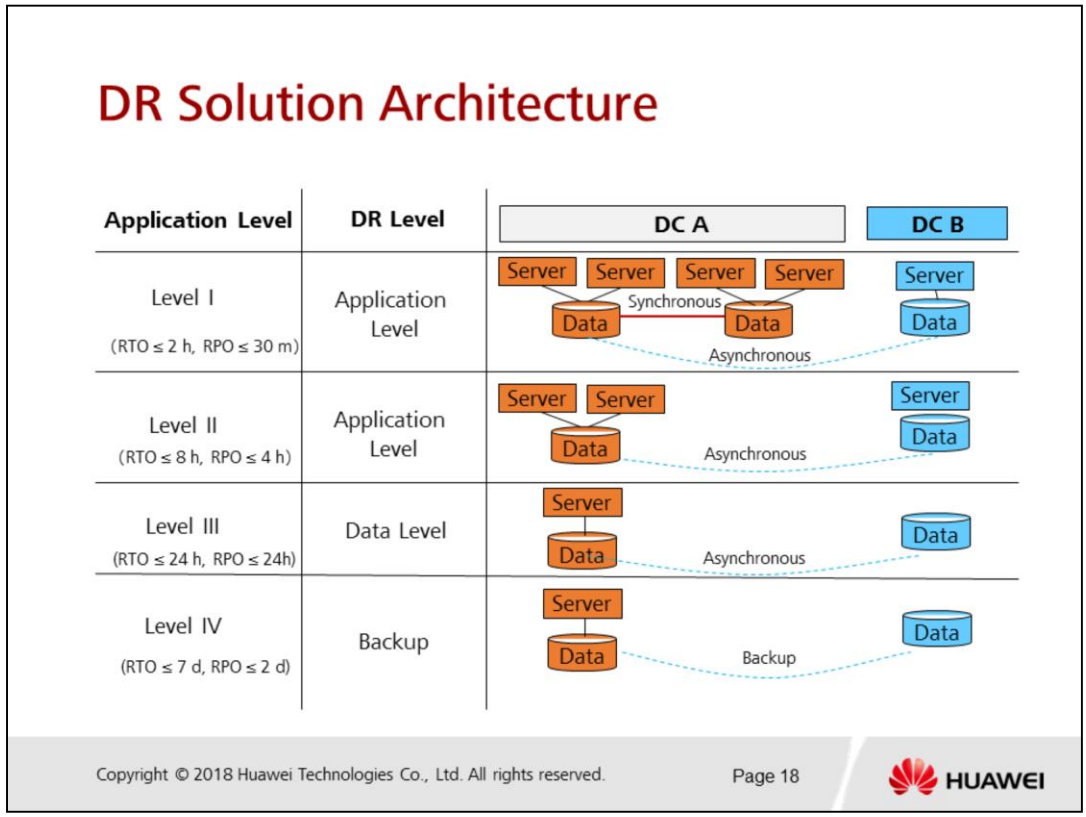
Contents



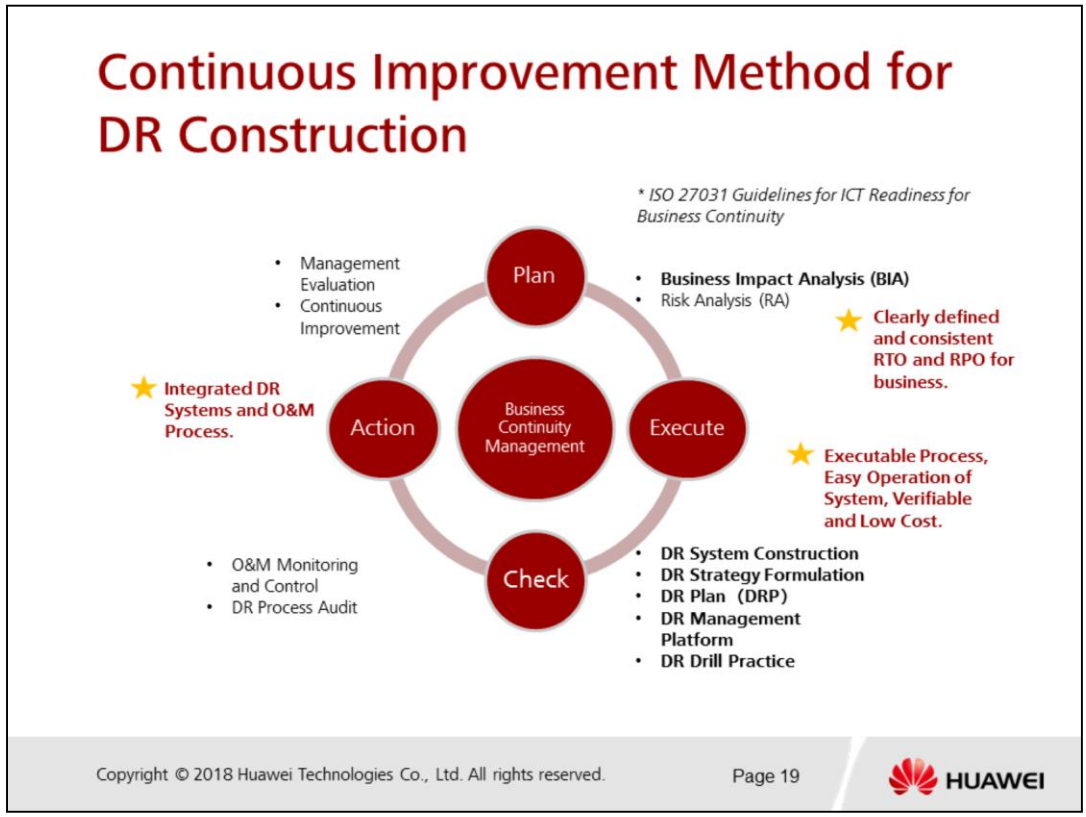
- Based on DR effect, the DR system is classified into data level DR, application level DR and business level DR.
- Data Level DR: Remote DR system data is a copy of the local key application data, when a disaster occurs at the local system, the system at least has an usable remote copy of key business data.
- Application Level DR: Building on top of the basis of data level DR, a set of backup environment equivalent to the local production system is set up remotely, including the configuration of host, network, application, and IP resources. When the local system encounters a disaster, the remote system can provide a fully usable production environment to takeover the services.
- Business Level DR: It is the DR plan for the whole business that requires all the physical infrastructures including the non IT systems such as phones and offices. When a huge disaster occurs, the original office will be destroyed, besides the data and the application restoration, we need to have a backup working environment that is able operate the business as normal.



- The main challenges of building a DR system lies within the investor and technical level.
- From the investor's perspective, the amount of investments needs to be viable and has a positive rate of returns. In short, the amount invested for DR system needs to be practical and it is not too high in budget or too low that it doesn't meet the requirements of the DR plan itself. It should have a practical ROI (Return of Investment) and also scalable when the business grows.
- From the technical perspective, the main point of consideration would be which technologies should be implemented to achieve the requirement of the DR plan as there are abundant choices out there in the market for the components of a DR system. The choice of technologies must be reliable and cost effective. Other than that, the technologies implemented need to have easy operation and maintenance process, so that the O&M cost is lower and the process is more efficient with limited number of personnel.



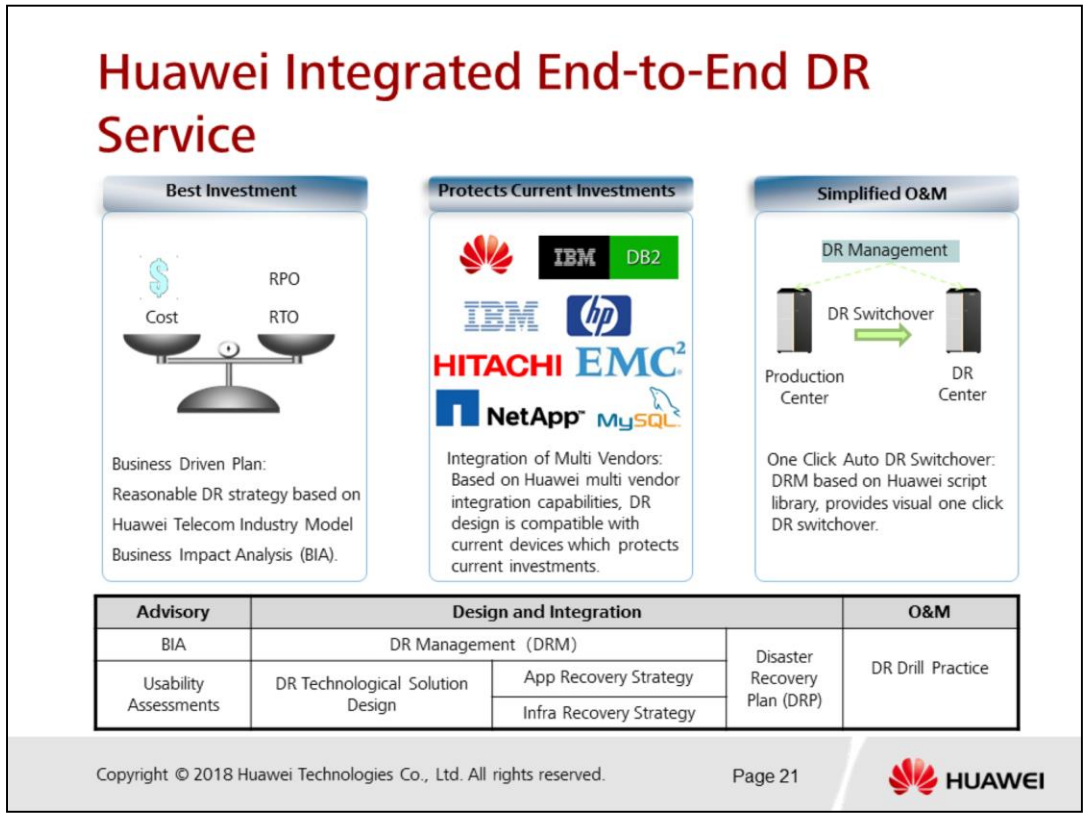
- BIA (Business Impact Analysis) analyzes the business continuity requirements from the business level. For the following example, lets consider BIA analysis for E-government service scenario. First of all, there is a need to sort out the services of the e-government before running the BIA analysis.
  - Consider the impact of downtime towards the openness, authority, social stability, government credibility, laws violations, and business scope. Impact ratings can be classified into 3 levels such as “low”, “medium”, and “high”. By calculating the sum of impact value in various businesses and sectors, we can derive the overall impact value for the downtime. The threshold for implementing DR is set at impact rating level 2 (impact value of 5-8).
  - By evaluating the impact of business downtime on 8 points of time (1h, 4h, 8h, 24h, 2d, 3d, 5d, 10d), we can derive the MAO (Maximum Acceptable Outage) for variety of businesses.
  - By analyzing the relationship between applications (including business support systems, integrated relationship between applications), we can analyze and derive the requirements of DR (RPO & RTO).
  - Based on RTO and RPO, we can classify the DR level for the e-government system into 4 different levels as shown on the table above, formulate the strategies for DR, and formulate the basis of DR solutions.
- Some countries like China published official documentations for DR standards and specifications. An example would be the document numbered (GB/T 20988-2007) titled “Information Security Technology - Disaster Recovery Specifications For Information System”.
- Social Security Center: Basic data must have a complete backup daily, and the core system RTO must meet the requirement of 4 hours.



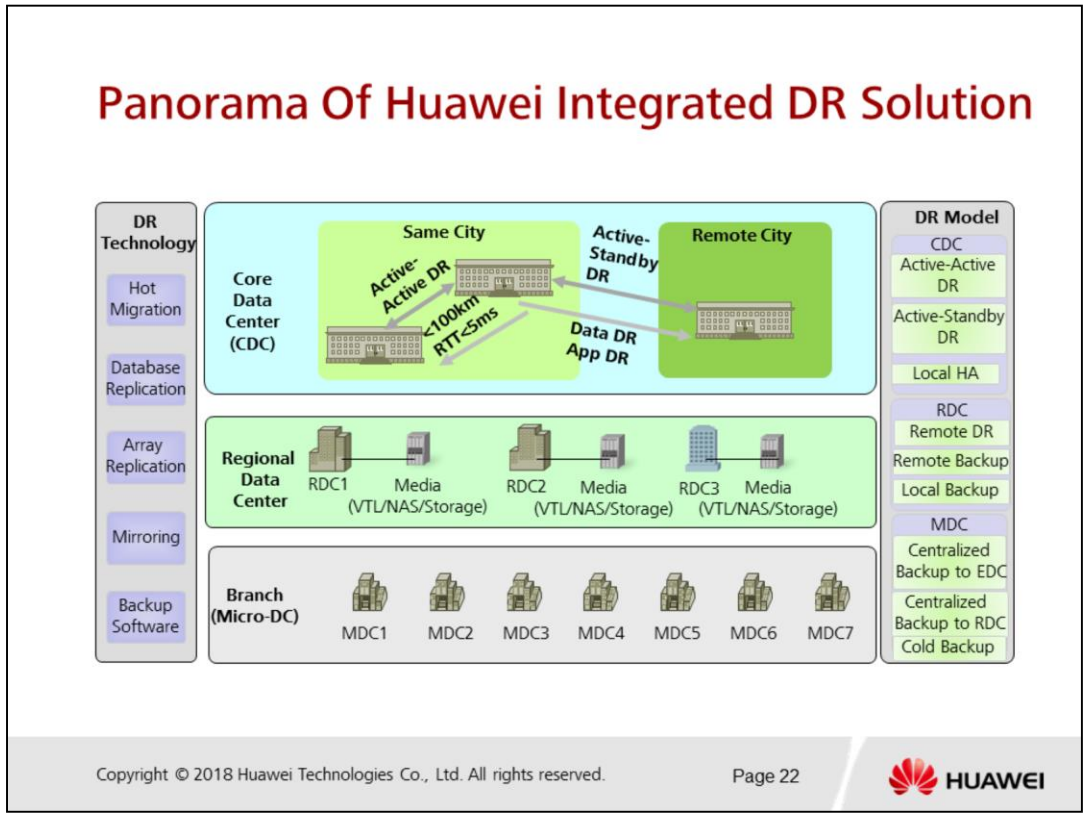
- The diagram above shows the continuous improvement method for the construction of DR systems based on the best practices in the industry and ISO guidelines.
- The process above serves as a guideline to construct, evaluate and manage the DR system to ensure that it is up to date and able to respond and recover from disasters efficiently.
- As technologies changes, more and more option is available for better DR system construction or management. As business changes, the requirements for DR may not be the same as the initial planning or setup. Hence, there is a need to continuously improve the DR system to ensure that it meets the current business requirements. It is also crucial to test the DR system or do simulated drill practices to ensure that the DR process is valid, suitable and all the personnel involved in the process are aware of their roles. This ensures that in the event of the disaster, the DR process can be carried out smoothly with lower amount of time to resume the business operations as usual.

Contents

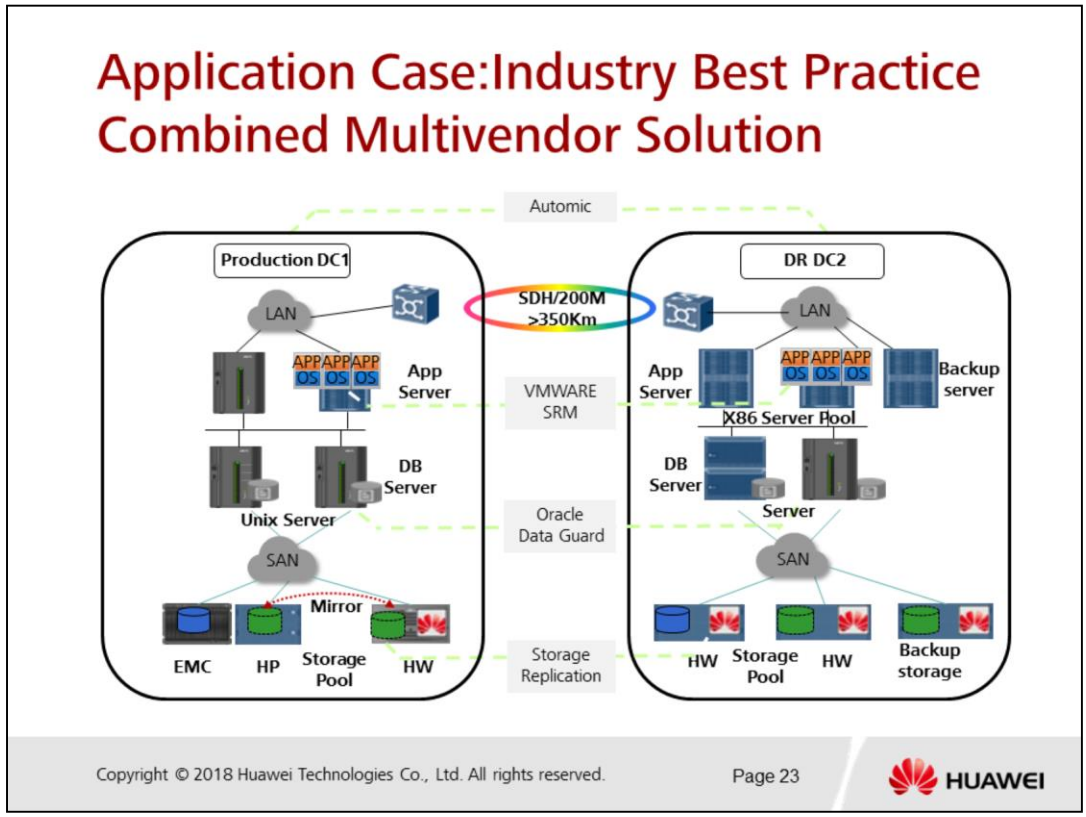
HUAWEI



- Business driven plan can be defined as the most reasonable DR target to achieve the best investment. It includes: sorting out the business systems, formulate the BIA and provide the most suitable DR strategy plan.
- Huawei's capabilities for multi vendor integration with solution design that is compatible with current devices, effectively protects current investments. Huawei provides complete DR solutions from data level to application level that can be configured to meet the different requirements of variety of businesses.
- One click auto switchover lowers the complexity of DR operation and maintenance. Other enhancements of Huawei DR solution are:
    - Visual daily management and switchover management: Through the use of DRM management platform, the daily O&M and the switchover process can be visualized and the progress of the switchover can be monitored in real time.
    - Switchover Drill Practice: The DR switchover process can be simulated through the DRM platform, which lowers the cost of O&M drill practice.
    - One click auto switchover: It is based on Huawei script libraries which allows servers, databases and DNS switchover to be scripted, and all the action script are run with an one click operation. Hence, in the event of a disaster, the switchover process from production to DR center can be completed with ease.



- The diagram above shows the panorama of the Huawei DR systems. Huawei's solution for disaster recovery and business continuity is comprehensive and covers all aspects of data protection, application recovery and data center level disaster recovery either within the city or from a remote region.
- Huawei's DR solution design is compatible with lots of different and latest DR technologies within the market, and can be built in various DR models to meet customer requirements.
- Different configurations in the levels of branches, regional data center and core data center allows a flexible and scalable DR system to be implemented which satisfies the different DR needs from each levels.

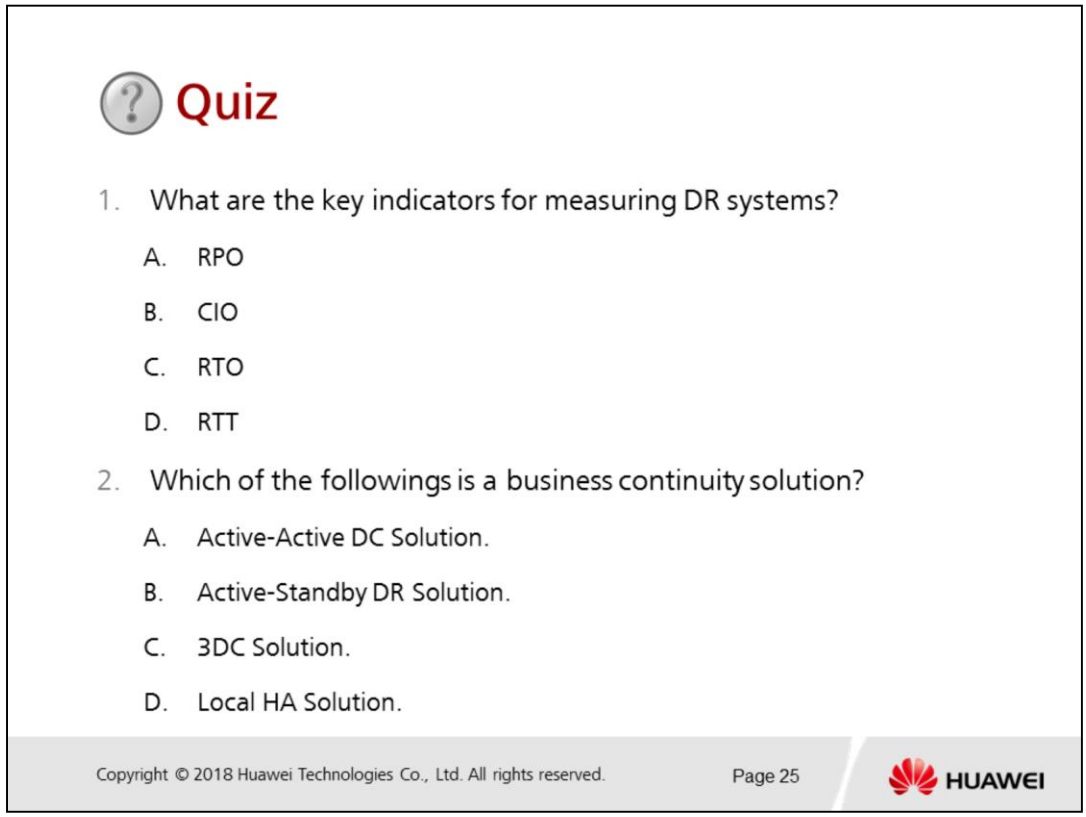


- Key Technologies of the solution:
  - Implements Active-Standby DC model over a distance of 350 km.
  - Main DC uses Oceanstor 6800 V3/18K with heterogeneous architecture of EMC/IBM/HP storage.
  - VMWARE SRM manages the virtual machine synchronization.
  - Oracle Data Guard manages the database synchronization.
  - Implements Huawei storage replication for data synchronization.
  - Implements Automic DRM software for automated DR management.

- Benefits to the customer:
  - Help the customer to solve the problems of constructing a one-stop IT disaster recovery center, and eliminate potential safety problems.
  - Dual insurance on the data restoration, increases data protection level.
  - Core application RTO is lower than 2 hours, RPO lower than 10 minutes.
  - Storage online dynamic expansion, which saves maintenance cost by 15%.

Summary

- This module mainly introduced:
  - The Challenges Of Business Continuity.
  - The Definition Of Business Continuity.
  - The Overview Of Business Continuity Solutions.
  - Panorama Of Huawei Business Continuity Solutions.



- Answers:
  - AC.
  - ABCD.

Thank You

www.huawei.com