IBM GROUP 5
CLOUD COMPUTING
PHASE-3

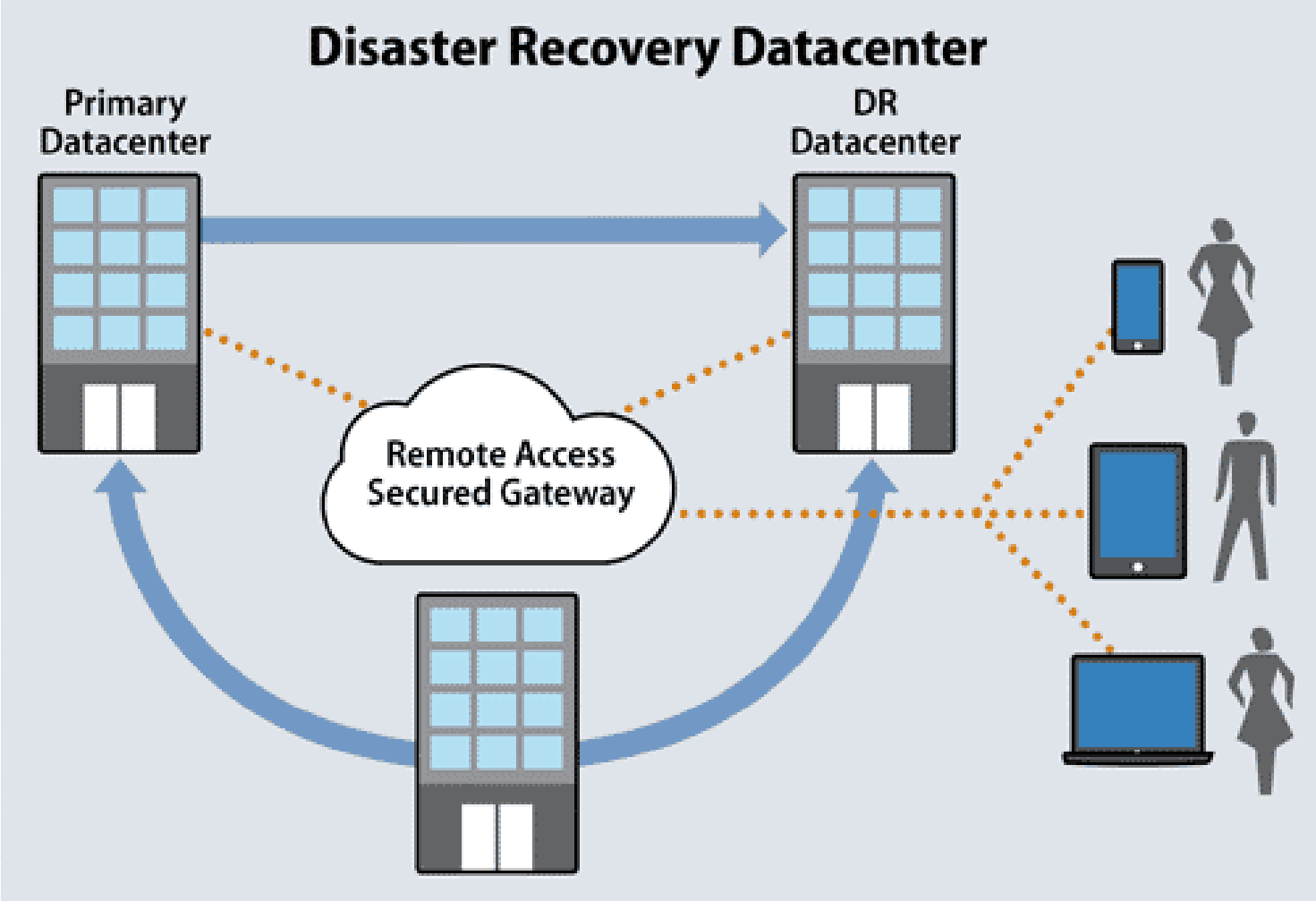
DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

- **Why Is Disaster Recovery Important?**
- Businesses rely on documents, files, servers, and applications for their daily operations. If sensitive data or a critical system is lost or goes offline, this can have a major impact on an organization, leading to financial losses, reputation loss, and even legal exposure.
- A disaster is an unexpected problem that can slow, disrupt, or destroy IT systems. This could be an earthquake or other natural disaster, a technical malfunction or equipment failure, human error, or an attack by malicious parties, either inside or outside the organization.

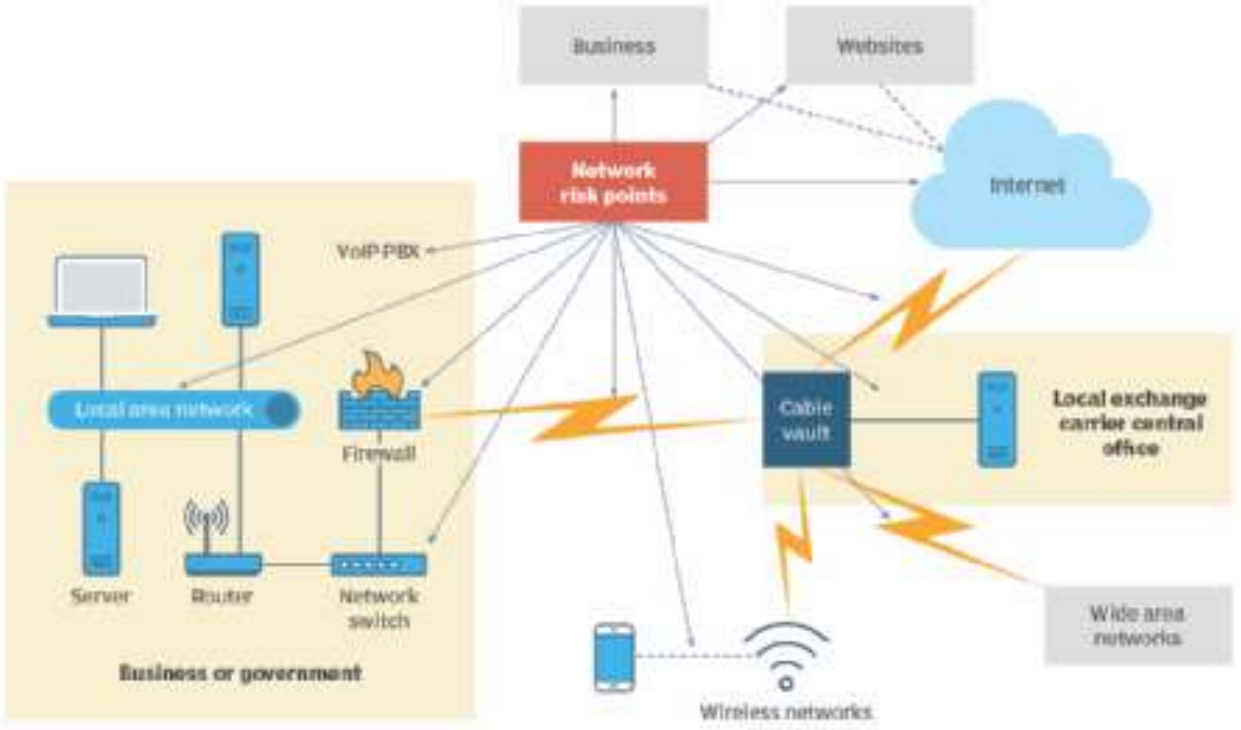
- **Ensure business continuity**—loss of data, limited access to business productivity tools, and downtime for customer-facing systems, can be highly disruptive for an organization. Disaster recovery enables quick restoration of affected systems, or failover to backup systems, enabling the business to continue functioning despite the disaster.
- **Improve system security**—implementing data protection, backup and recovery processes can limit the impact of ransomware, malware, or other security risks.
- **Improve customer retention**—in many cases, customers will not continue to do business with an organization after their personal data was lost or compromised, or after the business goes offline for a prolonged period of time. Business continuity helps maintain customer trust and ensure retention even in the event of a large-scale disaster. Organizations can also gain a competitive advantage by preparing for disasters better than others in their industry.
- **Reduce recovery costs**—most disasters will have a negative impact on an organization, but with effective DR solutions in place, the damage can be minimized and so is the cost and effort of recovering systems to their original state.

- # Types of Disaster Recovery Solutions
- **1. Data Center Disaster Recovery**
- Organizations with proprietary data centers must implement a disaster recovery strategy that addresses all IT infrastructure components in the data center and the surrounding physical facility. This strategy typically centers on backups to failover sites housed in secondary data centers or co location facilities. Business and IT leaders should document the various components of these physical facilities, including heating, cooling, power, fire response, and security controls.
- **2. Network Disaster Recovery**
- Network connectivity is critical for external and internal communication, application access, and data sharing in the event of a disaster. The network disaster recovery strategy should detail a plan to restore network services and ensure access to backup data and secondary storage sites.
- **3. Virtualized Disaster Recovery**
- Organizations can use virtualization to replicate workloads in a secondary location or cloud environment for disaster recovery. Virtualized DR is flexible, easy to implement, fast, and efficient—virtualized workloads have small IT footprints, support frequent replication, and enable fast failover initiation. Various data protection vendors provide virtual DR and backup products.

- **4. Disaster Recovery in the Cloud**
- With many cloud services available, organizations can host DR systems in a cloud environment rather than in a physical location. Cloud disaster recovery involves more than cloud backup. IT teams must configure automatic workload failover to the DR cloud platform for immediate recovery when a disruption occurs.
- **5. Disaster Recovery as a Service (DRaaS)**
- DRaaS is a commercially available cloud DR service that allows an organization to replicate and host its virtual and physical servers on a third party's infrastructure. The DR service provider is responsible for implementing the disaster recovery plan during a crisis based on the service-level agreement.
- There are various disaster recovery providers, given that DR extends beyond IT. Some vendors sell backup and disaster recovery tools, while others offer fully managed or hosted DR services. Disaster recovery also encompasses risk management, so some vendors provide additional security features such as emergency plans and incident response.


Disaster Recovery Datacenter
Primary Datacenter
DR Datacenter
Remote Access Secured Gateway

Network risk points to address in a DR plan



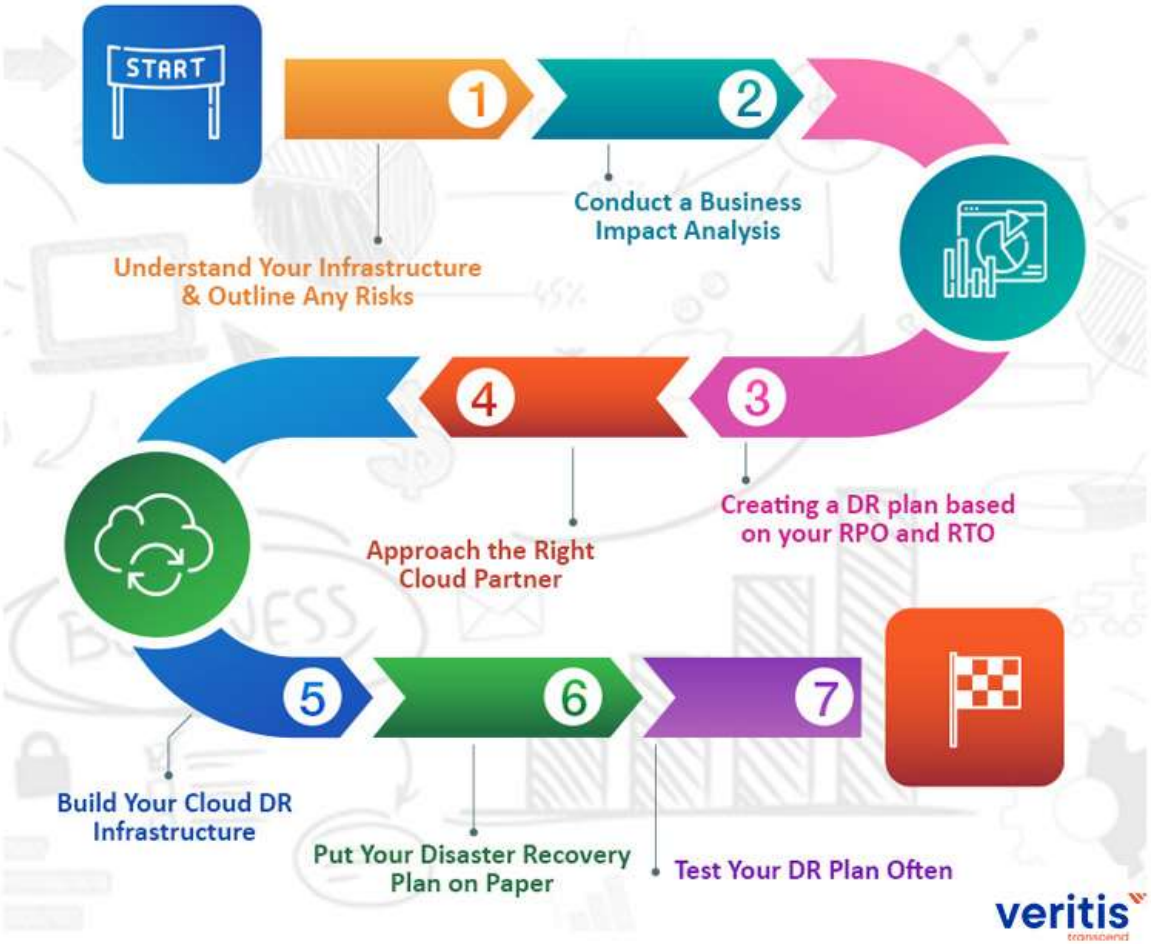
Traditional Architecture

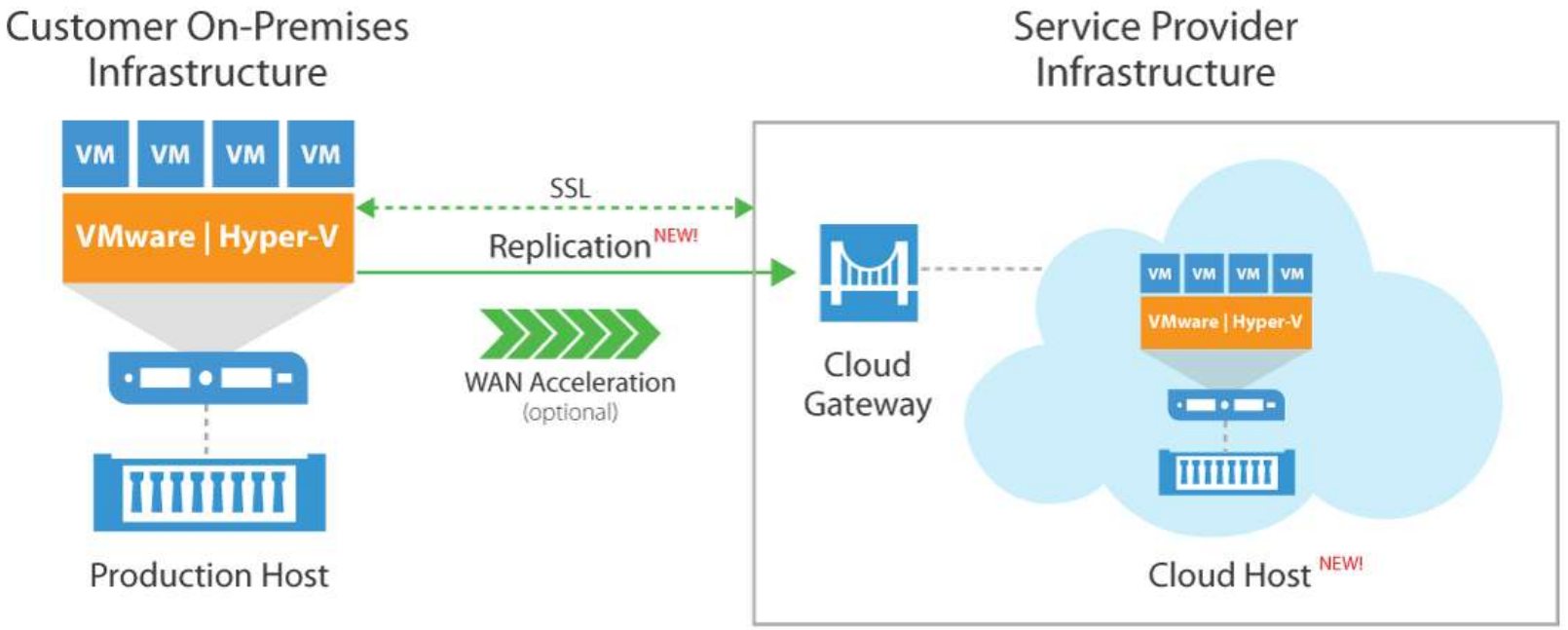
- Single operating system
- Single application

Virtual Architecture

- Virtualize many VMs using VMware Hypervisor

Cloud Disaster Recovery Plan




Customer On-Premises Infrastructure
Service Provider Infrastructure
VM
VM
VM
VM
VMware | Hyper-V
SSL
Replication NEW!
WAN Acceleration
(optional)
Cloud Gateway
VM
VM
VM
VM
VMware | Hyper-V
Production Host
Cloud Host NEW!

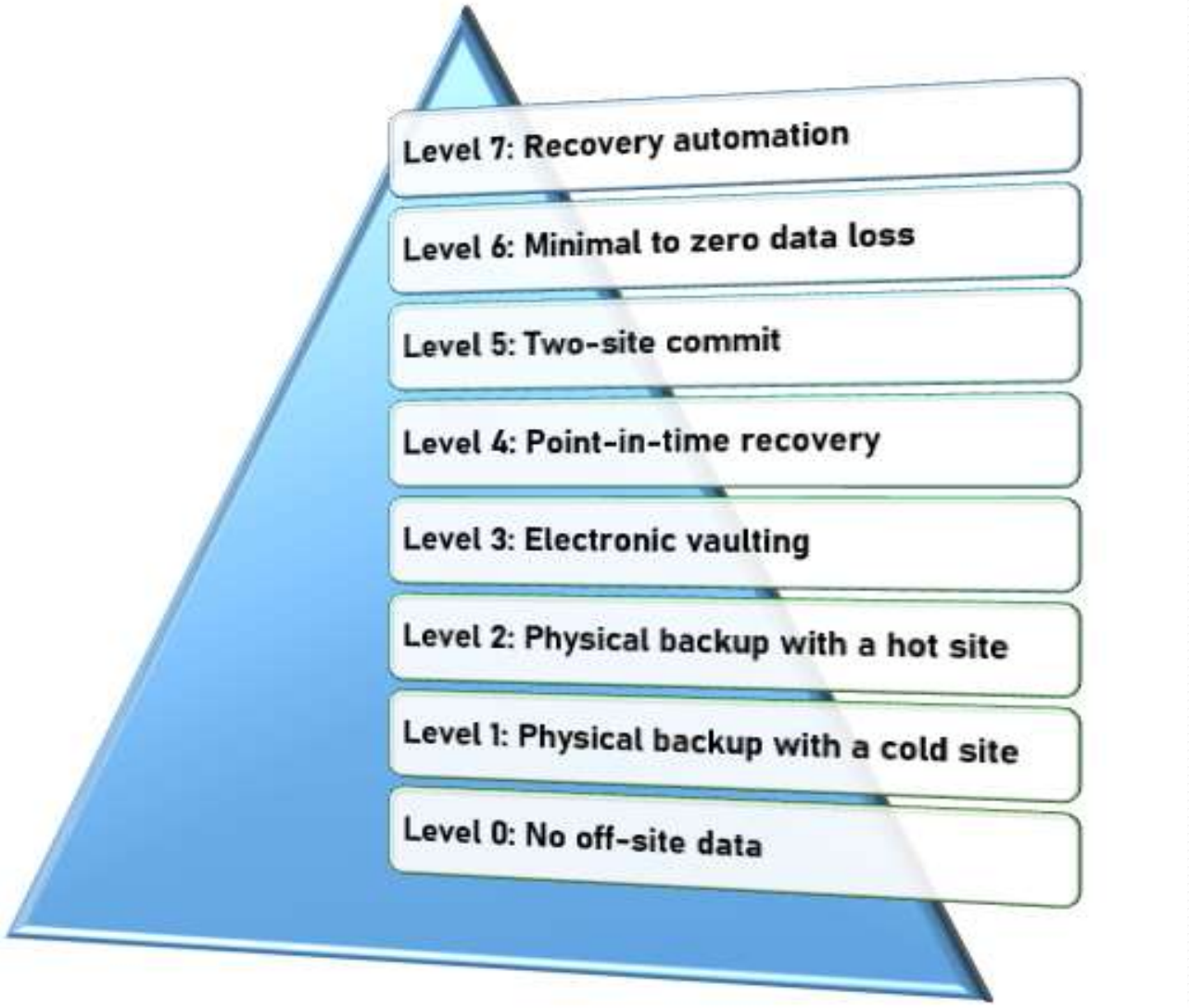
- **IT Disaster Recovery Plan Checklist**
- The first steps of the DRP process may not be found in the pages of the DRP itself. Rather, they encompass some elements of a Business Continuity Plan (BCP), which incorporates a DRP, to provide a better understanding of where your DRP lies within your organization's planning schema. Disaster Recovery Plans kick in when there is an issue of some sort, and mainly deal with restoring service, whereas a BCP will incorporate risk and business impact assessments, along with prevention measures.
- These goal-setting exercises and business reviews help ensure that all stakeholders agree on the definition of a successful recovery and that the enterprise is investing adequately in preparation and recovery to make it happen. They also ensure that data center disaster recovery best practices are being incorporated from the start.
- The DRP and surrounding processes entail the following key actions.
- **1. Assess Downtime Tolerance**
- Before you can plan for recovery, you need to know what the expectations are. For a company reliant on real-time, mission critical software, a few seconds of downtime is costly, so recovery expectations and investment in preparation will be high. For smaller or less tech-focused enterprises, longer outages may be acceptable and a less robust and expensive DR solution may suffice.
- Of course, network downtime tolerance often changes over time; e.g., as the business grows, products or services evolve, or customers with higher expectations come on board. Update the DR team's understanding of expectations so the plan can be modified accordingly.
- **2. Take Inventory**
- Before doing anything else, it's critical to take inventory. What systems are in place? What is the likely scenario if a system goes down? Does your organization implement data center redundancy to help protect against power outages or hardware failures?

- **3. Pinpoint Deficiencies**
- You'll also need to know your data center's weaknesses. What are your strategic weak points? Some of the top data center challenges include data center design oversights, power supply failures, and environmental issues that strain energy resources.
- **4. Define Recovery Objectives**
- Next, you need to determine your RTO and RPO. Let's break those down for you:
- ***Recovery Time Objective (RTO)***
- Your recovery time objective (RTO) is all about the amount of time you need to recover applications.
- ***Recovery Point Objective (RPO)***
- RPO indicates the age of the files that you need to recover for normal operations to resume.
- These recovery metrics are extremely similar in nature to network failure metrics like MTBF, MTTR, and MTTF.
- **5. Conduct Risk Assessment**
- Conduct a full risk assessment for your data center. What are the most likely threats you'll face and how likely are they to occur? Go beyond planning for natural disasters – how likely are you to face radiation exposure or explosives?

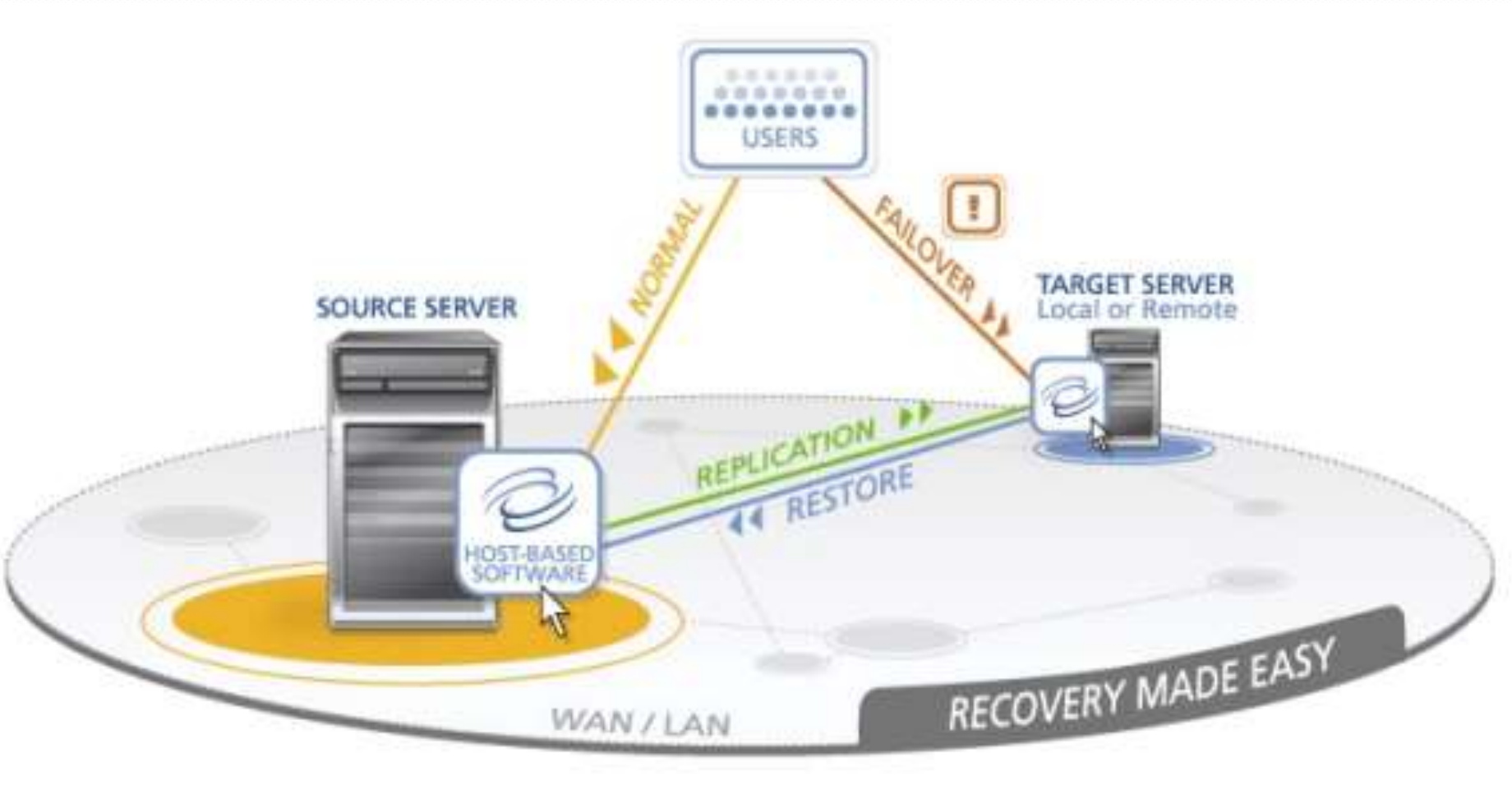
- **Network disaster recovery plan with Network Configuration Manager**
- A **network disaster recovery plan** is a set of policies to help you restore all your organization's network operations after a network disaster. A network disaster can range from performance degradation to complete network outage. While network disasters are often caused by human error, this page will list the common sources of network disasters, and how Network Configuration Manager acts as a **network disaster recovery tool** and helps solve them.
- **1. Network disaster due to bandwidth hogs**
- Organizations often invest a lot of money into acquiring large amounts of bandwidth that is shared by every user on the network. When a single user disproportionately consumes a lot of bandwidth on a typical network, it can affect the entire network. Situations like these lead to other users on the network experience lag, causing performance degradation.
- Network disaster recovery plan to fix bandwidth hogs

- **2. Network disaster due to faulty configuration changes**
- Network infrastructures are prone to human errors since they are subject to frequent manual changes. Such errors can cause vulnerabilities in the network that lead to network disasters. Shutting down interfaces is one such common error. Users shutting down an interface can render a group of devices inaccessible to everyone on the network.
- Network disaster recovery plan to fix faulty configuration changes
- Moderation of network infrastructure changes can be achieved through role-based access control and change notifications in Network Configuration Manager. With a role-based access control, every user is assigned a role which will define the devices they can access. With Network Configuration Manager you can assign operator or admin roles to users. While admin have access to all devices in the network, operators will have to make a request to the admin each time they try to change a configuration. Once a change is processed, the operator receives a notification of the status of the configuration upload.
- Network Configuration Manager also has a rollback mechanism to undo any configuration changes that disrupt network performance. The rollback mechanism helps you maintain business continuity.

- **IT mega trend: Virtualization disaster recovery**
- If you are deeply involved in the IT industry, you must understand how important disaster recovery is for an enterprise.
- **Disaster recovery (DR)** relies upon the replication of data and computer processing in an off-premises location not affected by the disaster. When servers go down because of a natural disaster, equipment failure or cyber attack, a business needs to recover lost data from a second location where the data is backed up.


Level 7: Recovery automation
Level 6: Minimal to zero data loss
Level 5: Two-site commit
Level 4: Point-in-time recovery
Level 3: Electronic vaulting
Level 2: Physical backup with a hot site
Level 1: Physical backup with a cold site
Level 0: No off-site data

- Virtual disaster recovery refers to the use of virtualized workloads for disaster recovery planning and **failover.** To achieve this, organizations need to regularly replicate workloads to an offsite virtual disaster recovery site.
- For enterprises in virtual environments, **VM replication** provided by hypervisor vendors may be enough. As for physical or hybrid environments, **physical to virtual conversion (P2V)** is still needed before replication.


USERS
NORMAL
FAILOVER
SOURCE SERVER
TARGET SERVER
Local or Remote
REPLICATION
RESTORE
HOST-BASED
SOFTWARE
WAN / LAN
RECOVERY MADE EASY

- **What makes a good disaster recovery plan**
- A good disaster recovery plan is the one that is best suited to the enterprises' actual situation. In practice, the following factors are most often taken into consideration:
- **Recovery Time Objective (RTO)** -- the measure of downtime
- **Recovery Point Objective (RPO)** -- the measure of data loss
- **Test Time Objective (TTO)** -- the measure of testing ease

- These recovery objectives vary according to disaster recovery solutions, such as the following graph:

Solution	Cost	RPO	RTO	TTO
Server Clustering	$$$$$	Near Zero	Near Zero	Near Zero (Impacts production data, ads risk)
Consolidated Recovery (virtualization)	$$$$	Minutes	Minutes	Minutes (No impact on production data)
Imaging (virtualization)	$$$	Hours	Hours	Minutes (No impact on production data)
Image Capture	$$$	24h	Hours	Hours (Requires additional hardware)
Tape/Manual Rebuild	$	24h+	Days	Days (Not practical)

Conclusion

- We have seen the three types of disaster recovery with IBM virtual cloud services.
- In the phase 3 – development part 2 we will see the rest of the types and processing datasets .
- The remaining types of disaster recovery plans are Disaster recovery in the cloud, Disaster recovery as a service.