Cloud Disaster Discovery

Efrizal Zaida, S.Kom., M.M.,M.Kom
efrizal@nurulfikri.ac.id

Disaster Recovery Plan

What is Disaster?

A disaster is a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources.

Type Disaster

1) Natural disaster

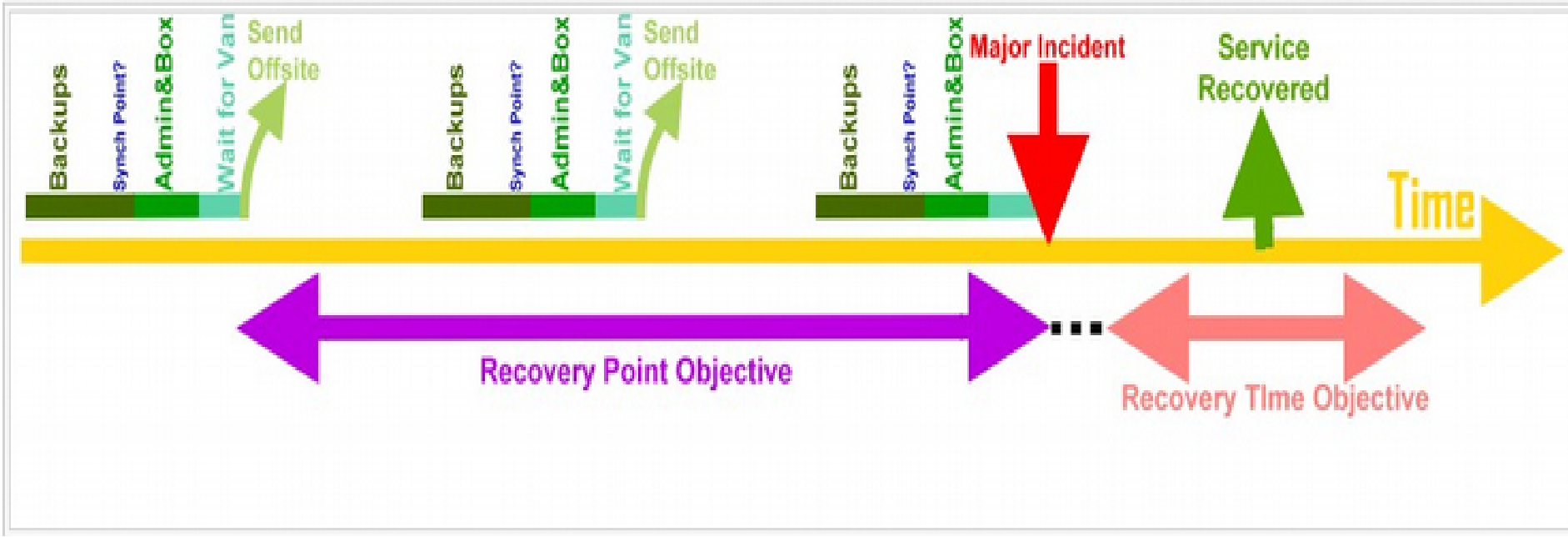
A natural disaster is a major adverse event resulting from the earth's natural hazards. Examples of natural disasters are floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. Other types of disasters include the more cosmic scenario of an asteroid hitting the Earth.

2) Man-made disasters

Man-made disasters are the consequence of technological or human hazards. Examples include stampedes, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation and acts of war. Other types of man-made disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism.

Kategori Jangka Waktu Antisipasi

- Strategi jangka pendek (*short-term*),
  - menyediakan fasilitas TI alternatif.
- Strategi jangka panjang (*long-term*),
  - menyediakan fasilitas TI yang permanen



IT DRP

Jika terjadi bencana, maka organisasi harus memobilisasikan semua kemampuan dan sumber daya yang dibutuhkan untuk melanjutkan kegiatan operasionalnya dan mengembalikan keadaan menjadi normal secepat mungkin karena waktu adalah uang.

Bencana

Mobilitas Sumber Daya

Kembali Operasional

Bencana dalam dunia IT

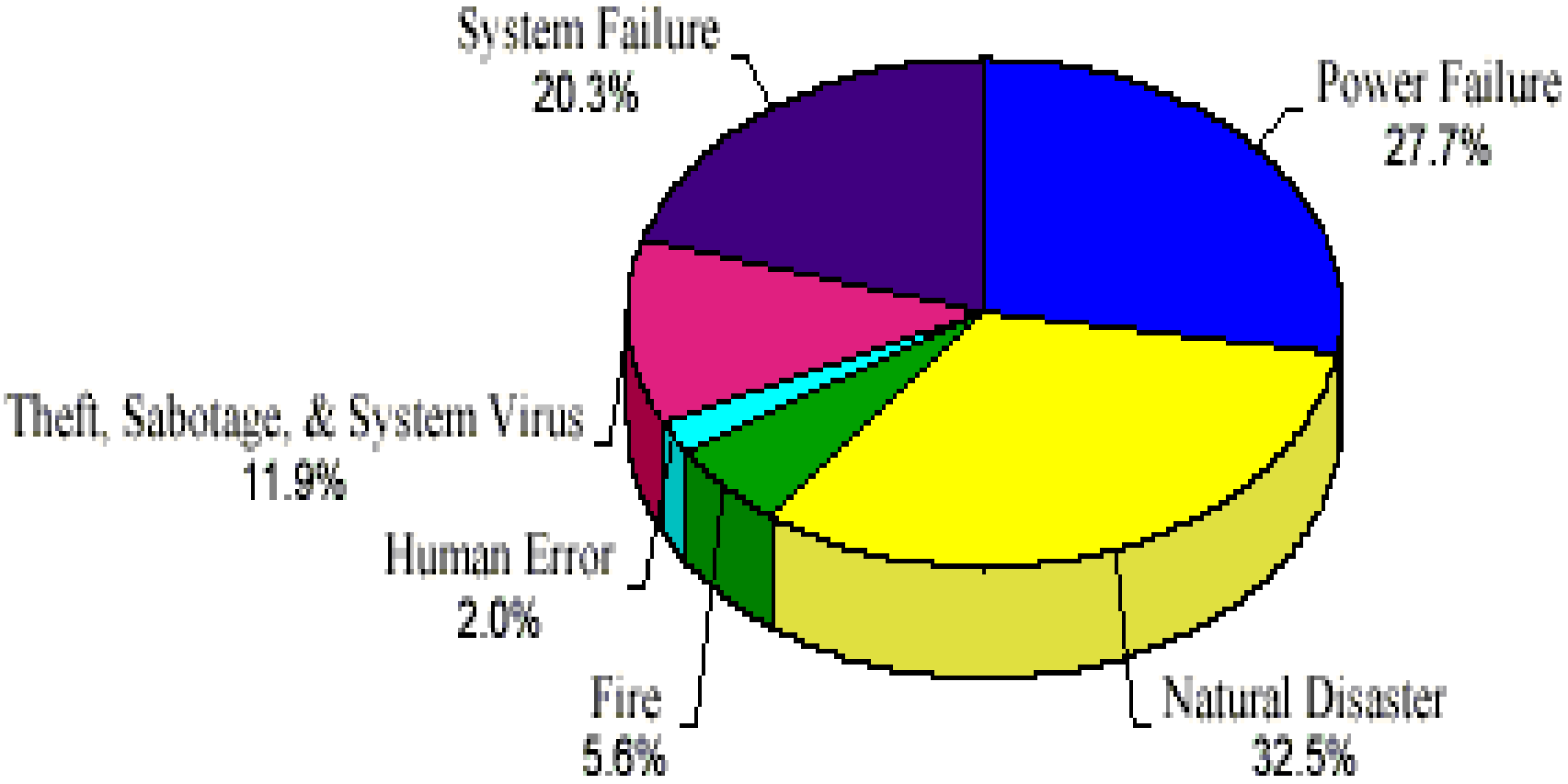
Kejadian yang mengakibatkan kegagalan sistem dan memberikan dampak yang membahayakan terhadap bisnis yang dijalankan

50% dari perusahaan yang pernah mengalami kegagalan sistem akibat bencana, tidak akan bertahan hidup dan 90% nya akan mati dalam 2 tahun.

BCP and DRP

- Business Continuity Planning and Disaster Recovery : melibatkan usaha persiapan testing dan peremajaan(update) yang dibutuhkan untuk melindungi proses bisnis yang paling penting.

Kategori Bencana dalam IT



Business Contiuity Plan

BCP adalah mengenai pembuatan perencanaan dan frame-work untuk menjamin bahwa proses bisnis dapat terus berlanjut dalam keadaan emergensi. Sedangkan DRP adalah mengenai pemulihan cepat dari keadaan emergensi atau bencana, sehingga hanya mengakibatkan dampak minimum bagi organisasi atau perusahaan.

- Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) adalah dua hal yang sangat penting dalam proses bisnis,
  - jarang menjadi prioritas karena
    - alasan memerlukan biaya yang mahal dan sulit penerapannya.
    - bencana adalah hal yang umumnya diyakini karena faktor alam yang tak dapat diprediksi dan tak dapat dicegah atau pun dihindari
- mendapatkan dukungan dari pihak manajemen.
  - Sudah terlalu sering BCP menempati urutan prioritas terendah, atau proyek ini ditangani staf junior.

Business Continuity Plan (BCP)

- Kontinuitas layanan TI perusahaan harus dijaga dari gangguan:
  - Bencana alam
  - Ulah manusia (disengaja atau tidak)
  - Kerusakan.
- Dibutuhkan perencanaan untuk mencegah, menangani, dan menanggulangi gangguan
  - *Policy* dan prosedur penanganan bencana.
  - Strategi pemulihan layanan.
  - Strategi minimasi dampak bencana.

Sekilas tentang BCP

- BCP adalah proses otomatis atau pun manual yang dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin kontinuitas layanan bagi operasi yang penting.

- BCP didisain untuk melindungi proses bisnis vital dari kerusakan atau bencana yang terjadi secara alamiah atau perbuatan manusia, dan kerugian yang ditimbulkan dari tidak tersedianya proses bisnis normal.

- Strategi meminimalisir efek dari ganguan dan mengupayakan berjalannya kembali proses bisnis

Tujuan & Manfaat BCP

Tujuan:

- meminimalisir efek dari kejadian atau bencana tersebut dalam sebuah perusahaan atau organisasi.

Manfaat:

- mereduksi risiko kerugiaan keuangan dan meningkatkan kemampuan perusahaan untuk memulihkan diri dari bencana atau gangguan sesegera mungkin.
- Perencanaan keberlangsungan bisnis juga harus dapat membantu meminimalisir biaya dan mengurangi risiko sehubungan dengan kejadian bencana tersebut.

- DRP meliputi :
  - Disaster Recovery Planning (DRP) (rencana pemulihan dari bencana)
  - Testing the disaster recovery plan

    (pengujian terhadap rencana pemulihan)
  - Disaster recovery procedures

    (prosedur pemulihan dari bencana)

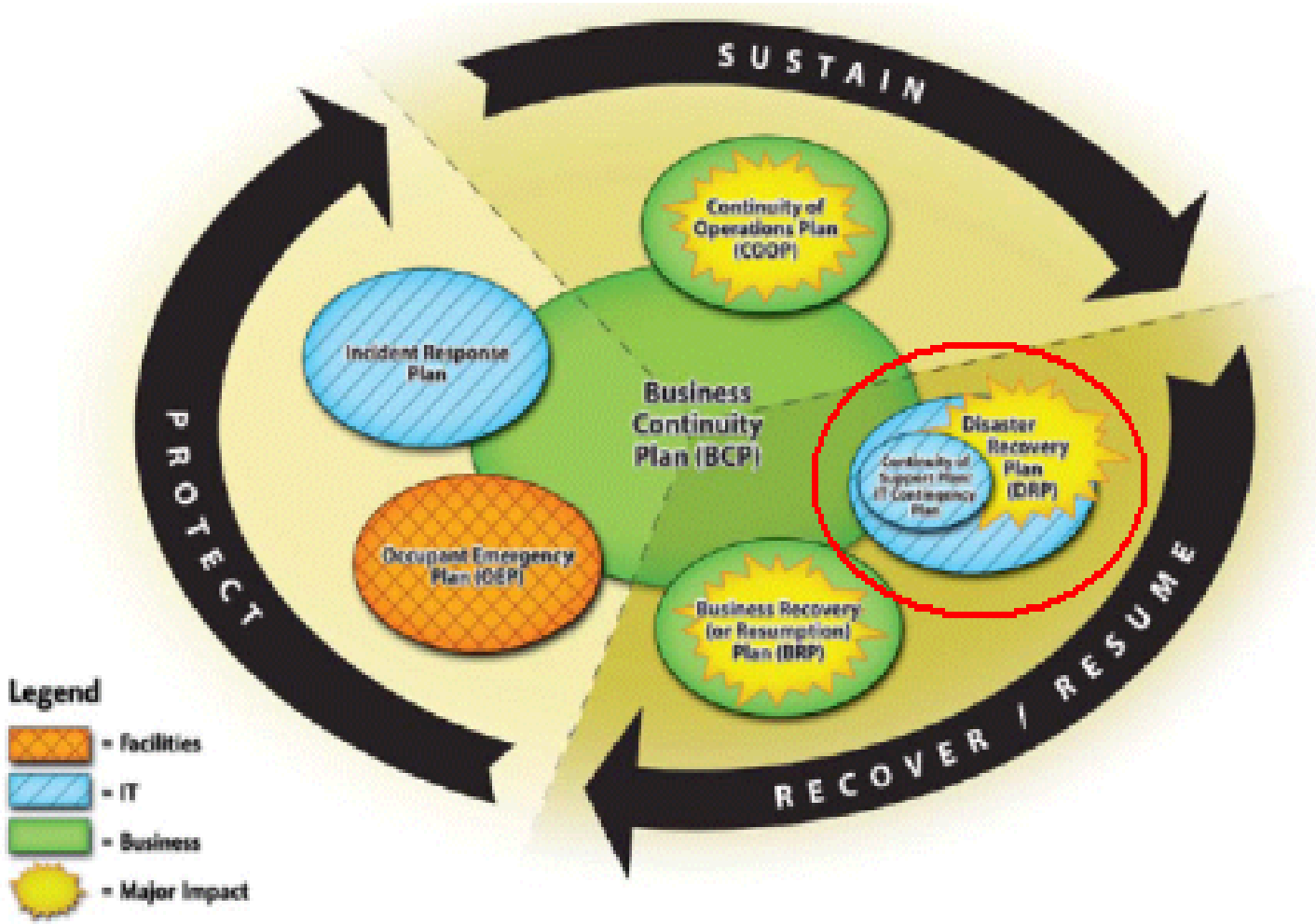
DRP Procedure

Table 8.2: Disaster Recovery Plan Testing Types

Level	Type	Description
1	Checklist	Copies of plan are distributed to management for review.
2	Structured walk-through	Business unit management meets to review the plan.
3	Simulation	All support personnel meet in a practice execution session.
4	Parallel Test	Critical systems are run at an alternate site.
5	Full-Interruption Test	Normal production shut down, with real disaster recovery processes.

BCP Objectives

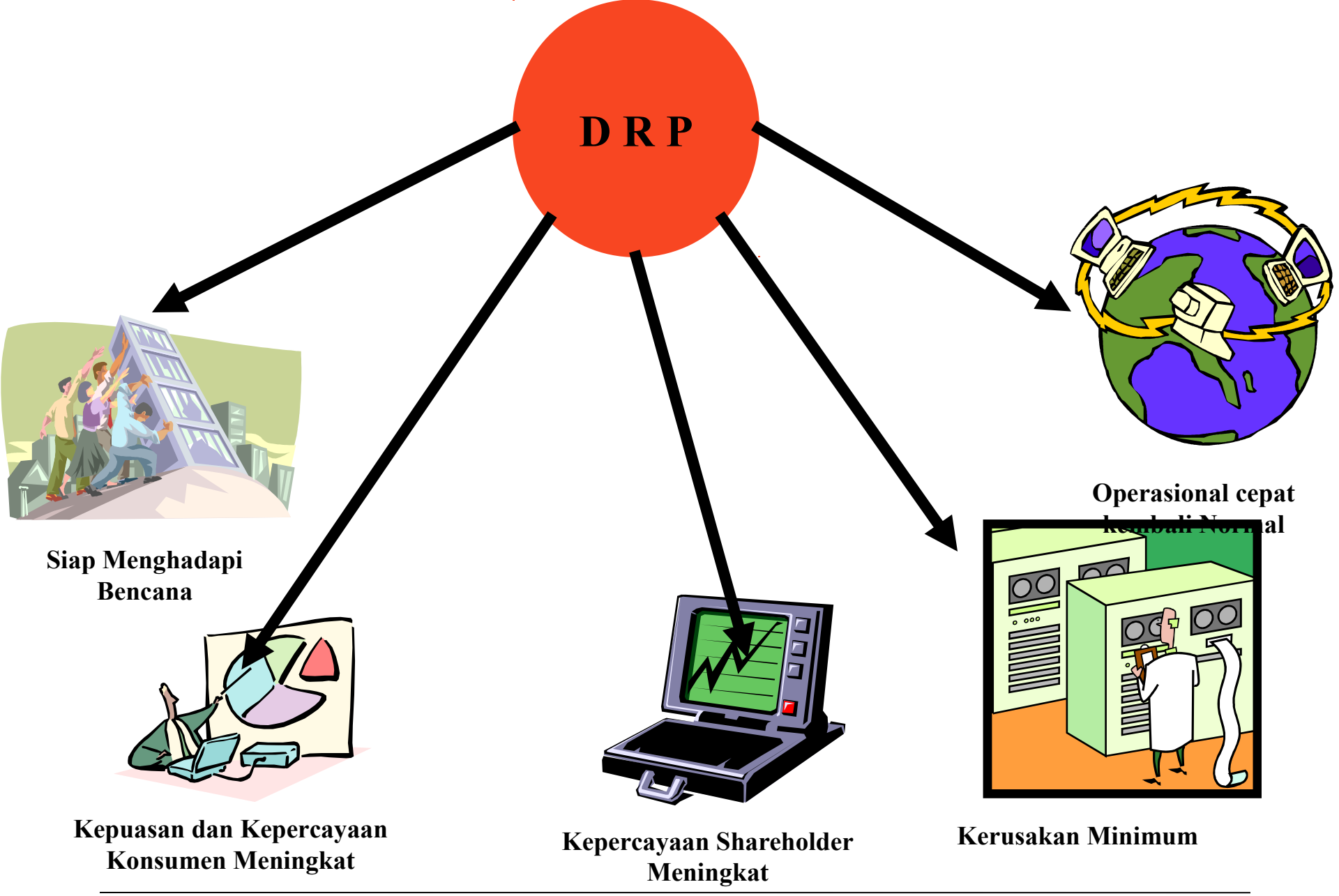
Areas Covered by an Emergency Preparedness Plan
(Adapted from a NIST Special Publication)



Filosofi

Keinginan organisasi untuk **melindungi dan mempertahankan citra positif organisasi**, termasuk melindungi dan mempertahankan aset fisik dan kelangsungan hidup karyawannya.

Citra positif organisasi ini termasuk di dalamnya adalah kepuasan konsumen yang tinggi dan tingkat kepercayaan shareholder yang tinggi pula


D R P
Siap Menghadapi Bencana
Operasional cepat kembali Normal
Kepuasan dan Kepercayaan Konsumen Meningkat
Kepercayaan Shareholder Meningkat
Kerusakan Minimum

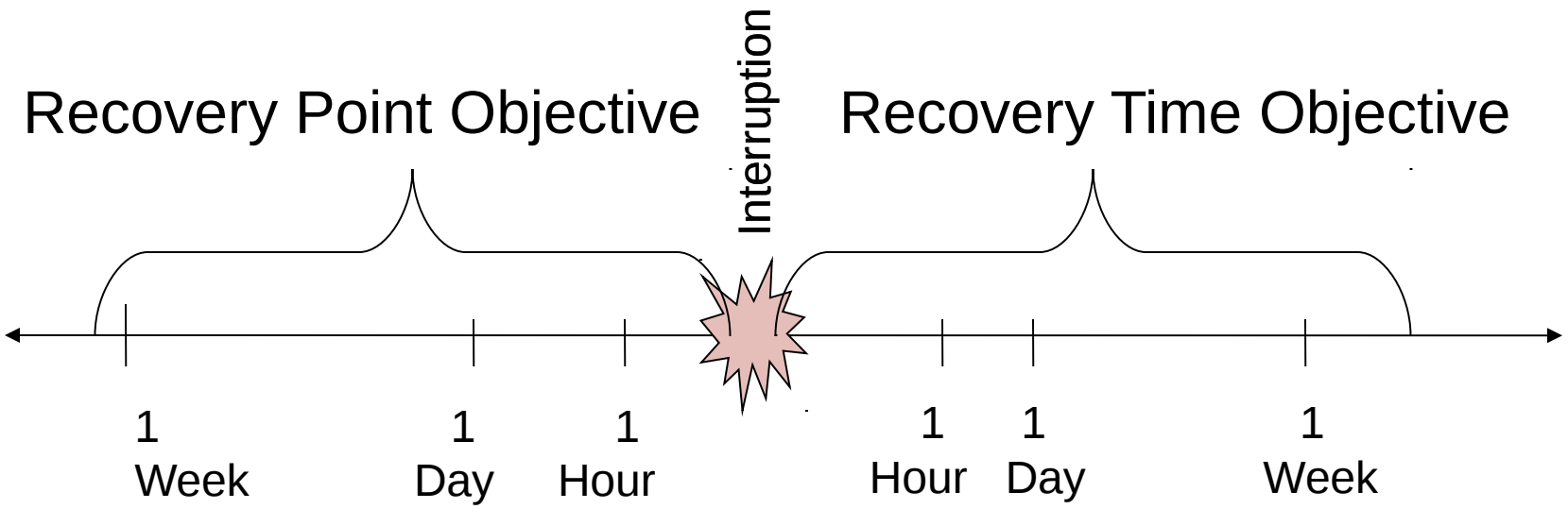
Critical Success Factor

- Recovery Time Objective (RTO)

  waktu yang dibutuhkan untuk melakukan recovery secara keseluruhan hingga sistem berjalan lagi
- Recovery Point Objective (RPO)

  jumlah data yang boleh hilang akibat bencana yang terjadi

RPO and RTO



How far back can you fail to?
One week's worth of data?

How long can you operate without a system?
Which services can last how long?

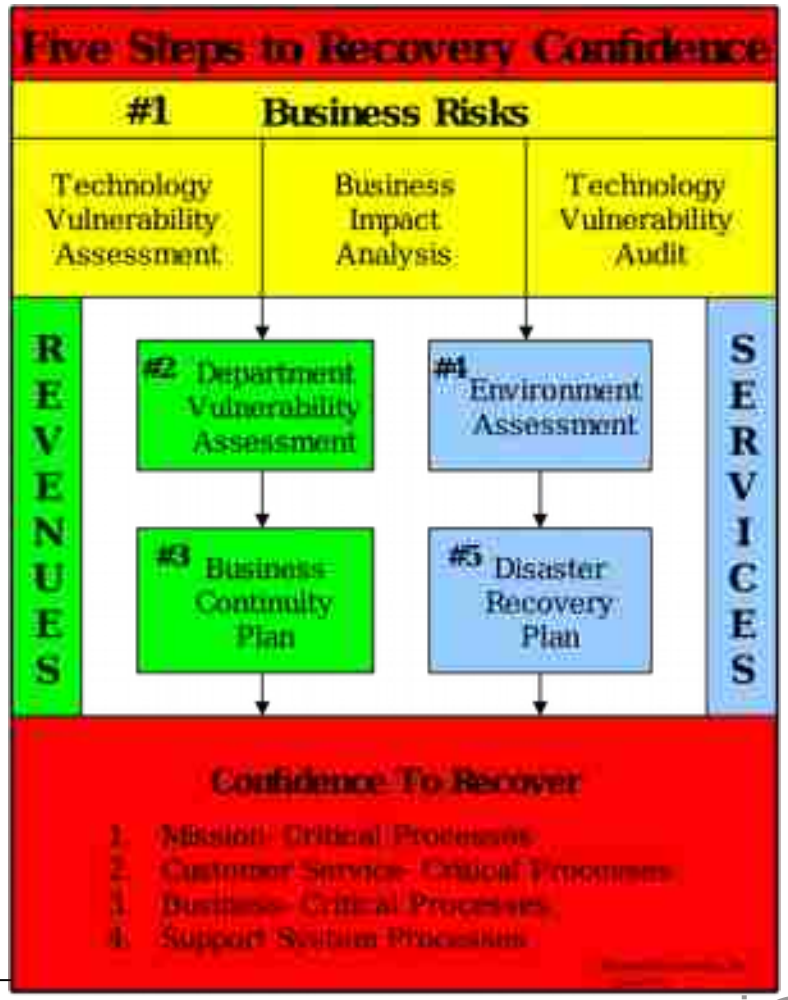
Disaster Strikes

What Would You Do?

Methodology

Business Continuity Planning
Disaster Recovery Planning

"Five Steps to Recovery Confidence"

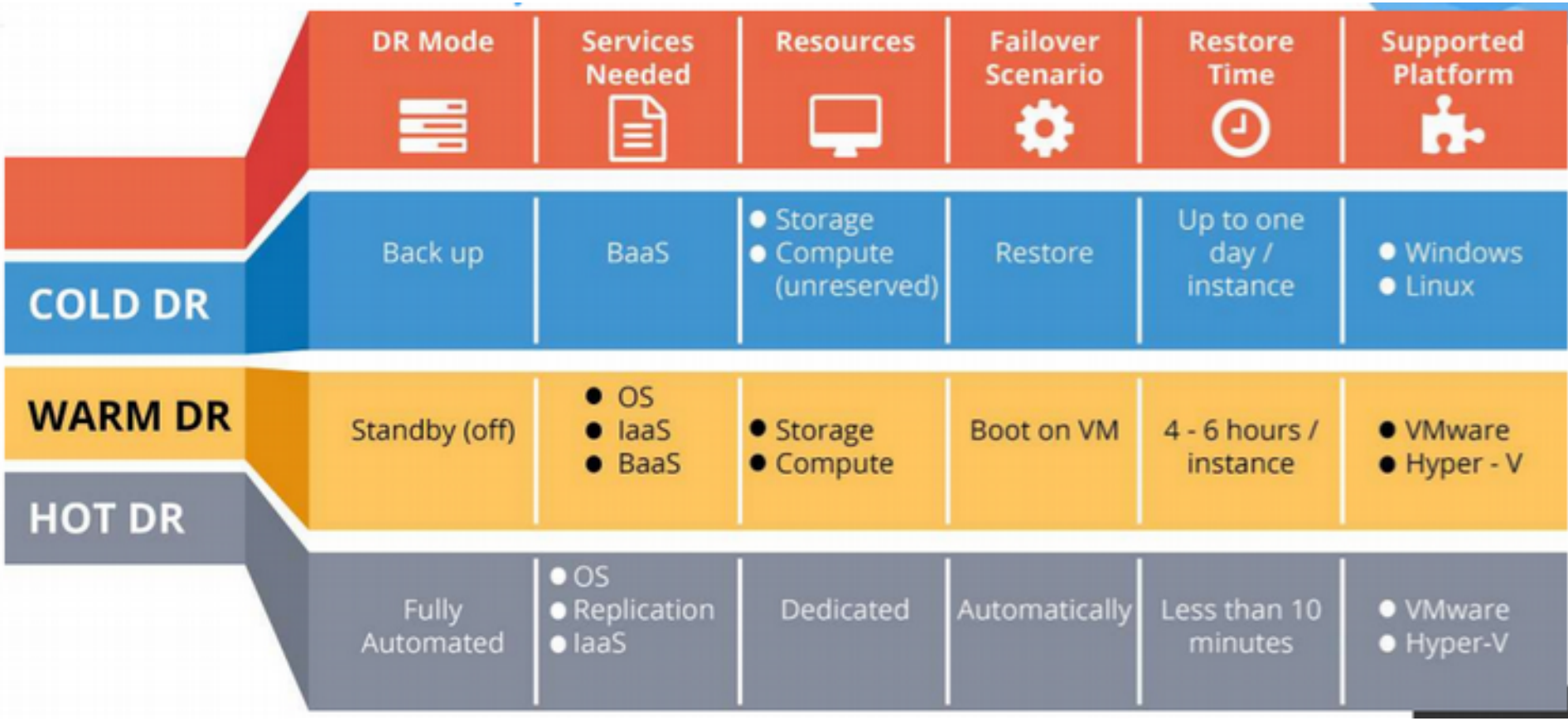


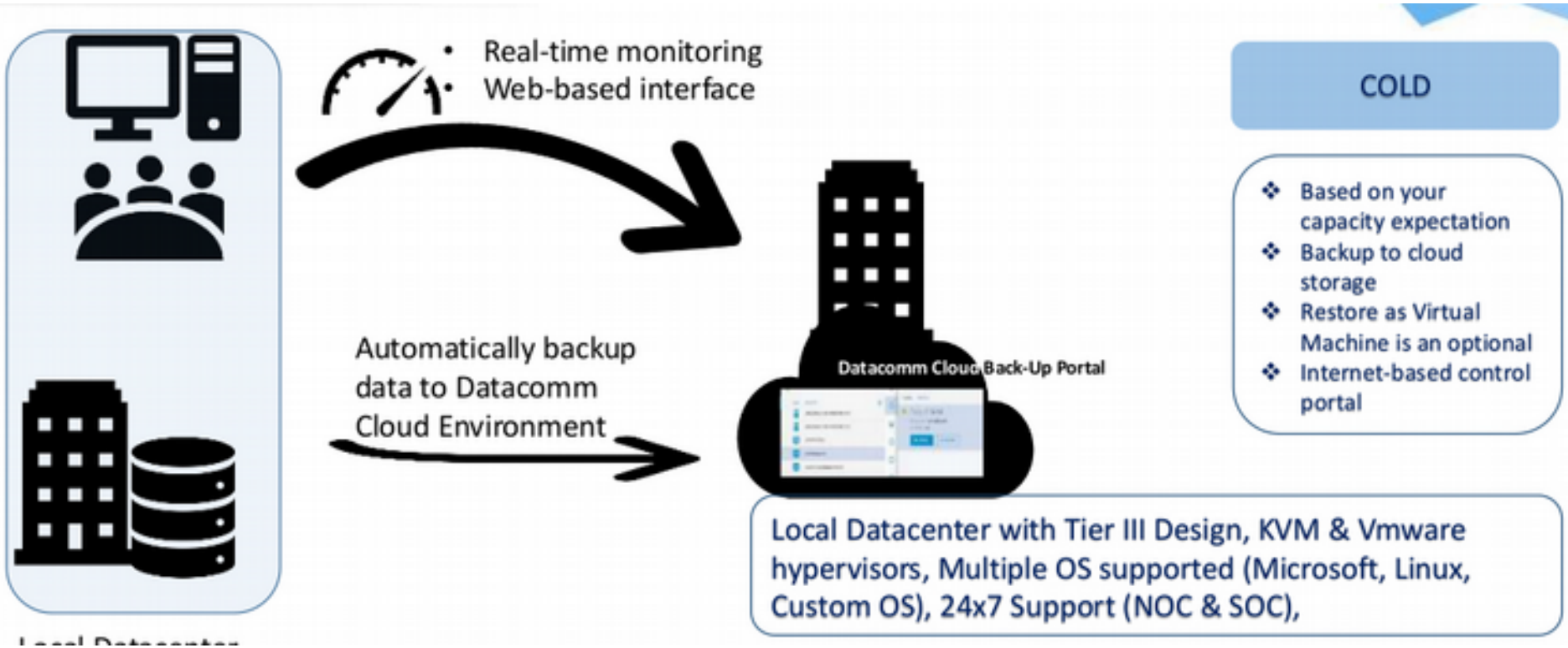
Costs	Traditional DR	Cloud-based DR
Datacenter for Disaster Recovery (including facilities utility and electrical power source)	Own manage	Cloud Service Provider
Stand-by Hardware System	Own manage	Cloud Service Provider
Manpower – Network Operation	Own manage	Cloud Service Provider
Manpower – System & IT Security Operation	Own manage	Cloud Service Provider
Capacity expansion	Own manage (procurement process + more hardware to manage)	Easily provided through flexibility and agility of Cloud
Expense	1.5 – 2X	1 – 1.2X

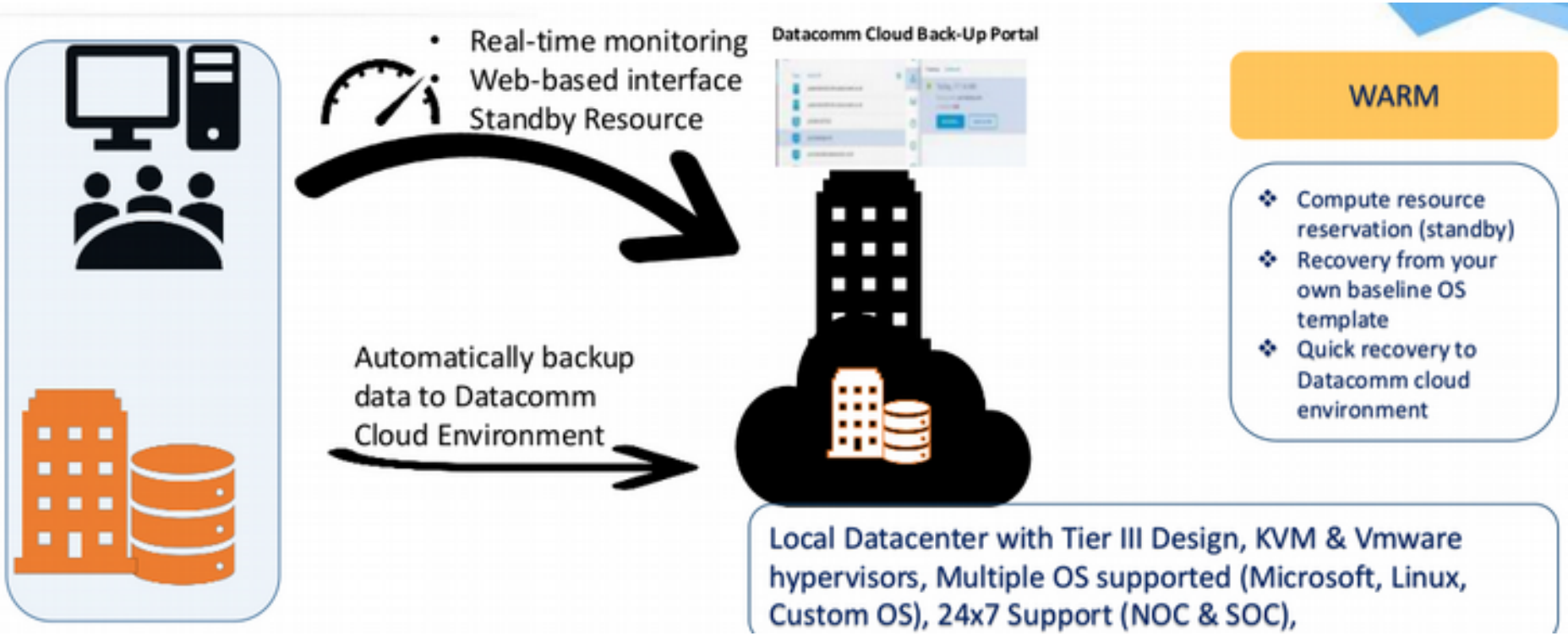
Disaster Recovery Considerations

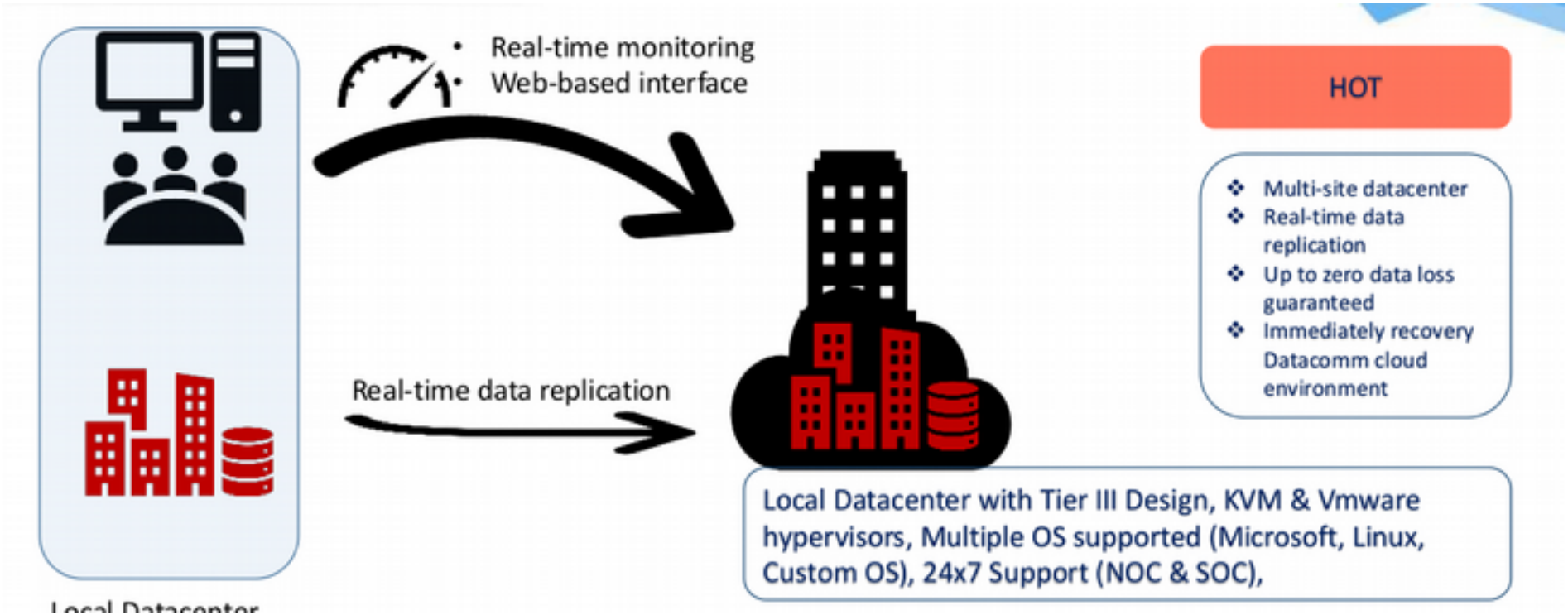
Why Cloud

Traditional DR	Cloud DR
+ More control on your server	+ No H/W cost and capital expense
+ Keeps company data private	+ Scalable
+ Data accessible locally	+ Pay for what you use
	+ Easily connect from everywhere, any devices
- Increase investment to build H/W and infrastructure	+ Data can be backup in the cloud regularly and efficiently
- More spending as company growth	
- More space	
- Maintenance cost	- Need internet connection
- Dedicated IT Support	- Trusting a third party to keep data secure
- No uptime guarantees	- Ongoing cost


DR Mode
Services Needed
Resources
Failover Scenario
Restore Time
Supported Platform
COLD DR
Back up
BaaS
Storage
Compute (unreserved)
Restore
Up to one day / instance
Windows
Linux
WARM DR
Standby (off)
OS
IaaS
BaaS
Storage
Compute
Boot on VM
4 - 6 hours / instance
VMware
Hyper - V
HOT DR
Fully Automated
OS
Replication
IaaS
Dedicated
Automatically
Less than 10 minutes
VMware
Hyper-V


Real-time monitoring
Web-based interface
Automatically backup data to Datacomm Cloud Environment
Datacomm Cloud Back-Up Portal
COLD
Based on your capacity expectation
Backup to cloud storage
Restore as Virtual Machine is an optional
Internet-based control portal
Local Datacenter with Tier III Design, KVM & Vmware hypervisors, Multiple OS supported (Microsoft, Linux, Custom OS), 24x7 Support (NOC & SOC),


Real-time monitoring
Web-based interface
Standby Resource
Datacomm Cloud Back-Up Portal
WARM
Compute resource reservation (standby)
Recovery from your own baseline OS template
Quick recovery to Datacomm cloud environment
Automatically backup data to Datacomm Cloud Environment
Local Datacenter with Tier III Design, KVM & Vmware hypervisors, Multiple OS supported (Microsoft, Linux, Custom OS), 24x7 Support (NOC & SOC),


Real-time monitoring
Web-based interface
HOT
Multi-site datacenter
Real-time data replication
Up to zero data loss guaranteed
Immediately recovery Datacomm cloud environment
Real-time data replication
Local Datacenter with Tier III Design, KVM & Vmware hypervisors, Multiple OS supported (Microsoft, Linux, Custom OS), 24x7 Support (NOC & SOC),
Local Datacenter

Disaster Recovery On Cloud

Key Features

- **High availability** – guaranteed 99.9% SLA data backup availability
- **Physical and virtual systems** – protection of both physical and virtual systems in one service
- **Automatic and scheduled backup** through online control portal
- Up to **zero data loss** guaranteed
- **File and disk image-based** backup - backup of selected files or complete disk images
- **Define your own baseline** OS template for recovery

Disaster Recovery On Cloud

Key features

- **Bare-metal recovery** – recovery to same or dissimilar hardware, even from the cloud
- **Comprehensive** - provides robust replication and offsite backup
- **Local and cloud storage** – support of local and safe cloud storage in our secure and local
- **Recovery reports** document execution of BC/DR processes, for easy auditing and reporting
- **'test-before-you-commit'** function allows test of a specific failover point before committing it, enabling 100% assurance that failover will be successful
- Test failover, including full remote recovery in a **sandboxed zone**

Sandbox for DR Testing

- Non-disruptive DR testing
- Create a test and development environment
- During the test, replication and the production environment is still in process
- Can be done during working days
- No downtime on the production environment

What is BaaS and DRaaS?

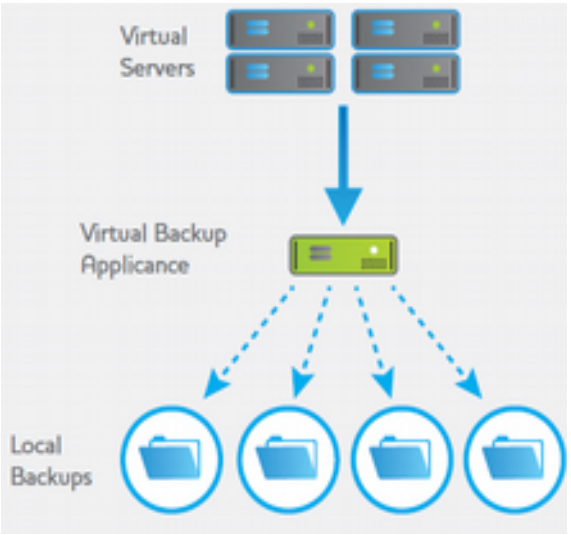
Backup as a Service

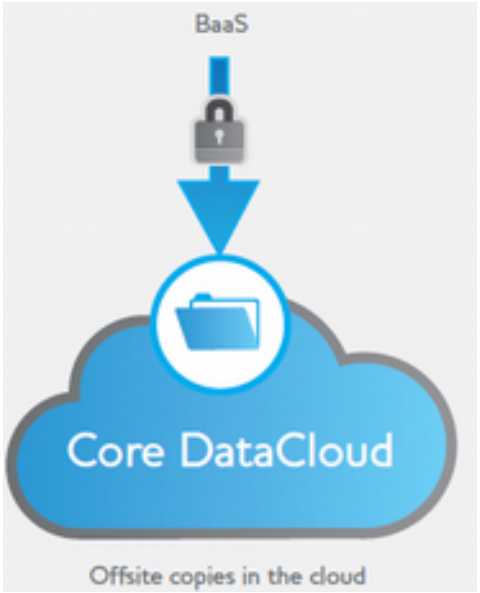
- Allows you to backup your servers both locally and to an offsite location

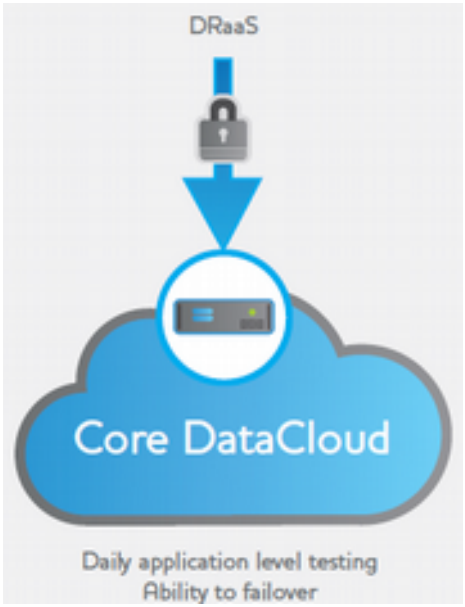
Disaster Recovery as a Service

- Gives you automated daily DR testing to application level. This will guarantee your applications will fail over successfully within pre-agreed SLA’s

How it works


Virtual
Servers
Virtual Backup
Applicance
Local
Backups


BaaS
Core DataCloud
Offsite copies in the cloud


DRaaS
Core DataCloud
Daily application level testing
Ability to failover

Build a Recovery Cloud

= PlateSpin Protect + Virtual Resources