The Datacenter of the Future

Karen Smolar
ksmolar@us.ibm.com
Principal Solution Architect
Client Engineering for Systems

IBM

Agenda topics

General

- Demand
- Sustainability
- Performance
- Simplification

Resiliency

- Status
- Combined HA and DR
- 2-sites vs. 3 and more sites
- Future items

DASD

- Response time
- Essential features and functions
- …..

TAPE

- Which data should be on TAPE ?
- TCT

Next Steps

- Get a clear status of where YOU are on the journey
- Compare your status with your goals
- Prioritize activities

If you do things like you always did them - why do you expect different results ?

General - What has changed in the last 5 or 10 years?

10+ Years Ago
- ❑ Minimize manual/paper processes
- ❑ Supplement existing capabilities
- ❑ Client server shifts to web based
- ❑ As long as it's faster than it was, it's good enough
- ❑ Failover fast when there is a problem

5 Years Ago
- ❑ Eliminate manual/paper processes
- ❑ Fast answers and client access, anywhere, anytime
- ❑ No failures, survive everything

Today -> Tomorrow
- ❑ Sustainability
- ❑ Agility
- ❑ Flexibility
- ❑ Predictability
- ❑ Simplicity
- ❑ Immediate responses
- ❑ Protect and recover from Cyber Attacks

Performance over the last several decades…..

DASD and Sysplex Performance

- 35 years ago, when I started with IBM, everything below 20msec DASD response time was considered “GOOD” (3880 controller with 3380 disks).
- Today, everything better than 0.5msec is considered “GOOD”. But nowadays we are talking about “all flash”, 32GB Ficon etc.
- We have not found a way to increase the “speed of light” (yet). Which means every kilometer distance between your controllers (for PPRC) adds 10µsec. If you have 10 kilometers distance between primary and secondary datacenter this is 10km x 10 µsec = 100µsec or 0.1 msec (best case).
- If you run an “active - active” Sysplex configuration the remote machine needs 0.2 msec.

What will be “good enough” in the future?

Resiliency over the last several decades…..

First came Disaster Recovery

- The intent was to make sure businesses would survive natural disasters even if it took a long time to recover.
- We've come a long way from those first tape based solutions. Disk based replication is now the standard.

Can you run for an extended period of time in your D/R datacenter and provide the same QOS?

Then came Continuous Operations and High Availability

- Expectations then shifted to the more common failures that didn't require failover to another datacenter and maybe didn't even result in an outage.
- Technologies like Parallel Sysplex, data replication, and GDPS took hold.

Are your critical applications fault tolerant?

Now we have Logical Corruption Protection

- Focus has shifted away from the processing and to the data itself.
- A newspaper in Germany did a survey among 400 medium size businesses. 2/3 of them got hacked, 42% out of the 2/3 (112) paid the ransom to gain access to their data.

What would you do if you were the victim of a ransomware attack?

Sustainability…..

Green datacenters

- Unfortunately, things like power consumption and carbon footprints we did not get much consideration when I was starting my career in IT.
- Floor space really only mattered for the “big boxes”… I had a client 20 years ago that had production servers running under someone’s desk.
- Servers were small and plentiful and ran dedicated workloads distributed all over.
- Our planet, our people and our businesses must focus on sustainability today.

How long will your current datacenter meet the needs of your growing business? Are you looking at consolidating to simplify or changing/moving to meet sustainability requirements?

Complexity

- With growth tends to come complexity which is harder to manage and harder to sustain.
- It prevents us from being flexible and agile. In the case of the mainframe this has led to resource and skill challenges.

Are you facing challenges associated with more traditional mainframe applications and operations?

Recommendation:

To get prepared for future demands, ask yourself…..

- Is my infrastructure able to scale?
  - DASD Response Time
  - LPAR Size
  - Number of systems per CEC
  - Overhead (Sysplex, Capture Ratio, …..)
- Am I adapting fast enough? Am I already playing catchup?
- Will I be able to run my mainframe in a couple of years once current mainframe staff is retired?

Resiliency

Resiliency is not a luxury anymore. It’s not just for the largest financial clients.

It is a necessity for every industry.

The challenge is that the threats are changing.

The requirements are more demanding than ever.

Disaster Recovery, High Availability, and Cyber Resiliency Considerations

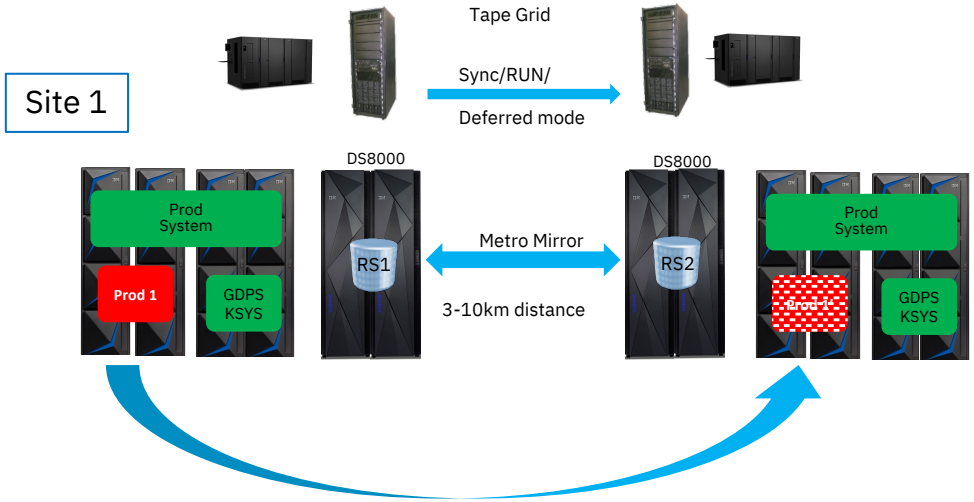
We spent the last 30 years focused on system and disaster level events ……

- Introduction of datasharing parallel Sysplex
- Introduction of PPRC and XRC around 1995
- GDPS got introduced in Fall 1998 to automate LPAR IPL and manage DASD
- RPO has gone from minutes/hours to seconds and even 0,
- RTO of several hours was considered acceptable but is being driven down to minutes

The demand for service today is unparalleled and growing …..

- End users are driving requirements for zero downtime. We will shop and bank somewhere else when we don't get it.
- Even short outages can have wide reaching impacts. Planes don't fly, credit cards don't work.
- Cyber attacks like ransomware are a very serious threat in these days. Although the mainframe is the most resilient and most securable, nothing is absolute. We don't know what unique threats hackers are coming up as we speak.

Yesterday’s / Today’s topology



- LPARs get moved from one datacenter to another in case of a CEC failure
- This results in at least 30 minutes downtime until service is restored
- DASD response times can hardly be improved - Hyperlink, read from secondary is the best you can do.

Combined HA and DR

Save infrastructure money because of combined HA and DR

Increased Sysplex and DASD response time overhead

No preparation for logical corruption recovery

CEC or LPAR Failure results in longer downtime as LPARs get moved / reipled

Regional disasters (flooding, fire, power outage, earthquake,….) are not covered

In many countries a remote datacenter is either required (US) or ”strongly recommended” (Germany)

Let’s THINK for a second ….

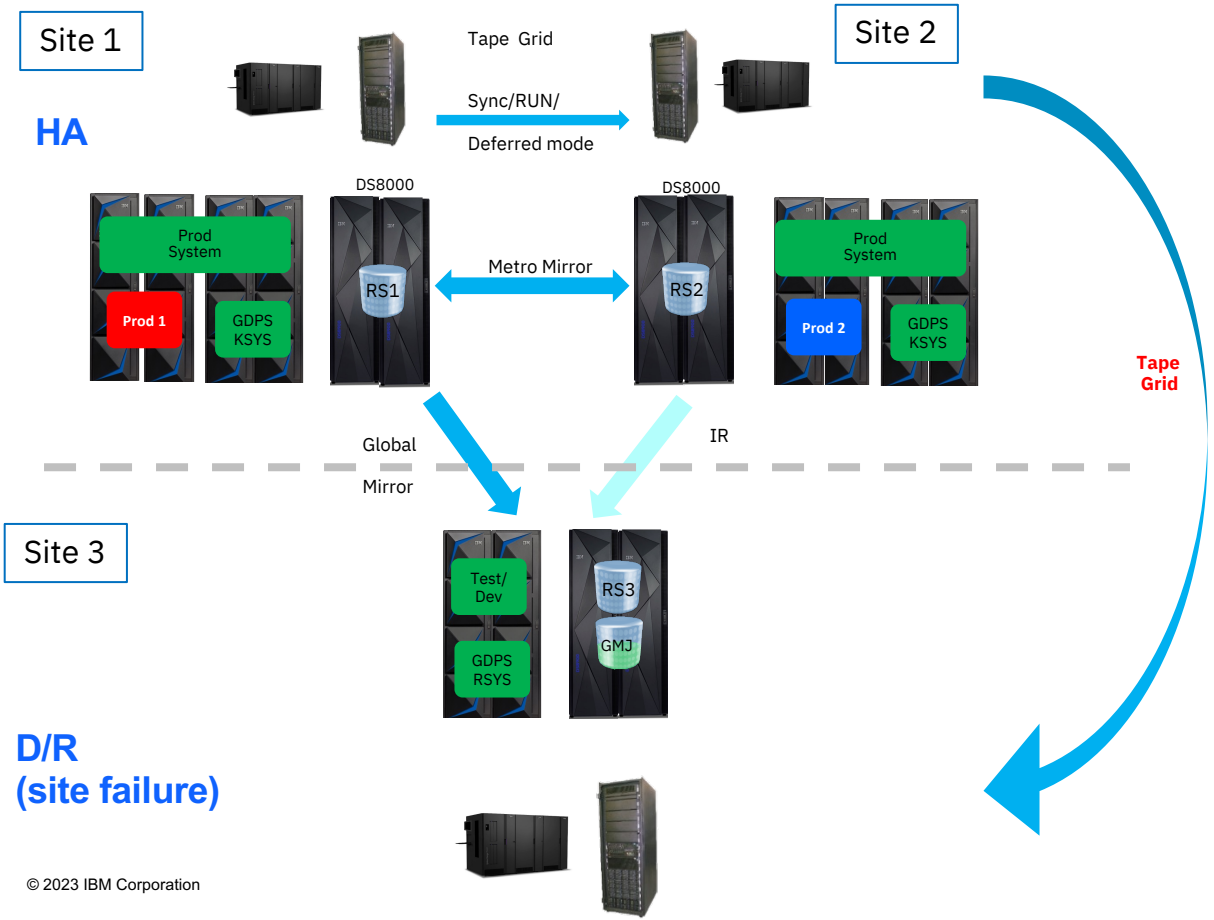
The speed of light will not improve in the foreseeable future. That just means distance becomes a much more important factor for response times.

Think about:

- Sysplex distance
  - If you loose one site (incl. CPU and CF) you need to IPL everything anyway in the surviving site. So, it does not matter too much for DR if the distance is 2 km or 2.000 km. The time to restore your service in case of a site failure is essentially the same.
- Synchronous disk replication
  - In an “all flash” disk environment a 10 km distance means 0,1 msec - just for the signal travelling time.
  - If we want to improve the DISK response times, we need to exploit concepts which do “synchronous IO’s” (like Hyperlink) instead of asynchronous (FICON)

Recommendation: Rethink your setup now

Topology Optimized for HA and DR



Combining local HA and remote DR

Reduced Sysplex Overhead

- Optimized DASD performance
- Extended TAPE availability
- Coverage for regional disasters

Cyber Vault implementation with no impact to production

- HA can be achieved by using two “datacenter cells” in the same building
- Two DASD controllers in D/R Site necessary to allow for HA in that site

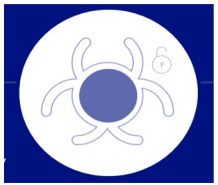
Sixty percent of businesses victimized by a cyber attack go out of business within six months.[1]

$4.54M

Average cost of a ransomware attack, not including the cost of the ransom itself.[2]

29 Days

Savings in response time for those with extended detection and response (XDR) technologies.[2]



$1M

Average difference in cost where remote work was a factor in causing the breach versus when it wasn't.[2]

83%

Of organizations studied have had more than one data breach.[2]

What would you do if it happens to you?

Pay the ransom?

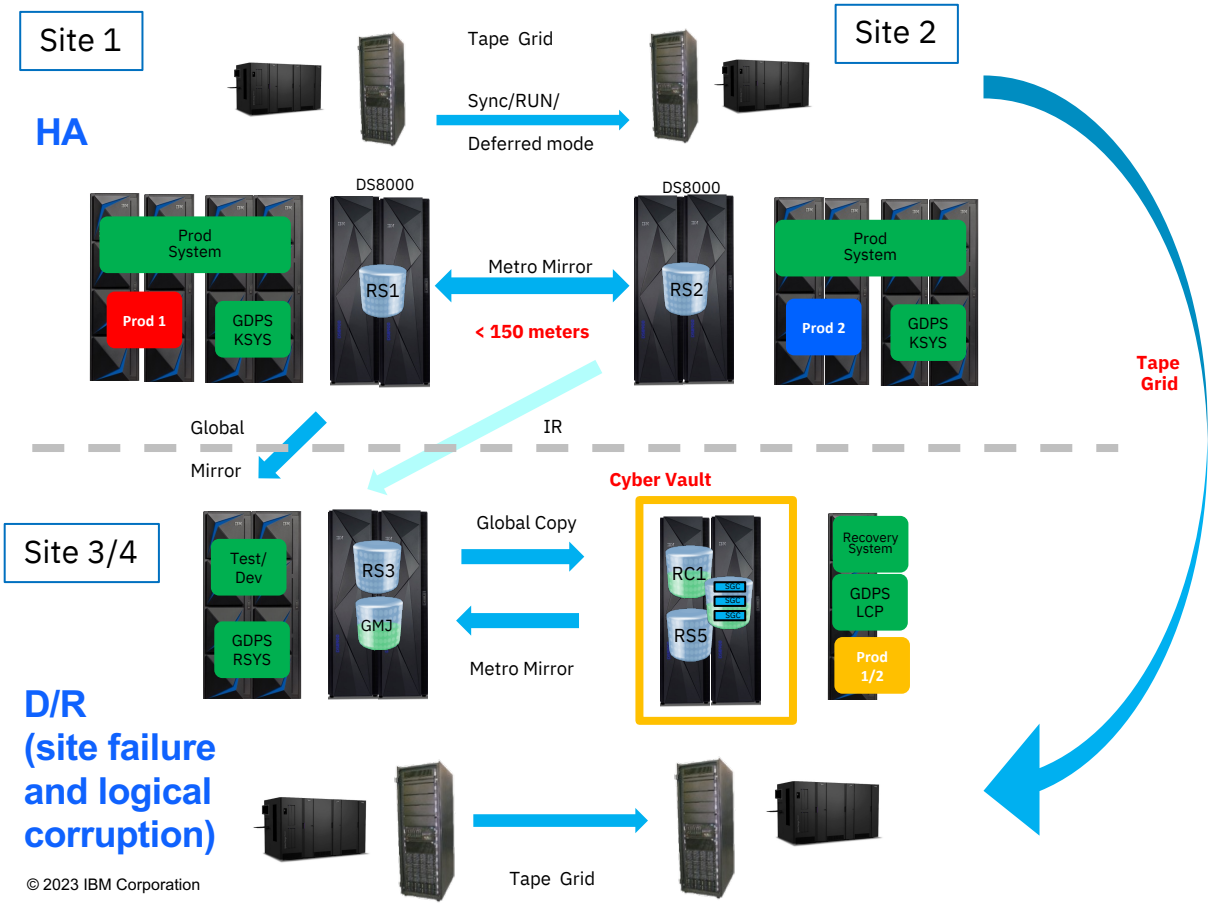
- Ransom is going up
- Hackers are stealing the data in addition to encrypting it

Use ransomware insurance?

- Regulators worldwide are pushing to eliminate insurance
- Insurance companies are restricting coverage
- Insurance companies are requiring data protection solutions to get coverage

[1]CNBC (https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html
[2]Cost of a Data Breach Report 2022 (https://www.ibm.com/reports/data-breach)

Topology Optimized for HA, DR and Logical Corruption



Combining local HA and remote DR

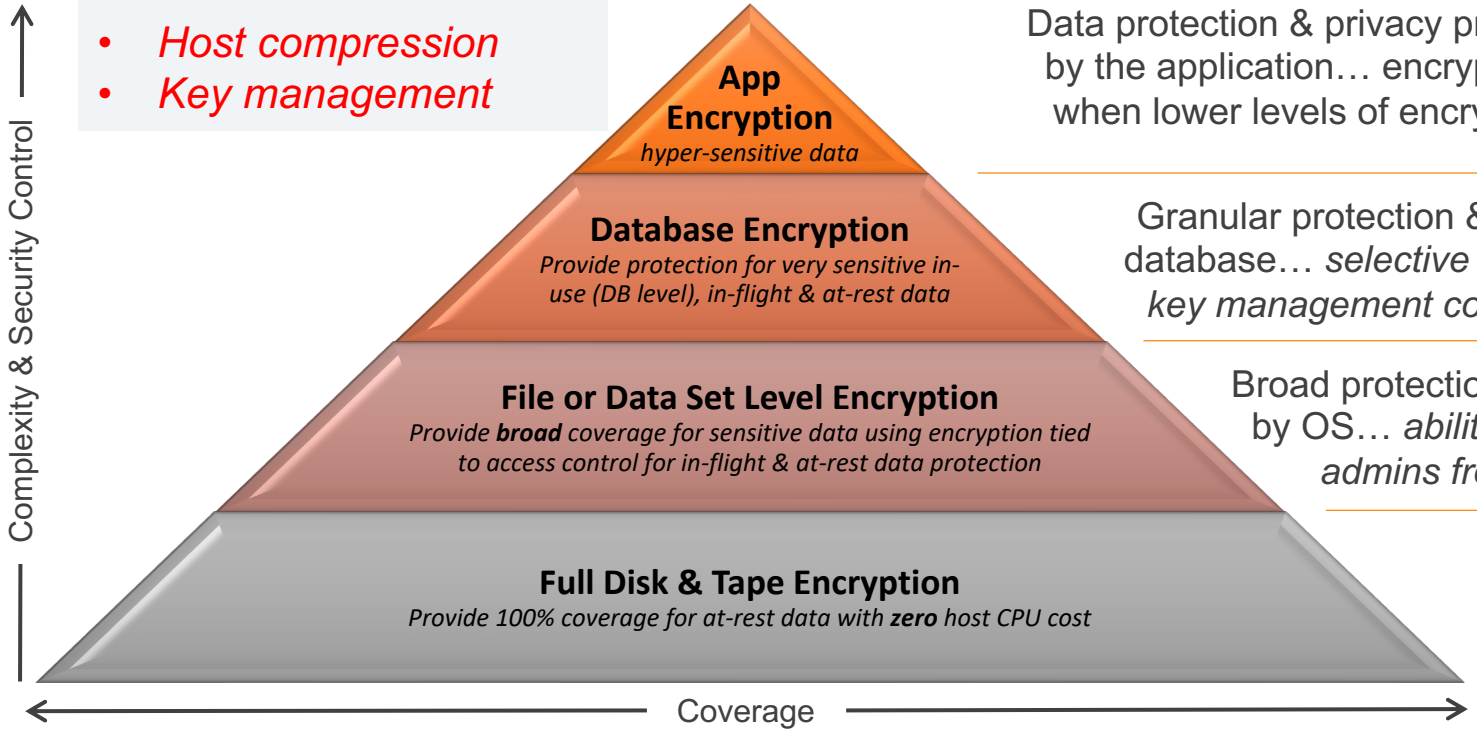
- Reduced Sysplex Overhead
- Optimized DASD performance
- Extended TAPE availability
- Coverage for regional disasters
- Cyber Vault implementation with no impact to production
- HA can be achieved by using two “datacenter cells” in the same building
- Global Mirror will be paused for some seconds each time a Safeguarded Backup is taken
- Two DASD controllers in D/R Site necessary to allow for HA in that site

Data Protection Considerations

Will your encryption strategy protect your data from hackers stealing it (and then holding it hostage)?

Are you prepared for pervasive encryption?

- *Host compression*
- *Key management*



Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

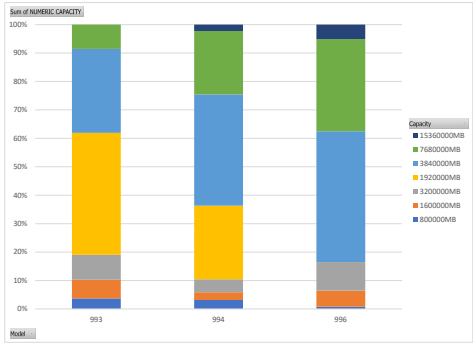
Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Protection against intrusion, tamper or removal of *physical* infrastructure

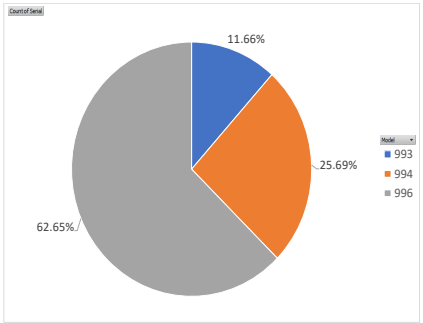
Primary Storage

Majority of capacity is now shipped in high-capacity Flash drives.

Smaller DS8910F systems using 1.9TB and 3.8TB drives
Larger DS8950F systems using 7.6TB and 3.8TB drives



This trend to all Flash has allowed more clients to use smaller systems with large Flash drives.



Implications of Flash trends

What can we expect in the coming years…..

- Flash media sizes will increase rapidly even in mainframe environments
  - Large drives will become prevalent in the near future
  - During this decade we would expect to see very large Flash drives in optimized Flash form factors
  - Peak sequential write workloads are often the primary driver when sizing Flash configurations

- Eventually even the largest parallel sysplex environments will be contained on a single primary storage system
  - Today this applies to a large majority of environments and in many cases multiple parallel sysplexes are consolidated on a single primary storage system

- Reduction in the total cost of storage has enabled expansion of storage topologies and this trend will continue and accelerate
  - Local Metro Mirror and HyperSwap for HA with remote replication for DR
  - Symmetrical environments with HA in all locations
  - Storage for full scale test environments
  - Storage for Cyber Resilience

Simplification and Exploitation

Is my configuration ready for the 21st Century

- What can be done to simplify z/OS storage environments?
  - Do we need 1,000s and 10,000s of volumes in a sysplex?
  - How many FICON channels do I need for a storage system?
  - Is my DFSMS configuration optimal for today's requirements?

- Am I exploiting all the capabilities that exist today?
  - HyperPAV and SuperPAV enable reduction to 16-32 aliases per LSS/LCU
  - zEDC compression can significantly reduce peak write workload
  - Enable and then exploit thin provisioning
  - Latency reduction technology such as zHyperwrite, read from secondary, zHyperlink

Backup and Archive

Backup and restore

What is your current strategy for backup and restore?

- Where are your backups?
- Can you restore fast enough?
- Can you restore to the point in time you need?
- Do you test the restore processes?
- Can you do a large scale restore or just smaller application data restores?

How will Cyber Resiliency requirements change what you do today?

Archive

What data are you archiving to virtual tape?

- Do you recall data for batch processing?
- Do you recall data for online read processing?
- Would this be better on primary storage?
- How does your current approach impact DR?
- How does (or will) your current archive strategy impact your Cyber Resiliency (Cyber Vault)?

When did I define my strategy for DFSMShsm migration?

- Is there data being migrated that would easily be kept on primary storage?
- Are you still using MIPS to save some storage? Does this still make sense with TFP?

Next Steps

Futures

Business demands are growing and technology continues to adapt…..

- IBM has already made certain features dependent on TFP for Software. This trend will continue in the future with more flexibility etc. Start planning for a migration to TFP, start negotiating with your ISVs if you haven't already.
- Features like Flex Capacity and System Recovery Boost are changing the way we think of resiliency.
- Pervasive encryption and other security enhancements position us to better protect data.
- High capacity, all flash storage provides both performance and scalability.
- Offerings like Dev/Test containers and zBuRST support more robust testing.
- Safeguard Copy and GDPS LCP combined with IBM Z HW and SW provide logical corruption protection.

It's time to assess your current architecture and ensure that you are able to leverage existing and future technology!

Recommendation:

- **Get a clear status of where YOU are on the journey. Be Realistic….**
  - Are you able to test at scale?
  - Can you test recovery from logical corruption incidents?
  - Would you survive a regional disaster?
- **Compare your current state with your goals…**
  - Be aware of demands and start early to get on the right track
  - Don’t underestimate projected demand. Sometimes things don’t develop linearly
- **Prioritize activities**
  - Which changes are most important to answer future demands?
  - Which changes can be easily started today to be prepared for the future?
  - Revisit old implementations. Don’t accept answers like ”it’s always be done that way” and “it works, don’t mess with success”

z/End

Q & A / discussion