

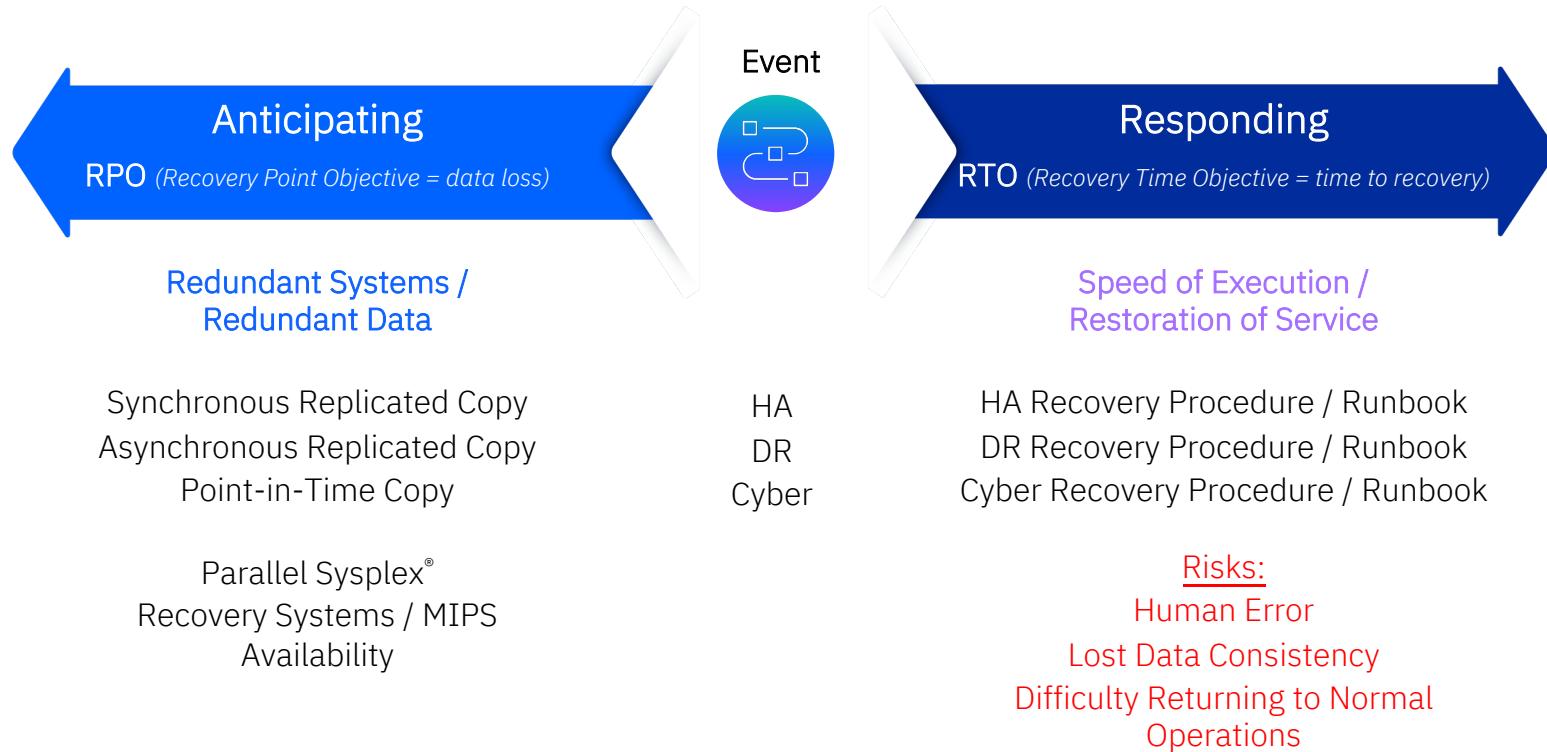
zSystems Resiliency

Maintaining Operations under
Natural (or not) Disasters

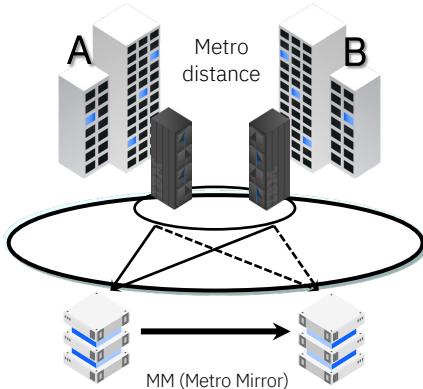
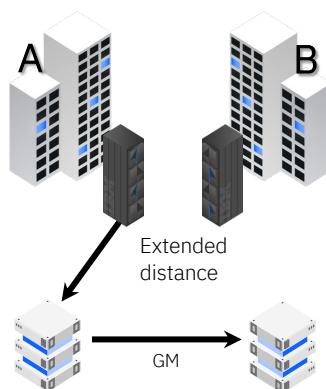
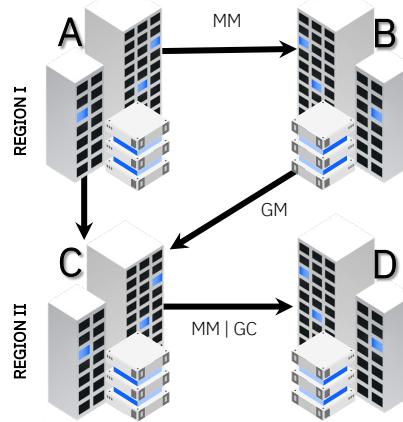
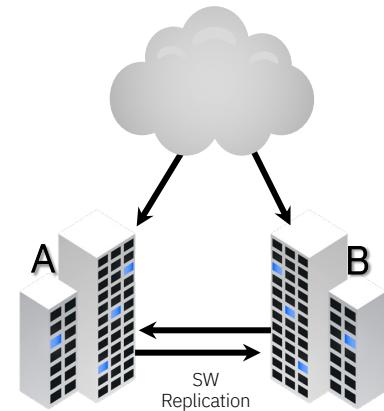
Diego Bessone
Director, WW Sales IBM Z



Anticipating and responding to an event is increasingly complex, and the speed and precision of response is increasingly critical



GDPS: Balanced HA/DR solutions designed to address different client requirements

GDPS Metro	GDPS Global	GDPS Metro Global	GDPS Continuous Availability
<p>Near-continuous availability and recovery at metro distances</p> <p>Systems remain active Multisite workloads can withstand site and storage failures</p> 	<p>Disaster recovery at extended distance</p> <p>Rapid systems DR with “seconds” of data loss</p> 	<p>Near-continuous availability regionally & recovery for 3-4 sites</p> <p>Metro near-continuous availability and out of region disaster recover</p> 	<p>Near-continuous availability, recovery & workload balancing</p> <p>Continuous availability at unlimited distances</p> 
3			

Business continuity The landscape is changing

Regulators around the globe are introducing more stringent policies in relation to business continuity and disaster recovery requiring more comprehensive and extended testing mandating clients switch over full production loads and operate for **30 days up to 6 month** out of their secondary data center.

FFIEC / NY DFS

Institutions should demonstrate, through testing that their business continuity arrangements can sustain the business until permanent operations are reestablished.

Involve a sufficient volume of all types of transactions to ensure adequate capacity and functionality of the recovery facility.

Exercises generally extending over a longer period to allow issues to fully evolve as they would in a crisis and to allow realistic role-playing of all the involved groups.

EU NIS 2 Directive

EU regulators are clearly indicating the emergence of new requirements that surpass prior legislation like Operational Resiliency (ex Basel III), dealing from component failure to acknowledge risks associated to cyber attacks.

When the service is Cross-European (ex Real Time Gross Settlement, EU Securities Settlements et cetera) ECB and EBA will supervise directly meaning companies must adhere to a “Resiliency testing framework”.

Regulators are asking to prove that a secondary Site (DR) is fully functional and can run production for a long time.

NIST Special Publication 800-53

CP-2(6) Plan for the transfer of mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

CP-4(4) Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

CP-7(6) Plan and prepare for circumstances that preclude returning to the primary processing site.

Preventive maintenance strategies

Enterprises need operations to continue uninterrupted while maintenance is performed, an issue is addressed, or a new component is installed

	Be proactive not reactive	Equipment repairs are costly	Remote management
	<p>Often, major outages, data interruptions, and downtimes are directly caused because simple, physical maintenance and care haven't been properly established</p> <p>By managing equipment with the right maintenance strategies, at the right time, data center operators can reduce capital and operating expenses, and—most important—improve uptime</p>	<p>Emergency equipment repairs come at a high cost—especially if you add in the ancillary costs of business disruption, downtime and reputational damage</p>	<p>According to a report released by Honeywell, nearly all respondents (96%) indicate remote management is (or would be) important to their facility, yet only 34% of those surveyed currently have such a system in place</p> <p>- Rethinking Data Centers as Resilient, Sustainable Facilities</p>

Avoidance of natural disasters, climate change, and COVID-19 impact

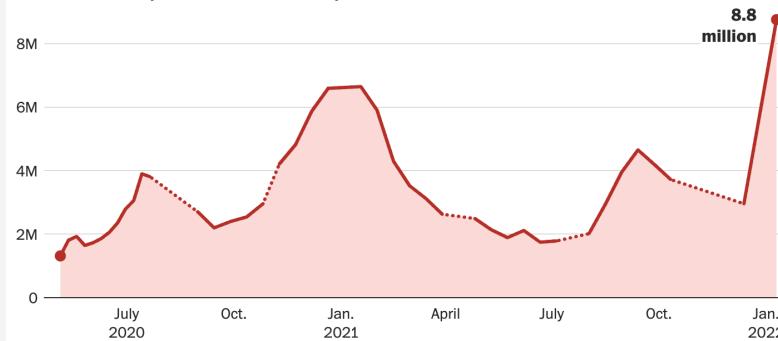
Texas Deep Freeze

Extreme cold shuts down data centers in Texas

Unprecedented weather conditions caused data center outages for bus carriers, healthcare companies, insurance providers, credit unions and the city of Austin

The omicron wave forced millions to stay home

Workers who stayed home because they had covid or cared for someone who did



Note: Dotted lines show gaps between survey waves. Before April 2021, those staying home because they had covid-19 symptoms were counted separately from those staying home to care for someone with the virus. Those categories have been combined.

Source: [Census Bureau's Household Pulse Survey](#)

THE WASHINGTON POST

COVID-19 continues to challenge data center industry

Strategic capacity planning is more critical than ever

More people than ever, especially with the recent omicron variant, are staying home and consuming data from video conferencing to streaming services

IBM z16 is built to build

We built a powerful and secure platform for business.
Let's build the future of yours.



Predict and Automate for Increased Decision Velocity

Apply insights at speed and scale to create new value in every client interaction

Increase productivity and lower operational costs with automation and AIOps



Secure with a Cyber Resilient System

Secure data and systems now and in the future with quantum-safe protection

Address ever-increasing regulations with automation for compliance

Plan and mitigate risk of potential future outages



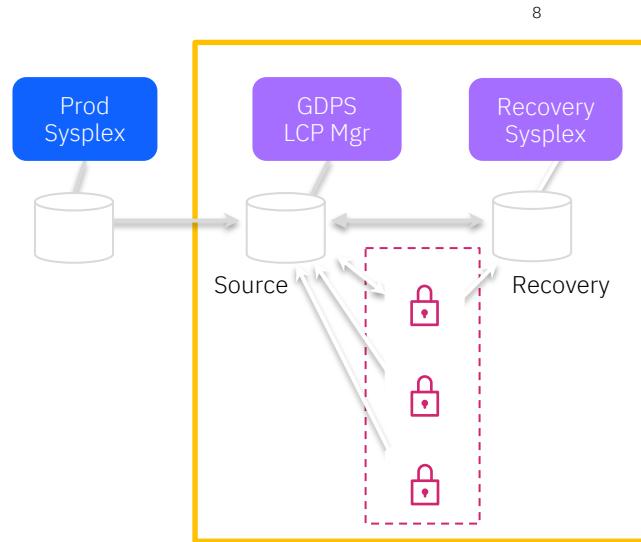
Modernize with Hybrid Cloud

Empower developers with agility to accelerate modernization of existing workloads

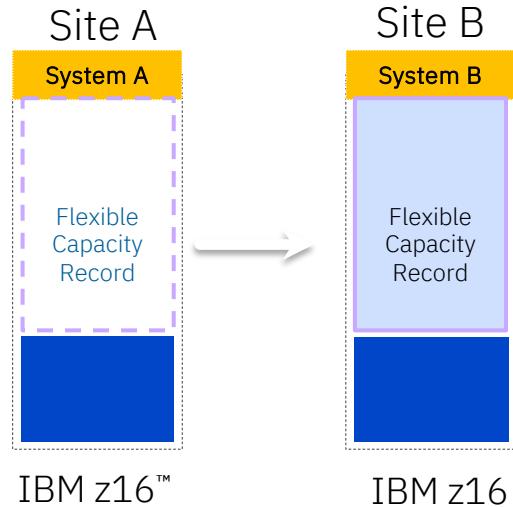
Enable integration of IBM z16 workloads with new digital services across the hybrid cloud

Important GDPS features that expand and enhance resilience capabilities

Logical Corruption Protection (LCP) Manager automates your cyber resiliency capabilities

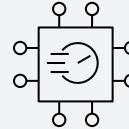
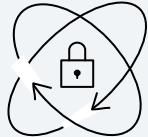
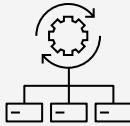


For Flexible Capacity: GDPS can automate the transfer of flexible capacity from one site to another



IBM Z Flexible Capacity for Cyber Resiliency

Plan and mitigate risk of potential future outages



Greater Flexibility

Dynamically shift production capacity between IBM z16 systems in different sites in seconds

Flexibility and elasticity for proactive outage avoidance, facility maintenance, compliance and disaster recovery – test and actual DR scenarios

Works in conjunction with other temporary record types

Complete Client Control

Remotely transfer capacity – no on-site personnel (IBM or client) required after initial set up

Flexibility over duration of capacity transfer, up to 1 year

Fully automatable using solutions such as GDPS

Integrates with System Recovery Boost for faster system and workload startup

Improved Compliance for Disaster Recovery

Simplify compliance and improve confidence both for testing and real DR scenarios

Closer mapping between test and production scenarios

IBM Z Flexible Capacity for Cyber Resiliency

Use Cases

Disaster Recovery & DR Testing



Transfer the capacity you need at your DR site to continue to run your business workloads. Automate and test recovery procedures for unplanned outages, including cyber attacks to provide near-continuous availability and disaster recovery.

Frictionless Compliance



Meet the ever-evolving stringent requirements of global regulators, allowing a highly automated and fast process to demonstrate a production site swap.

Facility Maintenance



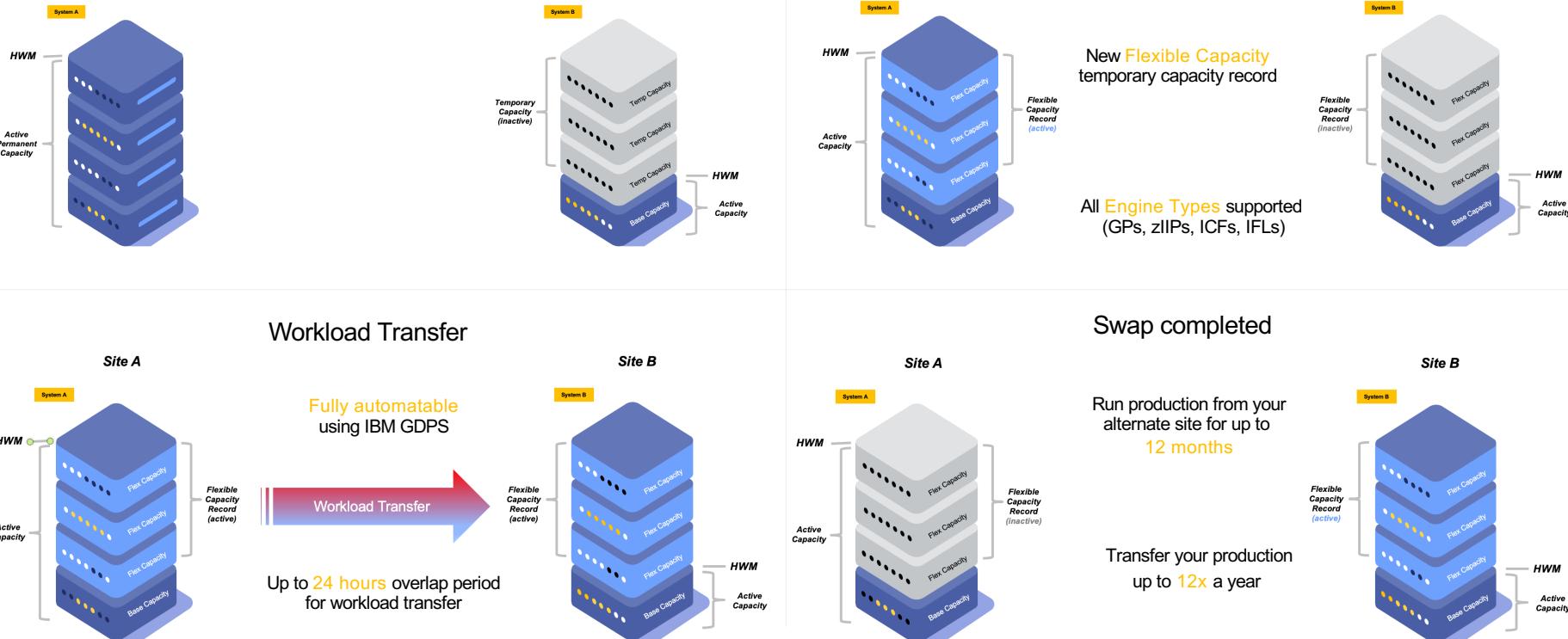
Run your production workload from your alternate site while you perform maintenance at your primary site with the capacity you need.

Pro-active Avoidance



Protect your critical business services from natural disasters. Avoid rolling power outages. Migrate your critical workloads to an alternate site before your business gets impacted and stay there for up to one year.

Technical Overview

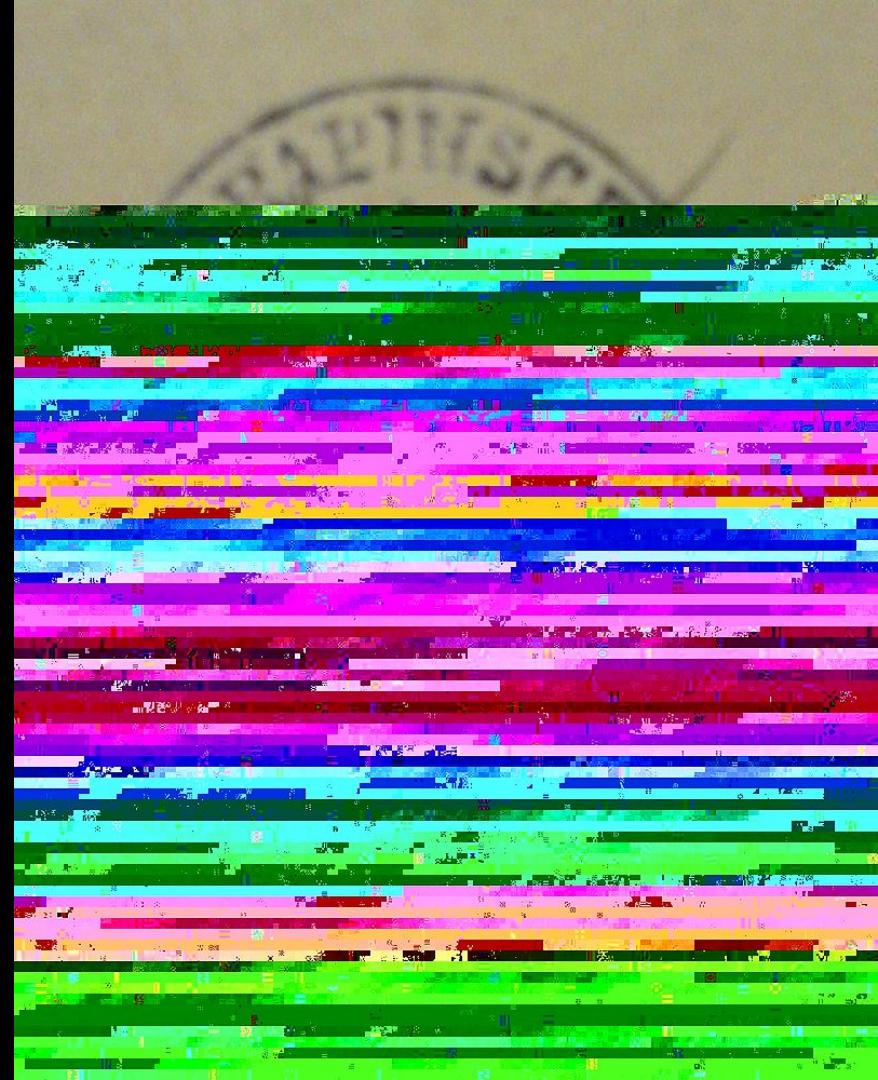


Logical data corruption

Data corruption refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

There are two types of data corruption associated with computer systems: **undetected** and **detected**.

Undetected data corruption, also known as **silent data corruption**, results in the most dangerous errors as there is no indication that the data is incorrect.



Why traditional resiliency solutions will not protect you from logical data corruption



	You have	What is required
Replication	Data is being replicated continuously but logical errors are also replicated instantaneously	Scheduled point in time copies stored in an isolated, secure location
Error detection	Immediate detection of system and application outages	Regular data analytics on point in time copies to validate data consistency
Recovery points	Single recovery point that likely will be compromised	Multiple recovery points
Isolation	All systems, storage and tape pools participate in the same logical system structure	Air gapped systems and storage so that logical errors and malicious intruders can not propagate
Recovery scope	Continuous availability and disaster recovery	Forensic, surgical or catastrophic recovery capabilities



Asia Pacific



2 minute read · September 26, 2024, 36 PM EDT · Last Updated 2 days ago



Australia flags privacy overhaul after huge cyber attack on Optus

Reuters

SYDNEY, Sept 26 (Reuters) - Australia plans to toughen privacy rules to force companies to notify banks faster when they experience cyber attacks, Prime Minister Anthony Albanese said on Monday, after hackers targeted the country's second-largest telecoms firm.

Optus, owned by Singapore Telecoms Ltd ([STEL.SI](#)), said last week that home addresses, drivers' licences and passport numbers of up to 10 million customers, or about 40% of the population, were compromised in one of Australia's biggest data breaches.

Summary of EU's Digital Operational Resilience Act (DORA)

The EU regulation proposal is a legislative attempt to streamline information security risk management processes to increase digital operational resilience across the Financial Services sector



What does it focus on?

Introduce a comprehensive framework to mitigate cybersecurity risks and **improve operational resilience across the Financial Sector**



Who does it apply to?

- Traditional financial entities
- „Fintech“ companies
- **Third party service providers of financial entities**



When will it apply?

- Expected to become **EU wide regulation in 2022**
- Allowing grace period of 12-18 months



Why should I care?

- **Avoid penalties**
- Mitigate impact of cyber threats
- Reduce time and costs of incident recovery



What can I do?

- **Take early action** to prepare for DORA's compliance obligations



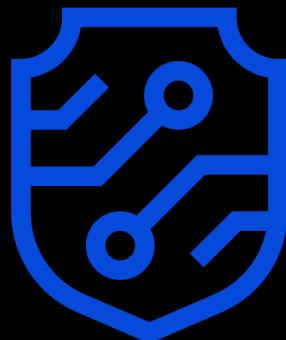
A penalty of **1% of the average daily worldwide turnover** of the impacted critical ICT third-party service provider in the preceding business year may be imposed. Other administrative penalties are advised by Member state authorities based on the nature of the breach.

Cyber resiliency on IBM Z

Cyber resilient systems must have the ability to anticipate, withstand, and recover from adverse conditions, stresses, or attacks.

Anticipate / Withstand

- ✓ Encryption everywhere
- ✓ Confidential Computing
- ✓ IBM Fibre Channel Endpoint Security
- ✓ IBM Enterprise Key Management Foundation
- ✓ Cryptographic acceleration with
Crypto Express7S
- ✓ Cryptographic coprocessor on every core with
CP Assist for Cryptographic Function (CPACF)
- ✓ IBM Guardium
- ✓ IBM Security zSecure

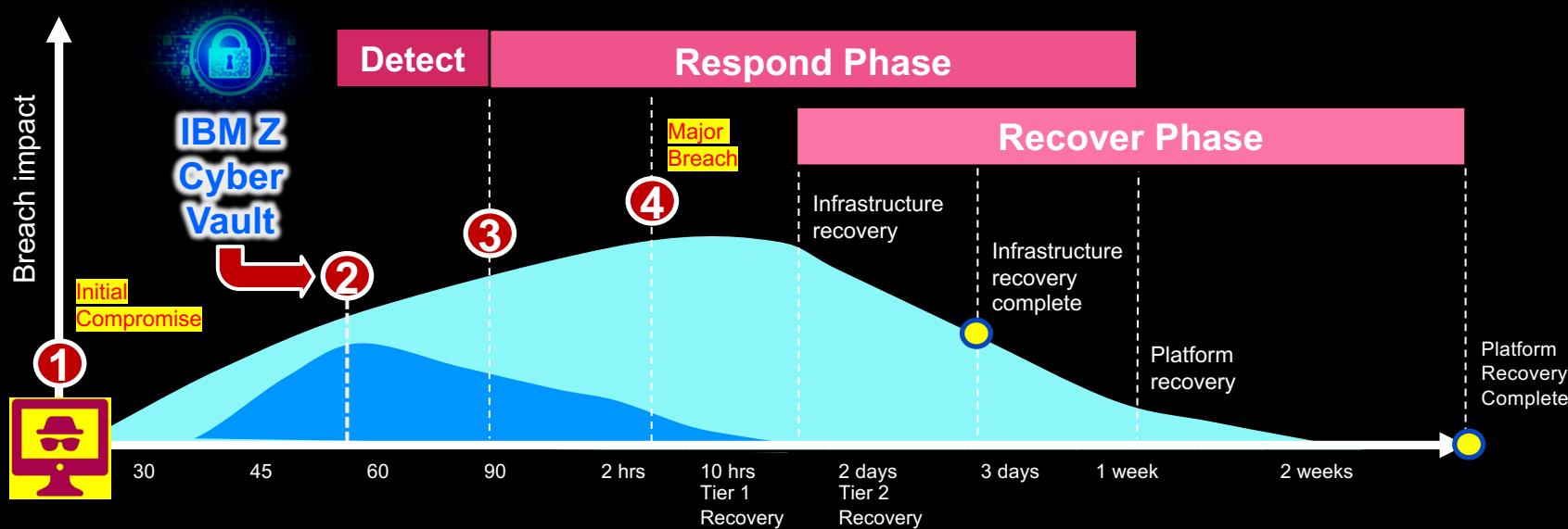


Recover / Restore

- ✓ GDPS
- ✓ High Availability
- ✓ Disaster Recovery
- ✓ IBM System Recovery Boost
- ✓ IBM Z Cyber Vault

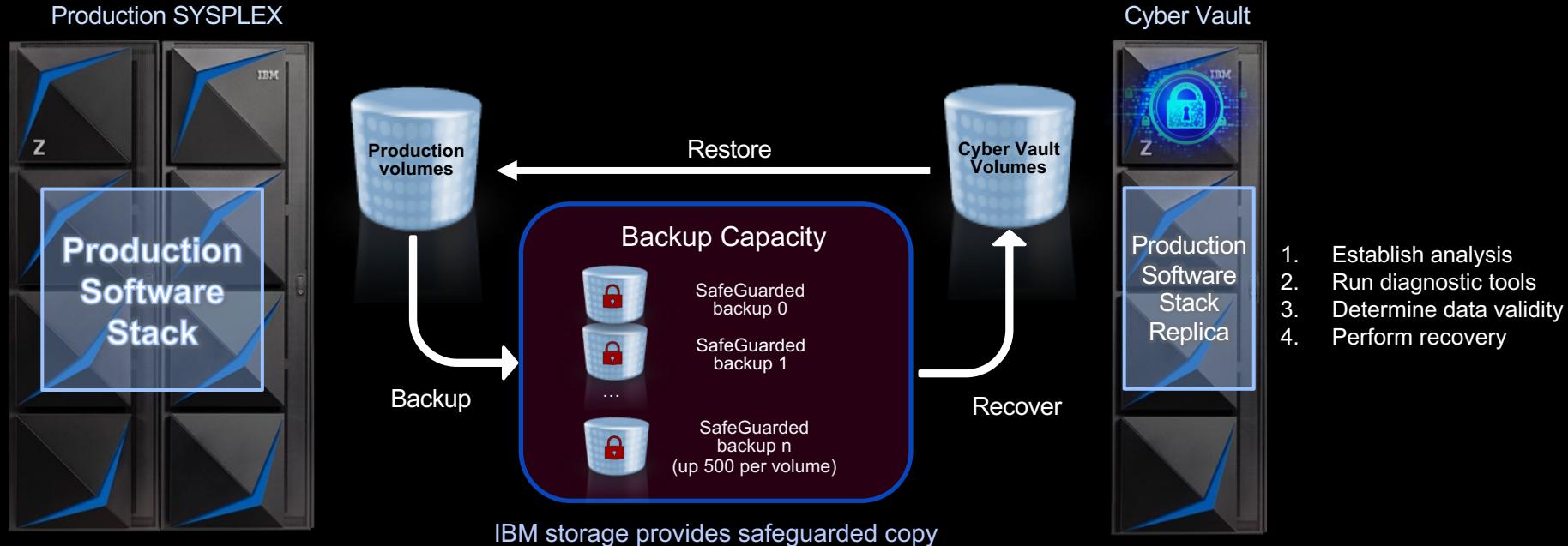
IBM Z Cyber Vault

Speedy recovery to significantly reduce the impact of breaches



- ① Corruption of data occurs ...
... but not yet detected
- ② Due to the Cyber Vault environment and the use of Safe Guarded Copy Technology, data is continuously checked, and corruption is found and corrected
- ③ Without the Cyber Vault environment corruption is detected much later and has a greater chance to spread
- ④ It takes even longer to identify all impacted data once the corruption has spread within the enterprise

IBM Z Cyber Vault



IBM Z Cyber Vault capabilities

Data Validation

Detect data corruption early or certify that the copy is clear



Forensic Analysis

Investigate the problem and determine the best recovery action



Surgical Recovery

Extract data from the copy and logically restore back to production environment



Catastrophic Recovery

Recover the entire environment back to a point in time copy



Offline Backup

Backup copy of the clean environment to offline tape media



IBM z/OS Utilities

IBM Z Catalog management tools

IBM Z Batch Resiliency

IBM DFSMShsm tools

IBM Security zSecure

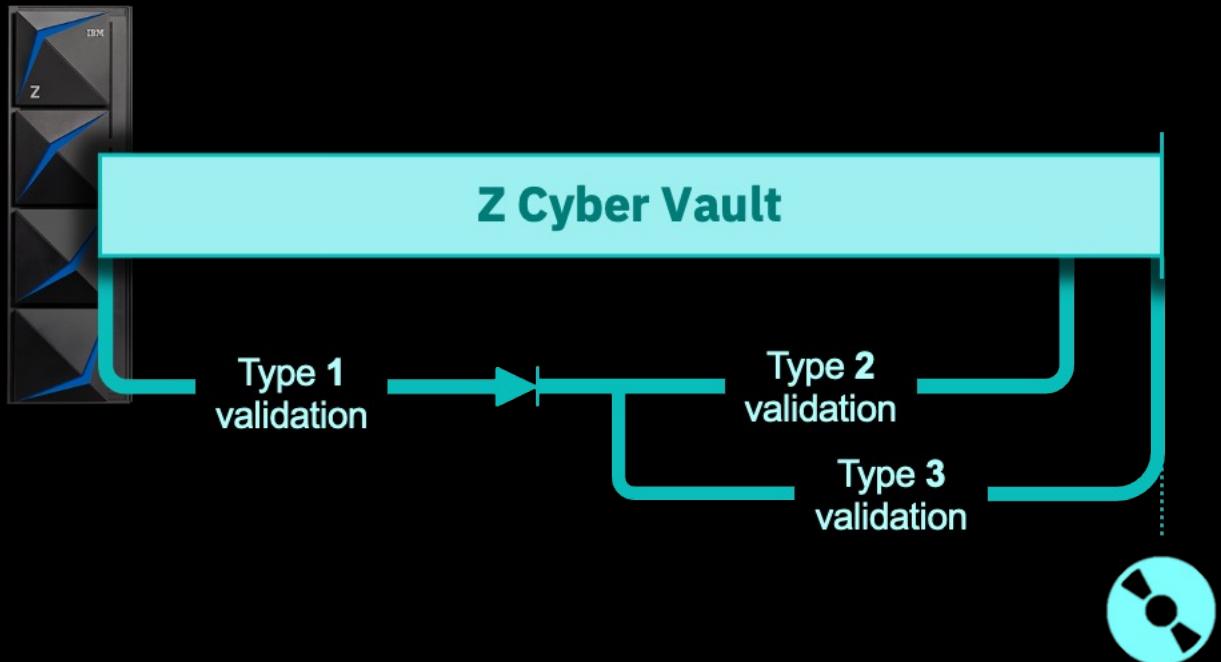
Db2 and IMS Tools

IBM Z Cyber Vault data validation

Type 1
z/OS system

Type 2
z/OS subsystems
& data structure

Type 3
Application data



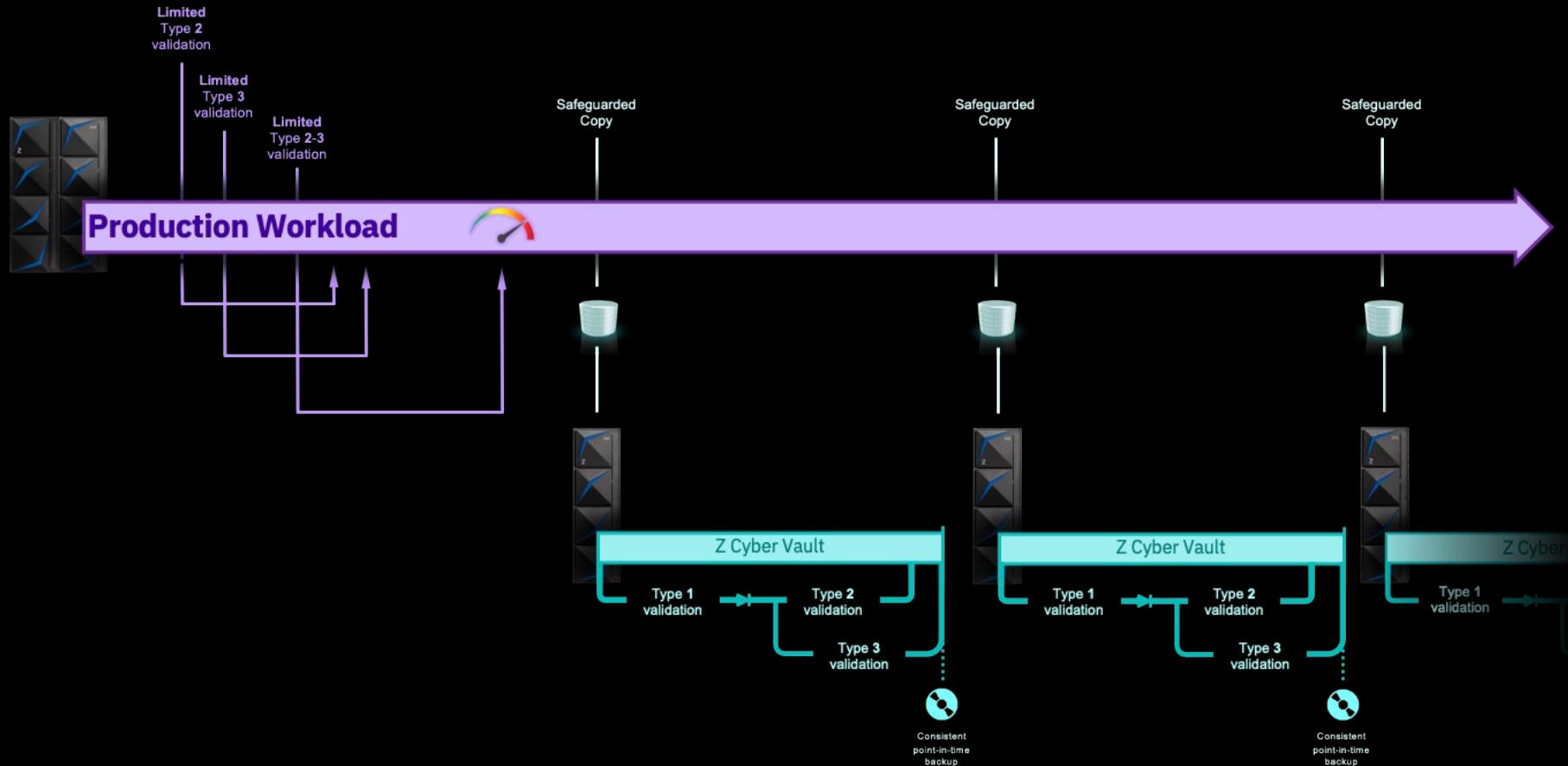
Consistent
point-in-time
backup

IBM Z Cyber Vault type 2 – data structure validation

We provide sample validation processes for 6 types of data structure validation activities, using included z/OS and subsystem utilities:

- Catalog IDCAMS Diagnose and Examine activities
- BCS-VVDS Examine activities
- VSAM KSDS files Examine activities
- RACF database data structure validation
- Db2 database data structure validation for a Db2 V11 standalone subsystem
- Db2 database data structure validation for a Db2 V12 data sharing subsystem

IBM Z Cyber Vault cycle



IBM Z Cyber Vault as a **sandbox**



- Cyber Range for **Pentesting** and **Ethical Hacking**
- Chaos Engineering experiments

IBM Z Cyber Vault software selection – Start here

Here are the recommended tools to manage and provide resiliency capabilities to the z/OS environment, including the z/OS catalog, DFSMShsm backup subsystem, and security related aspects to identify unauthorized activity.

Solution	P	CV	Capability
IBM Tivoli Advanced Catalog Management for z/OS Pointer checking for the catalog.	✗	✓	Data Validation
Recovery of a catalog, including forward recovery to specific point in time.	✓	✓	Recovery
IBM Tivoli Advanced Reporting and Management for DFSMShsm Verify inventory data set records are in sync with migration and backup copies.	✗	✓	Data Validation
Compare reports between safeguarded copies taken at different times and find differences.	✗	✓	Forensic Analysis
IBM Tivoli Advanced Audit for DFSMShsm Conduct trouble-free audits and automate corrective actions.	✗	✓	Recovery
IBM Security zSecure Audit Potential identification of malicious database activities to help identify starting point of corruption.			
IBM CICS VSAM Recovery CICS VSAM Recovery (CICS VR) is used to recover lost or damaged VSAM datasets. It determines which CICS logs and VSAM backups are needed and constructs the recovery jobs.			



IBM Z Cyber Vault software selection – Db2

These are the products that, following IBM Best Practices, provide resiliency capabilities for your Db2 databases.

IBM Db2 Utilities Suite

- The Db2 Utilities Suite is at the core of managing DB2 for z/OS. Helps minimize downtime associated with routine DB2 data maintenance, while ensuring the highest degree of data integrity. It provides Db2 data operations such as REORG, LOAD, UNLOAD and more.

IBM Db2 Log Analysis Tool

- Provides the ability to pinpoint who did what and when to business critical Db2 data. It enables the flexibility required to track data changes by automatically building reports of changes made to database tables, as well as isolate accidental or undesired changes made to data, and optionally undo or redo changes made to data.

IBM Db2 Recovery Expert

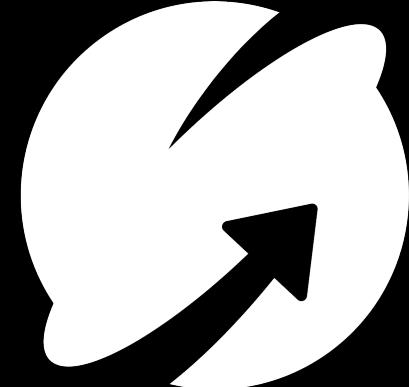
- Analyzes data and conditions to drive the necessary Db2 backup recovery processes to meet Recovery Time Objectives. Recovery plans provide cost and time estimations. with recovery jobs are built and validated PRIOR to execution. Supports point-in-time, dropped object, transaction, redirected, application, system level and disaster types of recovery operations.



IBM Z Cyber Vault software selection – IMS

These are the products that, following IBM Best Practices, provide resiliency capabilities to your IMS database and transaction processing subsystems.

Solution	P	CV	Capability
IBM IMS High Performance Pointer Checker	✗	✓	
Pointer checking IMS full function databases			
IBM IMS Fast Path Solution Pack	✗	✓	
Pointer checker function for Fast Path databases, aka DEDBs			
IBM IMS Recovery Solution Pack	✗	✓	
Database Recovery Facility component to validate all assets needed for recovery are available and can get to all of them			
IBM IMS Connect Extensions	✓	✗	
Collect and write data about IMS transactions coming in through IMS Connect			
IBM IMS Problem Investigator	✗	✓	
Deep dive analysis of IMS logs and IMS Connect Extensions journals			
IBM IMS Performance Analyzer	✗	✓	
Report on transactions that occurred during a specified period			
IBM IMS Recovery Solution Pack	✓	✓	
Recover specific IMS systems or databases based on the volume level backups			
IBM IMS High Performance Pointer Checker	✗	✓	
Repair specific segments in IMS full function databases without requiring full recovery			
IBM IMS Fast Path Solution Pack	✗	✓	
Repair specific segments in IMS Fast Path databases without requiring full recovery			
IBM IMS Queue Control Facility	✓	✓	
Recover and/or replay specific transactions			





Protect your **non-database-managed** data as **dynamically** as your online data

Modernize your non-database managed data to get **accurate, actionable insights**



Automate recovery in minutes



Streamline your backup process with minimal human effort

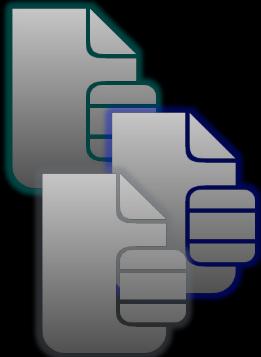


Prove compliance beyond planned events

IBM Z Cyber Vault software – non-database managed files



Database managers keep track of **database activity** (logs) and provide tools to **recover** to a consistency point



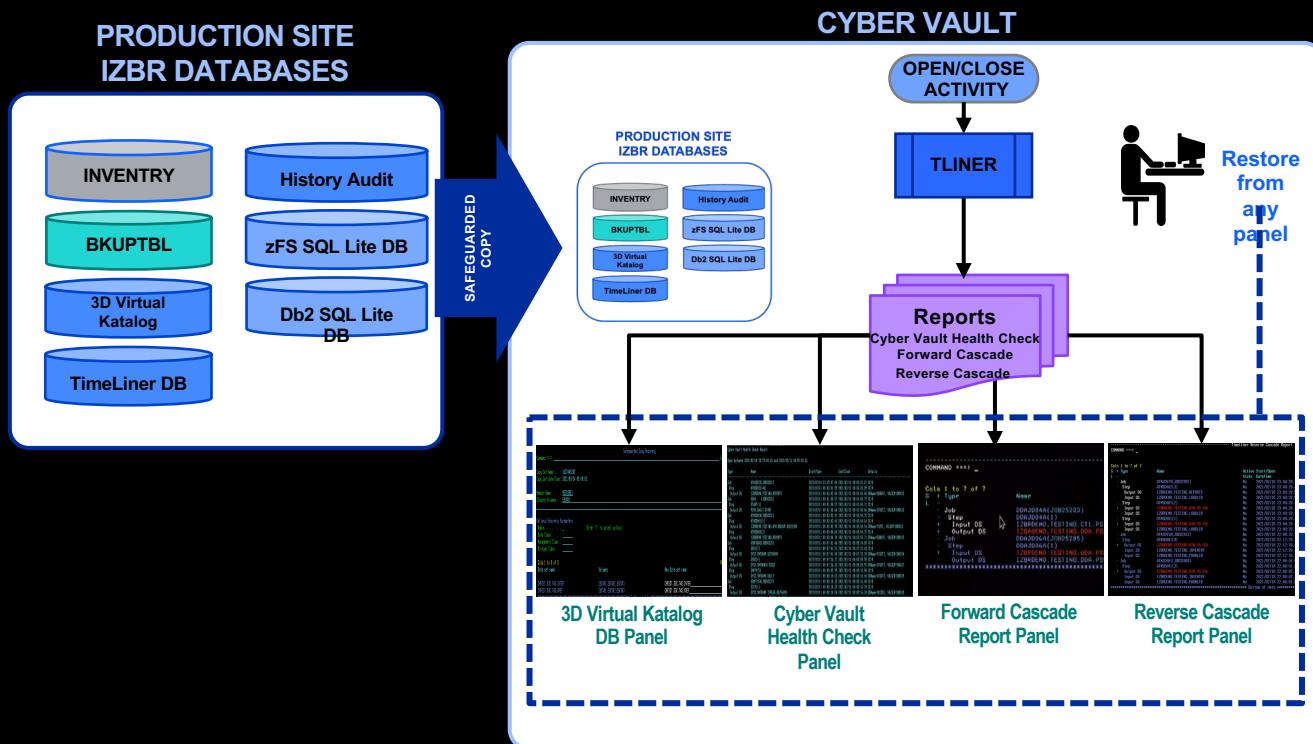
IBM Z Batch Resiliency v1.2 provides **log** and **recover** capabilities for non-database managed data, such as libraries, flat files, and VSAM datasets.

- Cyber Vault **health check** report for Safeguarded copies
- **TimeLiner reverse cascade** report for forensic analysis
- **TimeLiner forward cascade** report to create recovery plan
- **Panel driven** surgical recovery

Cyber Vault Support - Complete inventory of every data set in a Safeguarded Copy enables surgical recovery of any data set from Safeguarded Copy with Copy Services Manager (CSM) or GDPS LCP*

Capabilities to benefit recovery in IBM Z Cyber Vault deployments

- Surgical recovery of **any data set** using 3DVK database, automatically generating accurate restore JCL
- Cyber Vault Health Check report identifies “at risk” non-database managed data in air gapped copy
- Additional forensic capability is created through HISTORY, AUDIT and INVENTORY including identification of critical input tape data
- Reverse Cascade report assists forensic investigation of corruption by identifying jobs and steps that updated the corrupted files, and when
- Forward Cascade Report assists in developing a forward recovery plan for the applications that use the data that is recovered



* Watch this APAR!

APAR PH47869 – ‘Implement GDPS/LCP recovery support in IZBR’

GDPS/LCP or Copy Services Manager (CSM) is needed to manage SafeGuarded Copy

Manage the whole Data Corruption Protection lifecycle with the same tool you manage your CA and DR environment with –
GDPS/LCP is an enhancement to existing GDPS implementations. CSM can manage all DISK copy services.

GDPS Metro 4.3

LCP Management Profiles

Dashboard

LCP Profiles: 7

Profile: GOLD_SOC_R51

Created by: TESTR01

Creation date: 2020/05/09 09:41:07

Last modified by: Modified date:

Consistency Group	Replication Site	Management Profile	Capture Type	Volume Count	Copy Sets	Capture Count	Expedited Count	Last Capture Date	Last Capture Copy Set	Retention	Minimum Interval
PRODUCT1	1	GOLD_SOC_R51	SAFEGUARD	111	1	8	8	2020/05/09 09:42:19	001	MINUTE(1)	MINUTE(1)
PRODUCT1	1	RECOVERY	FLASHCOPY	108	1	0	0			N/A	N/A
PRODUCT1	1	UNASSIGNED	FLASHCOPY	16	3	0	0			N/A	N/A
PRODUCT1	2	GOLD_FC_R52	FLASHCOPY	16	2	0	0			MINUTE(1)	MINUTE(1)
PRODUCT1	2	GOLD_SOC_R52	SAFEGUARD	111	1	7	7	2020/05/09 09:41:42	001	MINUTE(1)	MINUTE(1)
PRODUCT1	2	RECOVERY	FLASHCOPY	109	1	1	0	2020/05/09 09:41:14	001	N/A	N/A
PRODUCT1	2	UNASSIGNED	FLASHCOPY	16	1	0	0			N/A	N/A

Last update: 2020/05/12 09:03:09

Health Overview

HyperSwap : OK

Current System: AZK1 AZK1P

Current Master: AZK1 AZK1P

GDPS version: GDPS V4.R3.M1

Region: STOCKHOLM

SDF Alerts

WTORs

Customer has GDPS installed?

GDPS/LCP to manage the data corruption protection solution is preferred

Create Session

Hardware type: DS8000, DS6000, ESS 800

Session type: Safeguarded Copy

Choose Session Type: Point in Time, FlashCopy, Safeguarded Copy (selected), Synchronous, Metro Mirror Single Direction, Metro Mirror Failover/Fallback, Metro Mirror Failover/Failover w/ Practice, Asynchronous, Global Mirror Single Direction, Global Mirror Failover/Failback

Create a Scheduled Task

How often do you want the task to run?

Schedule: Hourly (selected)

Every (hours): 1

Daily / Weekly: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Time [W. Europe Daylight Time]: 12:00 PM

No schedule

OK Cancel

Customer has CSM installed?

Integrate the data corruption protection solution

IBM Z Cyber Vault solution



IBM storage

Data volumes and active copies generated and maintained

DS8000 SafeGuarded Copy

Immutable backups

TS7700 Virtual Tape with Encryption and/or WORM

Secure air-gapped data vault

IBM Z and Software

The only System with a 99.99999% availability

EAL 5+ certified IBM Cyber Vault for Z LPAR for validation, testing and forensics

Data monitoring, consistency and anomaly detection

Management Software

IBM Security solutions

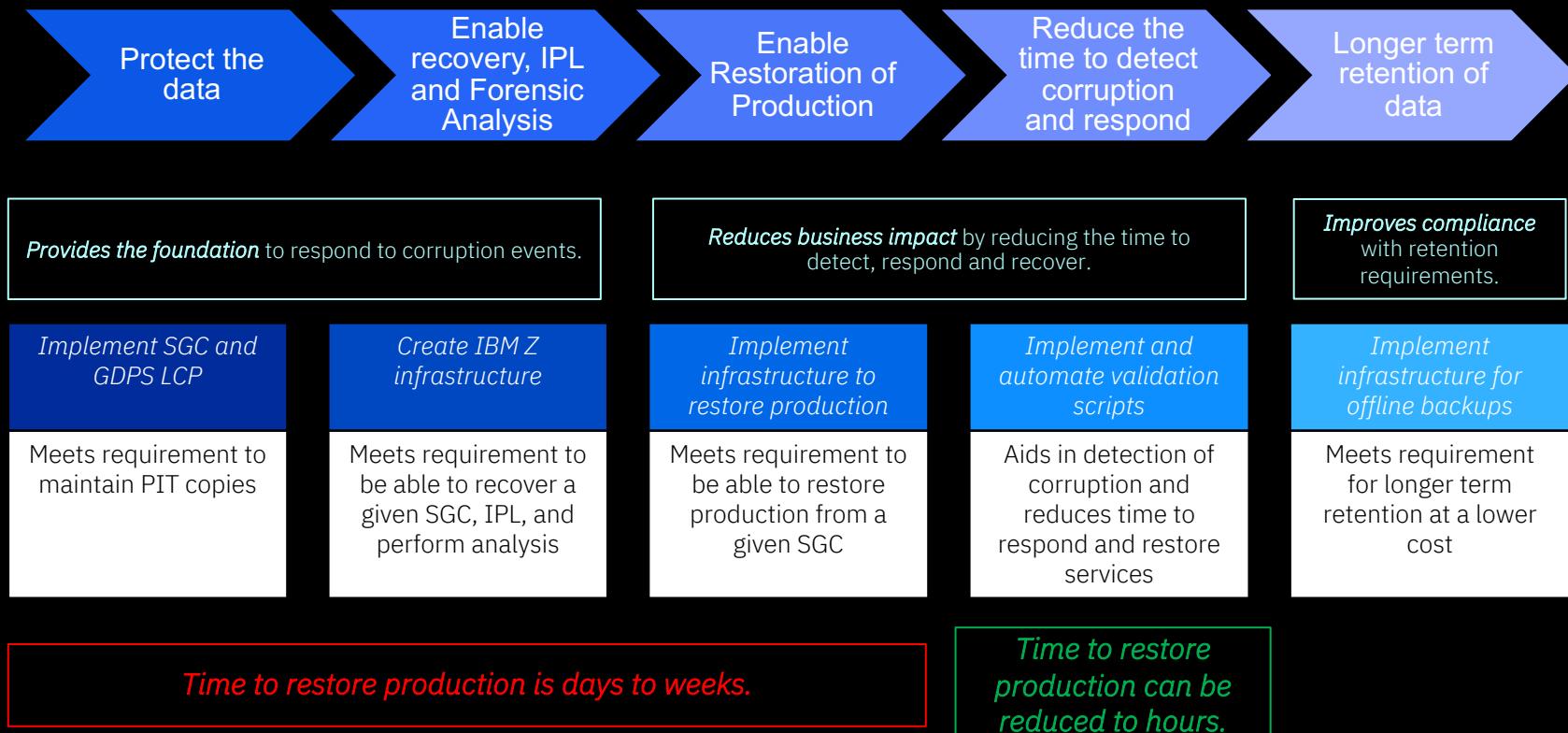
IBM Services

IBM GDPS provides services, clustering technologies, and server and storage replication and automation

Logical Data Corruption (LCP) and Copy Services Manager (CSM) enhancements manage the entire recovery environment

IBM Lab Services risk assessment and deployment services

The IBM Z Cyber Vault journey provides exponential value at each step.



- ✓ **Introduction and Overview**
- ✓ **Key threats**
- ✓ **Configuration Examples**
- ✓ **Planning and Considerations**
- ✓ **Storage sizing**
- ✓ **Safeguarded Copy & FlashCopy**
- ✓ **Infrastructure Design (GDPS, CSM, etc)**
- ✓ **Hardware Requirements**
- ✓ **Software stack**
- ✓ **Services**
- ✓ **Deployment and Implementation**
- ✓ **Sample code**

Draft Document for Review April 13, 2021 5:44 pm SG24-8511-00



Getting Started with IBM Z Cyber Vault

Bill White

Matthias Bangert

Cyril Armand

Roger Bales

Diego Bessone

Anthony Ciabattoni

Michael Frankenberg

Debra Hallen

DeWayne Hughes

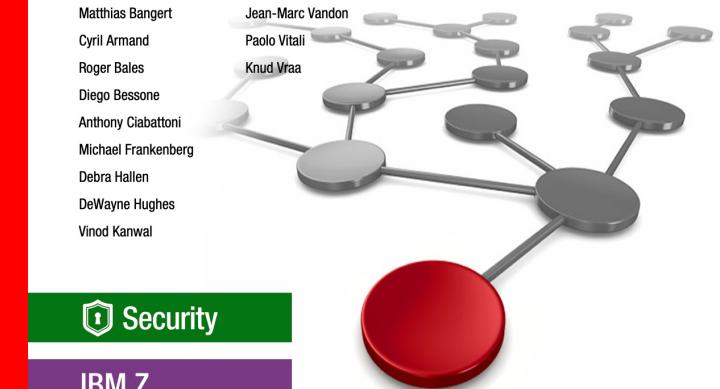
Vinod Kanwal

Karen Smolar

Jean-Marc Vandon

Paolo Vitali

Knud Vraa



Security

IBM Z

IBM

Redbooks

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM*

ibm.com*

IBM logo*

* Registered trademarks of IBM Corporation

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Zowe™, the Zowe™ logo and the Open Mainframe Project™ are trademarks of The Linux Foundation.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g. zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the "Authorized Use Table for IBM Machines" provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html ("AUT"). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Financing Available: IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. For more information, visit: ibm.com/financing.

© Copyright IBM Corporation 2020.

IBM Z Software New Orchard Road Armonk, NY 10504.

Produced in the United States of America, April 2020.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml. This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.