Fortifying IMS Against Cyber Threats

A Cloud-Era Resilience Blueprint

Gary Turner
IMS Software Consultant

Good Morning,

we've got a lot to talk about.

Gary
Turner

IMS Software Consultant

01. Resiliency, why does it matter?

02. Where to begin?

03. Capturing IMS Updates

04. Safeguard your Recovery Assets

05. Practice the plan

06. Q&A

Agenda

What's It Really Mean?

Resilience: The capacity to **withstand** or to **recover** quickly from difficulties

Operational Resilient Systems:

- **Stable**
- **Secure**
- **Robust validated recovery processes**

Is It Important?

Security remains a top priority

Overall, compliance and security are the top priority for survey respondents for the fourth year in a row, named by 61 percent of respondents. This focus on security has made an impact, with a five percent rise in respondents who report using a dedicated mainframe security information and event management (SIEM) solution compared to 2020, the first year security and compliance were named as the top priority in the survey.

The adoption of personally identifiable information (PII) solutions, privileged user monitoring, privileged access management (PAM), and other proactive security capabilities has also increased significantly.

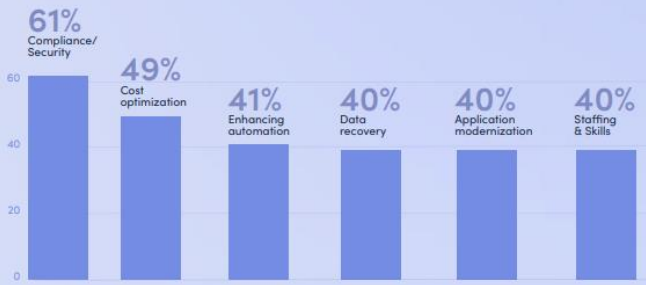
Which of the following security capabilities and/or components are actively used in your mainframe infrastructure?

- PII data ID software — 47%
- Application vulnerability scanning — 46%
- Privileged user monitoring — 45%
- Privileged access management — 44%
- External services for pentesting — 42%
- Send data to enterprise SIEM — 40%

2023 BMC Mainframe Survey Report 5

Other Priorities

While cost optimization remains near the top of the list, there was also a significant increase in the prioritization of enhancing automation, jumping from **36 percent in 2021** to **41 percent this year** and moving into the top three mainframe priorities, followed by a wide array of other priorities.



Top four mainframe priorities of extra-large shops*

2023 BMC Mainframe Survey Report

*Shops with more than 50k MIPS 6

Is It Important?

Digital Operational Resilience Act

Financial institutions must have a sound, comprehensive and well-documented ICT risk management framework

- European Commission legislation – effective 17 January 2023
- Enforceable from 17 January 2025
- Mitigate cyber-attacks –withstand, respond, and recover
- Robust framework with common set of standards
- Tested using third party penetration
- Prove compliance – demonstrate recovery

Digital Operational Resilience Act

Financial institutions must have a sound, comprehensive and well-documented ICT risk management framework

"When recovering from an ICT-related incident, financial entities shall perform multiple checks, including reconciliations, in order to ensure that the level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems."

Is It Important?

[2023 Ransomware Attacks Up More Than 95% Over 2022, According to Corvus Insurance Q3 Report]

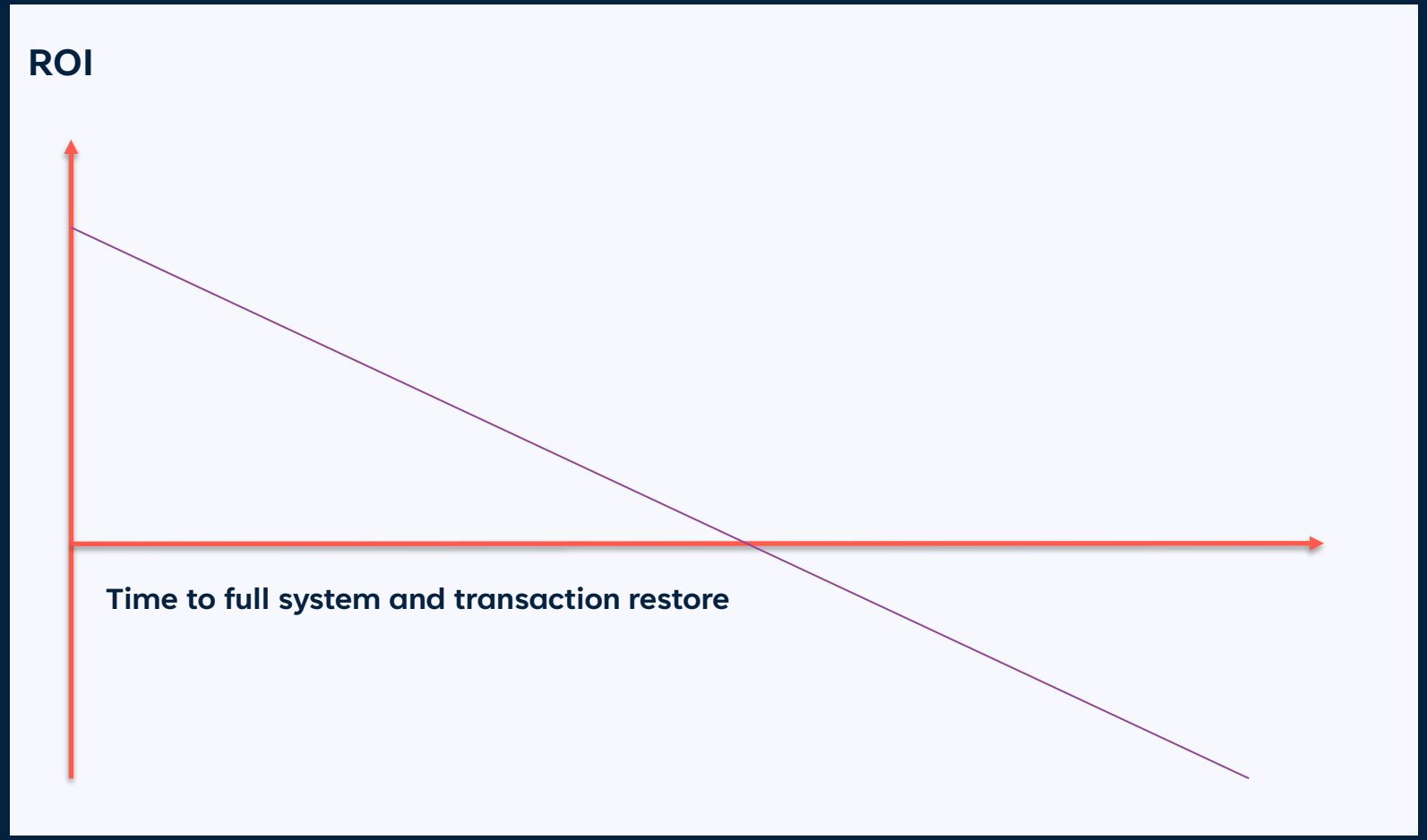
List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached

Top ten data breaches in 2023

	Organisation name	Sector	Location	Known records breached	Month of public disclosure
1	DarkBeam	Cyber security	UK	>3,800,000,000	September
2	Real Estate Wealth Network	Construction/ real estate	USA	1,523,776,691	December
3	Indian Council of Medical Research (ICMR)	Healthcare	India	815,000,000	October
4	Kid Security	IT services/ software	Kazakhstan	>300,000,000	November
5	Twitter (X)	IT services/ software	USA	>220,000,000	January
6	TuneFab	IT services/ software	Hong Kong	>151,000,000	December
7	Dori Media Group	Media	Israel	>100 TB*	December
8	Tigo	Telecoms	Hong Kong	>100,000,000	July
9	SAP SE Bulgaria	IT services/ software	Bulgaria	95,592,696	November
10	Luxottica Group	Manufacturing	Italy	70,000,000	May

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

The Economics of Resilience



The return on investment on your solution is realized at the point of execution – if operational restore take 48 hours+ the ROI goes negative

Where to begin?

Start with a good foundation

bmc

Image Copy

- Batch
- Fuzzy
- Incremental
- Snapshot

Building Backup Strategy

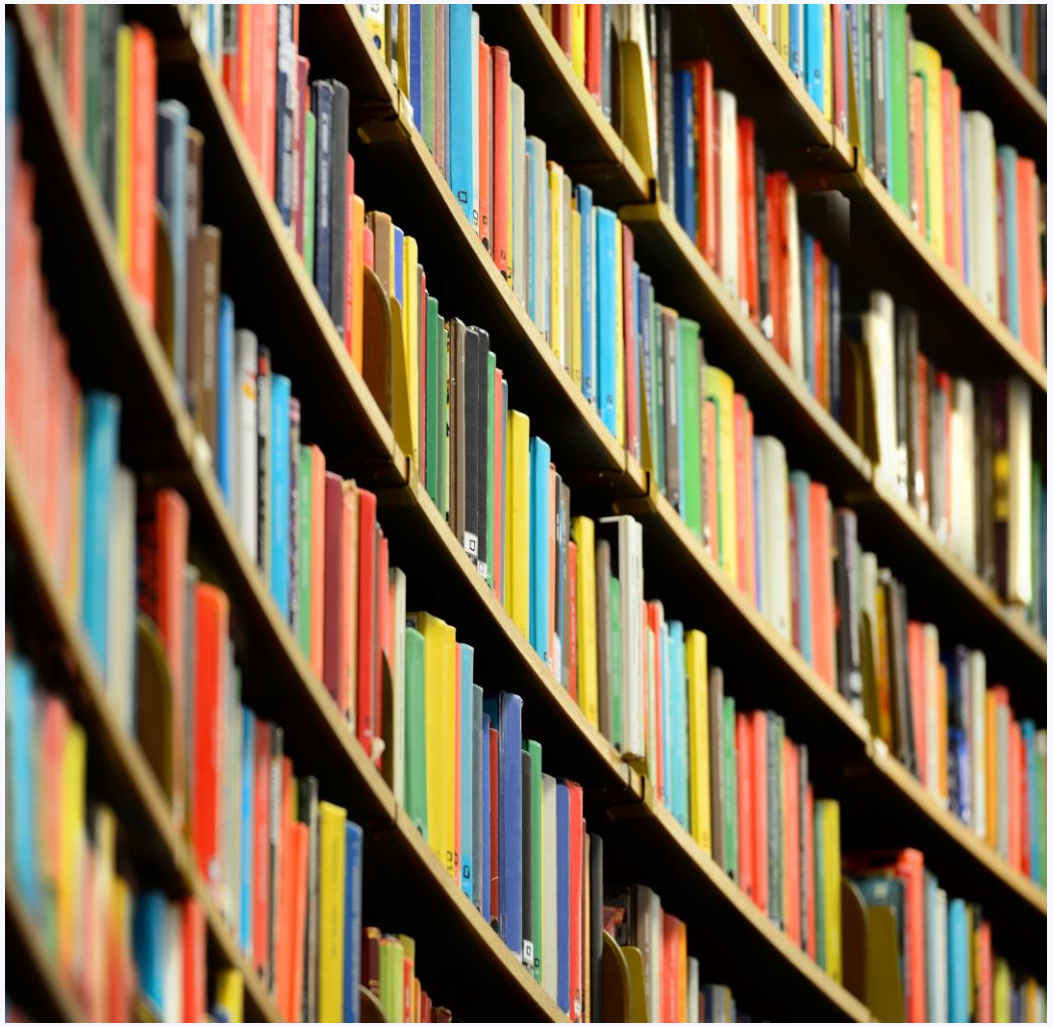
- Availability Considerations
- Image Copy by CAGRP or DBDSGRP
- Create multiple copies at once
- Asynchronous processing
- Stacking
- Virtual Image Copy
- Copy/Move Image Copy

Process Efficiently

- Conditional Image Copy
- IC Triggering by CA
- Capture data set allocations
- Compression
- Automatic Restart

What is an “Archive” Image Copy

- A special backup of a database or group of databases
- Current database definitions
  - IDCAMS, DBRC, DFSMDA, etc.
- Runtime modules
  - DBD, Compression, randomizers, Partition selection Exits, etc.
- A repository to keep track of each archive and associated resources
- Included in Recovery Plus for IMS



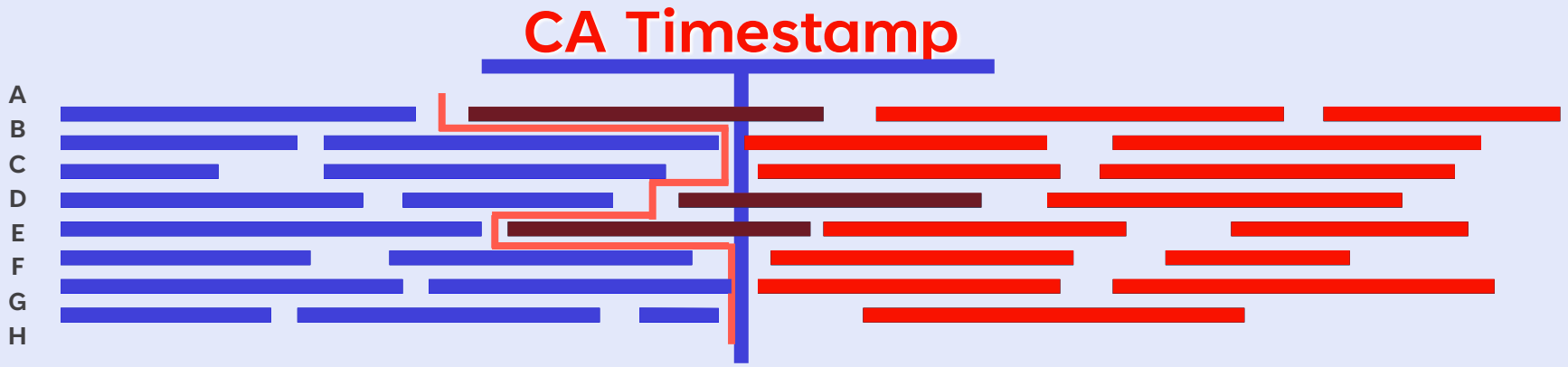
Capturing IMS Updates

bmc

Change Accumulation

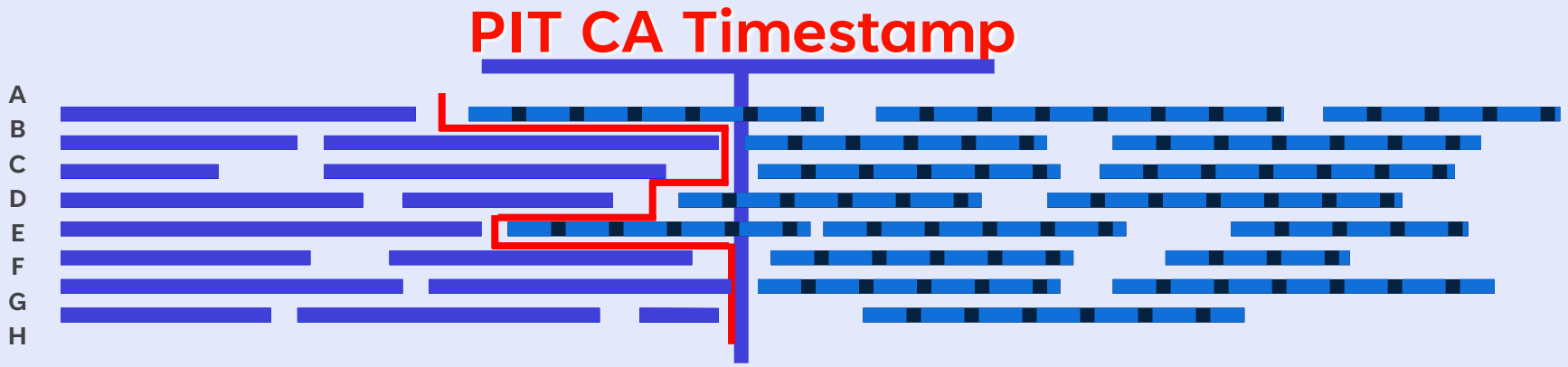
- Reduce Image Copy frequency
- Shorten recovery times
- Verify log data
- Reduce number of logs
- Utilize zIIP processors
- Produce multiple CA data sets

No Timestamp PITCA



- Change Accum Plus creates a logically correct PIT Change Accum
- Transactions that finished before the PIT are accumulated
- Transactions that finished after the PIT are *carried forward* to the next CA run
- No timestamp PIT CA can be used by the Incremental IC function to create a *logically correct* IC without touching the database.

Timestamp PITCA



- Change Accum Plus creates a logically correct PIT Change Accum
- Transactions that finished before the PIT are accumulated
- Transactions that finished after the PIT are ***DROPPED***
- CA is marked as invalid in RECON
- No need to transport SLDS
- Can only be used Recovery Plus

This timestamp can also be pushed over to a Db2 coordinated Recovery

Safeguard your Recovery Assets

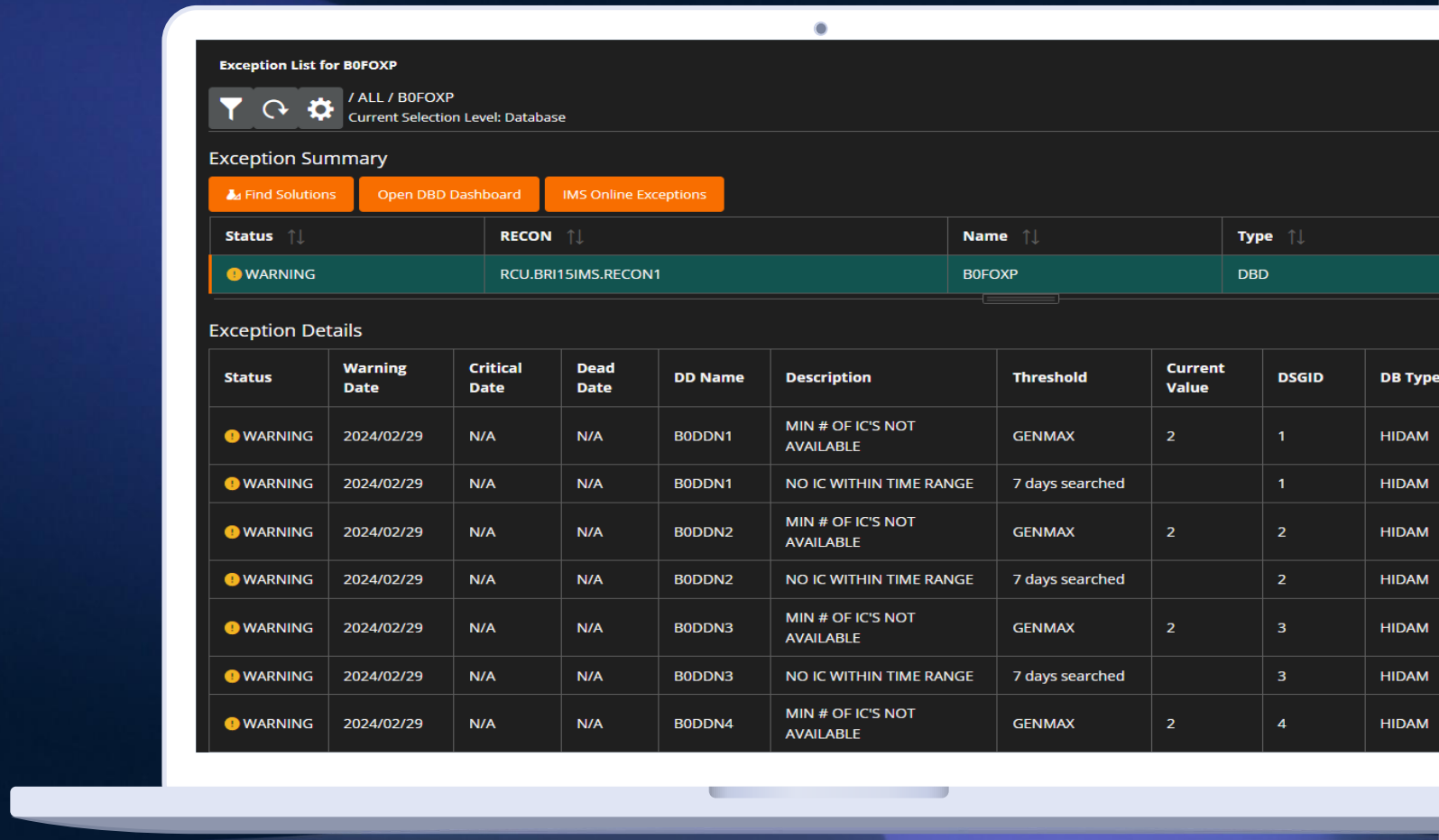
bmc

RECON Data Sets

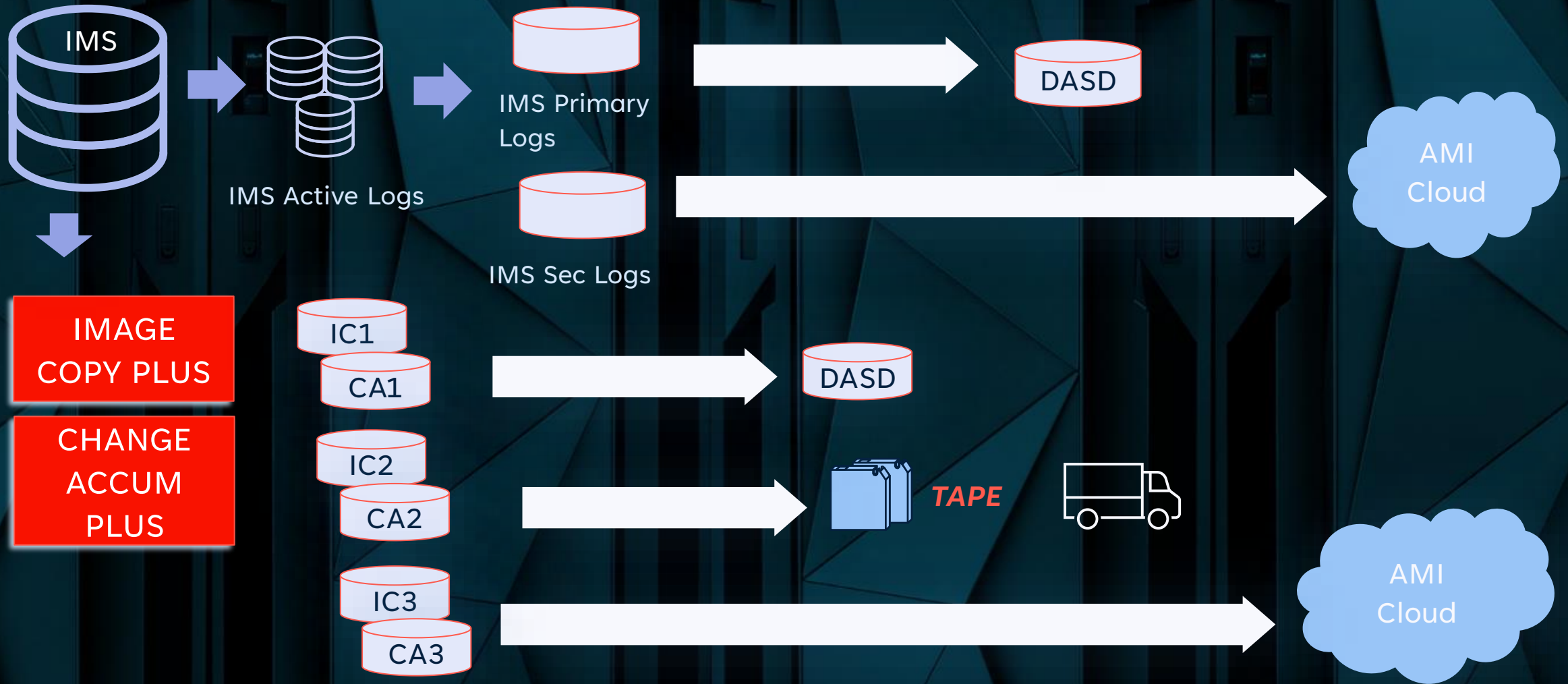
- Most important IMS data sets
- Back them up frequently
- DR RECON Cleanup Utility
- Recovery Extensions
  - AKA “RECON Extensions”

Recovery Advisor

Monitor your Recovery Assets!!



No Single Point of Failure



Practice, Practice, Practice!

bmc

Considerations

- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)
- Align recovery strategy with your Application teams
- Do existing procedures need to change?

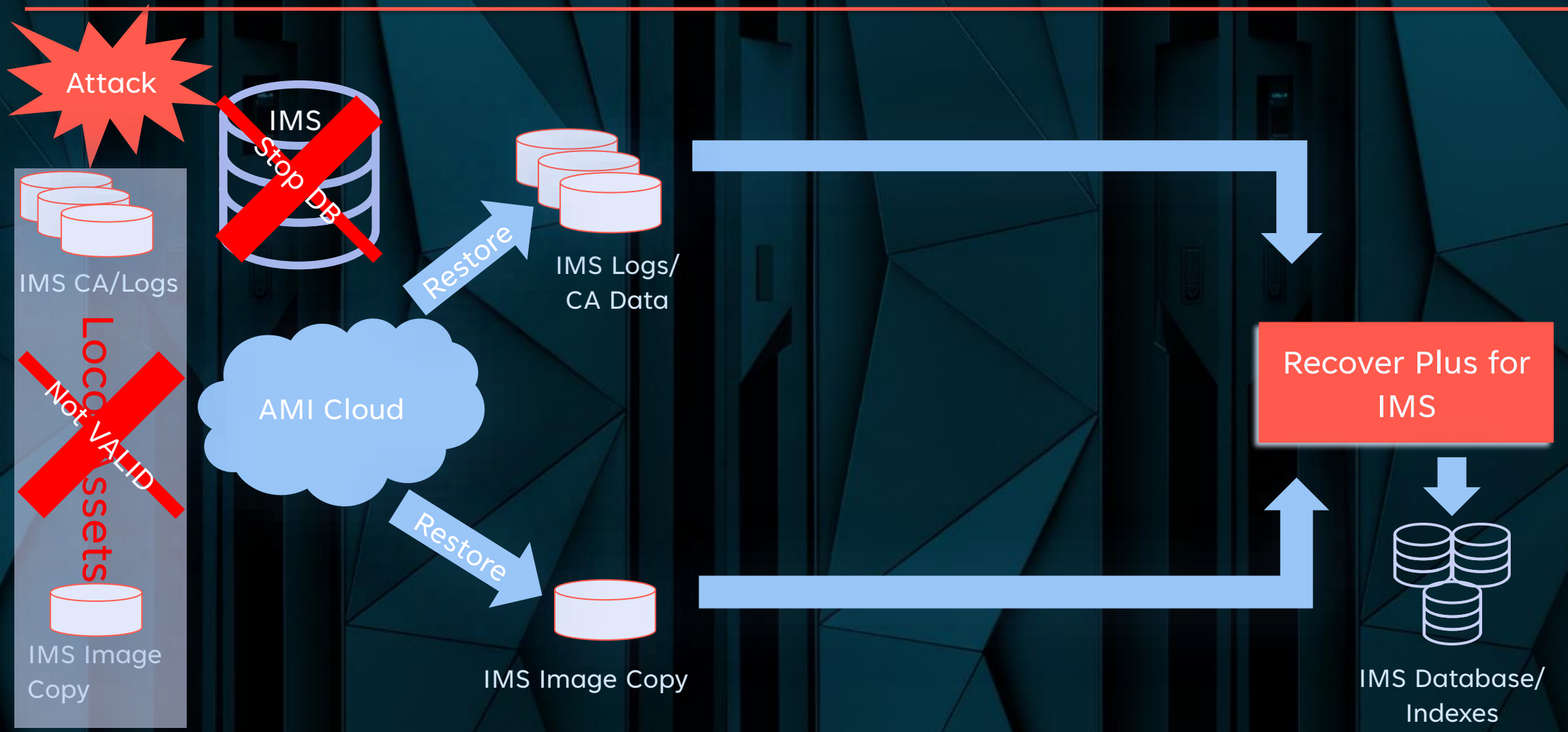
Testing the Recovery

- Building recovery JCL
- Find Recovery Points
- Log Analysis
- Disaster Recovery exercise
- Simulation
- Estimate

Pick Your Recovery Options

- Last Image Copy (LASTIC)
- Point-in-time CA (LASTPITCA)
- Point in Time (PIT)
- Recovery Extensions
  - SIC(n)
  - SCA(n)
- Secondary logs (SLOG)
- Automatic Restart
- Pointer check, Rebuild indexes/ILDS, and image copy during the recovery

Recovery - Demo



bmc

Closing Thoughts
Plan and TEST your Strategy

- Collect and monitor recovery assets
  - Image Copies
  - Change Accumulation
  - Logs
  - Don’t forget about the RECON!!
- TEST, TEST, TEST!!!

Questions?

bmc

Thank you