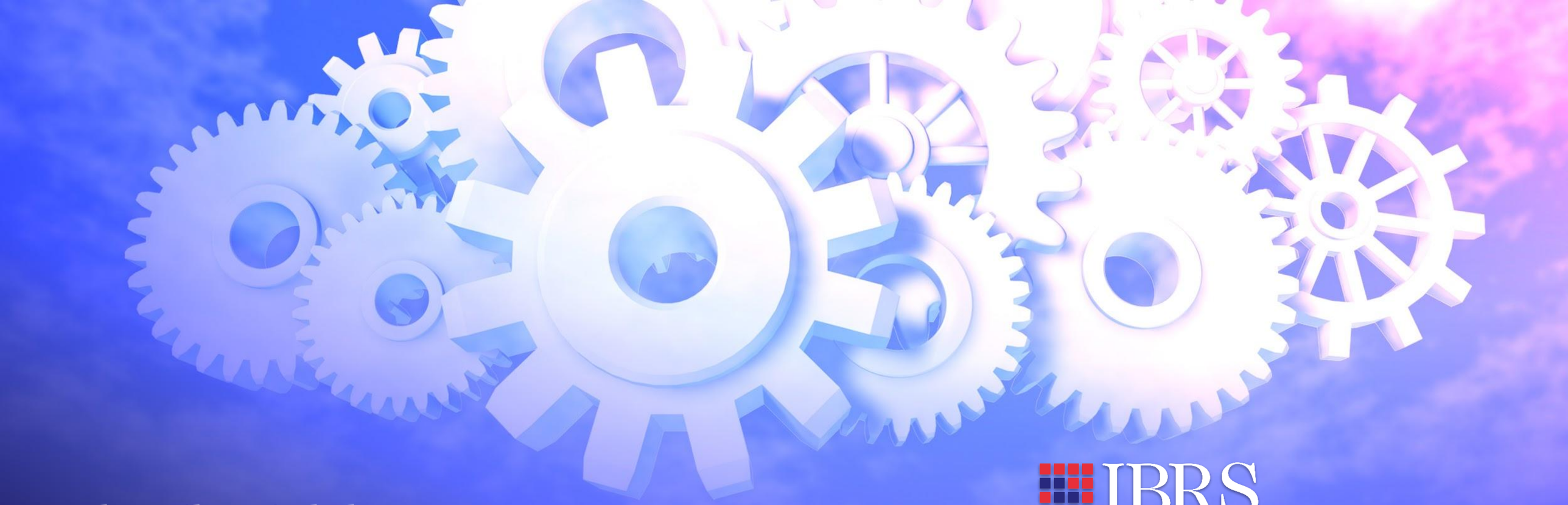


by Mike Mitchelmore

IBRS

Presentation

Business Impact Analysis for Cloud/SaaS IT Ecosystems

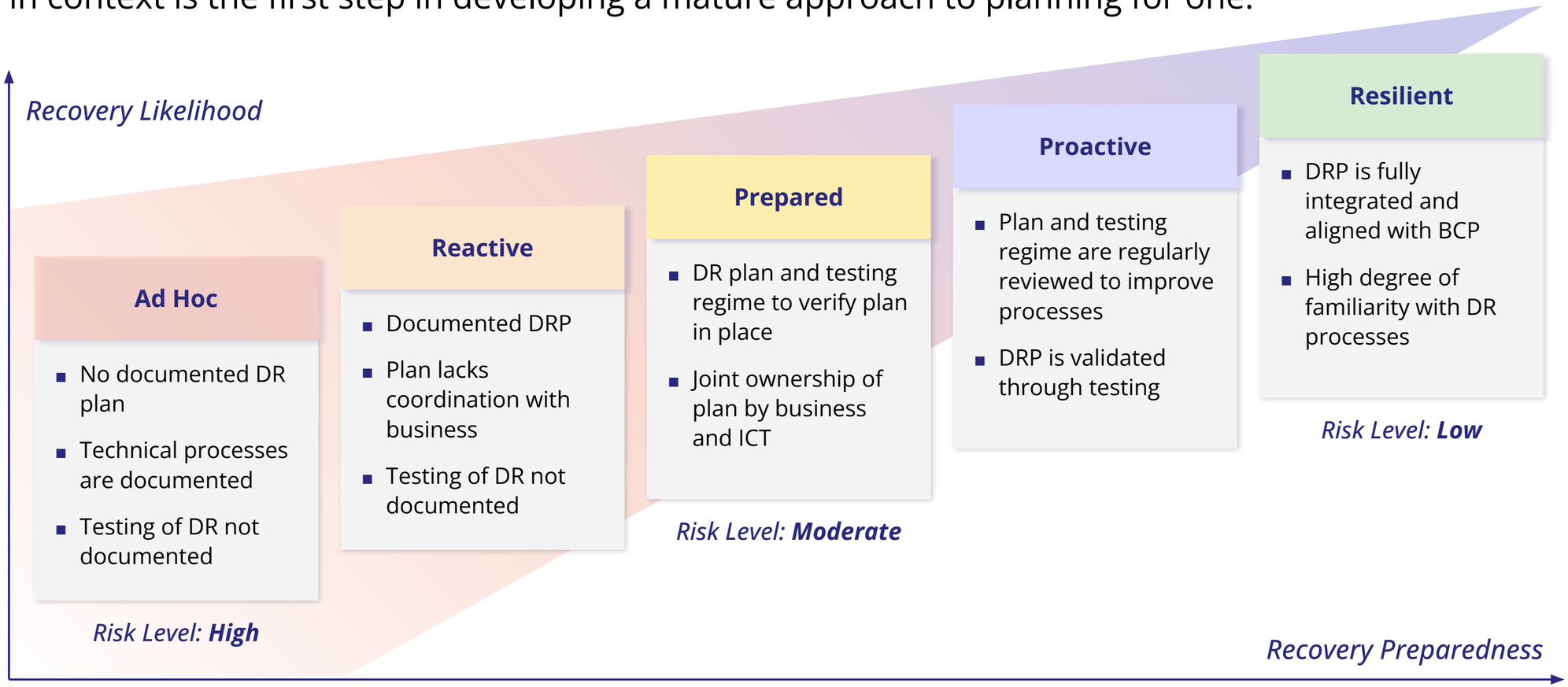
ICT Support to Disaster Recovery and Cyber Incident Response

Today's Goals

- What are the outcomes CIO's need from a business impact analysis (BIA) in a multi Cloud and SaaS IT ecosystem
- Recovery time objective (RTO) versus recovery point objective (RPO) in the Cloud and Software-as-a-Service (SaaS) world
- What you need to consider in your contract management of partner and provider contracts
- A renewed focus on data architecture. Assess methods to recover data to achieve an RPO of zero
- What investments do you need to improve people, process, and/or technology to better support business
- Q and A Session

Taking the Long Term View of DR Planning

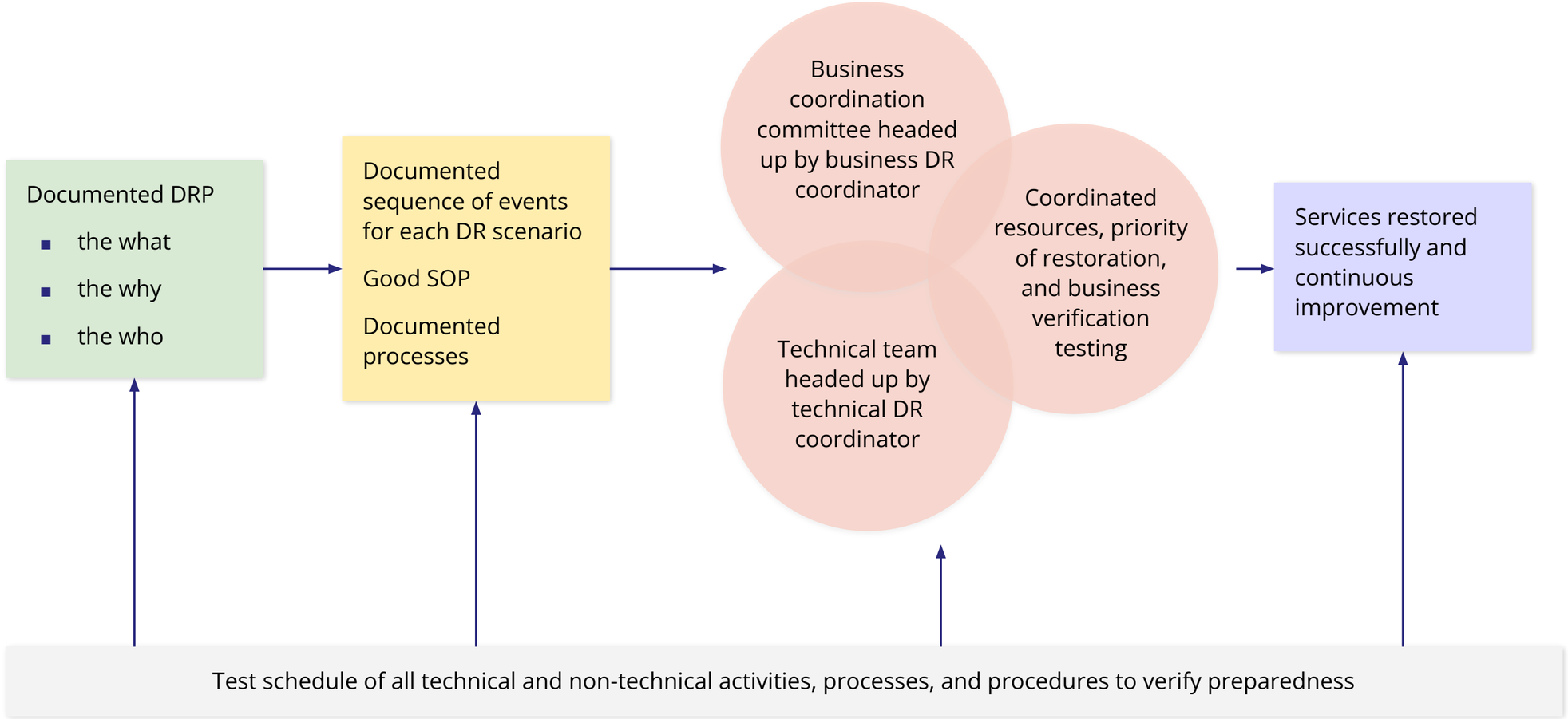
The concept of a disaster is often not well understood. The need to clearly put a disaster in context is the first step in developing a mature approach to planning for one.



BIA in a Multi Cloud and SaaS IT Ecosystem

- Determine the interaction of the business processes with the IT ecosystem
- Quantify costs associated with loss of service
- Quantify risks to business (e.g. direct financial, reputational, and contractual)
- Confirm the BCP correctly interacts with DR and Cyber Incident plans/strategies
- Understand the data feeds between Cloud and SaaS services within the business processes
- Determine priority of restoration based on impact of losing services for 1 day, >1 day, etc.

DR and Cyber Incident Planning Construct



RTO versus RPO in the Cloud and SaaS World

- Recovery Time Objective
- Recovery Point Objective
- Impact of the Cloud or SaaS providers contractual obligations
- Understanding data flows between Cloud and SaaS environments
- The opportunity of recovering data from upstream and downstream Cloud SaaS systems
- The need to do extra work to develop processes to better manage data in a DR event

Example Advice – AWS

Source: Disaster Recovery (DR) Architecture on AWS, Part I: Strategies for Recovery in the Cloud

Disaster recovery options in the cloud

Disaster recovery strategies available to you within AWS can be broadly categorized into four approaches, ranging from the low cost and low complexity of making backups to more complex strategies using multiple active Regions. Active/passive strategies use an active site (such as an AWS Region) to host the workload and serve traffic. The passive site (such as a different AWS Region) is used for recovery. The passive site does not actively serve traffic until a failover event is triggered.

It is critical to regularly assess and test your disaster recovery strategy so that you have confidence in invoking it, should it become necessary. Use AWS Resilience Hub to continuously validate and track the resilience of your AWS workloads, including whether you are likely to meet your RTO and RPO targets.

active/passive

Backup & Restore	**Pilot Light**	**Warm Standby**	**Multi-site Active/Active**
RPO / RTO: **Hours**	RPO / RTO: **10s of minutes**	RPO / RTO: **Minutes**	RPO / RTO: **Real-time**
▪ Lower priority use cases ▪ Provision all AWS resources after event ▪ Restore backups after event ▪ Cost: **$**	▪ Data live ▪ Services idle ▪ Provision some AWS resources and scale after event ▪ Cost: **$$**	▪ Always running, but smaller ▪ Business critical ▪ Scale AWS resources after event ▪ Cost: **$$$**	▪ Zero downtime ▪ Near zero data loss ▪ Mission critical services ▪ Cost: **$$$$**

Partner and Provider Contracts

- Assess the DR and Cyber Incident clauses in provider contracts relating to RTO
- Assess the DR and Cyber Incident clauses in provider contracts relating to RPO
- Complete gap analysis of contract and BIA for RTO and RPO
- Assess clauses in provider contracts related to test and reporting of DR and Cyber plans
- Align Cloud and/or SaaS provider contracts with BIA priorities
- Costs related to variation of contracts to align with BIA priorities

DR Cloud Considerations

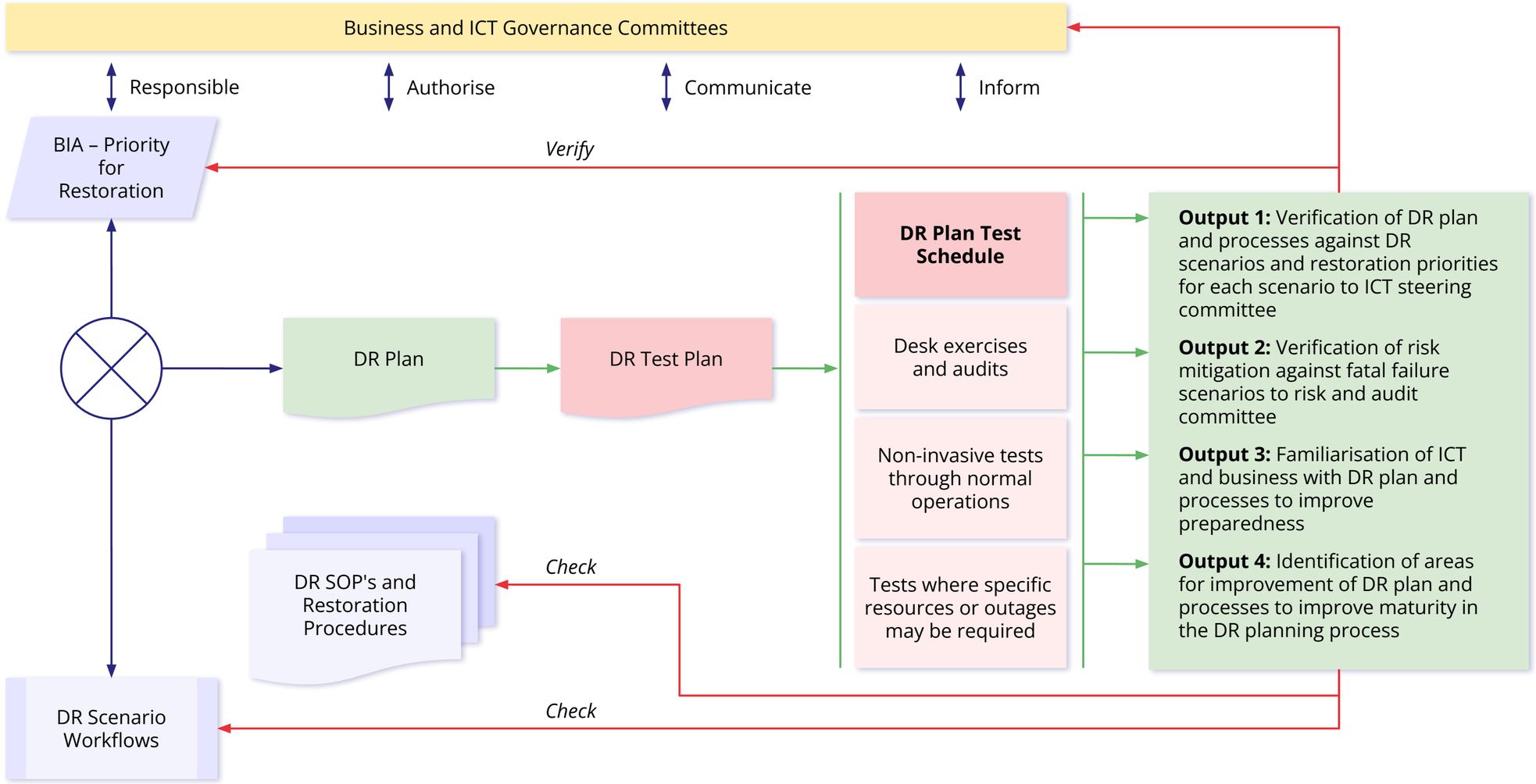
IBRS recommends the DR planning in the Cloud should look to address the following stages of the recovery:

- **Preparedness:**
  - Understand what the Cloud provider is contracted to deliver in terms of RPO and RTO
  - Understand the impact of data sovereignty and other policy settings for the use of Cloud and how does that impact how the Cloud provider designs and delivers your needs
  - Assess your architectural approach to DR in the Cloud

A Renewed Focus on Data Architecture:
Assess Methods to Recover Data to Achieve an RPO of Zero

- Document the data architecture for your Cloud and SaaS IT ecosystem
- Data feed dependencies across the IT ecosystem
- Segment the IT ecosystem based on data holdings
- Gain understanding on where data can be retrieved to achieve zero RPO for any one Cloud or SaaS disaster event
- Assess data caching to support zero RPO for any one Cloud/SaaS disaster event
- Develop and document processes for data to support zero RPO for Cloud or SaaS disaster event
- Develop test processes to confirm recovery of data works

Test Plan Verification



Investment Strategy

- People training and familiarisation
- Processes to ensure currency of information
- Technology?
- Contract management?
- Governance over BCP DR and Cyber Incident Response
- Once you complete a cycle – what are the lessons learned?


Q & A
IBRS

Submit an inquiry or *schedule a whiteboard session*

IBRS

IBRS | ANALYSIS INSIGHT JUDGEMENT

IBRS is a boutique Australian ICT Advisory Company.

We help our clients mitigate risk and validate their strategic decisions by providing independent and pragmatic advice while taking the time to understand their specific business issues.

https://ibrs.com.au info@ibrs.com.au 02 4758 9111 PO Box 519, Hazelbrook NSW 2779, Australia