DISASTER RECOVERY MUST WORK!

ADVISOR

Mike Mitchelmore

IBRS
ANALYSIS
INSIGHT
JUDGEMENT

CHAPTER 1

Disaster Recovery Planning (DRP)

WHOSE PROBLEM IS IT TO SOLVE?

Conclusion

With the growth of dependence on ICT for business to perform effectively, many organisations have increased risk associated with the ability of ICT to provide service continuity. ICT downtime means business is negatively impacted. Many organisations believe the disaster recovery (DR) plan is a problem that is ICTs to solve. Whilst ICT will lead the planning and do a lot of the heavy lifting when a disaster occurs, it can only be successful with the assistance and collaboration of its business partners. It will be the business that sets the priorities for restoration and accepts the risk. Both business and ICT need to be comfortable that the DR plan has been verified to ensure a reasonable expectation that recovery will be successful.

Observations

This is the first of 4 chapters on what organisations need to consider to ensure the maturity of the DRP process is effective and provides a high probability of success. Chapter 1 will set the scene, look at the levels of maturity, and identify the interdependencies. Chapter 2 will provide advice on how the DR plan should be developed. Chapter 3 will look at how the plan can be verified and the effect on your organisation's risk exposure. Chapter 4 will provide advice on how to grow maturity over time.

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. It is sometimes useful to understand where the incident and problem management processes leave off, and where the disaster recovery begins.

CHAPTER 1

Disaster Recovery Planning

WHOSE PROBLEM IS IT TO SOLVE?

In basic terms, there are three types of failure:

- **Minor level failure** where the failure is easily managed using the incident management processes and can be resolved quickly
- **Major level failure** where the failure is a major incident or problem which has impacted multiple business units and will require time and a higher level of coordination to resolve, and
- **Fatal level failure** where most if not all services are impacted and the only way to resolve the situation is to conduct a DR.

There are many possible causes for a fatal failure. The cause of the disaster could be environmental (loss of power grid, catastrophic failure of the services), an act of nature (fire, storm or flood), or criminal (cyber attack, domestic terrorist). Regardless of the cause, the event creates a need for ICT to complete a disaster recovery.

Where a DR is required, there are essentially only three scenarios to plan for:

- Recovery from online disk storage (where a duplicate data repository is available at an alternate site or Cloud service to the primary).
- Recovery from offline disk storage (where the online disk storage has been compromised and is not considered usable).
- Recovery from tape back-up (where all other disk storage and potentially both primary and secondary sites or Cloud services have been compromised).

The differences the scenarios represent to business are measured in the time to restore and to what extent data may be lost. Recovery from online disk storage or from alternate Cloud storage will be faster than offline disk storage, which is faster than tape. The data holdings for online disk storage will be near real-time, whereas offline disk storage will have a delay of several minutes, and tape several hours, which will impact the restoration point objective and will require the business to accept some data may not be immediately recoverable and in some instances transaction data may be lost.

Disaster Recovery Planning

WHOSE PROBLEM IS IT TO SOLVE?

DR maturity is a measure of the organisation's ability to plan for, test preparedness, conduct and continuously improve its probability of a successful recovery. Most organisations will find themselves at a Capability Maturity Model integration (CMMi) level of 1 or 2. The higher on the maturity scale, the higher the probability the recovery will be successful. The CMMi model (Figure 1 depicted below) aligns maturity using recovery preparedness against the likelihood of recovery is successfully executed.

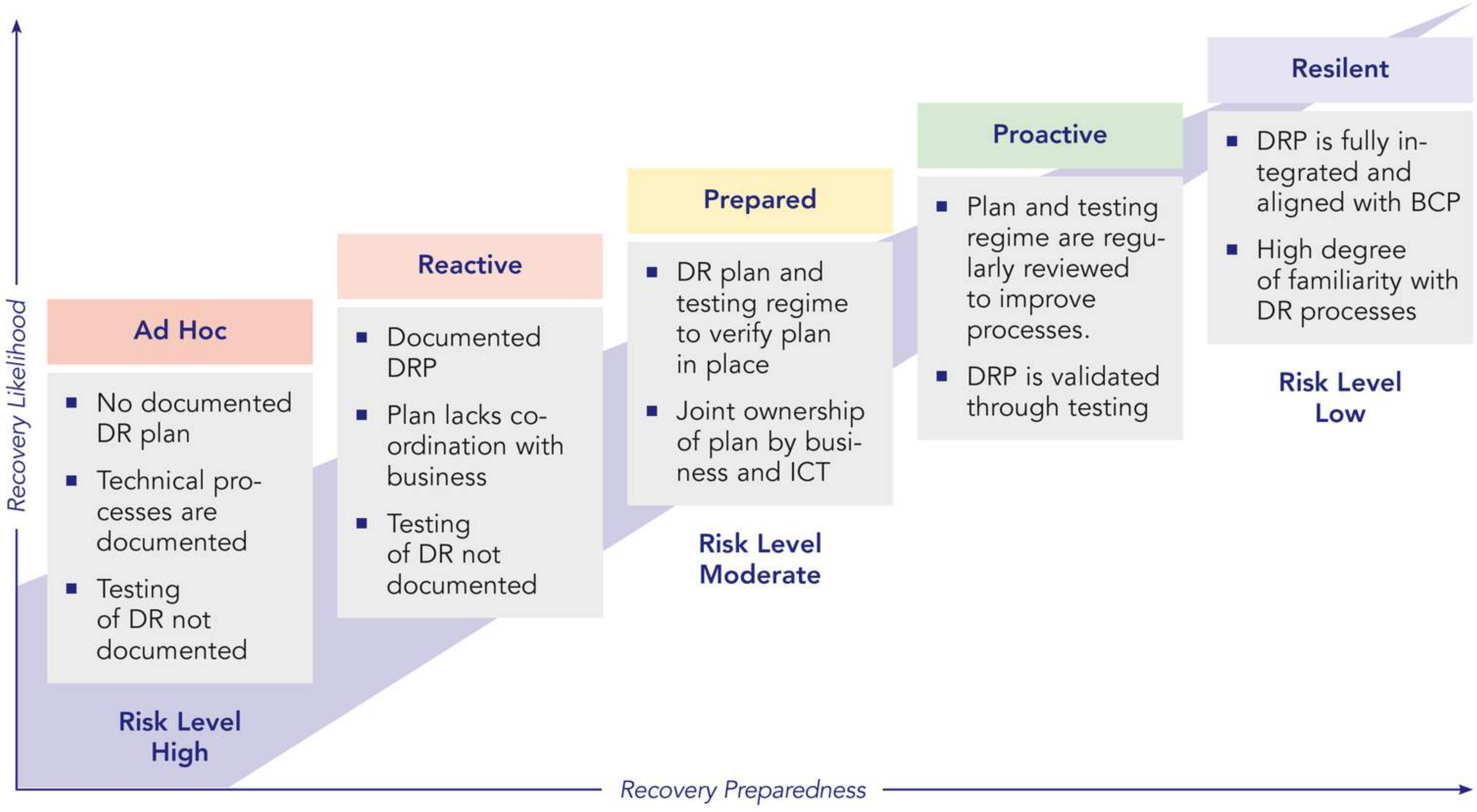

Recovery Likelihood
Ad Hoc
No documented DR plan
Technical processes are documented
Testing of DR not documented
Risk Level High
Reactive
Documented DRP
Plan lacks co-ordination with business
Testing of DR not documented
Prepared
DR plan and testing regime to verify plan in place
Joint ownership of plan by business and ICT
Risk Level Moderate
Proactive
Plan and testing regime are regularly reviewed to improve processes.
DRP is validated through testing
Resilent
DRP is fully integrated and aligned with BCP
High degree of familiarity with DR processes
Risk Level Low
Recovery Preparedness

Figure 1. Disaster Recovery - Capability Maturity Model

IBRS advice is a DR CMMi maturity of 3.5 to 4 is the minimum target to achieve. It is also advised that organisations accept the maturity will take time to build and the first step is to document the DRP and put a testing regime in place to verify preparedness (CMMi Level 2).

Disaster Recovery Planning

WHOSE PROBLEM IS IT TO SOLVE?

DR Interdependencies

The DR plan interdependencies that are essential for the plan to work effectively and the organisation's maturity to increase are:

1. Business impact analysis (BIA) for each business unit that details the priority of restoration if disaster recovery is triggered.
2. Agreed prioritisation of business unit services for restoration by the business executive.
3. A test plan to verify preparedness of the DRP processes that are executed over a set period (IBRS advises a 12-month cycle).
4. Business continuity plans (including the ICT business unit's BCP) should interleave with the DRP to provide coordination of priorities *on the day* and verification testing of services as they are restored before being returned to full operation.

To work with these interdependencies and to ensure the target maturity is reached there are a number of essential components for the DR to be effective. The key components are depicted in the diagram (Figure 2) below.

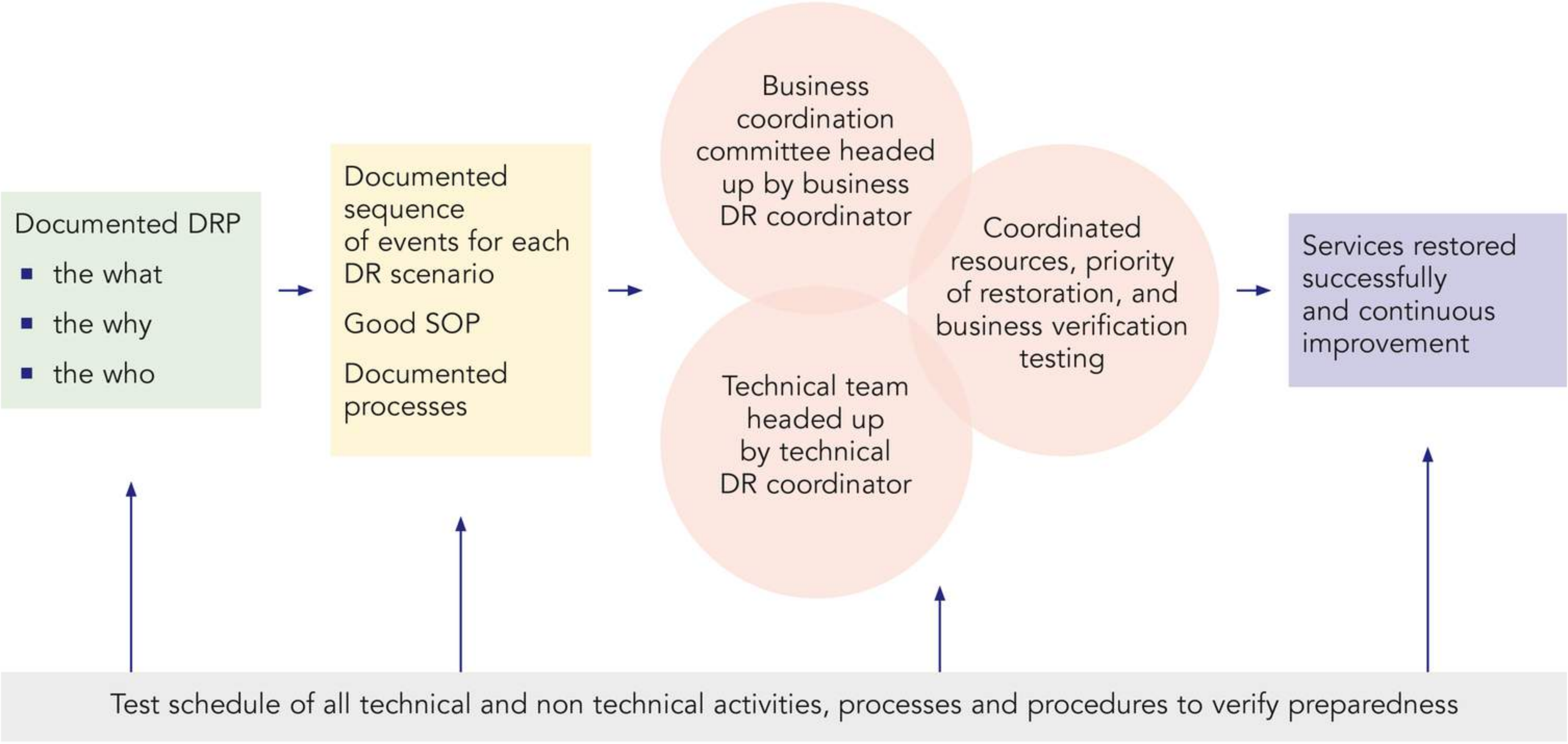

Documented DRP
▪ the what
▪ the why
▪ the who
Documented sequence of events for each DR scenario
Good SOP
Documented processes
Business coordination committee headed up by business DR coordinator
Technical team headed up by technical DR coordinator
Coordinated resources, priority of restoration, and business verification testing
Services restored successfully and continuous improvement
Test schedule of all technical and non technical activities, processes and procedures to verify preparedness

Figure 2. Disaster Model - Essential Components for Effective DR

Disaster Recovery Planning

WHOSE PROBLEM IS IT TO SOLVE?

The plan must be a collaborative document where business units provide impact analysis to the executive and the executive in turn endorses the priority for restoration of services. For example, if an organisation has several business units, and each unit has several services supported by ICT, the executive must provide ICT with direction on the services to be restored for each business unit in priority order. To then achieve this priority for restoration the plan must provide clear lines of demarcation and the need for close collaboration between the technical response and that needed for the business response. Also remember to have paper copies of it stored in multiple places, including off-site.

The final element in setting the scene for improving the organisation's maturity for disaster recovery planning is the need to understand it is not set and forget. The disaster recovery planning process is a living process where the components of planning are revisited and improved in a cyclic fashion. Figure 3 below identifies seven steps in the continuous improvement cycle for disaster recovery planning.

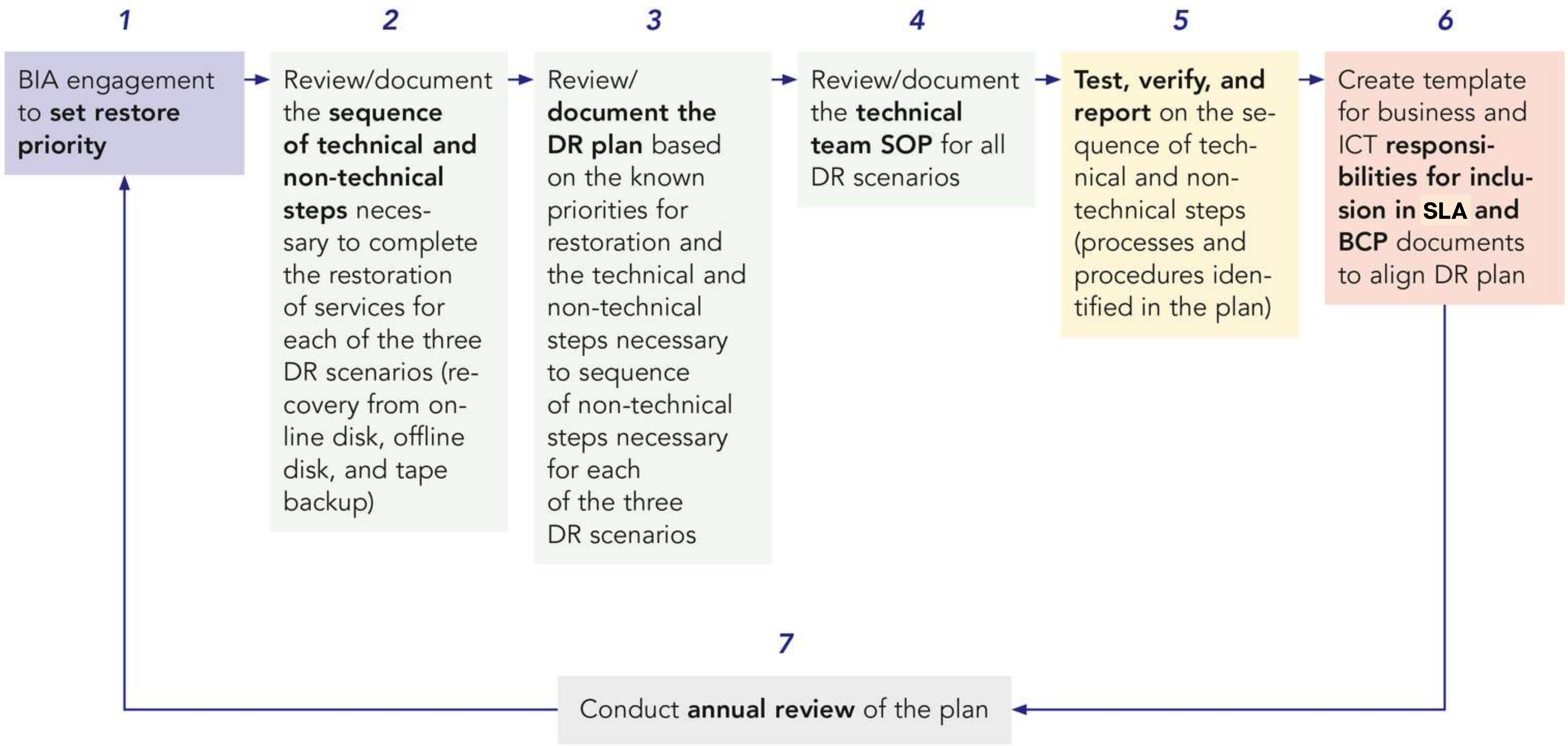

1
BIA engagement to **set restore priority**
2
Review/document the **sequence of technical and non-technical steps** necessary to complete the restoration of services for each of the three DR scenarios (recovery from online disk, offline disk, and tape backup)
3
Review/ **document the DR plan** based on the known priorities for restoration and the technical and non-technical steps necessary to sequence of non-technical steps necessary for each of the three DR scenarios
4
Review/document the **technical team SOP** for all DR scenarios
5
Test, verify, and report on the sequence of technical and non-technical steps (processes and procedures identified in the plan)
6
Create template for business and ICT **responsibilities for inclusion in SLA and BCP** documents to align DR plan
7
Conduct **annual review** of the plan

Figure 3. Roadmap for Implementation of DR Maturity Improvements

Disaster Recovery Planning

WHOSE PROBLEM IS IT TO SOLVE?

NEXT STEPS

CONVENE

Convene a workshop to discuss your current maturity level against the CMMi Model with ICT teams.

CONDUCT

Conduct a roundtable discussion with business leaders to clarify the risk exposure and the need for improvements in the maturity level in DRP.

DEVELOP

Develop an action plan to improve your DRP maturity.

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

Conclusion

The need to have a DR plan that is understood, agreed, and jointly owned by all elements of the organisation is essential in preparing for a disaster event. An effective DR plan will focus on managing the risk associated with completing a successful restoration and recovery in a time, and to a level of effectiveness, acceptable to business.

To ensure the plan is effective at mitigating the risks associated with completion of restoration and resumption of services after a disaster event; the DR plan must also clearly identify how the plan is to be verified and therefore reduce the risk of not completing a successful disaster recovery.

The key focus of the DR plan must always be about the restoring delivery of business functions. The technical delivery may be from ICT services on-premise, outsourced providers, or Cloud. Regardless of technical delivery to business, the impact of an ICT disaster event needs a verified plan!

Observations

With the push toward the use of Cloud offerings, some organisations may consider (wrongly in the opinion of the writer) that DR planning is the responsibility of the Cloud service provider (CSP). In many respects this architecture enhances the need for a good DR plan that is jointly developed by both ICT and business. *It's all about the business*, and only the business will understand the priorities for restoration, and only the business will be able to coordinate the impact to services should a disaster eventuate. Automated DR processes will not cover every aspect of the ICT platform, and the CSP(s), if involved, will need clear direction on priorities for restoration of services. Therefore, the need for coordination of the response to the disaster will remain necessary – which is a key outcome of any DR plan.

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

Many organisations mistake the need for effective standard operating procedure, automation of recovery toolsets and documented recovery procedures as central to an effective DR plan. Whilst important, the true central component of the DR plan is to ensure clarity on how the resolution of any disaster will be coordinated, both from a business and an ICT perspective, and to provide a clear understanding of restoration priorities.

The first chapter in this series provided a diagram that described how to mature your DR capability. The first three steps in the DR maturity improvement model, step 1 – engaging with business units to set the priority for restoration, step 2 – documenting the sequence of technical and non-technical steps necessary to complete the recovery, and step 3 – documenting the plan; are the basis of effective planning for DR.

The **first step** of business impact analysis (BIA) is a must-do. ICT should not assume to know the business priorities for restoration.

However, before your organisation starts the journey in developing a DR plan, it is important to define the disaster recovery scenarios that the plan will address. A minimum of two scenarios should be developed. The final number of scenarios will depend on the architecture in use.

IBRS recommends a strawman workflow diagram for each scenario be documented detailing the high level steps for the technical and non-technical workflow (processes) for each scenario. The strawman workflows will assist in the workshops for developing the BIA step 1, as well as step 2 and 3.

Possible recovery scenarios are:

- Recovery from online disk storage
- Recovery from offline disk storage
- Recovery from tape, and/or
- Recovery in a hybrid or multi-Cloud environment.

CHAPTER 2

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

The development of the organisation's BIA can take many forms. IBRS recommends that the approach taken embraces the following three elements as a minimum:

- Workshops with individual business units to establish a business unit point of contact should a disaster event occur, and to clearly identify the impact and priority for restoration when a disaster event occurs.
- Conduct of an analysis across all business unit priorities to identify an organisation-wide view of the risks associated with priority for restoration against:
  - Point of restoration (potential impact of lost data or staged restoration of full data point)
  - Estimated time to restore
  - Impact on reputation (impact on clients and customers)
  - Impact on productivity (impact on staff resourcing and revenue).
- Workshop with business executives and business unit points of contact to agree on an organisation wide priority for restoration.

The **second step** is to improve the initial strawman workflows to understand and document the sequence of actions that need to be undertaken to manage both the technical and non-technical elements of the restoration and recovery processes. The development of understanding of technical and non-technical processes will assist in developing a joint ownership of business and ICT in the plan being developed. It will also assist in understanding the impact a disaster will have on business and the potential time needed to effect the recovery of services.

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

The **third step** is then to document the plan, and gain sign-off from the executive and business units (including ICT). The DR plan should be seen as a key component of the document framework supporting the DR process. The plan should be an overarching document, rather than focusing on technical procedures. The plan will be supported by the BIA, the technical SOP's, automation tools to enable restoration, the DR test plan to verify the plan, and the test scripts for acceptance of services after the DR is activated.

In broad terms the DR plan should include the following:

- Purpose statement
- Description of DR scenarios being addressed
- Roles and responsibilities of the DR business coordination body (team), and the DR technical coordination unit(s)
- DR internal and external interdependencies (BIA, support contracts, outsourced services, etc)
- Validation test schedule
- Workflow for implementation of recovery for each identified scenario (both technical and non-technical)
- Detail on the restoration objective and the estimated time for recovery against each scenario
- Location of key supporting documents such as technical standard operating procedures (SOP's) and automation tools and procedures.

CHAPTER 2

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

Every DR plan will be unique to the organisation it is intended to support. IBRS recommends the DR plan should look to address the following six stages of the recovery:

- **Preparedness**: detailing the DR scenario procedures and processes test requirements to verify the plan has a high degree of probability for success.
- **Triage and Activation**: detailing the ICT technical teams' processes in identifying a fatal situation has occurred and recommends the scenario in which the DR is activated to the lead business DR coordinator.
- **Coordination and Authorisation**: identification of the DR business and DR technical coordination teams and their responsibilities.
- **Restoration**: the technical and non-technical processes to complete the recovery of all services for each scenario.
- **Verification**: business unit responsibilities to test the restored service and the criteria by which it is deemed fit to be placed back into production status.
- **Assessment**: requirement to collate lessons learned to identify improvements to the DR process.

Last but not least, IBRS considers it useful to maintain paper copies or offline media containing the BIA, DR plan, technical SOP's, and key information such as passwords and activation codes in a safe and secure location, yet still accessible during an emergency by key personnel.

CHAPTER 2

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

NEXT STEPS

ASSESS

Assess the disaster scenarios possible considering the architecture of your ICT environment.

DEVELOP

Develop workflows for ICT and business on the steps from disaster to recovery for each scenario.

CONVENE

Convene a workshop(s) with business units to discuss impact on business should a disaster occur and the priority to restore and time parameters against each application/service used by each business unit.

CHAPTER 2

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR PLAN

NEXT STEPS

CONDUCT

Conduct a roundtable discussion with business leaders to clarify the corporate priorities for restoration.

DEVELOP

Develop a DR plan for review, comment and agreement by business units and the executive.

DEVELOP

Develop a test plan to verify the DR plan can successfully complete recovery of services.

CHAPTER 3

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

Conclusion

Chapter three looks at how the DR plan can be verified. The DR plan is, in effect, a contingency plan to deal with the risk of a disaster. The DR test plan is a validation of the preparedness of the organisation to address these risks.

The need to have a DR plan verified is therefore essential if the contingency is to be effective. Just having a plan in place is not enough to mitigate the risk. The plan must be tested and verified as part of business as usual (BAU) to both increase familiarity with the plan, its SOP's and processes, and most importantly, improve the likelihood of success.

Observations

In many respects the DR test plan is the key to effective DRP. The focus of the test plan is to address the probability of success in mitigating the risks identified to the business should a DR be necessary. The most common risks associated with a disaster, and therefore the core the test plan must address, are as follows:

- Slow response to a disaster recovery event – recovery time objective (RTO) not achieved.
- Business priorities for restoration in a DR are incorrect – recovery priority objective (RPO) not achieved.
- Management and coordination of the DR plan causes unnecessary delay or confusion.
- Processes for restoration and recovery of services are missing or not followed correctly.
- Business units (including ICT) are unaware of their responsibilities in a disaster scenario.

CHAPTER 3

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

The test plan and its supporting schedule must therefore allow the organisation to action four key outputs, these being:

1. Verification of DR plan and processes against DR scenarios and restoration priorities for each scenario to the ICT steering committee (or equivalent).
2. Verification of risk mitigation against fatal failure scenarios to the organisation's risk and audit committee (or equivalent).
3. Familiarisation of ICT and business units with the DR plan and processes, to improve preparedness.
4. Identification of areas for improvement of the DR plan, and processes to improve maturity in the DRP process.

To achieve these outcomes, the test plan must address much more than just the technology aspects of a DR. The plan must cover:

- Governance of testing to provide the executive visibility and awareness of the organisations DR capability and preparedness.
- Testing of both the business and ICT coordination in a DR scenario.
- Testing to ensure the ICT architecture is fit for purpose.
- Testing of the technical and business processes necessary to recover from a disaster.

CHAPTER 3

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

The development of the test plan will require a collaborative approach to achieve these requirements. Through a collaborative process such as workshops, or working with multidisciplinary teams, organisations should seek to identify and document how to:

- Make the test plan responsive and integral to the existing ICT governance, and existing risk and audit oversight processes.
- Develop DR exercises and desk audits to test the effectiveness of management and coordination, of both business and technical resources, during a disaster event.
- Identify elements of each DR scenario workflow that can be tested using existing BAU tasks (for example, patching of software and restart of virtual machines would prove the ability to bring virtual machines online).
- Identify those elements of the DR scenario workflows that will require dedicated resources and potentially invasive testing which will need to be tightly scheduled, and which may require an outage of services.
- Develop methods to capture test data which allows effective reporting.

It may not be practical for an organisation to fully test a DR scenario as a single test event such as a full failover. Most organisations must therefore approach the testing of DR as a series of scheduled activities to simulate every action that will need to be completed. The test plan schedule is conducted over a set timeframe, within a framework, where the schedule of testing provides the necessary feedback and advice to the organisation.

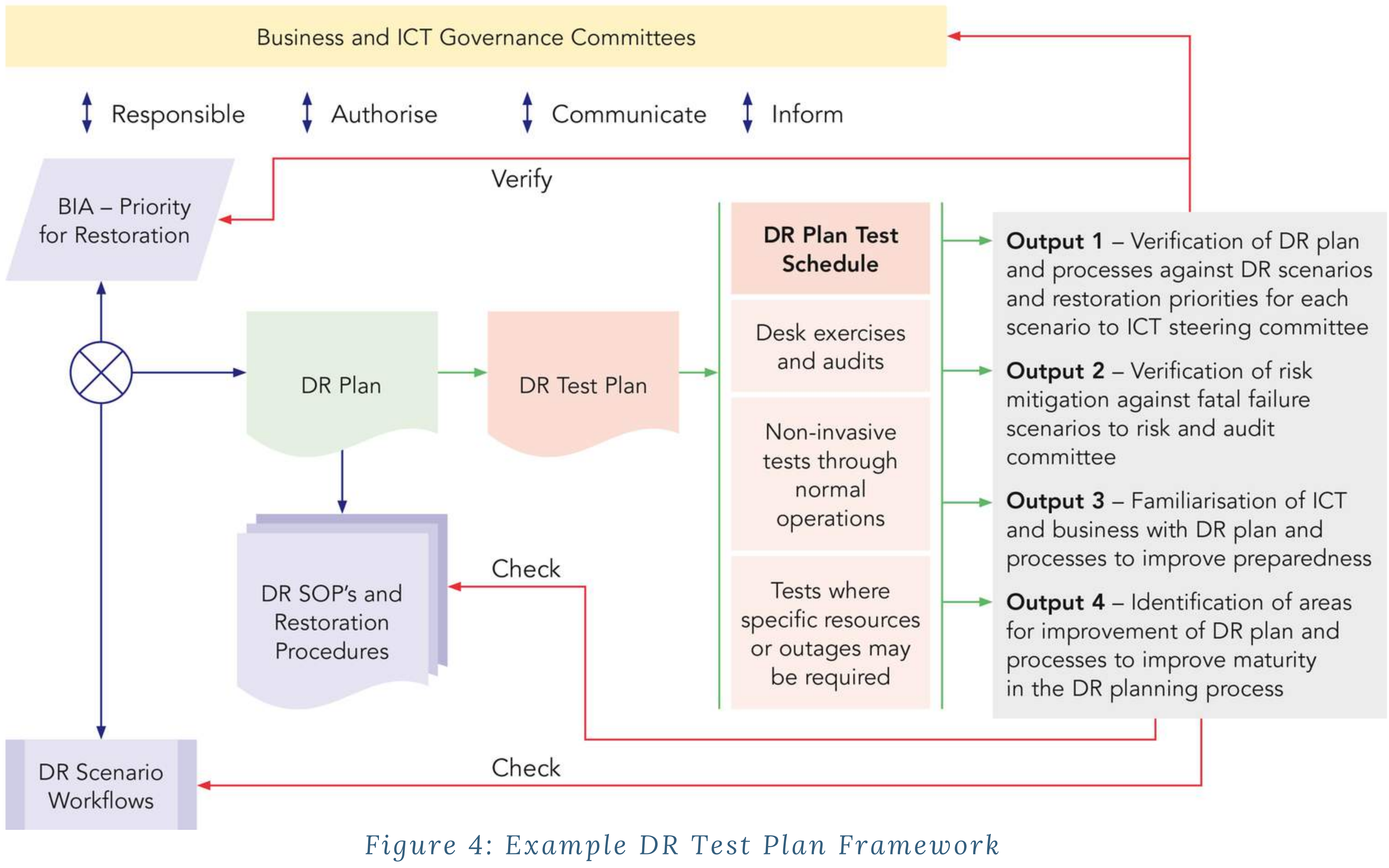
A framework of the DR test plan schedule must represent how each component of the DRP process is linked to meet the business needs. The verification of the DR plan and the test plan are the key aspects of the framework, which allows for the business to verify preparedness and increase awareness of the DR plan as a mitigation strategy against known risks to the business.

CHAPTER 3

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

Mapping of the test plan to the documented DR plan, SOPs and documented processes against the known business priorities will allow effective governance and ensure mitigation against the known risks are monitored. An example test plan framework is depicted in the figure below (Figure 4: Example DR Test Plan Framework):


Business and ICT Governance Committees
Responsible
Authorise
Communicate
Inform
Verify
BIA – Priority for Restoration
DR Plan
DR Test Plan
DR SOP's and Restoration Procedures
Check
Check
DR Scenario Workflows
DR Plan Test Schedule
Desk exercises and audits
Non-invasive tests through normal operations
Tests where specific resources or outages may be required

Output 1 – Verification of DR plan and processes against DR scenarios and restoration priorities for each scenario to ICT steering committee

Output 2 – Verification of risk mitigation against fatal failure scenarios to risk and audit committee

Output 3 – Familiarisation of ICT and business with DR plan and processes to improve preparedness

Output 4 – Identification of areas for improvement of DR plan and processes to improve maturity in the DR planning process

Figure 4: Example DR Test Plan Framework

The DR test plan should contain the following elements:

- Governance over the progress of testing to verify preparedness.
- Schedule of tests against each scenario and test type (exercise, non-invasive, and invasive).
- Method(s) for capture of test data and reporting of testing against time based milestones.
- Processes for identification and reporting on weaknesses and necessary improvements.
- Independent audit of the testing processes and outcomes.

CHAPTER 3

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

Many of the organisation's daily routine tasks will prove the processes needed for DR. However, many of the steps in the plan will either need a managed outage or a staged exercise to verify function and preparedness.

The structure of your test schedule should follow the workflow of each DR scenario. Some elements, such as the business and technical management, coordination of the recovery, and the call-out and contact procedures will be common for each scenario, as will many of the restoration steps.

There are therefore three levels of testing the DR test plan should consider:

- Desk exercises and audits needed to manage the response to a disaster scenario and to implement a disaster recovery.
- Non-invasive testing, such as noting the steps in the recovery process completed using existing BAU functions.
- Invasive testing, where BAU processes are unable to replicate the DR scenario workflows and there is a need to design and schedule tests. Although it may be possible not to impact the production platform, and therefore require an outage, these tests will need dedicated resources to conduct the test(s).

The test schedule should be progressed over a 6–12 month timeline, with regular milestones (monthly or quarterly) designed to inform governance bodies and management groups on viability of the plan and improvements where needed.

The outputs of each test must be captured to allow for reporting and analysis. Effective capture of the test data will allow for constructive analysis of the tests and will support accurate and timely reporting and feedback for improvement.

Last, but not least, the need to verify the test data against the restoration priorities (RTO, and RPO), the ICT infrastructure, and linkages to BCP processes will be critical in the identification of weaknesses or omissions in the DR plan itself.

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

NEXT STEPS

ASSESS

Assess the disaster recovery scenarios to determine the elements of both technology and business that should form the body of the test plan.

IDENTIFY

Identify the approach to include the executive and the organisations’ governance bodies on the viability and preparedness of the organisations’ DRP process.

CONSTRUCT

Construct the schedule of tests across two lenses detailing:

- The elements of the test plan common to the DR across each DR scenario.
- The elements of the test plan that are required to be exercise based, those that can be captured through non-invasive routine tasks, and those that require invasive testing using either dedicated resources and environment and/or require an outage of services.

CHAPTER 3

Disaster Recovery Planning

HOW TO DEVELOP AN EFFECTIVE DR TEST PLAN

NEXT STEPS

DEVELOP

Develop a test plan and schedule to verify the DR plan can successfully complete recovery of services.

IDENTIFY

Identify those elements that require to be incorporated into standard processes to allow for continuous improvement and ultimately improve the organisation’s DR maturity.

Disaster Recovery Planning

IMPROVING DR MATURITY

Conclusion

Chapter 4 looks at how to improve the DRP maturity of your organisation. The focus of improving maturity in DRP is to improve your probability of successfully meeting the needs of your business in the event of a disaster. Ensuring your DR plan and BCP are fully integrated and that all elements of the organisation have a high degree of familiarity with DR processes.

Importantly, your organisation must understand that maturity is both a journey and a target. To maintain the target maturity, your organisation must put in place a number of strategies that will be continually repeated to ensure the target is both met and maintained.

Observations

Chapter 1 introduced the concept of a DR capability maturity model, which rated an organisation's maturity for recovery likelihood to recovery preparedness rating, from ad-hoc maturity through to resilient. The focus of the maturity model is to minimise *unknowns* and increasing probability of successful recovery. (See "Figure 1. Disaster Recovery - Capability Maturity Model" in Chapter 1)

There are four key strategies needed to increase and maintain a high level of maturity. These are:

- Effective Governance: of DRP(s) and BCP(s).
- Regular Review: of DRP to continuously improve the plan.
- Repeatable Testing Schedule: of the DR plan to both test the components of the DRP and to increase familiarity of the recovery processes for both ICT (in-house and outsourced) and business personnel.
- Evaluation of Architecture: to both reduce complexity and reduce risks associated with recovery in a disaster scenario.

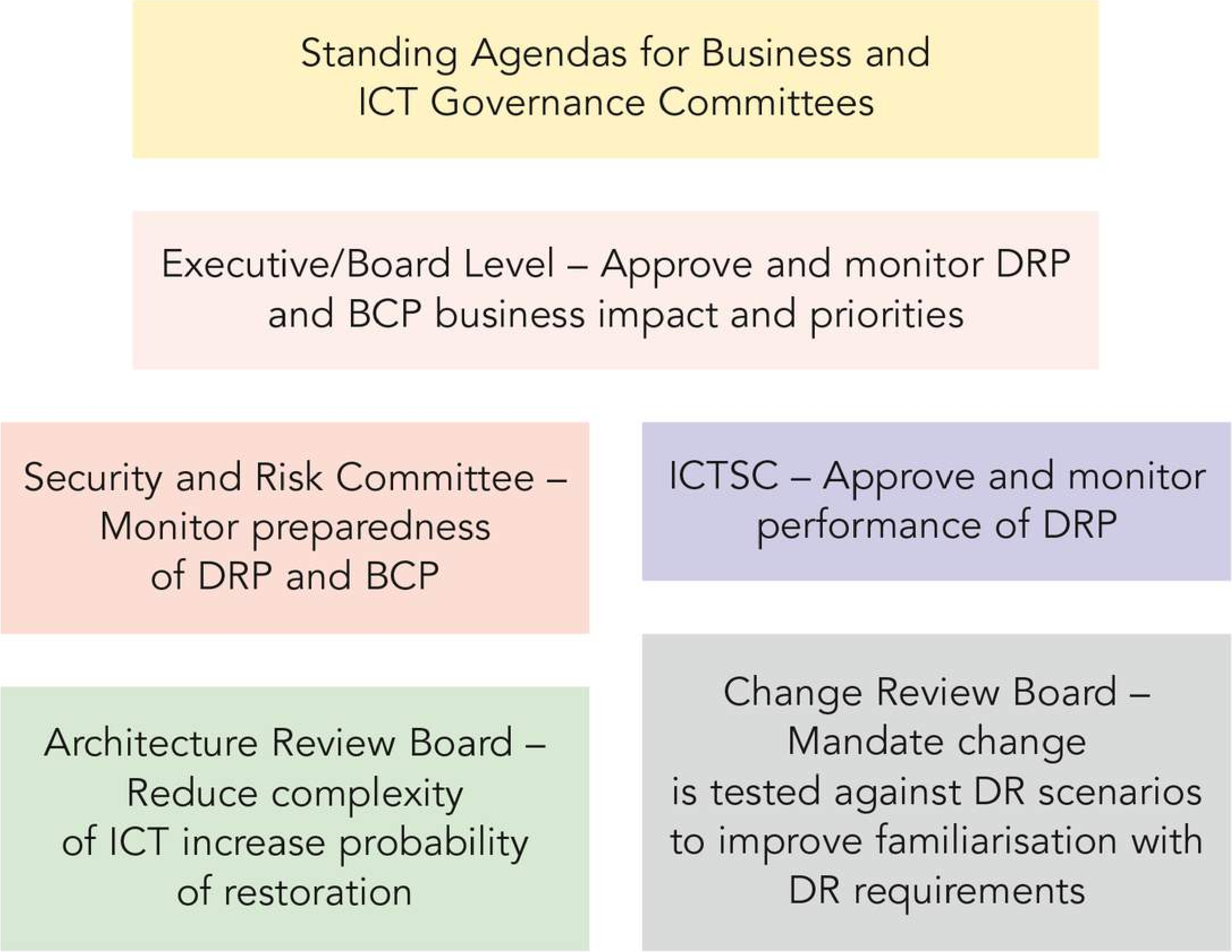
CHAPTER 4

Disaster Recovery Planning

IMPROVING DR MATURITY

Effective Governance:

The key governance bodies that oversee DR planning maturity are the executive board, security and risk committees, ICT steering (or strategy) committee, architecture review boards, and change review boards.



Standing Agendas for Business and ICT Governance Committees

Executive/Board Level – Approve and monitor DRP and BCP business impact and priorities

Security and Risk Committee – Monitor preparedness of DRP and BCP

ICTSC – Approve and monitor performance of DRP

Architecture Review Board – Reduce complexity of ICT increase probability of restoration

Change Review Board – Mandate change is tested against DR scenarios to improve familiarisation with DR requirements

Figure 5: Suggested Agenda Items for Governance Bodies

Figure 5 above recommends standing agenda items for higher level governance bodies, say quarterly, and for lower level governance bodies, for every agenda. The effect of standing agenda items will increase the visibility of DR planning, and improve maturity levels by ensuring the need to align business and ICT for DRP is front of mind. The impact of the mapping of agenda items for each level of governance will improve maturity in DRP, reduce overall risk, improve awareness of the processes for staff, and significantly improve support needed to increase the probability of a successful recovery.

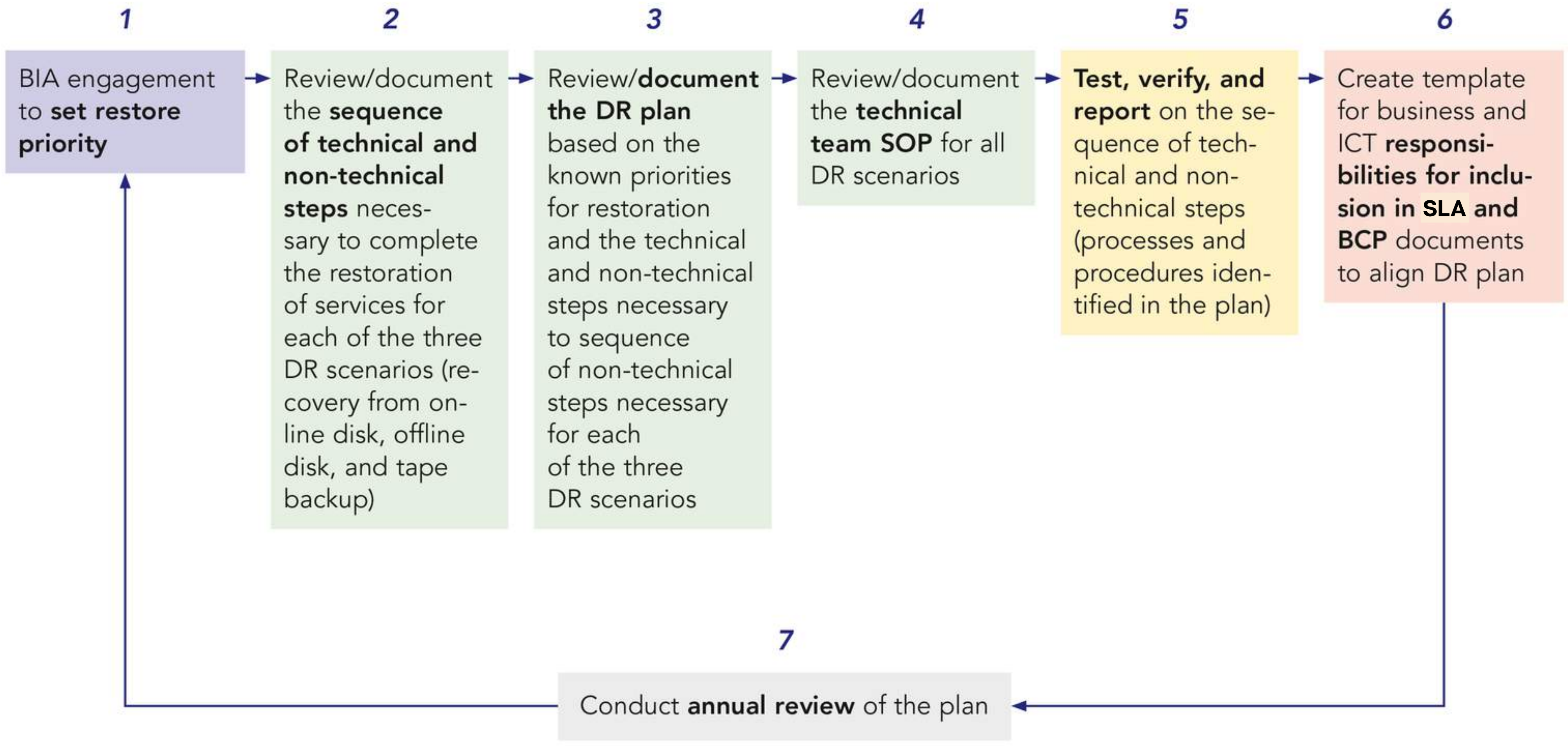
CHAPTER 4

Disaster Recovery Planning

IMPROVING DR MATURITY

Regular Review of DRP:

Where the DRP process imbeds continuous improvement in its processes, the ability to improve maturity by default will be the result. The first advisory in this series recommended the use of a series of steps which would allow for the DRP process to inbuild a continuous improvement cycle. The seven step approach to the DRP process will ensure your organisation uses the governance of ICT and business to monitor the outcomes, and allows for the annual review of the plan to ensure changes in business priorities, changes implemented to improve performance, updates in architecture to reduce complexity, and lessons learned from testing are incorporated to improve the plan and in doing so the maturity of the organisation.



1 BIA engagement to **set restore priority**

2 Review/document the **sequence of technical and non-technical steps** necessary to complete the restoration of services for each of the three DR scenarios (recovery from online disk, offline disk, and tape backup)

3 Review/**document the DR plan** based on the known priorities for restoration and the technical and non-technical steps necessary to sequence of non-technical steps necessary for each of the three DR scenarios

4 Review/document the **technical team SOP** for all DR scenarios

5 **Test, verify, and report** on the sequence of technical and non-technical steps (processes and procedures identified in the plan)

6 Create template for business and ICT **responsibilities for inclusion in SLA and BCP** documents to align DR plan

7 Conduct **annual review** of the plan

Figure 6: DR Continuous Improvement Cycle

CHAPTER 4

Disaster Recovery Planning

IMPROVING DR MATURITY

Repeatable Testing Schedule:

Most organisations are sufficiently complex that their ability to test DR in a single failover event is simply not possible. The need therefore to align a regular repeatable test schedule that encompasses all aspects of the DR plan is necessary.

Figure 4 (in chapter 3) depicts the DR test plan framework recommended in the third advisory of this series. In implementing this framework organisations will enhance the maturity of the organisation in two key ways. First it will allow the organisation to identify issues in a ‘fail safe’ environment. Second, it will ensure the greatest number of staff and service providers are exposed to the DR plan and how DR processes are to be implemented.

Evaluation of Architecture:

The fourth strategy to improve DR maturity in your organisation is to establish effective enterprise architecture (EA) practices. The focus of EA is to ensure ICT alignment to deliver business critical functions. In doing so it should allow for pattern control and configuration management that simplifies the delivery of services, as much as is possible. Effective EA will reduce complexity, cost and risk in delivery of ICT services for the business. Part of the EA value proposition is to analyse the DR plan and its testing regime, to provide the organisation’s executive with an independent view on the performance of the plan, and how it can be improved from an architectural perspective.

CHAPTER 4

Disaster Recovery Planning

IMPROVING DR MATURITY

In Summary:

This ebook on DRP has been a journey from understanding your organisation’s maturity, to the development of the DR plan, the validation of the plan, and how to establish strategies to ensure continuous improvement. The resultant improvement in your organisations DR maturity will reduce risk, and result in a higher probability of success in recovering services when a disaster eventuates. It will also greatly improve ICT’s understanding of the business priorities for your organisation, and business understanding of the value and capability of its ICT environment.

Disaster Recovery Planning

IMPROVING DR MATURITY

NEXT STEPS

MAP

Map existing governance processes and ensure standing agenda items are in place to ensure executive visibility of DRP.

ANALYSE

Analyse the current DRP processes to ensure a continuous improvement cycle is inbuilt.

ENSURE

Ensure DR testing processes provide feedback to the executive, and provide staff and service providers with familiarity and awareness of the DR processes.

Disaster Recovery Planning

IMPROVING DR MATURITY

NEXT STEPS

TASK

Task EA with the role of independent review of the DRP to ensure complexity and risks of an unsuccessful recovery are minimised.

COMPLETE

Complete an annual review of the plan to ensure all learnings, both business and ICT, are incorporated into future planning.

About

IBRS

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.

Submit an inquiry or schedule a whiteboard session

Save Time | Save Money | Mitigate Risk | In-Context Advice | Skills Development | Personal Touch

IBRS | ANALYSIS INSIGHT JUDGEMENT