

IT Disaster Recovery Guide

for the Financial Industry in Singapore



December 2025



Contents

1. Background	3
2. Best Practices Recommendations	3
2.1. Framework Structure	3
2.2. Disaster Scenarios	4
2.3. Business Impact Assessment and Effective Risk Management	4
2.4. Risk Treatment	6
2.5. Validation of Plan	6
2.6. Continuous Improvement	7
3. Acknowledgement	8

1. Background

- 1.1 Financial Institutions (“FIs”) in Singapore have rapidly adopted technologies such as cloud computing, artificial intelligence, and blockchain to enhance operational efficiency and drive innovation.
- 1.2 This digital shift has introduced increased complexity and risk, raising the importance of technology resilience to safeguard critical assets and customer data.
- 1.3 With disruptions from cyber-attacks and system failures becoming more prevalent, robust IT Disaster Recovery (DR) capabilities are essential to ensure timely restoration of critical services.
- 1.4 A joint working group comprising representatives from the ABS Standing Committee on Technology Risk and Resiliency (SCTRR) was formed. This guide reflects the group’s collective effort to share DR best practices from and for the industry.
- 1.5 This guide provides recommendations to help FIs strengthen DR strategies. It underscores the importance of minimising downtime and data loss, maintaining stakeholder confidence, and regularly reviewing and updating DR plans to address outdated procedures, evolving threats, and new system dependencies.

2. Best Practices Recommendations

2.1 Framework for DR

FIs should establish a comprehensive DR framework comprising strategy, policies, standards, and procedures (“documents”) that is commensurate with the FIs’s size, complexity, and operations. These documents should be clearly communicated to all relevant stakeholders, regularly reviewed, tested, and updated to ensure continued effectiveness.

- 2.1.1 The DR framework should begin with the identification of potential disaster scenarios that could impact the FIs’s operations.
- 2.1.2 FIs should conduct thorough risk assessments and Business Impact Assessments (BIA) for each identified scenario, evaluating potential impact, likelihood, vulnerabilities, and prioritising based on criticality.
- 2.1.3 FIs’s should define and document DR strategies for each scenario, including recovery and mitigation plans that align with business requirements and risk appetite. These strategies should clearly define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- 2.1.4 The DR plan should be validated through comprehensive testing to ensure the effectiveness of response and recovery processes. Validation exercises should confirm that RTOs and RPOs are achievable and that recovery procedures are executable under real-world conditions.
- 2.1.5 FIs should implement a process for continuous improvement, including regular reviews of DR plans to address changes in the operating environment, emerging threats, and new system dependencies. Lessons learned from incidents and testing should be incorporated into the DR framework to enhance resilience.

2.2 Disaster Scenarios

FIs should establish a structured process to identify and maintain a comprehensive inventory of potential disaster scenarios that may impact critical IT services. This includes scenarios such as infrastructure failures, cybersecurity incidents, software malfunctions, and third-party service disruptions.

Common disaster scenarios include:

- 2.2.1 Infrastructure – Data Centre Failure: This refers to the unavailability of an entire data centre hosting critical systems, leading to service outages. Causes may include loss of power or cooling resulting in hardware failure, restricted access to the data centre, or catastrophic events such as fire, flood, power grid failure, or structural damage. Failures in Infrastructure as a Service (IaaS) environment, such as public cloud platforms, are also included.
- 2.2.2 Infrastructure – Hardware Failure: These are component-level failures that affect compute, storage, or network infrastructure. Failures may also occur in Platform as a Service (PaaS) environment hosted on public cloud platforms.
- 2.2.3 Cybersecurity Incidents: These involve threats that compromise applications or infrastructure, resulting in service outages or data breaches. Examples include cyber-attacks that disrupt services, ransomware attacks involving data theft or malware deployment, and zero-day malware affecting end-user devices.
- 2.2.4 Software Failures: These occur when software updates or configuration changes corrupt applications across High Availability (HA) environments. This may include failures in virtualisation platforms, cross-site cluster breakdowns, or major application releases that result in system-wide outages or data corruption.
- 2.2.5 Third-Party Service Outages / Connectivity Failures: These disruptions are caused by failures in services provided by external vendors or connectivity issues with third-party service centres. Scenarios include CDN (Content Delivery Network) failures, cloud Web Application Firewall (WAF) outages, telco disruptions, change failures at third-party providers, cybersecurity incidents at vendor sites, and issues with Software as a Service (SaaS) platform.

The scenarios provided above are non-exhaustive, and FIs should regularly review and include other relevant scenarios to ensure their DR plans remain comprehensive and effective.

2.3 Business Impact Assessment and Effective Risk Management

FIs should conduct structured reviews aligned with their Business Impact Analysis (BIA) and Incident/Crisis Management Frameworks to ensure that disaster recovery (DR) planning is comprehensive and risk informed. These reviews should include evaluating the potential impact of disruptions on critical business services and functions through the Business Impact Assessment, identifying and assessing risks associated with IT systems, applications, and dependencies via Risk Assessment, and prioritising recovery efforts by ranking them based on business criticality and risk exposure.

The following principles support effective IT DR planning:

- 2.3.1 Critical Services and Dependencies: Identify Critical Business Services (CBS) and Critical Business Functions (CBF) and map dependencies, including IT systems, applications, infrastructure, and third-party services, to establish a clear link between Business Continuity Planning (BCP) and IT DR.
- 2.3.2 Impact Assessment: Assess the upstream and downstream dependencies of technology assets across the end-to-end service journey and consider the interconnectedness of systems and their role in service delivery.
- 2.3.3 Review and Validation: Periodically review and revalidate the process to ensure it reflects current operational realities, technology changes, and emerging threats.
- 2.3.4 Recovery Strategy Alignment: Ensure that BCP and DR plans prioritise recovery based on the outcomes of the impact and risk assessment and focus on minimising downtime and maintaining service continuity.
- 2.3.5 Internal and External Factors: Impact assessments should account for regulatory requirements, real-time incident learnings, industry best practices and market and geopolitical conditions.
- 2.3.6 Training and Awareness: Regularly train process owners and subject matter experts (SMEs) to ensure clear understanding of their roles and responsibilities and adequate awareness of the DR process and its importance.

Following the assessment process, FIs should derive actionable insights to inform and strengthen their IT DR strategy. The key outcomes include:

- 2.3.7 Recovery Objectives Definition: FIs should take into consideration the potential financial, customer, and regulatory impact of disruptions to define appropriate Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- 2.3.8 Scenario-Based Risk Evaluation: FIs should conduct pre-implementation risk assessments to evaluate the potential impact of various disaster scenarios before finalising DR plans. Post-implementation assessments should also be performed to measure residual risks and validate the effectiveness of implemented recovery strategies.
- 2.3.9 Validation of DR Effectiveness: The level of assurance in DR capabilities depends on the robustness of the validation process. This includes the quality and relevance of test data, the breadth of user participation, the extent of system functionality tested, and the documentation of validation results and findings.
- 2.3.10 Prioritisation and Governance: FIs should clearly define and justify recovery priorities for each system, particularly in scenarios involving multiple concurrent failures. Clear ownership and accountability should be established for invoking DR procedures, managing recovery sequencing, and authorising deviations from predefined priorities based on situational needs.

2.4 Risk Treatment

An effective and well-rehearsed response plan is essential for enabling FIs to promptly detect disruptions, activate recovery procedures, and communicate with stakeholders in a timely and coordinated manner. The response plan should incorporate the following key components:

- 2.4.1 **Failure Detection and Monitoring:** FIs should implement mechanisms to detect and monitor failures across all identified disaster scenarios. Early detection is critical to enable timely response and minimise potential impact.
- 2.4.2 **Stakeholder Escalation Protocols:** A clearly defined escalation framework should be established to ensure prompt notification of relevant stakeholders, including the Major Incident Response Team, Technology teams, and Business Units.
- 2.4.3 **Incident Impact Assessment:** Upon detection of an incident, FIs should conduct a structured impact assessment to determine the severity of the disruption and assess whether DR procedures need to be activated.
- 2.4.4 **Execution of Recovery Procedures:** FIs should be prepared to execute recovery procedures efficiently and in alignment with predefined DR objectives, ensuring that critical services are restored within acceptable timeframes.
- 2.4.5 **Communication and Escalation Planning:** The response plan should clearly define roles and responsibilities for internal and external communications. This includes timely updates to downstream teams, customers, regulators, and strategic partners to maintain transparency and manage stakeholder expectations.

2.5 Validation of plan

Recovery strategies and their corresponding plans should be regularly validated and formally documented, especially after significant changes to system configurations or infrastructure. This ensures they remain relevant, effective, and aligned with business impact assessments. The validation exercise should be supported by a formal report comprising the following components:

- 2.5.1 **Test Documentation:** Clearly define the scope, objectives, success criteria, and results of each test conducted during the validation exercise.
- 2.5.2 **Root Cause Analysis and Gap Identification:** Document any root causes or gaps identified in failed tests to support continuous improvement and refinement of recovery strategies.
- 2.5.3 **Re-testing Protocol:** Failed tests should be re-tested within a predefined timeframe, determined based on the associated risk assessment and business criticality.

FIs may refer to the IT DR Maturity Model (Appendix C) to assess recovery capabilities across individual applications or entire data centres hosting IT services. This model offers a structured and consistent benchmark to evaluate current maturity levels and develop a roadmap for enhancement. Each maturity level may be qualified with exclusions, where applicable, to reflect specific operational or architectural considerations.

2.6 Continuous Improvement

To ensure the continued effectiveness and relevance of IT DR capabilities, FIs should regularly review and enhance their DR strategies, plans, and procedures. This assessment should be conducted at least annually, or more frequently as required, and should encompass the following key activities:

- 2.6.1 Regulatory and Industry Alignment: Incorporate changes in regulatory requirements and industry best practices into the DR framework.
- 2.6.2 Business and Technology Updates: Ensure DR plans reflect evolving business needs and changes in technology architecture or stack.
- 2.6.3 Threat and Risk Evaluation: Continuously identify and assess emerging internal and external threats, vulnerabilities, and risk exposures.
- 2.6.4 Drills and Simulations: Conduct regular exercises simulating one or more disaster scenarios (as outlined in Section 2.2) to validate readiness and reinforce staff familiarity with their roles.
- 2.6.5 Feedback Mechanism: Establish channels to gather insights from personnel involved in recovery efforts, informing future enhancements.
- 2.6.6 Documentation Maintenance: Keep all DR documentation current, including contact lists, recovery procedures, and resource inventories.
- 2.6.7 Training and Awareness: Provide ongoing training to staff on DR procedures and promote awareness of the importance of DR planning.
- 2.6.8 Resource Sufficiency: Ensure adequate personnel, technology, and budgetary resources are allocated to support the DR strategy.
- 2.6.9 Cross Functional Engagement: Involve stakeholders across departments to ensure alignment with business objectives and incorporate diverse perspectives into the planning process.

3. Acknowledgement

This guide is developed by the IT Disaster Recovery working group members from:

Financial Institutions:

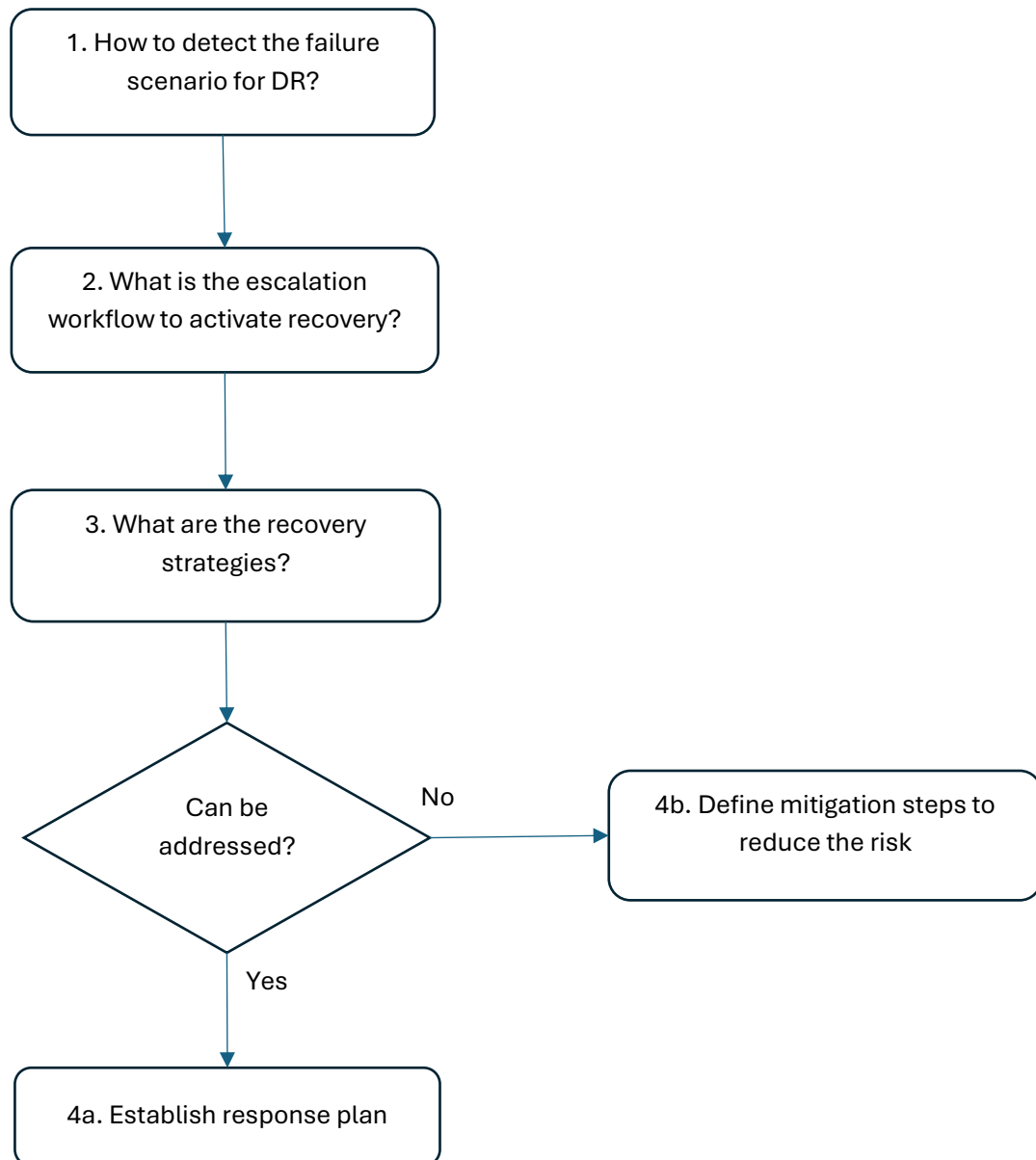
1. DBS Bank Ltd (Working Group Lead)
2. OCBC Bank (Working Group Lead)
3. ANZ (Working Group Lead)
4. Bank of America
5. Citibank
6. HSBC Bank (Singapore) Limited
7. Maybank Singapore Limited
8. MUFG Bank Ltd
9. Standard Chartered Bank (SCB)
10. Sumitomo Mitsui Banking Corporation (SMBC)
11. JP Morgan
12. SGX
13. United Overseas Bank Limited

In addition, the paper was completed with the guidance and support of:

1. ABS Standing Committee on Technology Risk & Resilience (SCTRR)

4. Appendix

Appendix A: High-level Flow and the Recommendation for Risk Treatment



Step	Recommendations
1. How to detect the failure scenario types for DR?	1. Each FI should have Incident Management framework which would cover the detection of failure scenario types.
2. What is the escalation workflow to activate recovery?	<ol style="list-style-type: none"> 1. The authority to invoke DR should be clearly defined. 2. The criteria and process to invoke DR should be clearly defined.
3. What are the recovery strategies?	<ol style="list-style-type: none"> 1. Recovery strategies should be developed to address applicable disaster scenarios. Recovery strategies should address 3 objectives. <ol style="list-style-type: none"> a) Recover the system. b) Recover the data (from data loss or corruption). c) Support the recovery of the CBS that the system is supporting 2. Examples of recovery strategies cover different scenarios but are not limited to the below: <ol style="list-style-type: none"> a) Automated failover to DR site b) Manual failover to DR site c) Recover from backups at Production site with data loss. d) Recover from backups and play back transactions from available logs up to RPO. e) Combination of above 3. Recovery strategies should define cases where no technical recovery is possible and a BCP is required. 4. Recovery strategies should be signed off by management.
4. Establish response/recovery plan	<ol style="list-style-type: none"> 1) Recovery plan for each system should be documented as per recovery strategy for each scenario. 2) Recovery plans should be developed to meet RTO and RPO. 3) Recovery plan should consider requirements such as <ol style="list-style-type: none"> a) Technical recovery steps b) Technical and resource dependency c) Business verification test d) Success criteria e) Roles and responsibilities of the relevant personnel 4) Recovery plan should be signed off by management.

Appendix B: IT DR Maturity Model

Maturity Level	Validation approach for Data Center failure scenario	Outcome
5	<u>Live Flip of DC or applications(s)</u> with short notice <i>(i.e., less than 48 hours)</i>	Ready to handle real DR event/scenario.
4	<u>Live flip of DC</u> in planned window	Ready to run LIVE workload for all IT services from DR env isolating primary data center.
3	<u>Live flip per application(s)</u>	Ready to run LIVE workload from DR env for a period.
2	<u>DR drill (no live transaction)</u>	Ready to execute DR plan meeting RTO and RPO.
1	<u>Tabletop exercise</u>	Understanding of scope and documented plan.

* Maturity level 4 and 5 are assumed to be already isolated from primary data center either physically or logically.

Scenario 1a - Infrastructure - Data Centre failure

Exercise Title	<<Input the title of your exercise>>
Maturity Level	<input type="checkbox"/> Maturity Level 1 <input type="checkbox"/> Maturity Level 2 <input type="checkbox"/> Maturity Level 3 <input type="checkbox"/> Maturity Level 4 <input type="checkbox"/> Maturity Level 5
Exercise Objective, Scope and Approach	<p>The DR validation is done via the below approach</p> <input type="checkbox"/> Tabletop <input type="checkbox"/> DR Drill with no production workload <input type="checkbox"/> Application(s) flip with production workload and run production in alternate site for xx hours or xx days <input type="checkbox"/> Planned full Data Centre failover to alternate site and run production in alternate site for xx hours or xx days <input type="checkbox"/> Recover Data Centre in alternate within short notice or real incident and run production at alternate site for xx hours or xx days <Brief description of scope>
Exercise Outcome	<ol style="list-style-type: none"> 1) xx application(s) met agreed RTO and RPO objective. xx application(s) failed to recover within agreed RTO and RPO. 2) Applications failed over to alternate site and met business owner validation 3) Application(s) run with production workload at alternate site for xx hours or xx days.
Follow Up Actions	<Indicate follow-up actions to address issue(s) encountered during the exercise>

Scenario 1b - Infrastructure - Hardware failure

Exercise Title	<<Input the title of your exercise>>
Maturity Level	<input type="checkbox"/> Maturity Level 1 <input type="checkbox"/> Maturity Level 2 <input type="checkbox"/> Maturity Level 3 <input type="checkbox"/> Maturity Level 4 (Not applicable) <input type="checkbox"/> Maturity Level 5
Exercise Objective, Scope and Approach	<p>The DR validation is done via the below approach (<i>only keep one and remove the rest</i>)</p> <input type="checkbox"/> Tabletop <input type="checkbox"/> DR Drill with no production workload <input type="checkbox"/> Hardware failover via planned exercise and run production workload on redundant hardware <input type="checkbox"/> Recover from hardware failure and run production workload in redundant hardware <Brief description of scope>

Exercise outcome	1) Failover completed in xx hours or xx mins. 2) Production workload failover and run production on redundant hardware.
Follow Up Actions	<Indicate follow-up actions to address issue(s) encountered during the exercise>

Scenario 2 - Cybersecurity Incidents

Exercise Title	<<Input the title of your exercise>>
Maturity Level	<input type="checkbox"/> Maturity Level 1 <input type="checkbox"/> Maturity Level 2 <input type="checkbox"/> Maturity Level 3 <input type="checkbox"/> Maturity Level 4 (Not applicable) <input type="checkbox"/> Maturity Level 5
Exercise Objective, Scope and Approach	<p>The DR validation is done via the below approach (<i>only keep one and remove the rest</i>)</p> <input type="checkbox"/> Tabletop <input type="checkbox"/> Drill is conducted in isolated environment with no production workload <input type="checkbox"/> Planned application(s) recovered with production workload and run production workload <input type="checkbox"/> Recover application(s) within short notice or real security incident and run production workload
Exercise outcome	<p><Brief description of scope></p> <p>1) <i>System restored and</i> met agreed RTO and RPO objective 2) Application services recovered and met business owners' expectations.</p>
Follow Up Actions	<Indicate follow-up actions to address issue(s) encountered during the exercise>

Scenario 3 - Third Party service outage / Connectivity failures

Exercise Title	<<Input the title of your exercise>>
Maturity Level	<input type="checkbox"/> Maturity Level 1 <input type="checkbox"/> Maturity Level 2 <input type="checkbox"/> Maturity Level 3 <input type="checkbox"/> Maturity Level 4 (Not applicable) <input type="checkbox"/> Maturity Level 5
Exercise Objective, Scope and Approach	<p>The DR validation is done via the below approach (<i>only keep one and remove the rest</i>)</p> <input type="checkbox"/> Tabletop with third party vendor <input type="checkbox"/> DR Drill with third party vendor <input type="checkbox"/> Planned third party failover and run production workload <input type="checkbox"/> Recover from third party failure/incident and run production workload
Exercise outcome	<p><Brief description of scope></p>
Follow Up Actions	<Indicate follow-up actions to address issue(s) encountered during the exercise>

Exercise outcome	1) xx application services met agreed RTO and RPO objective after third party failover. 2) Application services recovered and met business owners' expectations.
Follow Up Actions	<Indicate follow-up actions to address issue(s) encountered during the exercise>

Scenario 4 – Software failures

Exercise Title	<<Input the title of your exercise>>
Maturity Level	<input type="checkbox"/> Maturity Level 1 <input type="checkbox"/> Maturity Level 2 <input type="checkbox"/> Maturity Level 3 <input type="checkbox"/> Maturity Level 4 (Not applicable) <input type="checkbox"/> Maturity Level 5
Exercise Objective, Scope and Approach	<p>The DR validation is done via the below approach (<i>only keep one and remove the rest</i>)</p> <input type="checkbox"/> Tabletop <input type="checkbox"/> DR Drill with no production workload <input type="checkbox"/> Planned application(s) recovered with production workload and run production workload <input type="checkbox"/> Recover application(s) within short notice or real software incident and run production workload
	<Brief description of scope>
Exercise outcome	1) <i>System restored and</i> met agreed RTO and RPO objective 2) Application services recovered and met business owners' expectations.
Follow Up Actions	<Indicate follow-up actions to address issue(s) encountered during the exercise>