Why DRP (Disaster Recovery Plan)

1.
INTRODUCTION

DRP – Why & What

CNII – Critical National Information Architecture

Assets (real & virtual), systems & functions that are vital to the nations:

DEVASTATING IMPACT ON INCAPACITY OR DESTRUCTION

- National economic strength.
- ***National image*.**
- National defence and security.
- ***Government capability to function.***
- Public health and safety.

.

Defined by:

CNII SECTORS

- National defense and security.
- ***Banking & Finance.***
- ***Information & Communication.***
- Energy.
- Water.
- Transportation.
- Heath Services.
- ***Government.***
- Emergency Services.
- Food & Agriculture.

TYPE OF BUSINESS CONTINUITY MANAGEMENT

- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Business Resumption Plan (BRP)
- Contigency Planning

Disaster Recovery Plan (DRP)

- To outline key recovery steps during and after disaster till financial system return to normal operation.
  - Guidelines for plan activation and recovery procedures.
  - Technical response flow and recovery strategies.
  - In accordance with BCM, references to Business Resumption Plan and business dependencies.

Disaster Recovery Plan (DRP)

- DRP objectives include:
  - To mobilize core group of leaders to assess the technical ramifications of a situation.
  - Set technical priorities for the recovery team during recovery period.
  - Minimize disruption impact to the business.
  - Stage the restoration of operations to full processing capabilities.
  - Enable rollback operations once the disruption has been resolved.
  - To identify significant dependencies within technical, business and third party group.
  - To ensure the proposed contingency arrangements are cost-effective

DISASTER RECOVERY CENTER (DRC)

Alternative site where organization relocates their IT infrastructure and/or continue business when the main data center is failed to operate due to disaster (flood, fire, earthquake, bomb blast, building collapse etc.)

HOT SITES

- Duplicate the original site organization.
- Real time synchronization between DC and DRC**.**
- Organization can relocate with minimal losses to normal operations in the shortest recovery time.
- Expensive to operate.

.

WARM SITES

- Warm sites will have established hardware and connectivity in a smaller scale than the original production.
- Data is replicates from DC to DRC in defined interval of time.

COLD SITES

- Cold sites provide basic infrastructure but without setting up hardware.
- Backup data depending on external medium backup.
- Least expensive to operate but take longer time in recovery.

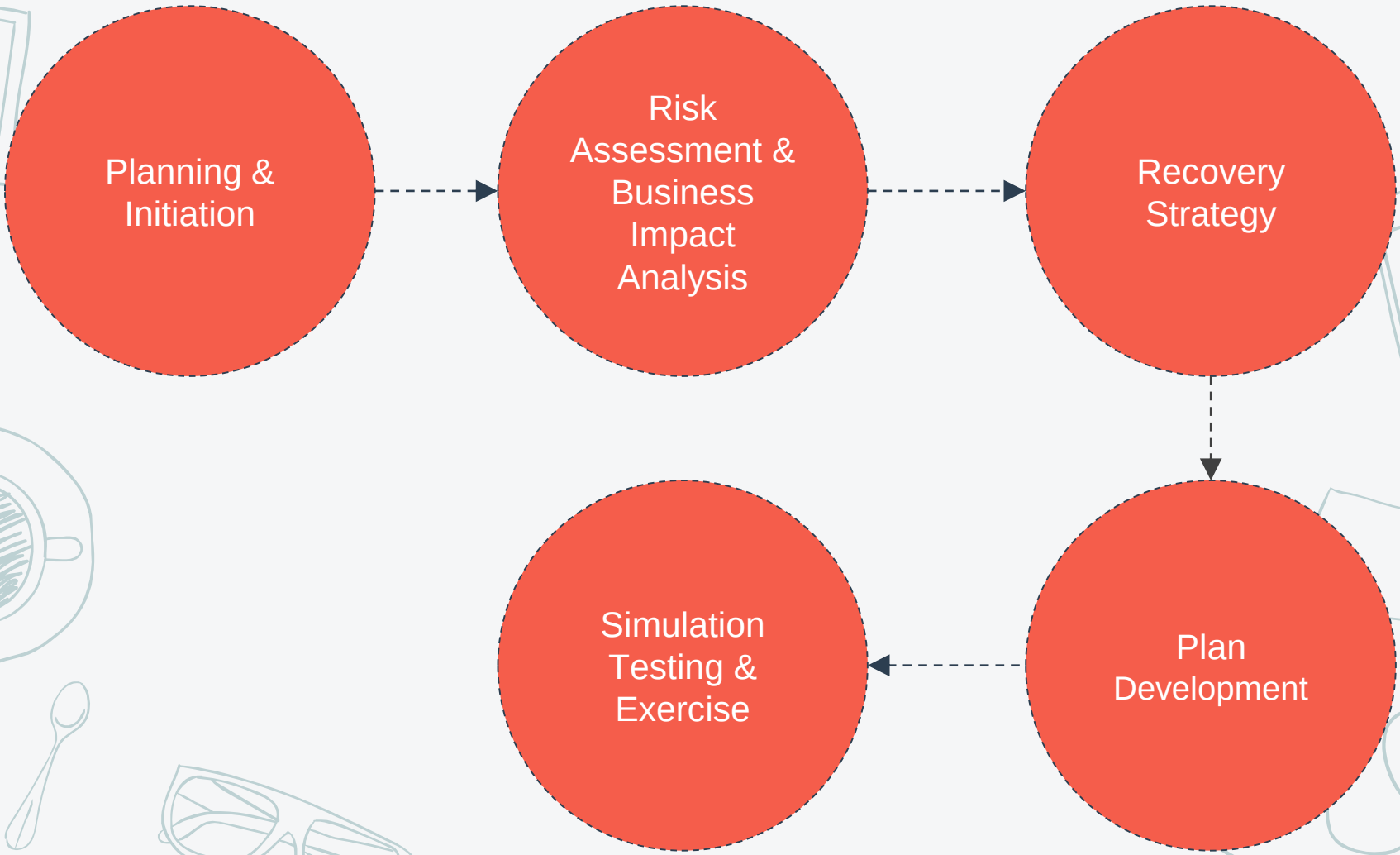
Disaster Recovery Center (DRC)

- Basic guidelines on selecting DRC location:
  - Different power grid.
  - As close as the DR team can easily access and as far as the location is not affected by the same disaster.
  - Cost-benefit analysis.

2. DEVELOPING DRP

DRP Life Cycle

DRP Development



DRP Development

Planning & Initiation

Phase 1: Planning & Initiation

Develop a detailed project management plan facilitating collaborative approach to direct subsequent DRP phases.

DRP Development

Risk Assessment & Business Impact Analysis

Phase 2: Risk Assessment & Business Impact Analysis

Risk Assessment – Identifying the threats, hazards and likelihood which can impact financial system infrastructure.

Business Impact Analysis – Identify disruption impacts and allowable outage time, Maximum Tolerable Time (MTD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Maximum Tolerable Downtime (MTD) – Maximum period of time that a given business process can be inoperative before the organization's survival at risk.

Recovery Point Objective (RPO) – The age of files that must be recovered from backup storage for normal operations to resume as a result of system failure.

Recovery Time Objective – The targeted duration of time and a service level within which a business process must be restored after a disaster.

DRP Development

Recovery Strategy

Phase 3: Recovery Strategy

Establish recovery strategy for financial system.

Recovery strategies include for users, network, servers, application/data and infrastructure.

Altenative site (DRC) selection either Cold, Warm or Hot Site.

Perform Cost-Benefit Analysis where necessary.

DRP Development

DRP
Development

Phase 4: Developing DRP

Documenting the selected strategies and disaster recovery procedures.

Proposed DRP content:

- Document Control.
- Distribution List.
- Version Tracking.
- References.
- Term & Acronyms.
- Internal Contacts.
- External/Third Party Contacts.
- Introduction, purpose of document, objective and scope.
- Disaster Recovery Organization Chart.
- DRP Call Tree
- Strategic Principles & Assumptions
- RTO, RPO & MTD.
- Activation Plan: Activation & Notification Phase, Recovery Phase and Post Disaster Phase.

DRP Development

DRP
Development

Phase 4: Developing DRP

Proposed DRP content:

- List of ICT Hardware & Equipments.
- List of Related Non-ICT Equipments/Infrastructure.
- Backup & Restore Policy.
- Network Diagram (Both DC & DRC).
- DR Organization Structure, Roles & Responsibilities.
- List of systems & sub-systems.
- Related Forms, Checklists & Appendixes.

DRP Development

Simulation Testing & Exercise

Phase 5: DRP Simulation

DRP Simulation Testing must be performed at least once a year.

The resulting financial data/reports from simulation testing must be verified by Account/Finance Department.

In documenting DRP, don’t write a book, write a well-structured and easily understood plan which will help our organization recover as quickly and effectively as possible from an unforseen disaster.

THANK YOU

Muhammad Azhar Fairuzz Hiloh
azhar@anm.gov.my