ISMS EXCERPTS – BUSINESS CONTINUITY MANAGEMENT

aspire SYSTEMS | attention. always.

BUSINESS CONTINUITY

✓ **BCM** is a business-driven process through which the organization manages the impacts to the business continuity of operations due to threats. BCM involves

  ✓ Proactively build resilience in the organization to mitigate the disruptions to the business and to achieve the objectives

  ✓ Provide ability to restore key processes and services within accepted service level agreements

  ✓ Provide mechanisms to safeguard the interests of key stakeholders, organizations reputation, brand and trust due to business disruptions

  ✓ Protection of critical Assets / Information required for Business Continuity

✓ Refer Aspire-Business Continuity & Disaster Recovery Management-Procedure and BCM framework for more details

BUSINESS IMPACT ANALYSIS (BIA)

✓ The organization shall identify the impact of disruptions of its services in the order of importance for all the projects using Business impact analysis activity

✓ The parameters considered for the same is as below :

✓ Contractual Obligation

✓ Regulatory Liability

✓ Financial Loss

✓ Confidential

✓ Company Reputation

✓ Customer Confidence

✓ Project Delivery for the Month

Maximum Tolerance Period Disruption (Downtime):

✓ During the time of BCP invocation, this parameter will be used to prioritize the recovery process. This value is a combination of downtime and the criticality of the downtime.

3

BUSINESS IMPACT ANALYSIS

Recovery point objective

- ✓ This is the acceptable loss of information for a project in terms of hours of work. This value will determine the backup

    frequency for the project.

Consider the following examples to calculate RPO:

- ✓ If the default incremental backup is sufficient for the project, then the value for RPO will be 24 hours.

- ✓ If project defines RPO to be 5 hours, then the backup frequency for this project should be every 5 hours.

BUSINESS CONTINUITY OPERATIONS

Initial Response Phase

✓ The Initial Response phase begins as soon as an employee informs ISF(Information Security Forum/ERT (Emergency Response Team) team of an interruption event that has occurred, or is about to occur

Assessment Phase

✓ The Assessment Phase begins as soon as the ISF is notified of an event. It ends when the predetermined threshold of a disaster situation has been met and the DAT(Disaster Assessment Team)/ISF agrees to declare a disaster and begin the Activation Phase

Emergency Declaration Phase

✓ Declaration of disaster is based guidelines specified in section 'Categorization of disaster'. The emergency declaration phase declares the event as Major or Minor.

System Recovery phase

✓ All activities required to restore the mission critical functions that are affected primary site(s)/ secondary site(s).

BUSINESS CONTINUITY OPERATIONS

✓ All activities required to restore all designated data processing systems, functions and facilities that are required to support mission critical business functions.
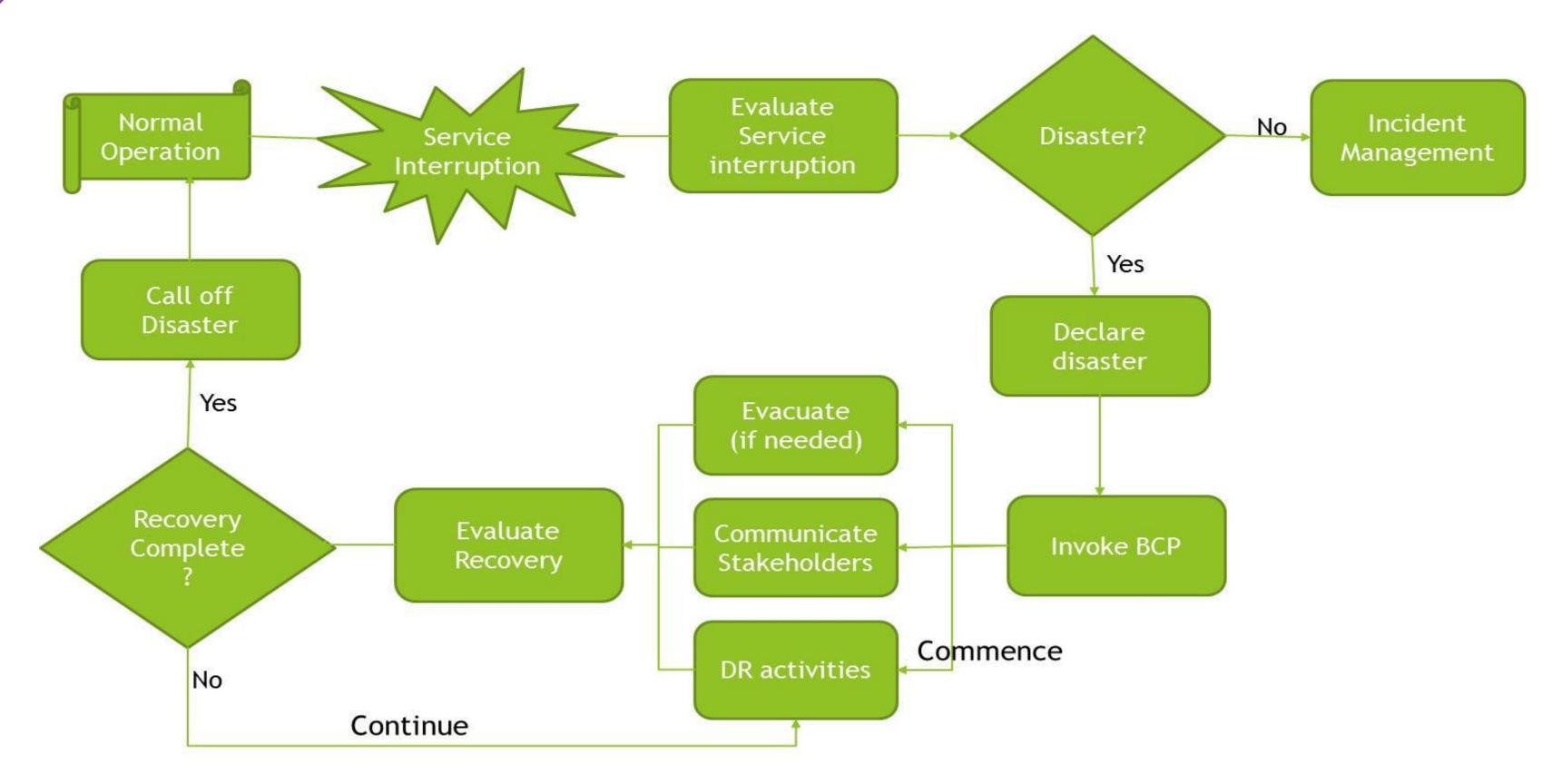
Business functions Start-up Phase

✓ Validation of restored systems' functionality and data integrity

✓ Evaluation of data recovery point and determining any data loss

✓ Controlled restart of business function operations

Return to normalcy phase

✓ This phase begins when the ISF/DAT makes the decision to return declare the normalcy of operation. It ends as soon as full operations have been re-established at all affected sites

BUSINESS OPERATIONS FLOW CYCLE

BUSINESS CONTINUITY OPERATIONS

Disaster response life cycle

After a disaster, the standard response life cycle is as follows
- ✓ The DAT/ISF will assess the level of damage and decide to invoke a BC plan,   what kind of plan and notify the team
- ✓ The provision of emergency service if required
- ✓ Prioritize recovery and commence restoration activity
- ✓ Resume normal operation

Acronyms

- ✓ BCP – Business Continuity Plan
- ✓ BIA – Business Impact Analysis
- ✓ CISO – Chief Information Security Officer
- ✓ DAT – Disaster Assessment Team
- ✓ DRC – Disaster Recovery Coordinators
- ✓ DR – Disaster Recovery
- ✓ ERT – Emergency Response Team
- ✓ ISF – Information Security Forum
- ✓ RTO – Recovery Turnaround Objective (Or) Recovery Time Objective
- ✓ RPO – Recovery Point Objective

THANK YOU :)