Methodology - Business Impact Methodology (BIA) and Risk Assessment (RA)

Title	Methodology – Business Impact Analysis and Risk Assessment
Classification	Internal Use Only
Author	Probal Choudhuri
Reviewer (suitability and adequacy)	BCMS Manager
Approver (suitability and adequacy)	CEO/MD
Policy/Document Owner	
Current Version	Draft
First Document Release Date	

Modification History:

S. No.	Description of Change	Date of Change	Version No.
1			
2			
3			

Table of Contents

1. Purpose and Objective

Business impact analysis (BIA) is an essential component of an organization's enterprise risk management. It includes an exploratory component to reveal any vulnerability, and a planning component to develop strategies for minimizing risk. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of resources in the case of a disaster. For example, a business may be able to continue more or less normally if the cafeteria has to close, but would come to a complete halt if the information system crashes.

The purpose of this document is to define a step-by-step process of doing BIA and RA in Company. Kindly note that this document complements the Information Security Management System (ISMS) risk assessment (RA) approach. In the current ISMS –asset-group wise risk assessment is performed – which identifies vulnerabilities that can be prevented. The process of vulnerability identification in this BIA/RA is aimed at managing 'black swan' events – and therefore focuses on 'complete' outage preparedness, and a 3 layer approach to recover all teams and services in the order of business priority.

2. ISO 22301 Reference

Clause 6.1 – Actions to address risks and opportunities
Clause 8.1 Operational planning and control
Clause 8.2 – Business Impact Analysis and Risk Assessment

3. Context

The context is line with Context Assessment as define the BCMS – Scope statement, and covers all business requirements.

4. Criteria

The criteria for business impact analysis and risk assessment includes all aspect of business operations. There are no teams or services that are left out within the scope.

5. Scope

The scope of BIA applies to all areas of the organisation.

6. BIA Definition in ISO 22301

process of analyzing activities and the effect that a business disruption might have upon them

7. BIA and RA Process Steps

Step 1 – Team Classification for Business Continuity

This step involves the following:

- Meeting each team and understanding the scope of work.
- This resulted in classifying every team in one of the four classifications:
    - Essential Physical Infrastructure Services (EPIS) – Teams responsible for ensuring health and safety of personnel in case of crisis. They will be first to be available onsite.
    - Revenue Generating services (RGS) – Team responsible for performing and fulfilling customer SLA/commitments. They drives the physical space requirements including MTPOD/RTO/MBCO/RPO requirements in a 2 layered approach.
    - Essential technology Services (ETS) – Teams responsible for restoring technology services that includes application/network and other technology services
    - Delayed Start Services (DSS) – Teams that can wait during crisis and are last in the process of recovery.

Step 2 – Identification of Mission Critical Activities (MCA) for RGS

This step involves the following:

- Understanding and documenting the individual MCA for each customer.

Step 3 – Understanding scope of continuity requirements

This step involves the following:

- Understanding and documenting the individual MCA for each customer.
- Understanding the maximum tolerable period of disruption
- Understanding the minimum service levels or minimum business continuity requirements
- Understanding and documenting minimum requirements (layer 1) and pending (layer 2) requirements for recovery
- Consolidating the requirements by team and by location to understand