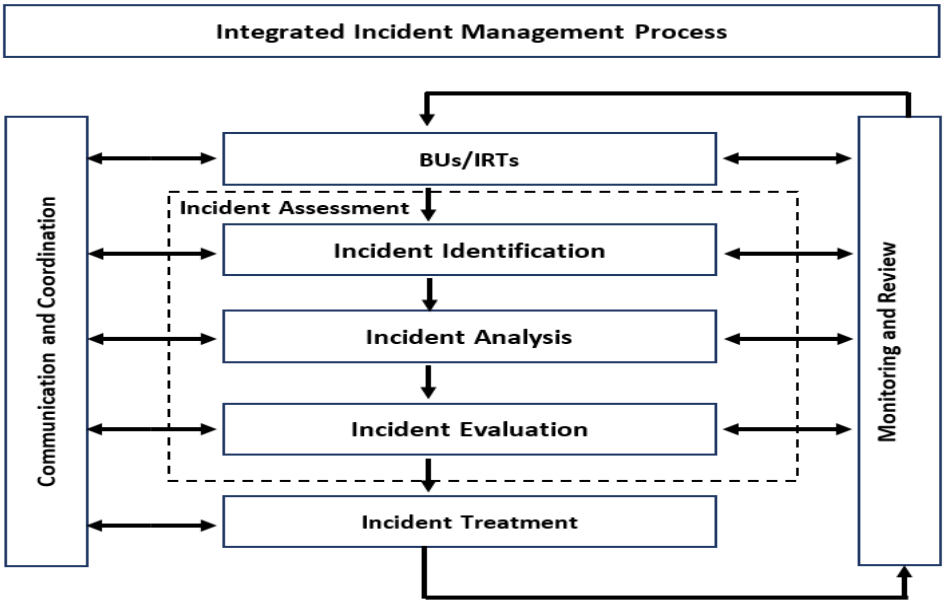
GUIDELINES AND PROCEDURES FOR INCIDENT REPORTING

A. Integrated Incident Management Framework (IIMF)

The Bank's IIMF shall adopt the basic principles of risk management by setting the standard in the incident management process: incident assessment, monitoring and review, communication and coordination in all levels of the Bank's operations.



B. Incident Response Team (IRT)

1. Planning and Preparation

The IRT shall be designated to the Head of the Business Unit (BU) based on the covered incident. IRTs may assemble their own team members and involve other BUs and/or Subject Matter Experts (SME), as necessary, to appropriately address the incident. The IRTs shall ensure that relevant/critical information are duly documented and that the flow of communication, coordination, reporting and monitoring are efficiently observed.

2. Detection and Reporting

a. Identification (Knowledge, Monitoring of Indicators)

Immediately upon knowledge of the incident, the BU shall check the **Impact Description** and its corresponding **Priority Level** as identified in DBP's IIMF policy. The higher level of priority shall be assumed in the event of conflict or uncertainty among the different impacts.

b. Reporting (Notification, Update, Escalation)

i. The BU (source of incident or witness) shall immediately report the incident to the IRT/s through telephone and/or e-mail within the date of knowledge. The BU shall prepare an Incident Report and submit to the IRT, copy furnished the Operational Risk Management Department (ORMD),

Compliance Management Group (CMG), Internal Audit Group (IAG) and ISRMD for information security related incidents.

ii. The BU shall provide follow-up/final report based on the IRT's incident assessment /root cause analyses, as necessary.

iii. The BU shall monitor and report to ORMD the status of action plans.

iv. The IRT should respond and escalate the incident based on the priority level in a timely manner.

c. Incident Assessment and Decision

Incident assessment involves consideration of the causes and source of the incident, its consequences, and likelihood of recurrence. It leads to the determination of possible actions and decision on the most appropriate treatment and strategies that will provide adequate procedural and system controls to mitigate/address repetition of similar incidents.

d. Response

Below sets of response may be applied by the IRT, as applicable:

i. ***Contain/Resolve/Eradicate***
The intention is to return to normal business operation.

ii. ***Assessment (Evaluation, Feedback)***
The incident is re-created under a controlled condition to accurately understand the order of events that led up to the incident***.***

iii. ***Recover (Restoration, Restitution, Resumption)***
The instruction or identified remedy is applied to an incident.

e. Closing of Incident/Lessons Learned (Recommend improvement and implement change)

The IRT/BU shall assess the effectiveness of the recommended controls/mitigations to ensure non-recurrence and/or minimize losses from similar incidents. Closed incidents shall be properly documented and confirmed by concerned BUs.

The IRT/BU shall continually monitor and review the incident and its influencing factors or consequences to identify changes and/or effects that may affect the Bank's policies and processes. Recommendation for improvement and its implementation shall also be part of the status monitoring and reporting by ORMD.

Lesson/s learned from previous incidents shall be used as bases to address similar incidents in the future.