Doc No.: SOP/ITG/64
Process Owner: Information Technology Group
Version No.: v1.0
Last Reviewed on: 30-06-2019
Next Review Date: 30-06-2021

Standard Operating Procedure

for

Incident Reporting - Application Support

1.0 Name of standard operating procedure

Incident Reporting - Application Support

2.0 Scope of applicability:

Incident Reporting - Application Support process is the process of Incident Management through reporting of application availability and functionality related issues by internal users, investigation and analysis of the reported incident and then resolution/recovery by designated ITG teams.

Each application serviced by the technology teams has multiple levels for handling of reported incident, depending on the complexity and severity of the incident.

Level-1 (Support Team) is the first level service desk team from Business Technology Operations, responsible for quick analysis of the reported incident. Scope of Level-1 activity is to analyses the incident, match it with known-errors, referencing it with known workarounds, if any, and provide quick first-line fix. Reported incidents or problems which cannot be resolved at this level or a new problem identified is referred to the Application team termed as Level-2, for further analysis and resolution.

Level-2 (Application Team) is the problem management team from Technology Services Group responsible for further analysis of incidents referred by Level-1 team. Scope of Level-2 activity is to further analyses reported incidents, group multiple occurrences of related incidents to identify problems, modify an IT service in order to resolve a problem through change management. At times, depending on complexity, the incident is transferred to or parked in vendor / development team's tray for further resolution.

Level-3 (Internal development team or external vendor) is the team responsible for ultimate analysis of the issues referred by level-2, identify and confirm new system bugs, suggest temporary work around and design permanent fix.

3.0 Distribution list:

Name of the groups to whom the process has to be communicated for their roles in providing the information to the Principal Group

Groups involved in the execution of the process

Sl. No.	Name of Group	FPR from the Group
1	BTO	Ashok Thiagarajan

4.0 Procedures for the Process:

I) Process:

Sl No.	Process step	Responsibility	TAT	Exception/Deviation if allowed
1	The IHelpdesk application is accessible over the intranet and can be reached through the universe site. Login to the IHelpdesk application. After logging in, the user has to click on label- "NEW SERVICE REQUEST". This further has 3 levels i.e."Type", "Area" and "Sub Area" to choose desired application and service request type. Under "Type", value of "IT APPLICATION CALLS" is to be picked. Under "Area", list of all the applications supported by the technology teams is available, Application name for the specific incident is to be picked. Under "Sub Area" users can pick between "Application Slow or Down" or "Report an Issue" depending on the nature of incident.	Creator	NA	NA
2	Under "Type", value of "IT APPLICATION CALLS" is to be picked. Under "Area", list of all the applications supported by the technology teams is	Creator	NA	NA

	available, Application name for the specific incident is to be picked. Under "Sub Area" users can pick between "Application Slow or Down" or "Report an Issue" depending on the nature of incident.			
3	ChatBot (interactive agent) has been implemented for 22 applications. ChatBot has been configured with basic Q&A which enables the user to get the solution to the query without raising the SR. After selecting the relevant information in point 1 and 2 On clicking "GO" button, "Athena" ChatBot will pop-up and user can type the query in a text input box. System will display option of matching Questions which user need to select as per their requirement. ChatBot will evaluates and responds to user input. In case the ChatBot does not resolve the query, it will prompt user to raise the Service request and user will; be re-directed to helpdesk page.	Creator	NA	NA
4	In which Applications ChatBot is not been configured, Normal Service Request will be raise by following Step 1 & 2. Once On clicking "GO" button, detailed incident reporting form is loaded. The form is filled and submitted to	Creator	NA	NA

	generate a service request.			
5	IHelpdesk service requests first land in Level-1 team's tray. On this step, Level-1 team can either close the service request on resolution or if no solution is available, forward the same to Level-2 team's tray for further investigation and analysis. Service requests for incidents not matching with a known error and known root cause are further assigned to Level-3.	Level 1& Level 2 & Level 3 teams	For every level, TAT and escalation matrix is defined in BPD site.	NA
6	On resolution of incident or problem, Level-1 or Level-2 teams update the closure remarks. Level-3 team does not have authority to close a service request. They can only assign a service request back to Level-2 tray with comments. Auto-closure mail with closure remarks is triggered to the originating user by IHelpdesk system.	Level 1& Level 2 & Level 3 teams	NA	NA
7	Level-1, Level-2 and Level-3 teams can seek clarifications from the service request originator by assigning the service request back to the originator's tray.	Level 1& Level 2 & Level 3 teams	In case of non-confirmation by the users for 3 days, the service request gets auto closed by IHelpdesk system.	NA

8	For critical applications, user satisfaction feedback has been implemented by removing service request closure right from Level-1 and Level-2. Instead of closure, service requests are assigned to the originating user's tray for confirmation. Users not satisfied with the resolution have the right to either reassign the service request back to respective Level-1 / Level-2 trays or close the service request with options to indicate their level of satisfaction with the resolution provided. In case of non-confirmation by the users for 3 days, the service request gets auto closed by IHelpdesk system.	Creator	In case of non-confirmation by the users for 3 days, the service request gets auto closed by IHelpdesk system.	NA

Process for Reporting of Major Incidents to MAS

Monetary Authority of Singapore (MAS) had issued a notice (MAS Notice 644) on June 21, 2013 which becomes effective from July 1, 2014. Requirements specific to Application support are enumerated below:

1. A bank shall make all reasonable effort to maintain high availability for critical systems. The bank shall ensure that the maximum unscheduled downtime for each critical system that affects the bank's operations or service to its customers does not exceed a total of 4 hours within any period of 12 months.
2. A bank shall notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.
3. A bank shall submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident.

The critical systems identified for the Singapore operations of the Bank are i-Core, Murex, Retail Internet Banking (RIB), SWIFT (Alliance and Messaging) and One Key Assurity. These critical systems are further categorized as applications requiring 24x7 availability (i-Core, RIB & One Key Assurity) and applications critical for branch operations but not requiring 24X7 availability (Murex and SWIFT). However, the functionality provided by Central Stand In

Server (CSIS) during the period when scheduled end of day and beginning of day are carried out on i-Core shall be considered as continuity of services

Sl No.	Process step	Responsibility	TAT	Exception/Deviation if allowed
1	Any system malfunction (i.e. failure in any of the critical systems as defined hereinabove) shall be reported by branch users or the appointed monitoring agency or by officials in the Information Technology Group by logging a service request (SR) in i-Helpdesk.	Singapore Branch Users		
2	Any IT security incident which impacts the operations of the Singapore branch or materially impacts the Bank's service to its customers in Singapore shall be reported by Security Operations Center (SOC). Designated BTO/ISG shall be notified by the system for all the incidents reported.	Security Operations Center (SOC)		
3	Based on such preliminary review, if the reported incident qualifies as a potential case for "relevant incident" as per the definition enunciated in MAS Notice 644, BTO (in case of system malfunction) or ISG (in case of IT security incident) shall prepare a summary of the incident in the template as required by MAS and forward it to a designated Singapore Incident Response Team.	BTO/ ISG team		

4	The Singapore Incident Response Team (Members as Respective BT heads, ISG head, SG operation head, Infrastructure head) shall review the incident and take a final decision on whether the incident qualifies as a "relevant incident" as per the definition enunciated in MAS Notice 644. If the decision is in the affirmative, the incident shall be reported to MAS.		Not later than 1 hour, upon the discovery of a relevant incident	
5	For such "relevant incidents" which are reported to MAS, the relevant team(s) shall complete the Root Cause Analysis (RCA). The format of RCA as required by MAS is contained in Annexure A-1. The RCA shall be reviewed by the IT Compliance team, the concerned Business Head(s) and the concerned Business Technology Head(s) and after their clearance, it shall be forwarded to the Singapore branch for onward submission to MAS.	Singapore branch	10 calendar days.	

For One Key Assurity application, responsibility for tracking of downtime and incident reporting with respect to MAS 644 will be with Singapore Branch only, as the application is being maintained locally.

For tracking of consolidated downtime, so as to maintain maximum of 4 hours in last 12 months as mandated by MAS 644, IT Compliance will introduce monthly KRI for Singapore critical applications.

All major downtime, including for applications of Singapore geographies are

currently presented to the IT Steering Committee.
For relevant and qualified incidents reported to MAS, concerned Technology Operations teams shall analyze the trend of recurring incidents relating to MAS identified application supported by them and submit a quarterly trend analysis report based on the RCA summary already submitted to MAS to Singapore branch team SPOCs, Singapore Incident Response Team and the IT compliance team, within 2 weeks from the end of quarter. Format for the trend analysis report shall be as per the details in Annexure A-2. No report is to be published, if there are no relevant and qualified incidents during last quarter. MAS identified applications currently supported by Technology Operations teams are iCore, Murex, Retail Internet Banking RIB and SWIFT Alliance and Messaging. For One Key Assurity application, responsibility for analyzing the trend and quarterly reporting will be solely with Singapore Branch, as the application is being maintained locally.

II) Validation to be performed, if applicable:

For critical applications, user satisfaction feedback has been implemented by removing service request closure right from Level-1 and Level-2. Instead of closure, service requests are assigned to the originating user's tray for confirmation. Users not satisfied with the resolution have the right to either reassign the service request back to respective Level-1 / Level-2 trays or close the service request with options to indicate their level of satisfaction with the resolution provided. In case of non-confirmation by the users for 3 days, the service request gets auto closed by IHelpdesk system.

5.1 Submission of information to Principal Group (if applicable):

The Mode of Submission - iProcess

5.2 Annexures, if applicable:

Sl No.	Annexure
1	The format of RCA as required by MAS is contained in Annexure A1
2	Format for the trend analysis report shall be as per the details in Annexure A-2

Annexure A-1

Incident Report template

1. Reporting Staff's Particulars

Name of institution:	

Name of reporting staff:	
Designation:	
Telephone:	
Email:	
Date :	

2. Executive Summary

Date, start time, end time Date	
Nature of Incident	System Malfunction/IT Security Incident/Others*.
Cause of incident	
Incident description	

3. Impact of Incident

a. System/ operations

Critical systems impacted	Affected business / Operations
Name of system(s) affected	Describe how business and operations were / will be affected as a result of the Incident.

b. Customer Impact

Are retail and/or corporate customers affected?	Retail / Corporate / Both / None Impact description

Impact description	Describe how customers were / will be affected by the Incident, e.g., number of customers, which service is unavailable, monetary losses etc.

c. Others

Describe other possible implications, e.g., financial and legal, that the incident will / may have on the institution.

Chronology of Events

Time (hr/min)	Description
State the corresponding time for each	Provide a detailed chronological description of the various events of the incident. Events to cover include, but not limited, to the following: a. Incident discovery; b. Escalation to senior management, including approvals sought for implementing interim measures, if any; c. Stakeholders informed or involved; and d. Decision/activation of BCP and/or IT DR.

4. Detailed Root-Cause Analysis

Identify the root cause of the Incident and the actions taken to resolve the issue. Examples include: a. Cause of problem*; b. Interim measures to mitigate/resolve the problems, and reasons for taking such measures; and c. Steps identified or to be taken to address the problem in the longer term. (*Please describe technical details, if applicable)

5. Conclusion

Preventive actions for future incidents	List the corrective actions that were / will be taken to prevent a Recurrence of similar incident
Is the problem resolved? Yes/No*	Yes/No* *Target date of resolution_____ (DD/MM/YY).

Annexure A-2

Template for the trend analysis report

Executive Summary

(The reporting period and brief summary of the reported incidents needs to be mentioned)

Incidents by Type

(A summary of the incidents based on the type)

Incidents by Severity

(A summary of the incidents based on the severity)

Incidents Recurring Trend

(Trend analysis based on recurring incidents)

Detailed analysis for all the Incidents in the reporting period

- Description

- Analysis

- Action taken