

Citigroup Technology Infrastructure, Asia Pacific

1943

VOLUME : 4 - PROCEDURES & WORK INSTRUCTIONS

DOCUMENT : **125 - CTI INCIDENT & PROBLEM
MANAGEMENT PROCEDURE**

Version 2

Implementation Date: 1 Dec 2006

APPC Reference: QM3/4/125

Distributed Operations Reference: 31Dec2004/Version 3.0

ORIGINATOR:


RAJESH BALARAMAN
Regional Problem Management Group

COPYRIGHT NOTICE

Copyright © (2006) by Citigroup

All rights reserved. These materials are confidential and proprietary to Citigroup and no part of these materials should be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor should the materials be disclosed to third parties without the express written authorization of Citigroup.

VERSION HISTORY FOR INTEGRATED PROCEDURE

Version 2 Revisions:

- a) Revised the PCM to comply with L2 standards V5.0 Published on 31 Aug 2006
 - Usage of ITIL terminology
 - Adoption of 2-Dimensional Severity classification (Impact+Urgency)
 - Maintenance and reference to CTI ASPAC specific "Known Error" list

Version 1.21 Revisions:

- a) Added Section 3.2.11 with Definitions of Manual Workaround processes and corresponding escalations needed.

Version 1.2 Revisions:

- a) Updated Section 3.2 on Escalation & Notifications to accommodate special situations.
- b) Updated Section 3.2 on Notifying Compliance (GCRM) on Incidents reported to regulators.
- c) Updated Section 3.2 on Notifying Singapore Country Compliance, Country CCO and Regional Compliance on Incidents reported to regulators.
- d) Updated Section 3.2 to include Excerpts from *Escalation Procedure for Citigroup Services (Japan)*

Version 1.1 Revisions:

- (a) Updated sections to comply with new CITMP Level 2 standards for Problem Management document published on 10 Feb 2006.
- (b) Adopted Severity guidelines and Incident Escalation process standards from CITMP Level 2 standards for Problem Management document
- (c) Integrated Crisis Communication procedure (QM3/4/168) in to this document
- (d) Documented Maker / Checker post-mortem process in Section 3.5.
- (e) Incorporated MAS and HKMA notification mandates in relevant sections.
- (f) Included Japan specific requirements as part of post-mortem reporting process.

Version 1.0 - Integrated CTI Asia Pacific Problem Management Procedure

VERSION HISTORY FOR APPC

VERSION 7 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: DECEMBER 23, 2005
India DC has started using VIRTUALTECH (problem tracking tool) instead of PARTNER (which was the earlier tool used). Hence, the same was changed in the procedure document for MRDC & BRDC.	
VERSION 6 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: DECEMBER 7, 2005
Updated references & removed obsolete information. Updated - Weekly / Monthly Problem Management Scorecard to include GPMS Tickets for Emergency Changes Update - Generating Weekly / Monthly Problem Management Scorecard to include List of GPMS tickets related to Emergency Changes Monthly.	
VERSION 5 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: AUGUST 5, 2004
1) Remove section on Problem Management Life Cycle as this will be mentioned in the new Problem Management document. 2) Modified document name. 3) To mention APPC PMO website and all reports generated by APPC RPMG.	
VERSION 4 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: MARCH 30, 2004
To include BRDC/MRDC.	
VERSION 3 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: SEPTEMBER 26, 2003
To add the following: 1) Section 3.4.5.a.1 to cater for the Midrange Audit issues, 2) Appendix B - General Guidelines for EMS Reporting.	
VERSION 2 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: JUNE 25, 2003
Compliance with CITMP release 1 and Global TI Standard. Implement Citigroup Branding Requirement.	
VERSION 1 (PREVIOUS VERSION)	DATE OF IMPLEMENTATION: FEBRUARY 25, 2003
Initial version.	

VERSION HISTORY FOR DISTRIBUTED OPERATIONS

Version No.	Author	Published Date	Description of changes
3.0	Monica Wong	Dec 31, 2004	To include Australia into the list of countries following the procedure To replacing GTMS and GPMS with Virtual Tech as the Trouble Ticketing System
02.1	Monica Wong	April 01, 2004	Update Contacts
02.0	Monica Wong	Jun 30, 2003	Revised based on CITM Policy Rev 1, incorporating SIRT and COB. Follow "Global Problem Management Process Standards".
01.1	Monica Wong	Dec 18, 2002	Revised based on feedback from ARR. EMS replaced SCS as the Outage Reporting System starting Dec 9, 2002.
01.0	Monica Wong	Nov 06, 2002	First Release

Note: The above version history is retained for information only.

APPROVAL

APPROVED BY:

Venkat 1 Dec '06

VENKAT NARAYANAN
Regional Problem Management Head

Ramon V. Karingal

RAMON V. KARINGAL
APPC Director

Anthony K.C. Lee

ANTHONY K.C. LEE
Distributed Operations Head

12/8/2006

TABLE OF CONTENTS

1. INTRODUCTION	6
1.1 OBJECTIVE.....	6
1.2 SCOPE.....	6
1.3 DOCUMENT REVIEW	6
1.4 REFERENCES	6
2. ROLES AND RESPONSIBILITIES.....	8
2.1 REGIONAL PROBLEM MANAGEMENT GROUP.....	8
2.2 CUSTOMER SERVICES.....	8
2.3 SUPPORT UNITS / RESOLVERS	8
2.4 MANAGEMENT	9
2.5 BUSINESS USERS.....	9
3. THE INCIDENT & PROBLEM MANAGEMENT PROCEDURE	10
3.1 DEFINITION OF TERMS	10
3.2 DETECTION AND RECORDING	10
3.2.1 Incident Ticket Logging	10
3.2.2 Virtual Tech	11
3.2.3 EMS	11
3.2.4 Service Desks & Ticket Logging	11
3.3 ESCALATIONS & NOTIFICATIONS.....	12
3.3.1 Escalation List	14
3.3.2 Escalation and Notification	15
3.3.3 Escalation and Notification to Engineering Support.....	15
3.3.4 Incident Escalation and Notification (Special Situations).....	15
3.3.5 Notifying Compliance On Incidents Reported to Regulators	16
3.3.6 Work around During Incident Resolution	16
3.4 INCIDENT HANDLING	17
3.4.1 Classification & Initial Support and Investigation & Diagnosis.....	17
3.4.2 Resolution and Recovery	18
3.4.3 Incident Closure	19
3.4.4 Incident ESCALATION Logs	19
3.5 PREVENTION AND CONTINUOUS IMPROVEMENT	19
3.5.1 Incident & Problem Management By Regional Problem Management Group	19
3.5.2 BRDC.....	20
3.5.3 MRDC.....	20
3.6 POST MORTEM REPORT.....	21
3.7 PROBLEM MANAGEMENT METRICS	23
3.7.1 Metrics Reporting for CTI	23
3.7.2 Weekly / Monthly Problem Management Scorecard for APPC.....	24
3.7.3 Weekly Problem Management Report for CTI AP.....	25
3.7.4 Service availability and reliability.....	28
3.7.5 Managing VT tickets.....	28
3.7.6 Managing MTTR performance for Datacenter.....	29
3.7.7 Management Reviews for CTI	29
3.8 COORDINATION.....	30
3.8.1 APPC	30
3.8.2 BRDC.....	30
3.8.3 MRDC.....	30
3.8.4 Distributed Operations	31
A. APPENDIX – GENERAL GUIDELINES.....	32
A.1 SEVERITY LEVEL ASSESSMENT & EMS REPORTING GUIDELINES	32
A.2 POST-MORTEM REPORT GUIDELINES.....	33
B. APPENDICES SPECIFIC TO DISTRIBUTED OPERATIONS.....	35

TABLE OF CONTENTS

C.	MASNET CIRCULAR ON BUSINESS CONTINUITY MANAGEMENT	36
D.	HKMA INCIDENT REPORTING GUIDELINES	37
E.	CRISIS COMMUNICATION PROCEDURE.....	39
E.1	OBJECTIVE	39
E.2	SCOPE.....	39
E.3	ROLES AND RESPONSIBILITIES.....	39
E.4	EMAIL UPDATES.....	40
E.5	CONFERENCE BRIDGES.....	40
E.6	POST MORTEM REPORTS	41
E.7	SAMPLE EMAIL UPDATES DURING A CRISIS SITUATION	41
E.8	CRISIS COMMUNICATION - CROSS FUNCTIONAL PROCESS MAP (1 OF 3).....	43
E.9	CRISIS COMMUNICATION - CROSS FUNCTIONAL PROCESS MAP (2 OF 3).....	44
E.10	CRISIS COMMUNICATION - CROSS FUNCTIONAL PROCESS MAP (3 OF 3).....	45
F.	EXCERPTS FROM ESCALATION PROCEDURE FOR CITIGROUP SERVICES (JAPAN).46	
G.	INCIDENT ESCALATION LOG TEMPLATE.....	47

1. INTRODUCTION

1.1 OBJECTIVE

The purpose of this document is to define and establish the Incident & Problem Management Procedure to support the Citigroup Information Technology Management Policy (CITMP) for Problem Management – January 2004 version ([Level 1](#)) as well as the Citigroup Technology Infrastructure Standard ([Level 2](#)) on Problem Management. The procedure includes both Incident Management and Problem Management as defined by ITIL.

This document serves as the guideline for various CTI Asia Pacific groups in Datacenters and Distributed Operations, in performing their functions while ensuring compliance to CITMP Policy and Standard on Problem Management.

1.2 SCOPE

This procedure shall apply to all reported Incidents and Problems affecting the delivery of Production Services supported by CTI Asia Pacific. Incident & Problems relating to the environmental / infrastructure are included as being part of the Production Services.

Korea Data center has adopted the Level 3 Problem Management Procedure of Citibank Korea Inc.

This document fits the description of the Process Control Manual (PCM) described in the Level 2 Standard.

The scope of this procedure covers:

- Detection and Recording (formerly termed as *Identification and Documentation**)
- Escalations and Notifications
- Classification and Initial Support (formerly termed as *Determination**)
- Investigation and Diagnosis (formerly termed as *Determination**)
- Resolution and Recovery (formerly termed as *Bypass and Recovery**)
- Closure (formerly termed as *Resolution**)
- Coordination
- Prevention and continuous improvement

* Note: As referenced in CITM Policy.

1.3 DOCUMENT REVIEW

CTI Asia Pacific Regional Problem Management Group (RPMG) is responsible for reviewing and maintaining this document. The document will be reviewed annually or whenever there are updates or changes to the Citigroup Information Technology Management Policy, Citigroup TI Standard on Problem Management or changes in the Problem Management function.

1.4 REFERENCES

- [CITMP Level 2 Standards for Problem Management](#)
 - o http://www.citigroup.net/ti/compliance/citmp_level2.htm
- Doc. No. QM3/4/21 – [APPC Continuity of Business Plan](#)
 - o http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/iso/docs/level3/work/cob/qm3421/COB_PLAN.pdf
- Doc. No. QM3/4/86 – [Customer Services Guide](#)

- o <http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/iso/docs/level3/work/dco/qm3486/frame.htm>
- [Problem Management Procedure for India Data Centers](#)
 - o http://cti.asiapacific.citigroup.net:8800/idc/idc_citmpurl.htm
- [Virtual Tech Documentation](#)
 - o <https://virtualtech.eur.nsroot.net/virtualtech/documentation/>
- [Executive Monitoring System \(EMS\) User Guide](#)
 - o https://eur-emsweb.eur.nsroot.net/emstrn/html/EMS_Training_Package.html
- [Security Incident Response Team \(SIRT\) Process](#)
 - o http://cti.asiapacific.citigroup.net:8800/isc/IS/Training_Materials/CTI AP SIRT.ppt
- [CTI Regional Problem Management Group Website](#)
 - o <http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/csweb/appcpmo/index.htm>
- [Service Availability and Reliability Framework Process](#)
 - o <http://ato.citicorp.com/Update/SARFramework2.1.doc>
- [Appendixes & Forms for Distributed Operations](#)
 - o <http://cti.asiapacific.citigroup.net:8800/distops/policies/Working file probproc.doc>
- Incidents and Errors Escalation Procedure for Citigroup Services (Japan) Ltd
 - o Registry No.: Com-06013
- [Incident Management Playbook](#)
 - o <http://www.citigroup.net/ti/IncidentProblem/>

2. ROLES AND RESPONSIBILITIES

The RPMG (Regional Problem Management Group) is responsible for the maintenance and administration of the Incident & Problem Management Processes and related procedures.

2.1 REGIONAL PROBLEM MANAGEMENT GROUP

- Maintain and administer the Incident & Problem Management Procedure. This includes the management of incident & problem tools.
- Provide weekly Management reporting updates on incident & problem metrics.
- Perform annual reviews of the Incident & Problem Management Procedures effectiveness.
- Review and ensure that all reported incidents are resolved / closed within the stipulated standard. Root cause and resolution details are adequately documented.
- Establish an effective communication channel to provide feedback to all affected parties, upon receiving progress updates from the support units.
- Conduct post-mortem meetings for selected Incident & problems viz. Crises, chronic problems and incidents that are reportable to Regulators.
- Conduct periodic Problem Management review meetings with all relevant stakeholders to analyze trends and develop appropriate action plans. This is to minimize and eliminate repeat occurrences and to improve service availability.
- Other than facilitating the recording (documenting) of incidents handled by partners in Business Aligned Technology organizations, the scope of Regional Problem Management Group is limited to CTI resolved incidents / problems.

2.2 CUSTOMER SERVICES

Customer Services are the initial point of contact for Businesses to report incidents.

- Performs 1st level Incident determination and assessment.
- Ensure all incidents logged are properly recorded, assigned and classified.
- As part of the communication channel, provide notification updates to the respective country help desk, support units and end-users.

Note that the incidents reported by users in the following areas are handled directly through the Virtual Tech (Virtual helpdesk) system:

- Workstations
- Voice (PABX, Voicemail)
- LAN (Servers, hubs, cabling, gateway, connectivity)
- WAN (CSPAN, GRN)
- Profiles (Host, Email)
- Market data
- Value-added services (mobile phones, intra/internet access, pagers, video conferencing, blackberry)
- Local business applications
- CTI and Application Production Support groups

2.3 SUPPORT UNITS / RESOLVERS

Teamwork is the key to an effective Incident & Problem handling process that will result in a faster resolution in the event of a service disruption. The following serves as a guide to all Support Units including those in CTI Asia Pacific as well as in Business Aligned Technology organizations:

- Respond to 1st level ticket assignment upon notification.
- Perform 1st level investigation to determine correct assignment.
- If assignment is correct, accept responsibility for the assigned ticket; validate the information and details. If incorrectly assigned, either:
 - o Inform Customer Services (CS) or users to reassign ticket to the appropriate group if the support personnel does not know which group should own the ticket

OR

- o Accept the ticket and reassign ticket to the correct group to investigate further.

- Perform the required investigative / corrective action steps and provide a solution and document resolution details. If investigation shows that the incident may not belong to a particular group, the ticket should be reassigned to the appropriate support group.
- Adhere to the resolution standard timeframe in accordance with the severity level.
- Record all relevant incident resolution details and root cause findings in the trouble ticket.
- For Severity-1 and Crisis-related incidents, provide updates to the Regional Problem Management Group on the resolution progress and an estimate for providing the solution.
- Perform Management escalation as required.
- Ensure sufficient information is provided in the trouble ticket for creation of an EMS ticket for all severity 1 incidents.
- Conduct regular Problem Management review meetings with all relevant stakeholders to analyze trends and take appropriate actions.

2.4 MANAGEMENT

- Receive and review the escalations and take appropriate action steps.
- Review the management reports on incident metrics and problem trend analysis.
- Formulate improvement or corrective action plans (where relevant and necessary).
- Participate in the Problem Management review meetings and provide Management guidance, support and directions.

2.5 BUSINESS USERS

- Report the incident through the Virtual helpdesk (VT), APPC Customer Services or to local in-country Helpdesks (where applicable).
- Provide full details on the incident and the associated business impact.
- Review and validate the solution provided to ensure that the incident is resolved.

3. THE INCIDENT & PROBLEM MANAGEMENT PROCEDURE

3.1 DEFINITION OF TERMS

Term	Definition
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of service.
Incident Management	The IT process for restoring service levels as quickly as possible during an incident, while minimizing the adverse impact on business operations.
Incident Diagnosis	An incident diagnosis is a determination of the nature of an incident, including which Configuration Items were affected and how they went wrong. Enough detail is required to support a resolution plan.
Incident Impact	Incident Impact is a measure of the business criticality and scale of an incident. Impact is calculated based on the answers to a questionnaire in Severity Level Assessment Matrix. There are three possible impacts: High, Medium and Low.
Incident Urgency	Incident Urgency is a measure of how quickly the incident must be resolved, for example if there are deadlines coming up. Urgency is calculated based on the answers to a questionnaire in Severity Level Assessment Matrix. There are three possible urgencies: High, Medium and Low.
Incident Status	The incident status indicates progress of the incident through the lifecycle. Possible values are: - Recorded - Accepted - Scheduled - Diagnosed - Resolved - Closed.
Problem Management	The IT process for carrying out root cause analysis, publishing post mortems, performing trend analysis as well as providing Intensive Care support where required. The objective of Problem Management is to uncover and resolve known errors in the environment.
Known Workaround	A known workaround is an identified means of resolving incidents of a particular type, which can be looked up as required. Known workarounds resolve the incident but not its underlying root cause.
Severity	Severity is a measure of the amount of resources and escalations that must be put into resolving an incident. There are three possible values - Severity 1, 2, and 3, with Severity 1 being the most severe. A subset of Severity 1 incidents are dealt with as Crises. The Severity Level Assessment Matrix uses a two dimensional impact and urgency factors to determine the severity of an incident.

3.2 DETECTION AND RECORDING

3.2.1 INCIDENT TICKET LOGGING

When an Incident is detected or reported and entered into the ticketing system (e.g. Virtual Tech), the following information should be captured at the minimum.

- Client information (e.g. name, phone, location, cost center)
- Incident category (e.g. desktop/monitor)
- Incident description (details gathered from clients, alerts and internal communications)
- Incident Impact and Incident Urgency statements
- Time and date of the incident occurred, detected and recorded
- Creator of the ticket and the person or group to which it was assigned

Such tickets logged are retained in the relevant ticketing system for periods equal to or longer than the minimum ticketing records retention period mandated by Level 2 standards.

3.2.2 VIRTUAL TECH

All entities in CTI AP make use of VT. Incidents are entered at inception and updated after resolution in the Virtual Tech ticketing system.

Refer to Virtual Tech Documentation for more information.

For historical purposes, the incident tickets maintained and closed in GPMS ticketing system information would be retained as per the current ticket retention requirement.

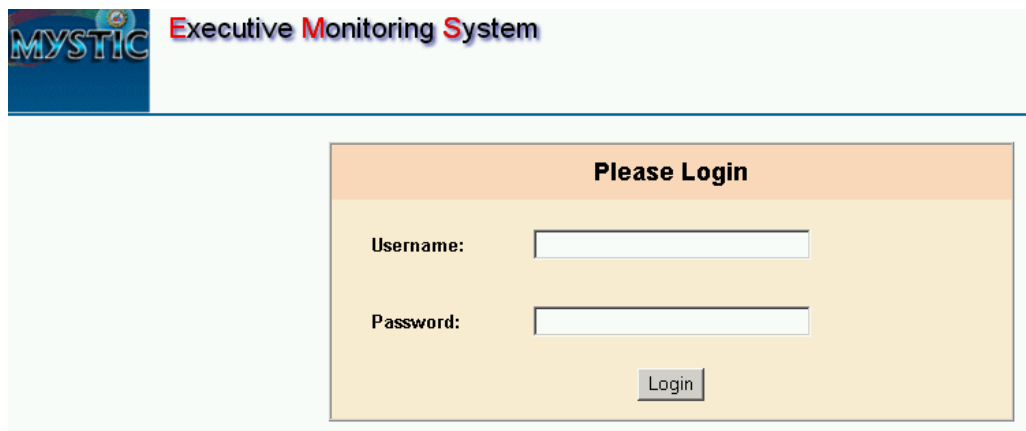
3.2.3 EMS

Executive Monitoring System (EMS) is a web-based executive notification system for all severity 1 and a subset of severity 2 incidents that are managed by CTI Regional Problem Management Group. These incidents have to be entered at inception and updated throughout the lifecycle of the incidents.

RPMG has to ensure the timely entry and up-keep of incident data in EMS system until incident closure.

General guidelines for EMS reporting are outlined in the Appendix section of this document.

Access to EMS requires a LOGIN ID to Mystic Information Center located at <http://ems.ny.ssmb.com/ems/index.asp>



The User guide for EMS can be found at [CITITECH Guide To EMS.](https://eur-emsweb.eur.nsroot.net/emstrn/html/EMS_Training_Package.html) (https://eur-emsweb.eur.nsroot.net/emstrn/html/EMS_Training_Package.html)

Please enter your MYSTIC login id and password in the logon panel shown able to gain access to the EMS system.

3.2.4 SERVICE DESKS & TICKET LOGGING

APPC Customer Service Helpdesk is responsible for logging incidents reported by users and/or technical support teams for incidents detected and reported for services offered in APPC. The procedure for Call and Incident Logging can be found in the doc. no. QM3/4/86 – Customer Services Guide.

Where the incident reported has an adverse impact or a potential adverse impact on the services offered to the customers or internal users, the incident is “actionable” and APPC Customer Service Helpdesk shall ascribe status accordingly to facilitate escalation.

The following calls received by APPC Customer Service Helpdesk are generally not recorded:

- Call transfer to staff telephone extensions or personal lines
- Request for IDD call assistance
- General enquiries.

The Virtual Ticket system is used as a virtual helpdesk for incidents logged for services offered by CTI Asia Pacific Distributed Operations or BRDC/MRDC. In such cases, the Individual who logs the incident into the Ticketing System is responsible for recording all details accurately. Incidents are entered into and tracked from the VT (Virtual Tech system) until closure.

The individual recording the incident in the ticketing system is responsible for initial classification of the impact and urgency of the incident. Based on these input, the VT system assigns the appropriate severity level to the ticket as per the Severity Level Assessment Matrix established in Level 2 Standards document. For incidents assigned to non-Citigroup resolvers (3rd party, vendors, associations etc.) a related ticket / tracking number is cross-referenced in the VT.

In addition to the incident tickets recorded by APPC Helpdesks, respective users or user coordinators, tickets are also recorded in VT by the monitoring systems such as Tivoli for appropriate action by support teams.

3.3 ESCALATIONS & NOTIFICATIONS

Escalation Process defines the means by which a person or group contacts another person or group with the intention of having them take particular action in helping to resolve the incident or make a required decision. An escalation can be done in many forms but verbal escalations will be required for crisis and severity 1 incidents.

Examples of escalations would be:

- ♦ A Command Center troubleshooting an incident realizes that a server is not responding to any login attempts. They escalate to the server support team for further troubleshooting and resolution.
- ♦ An earthquake destroys a main office location and a decision needs to be made to invoke COB. An escalation is made to the TI Region Head to make a decision in invoking COB.

Notification Process defines the means by which a person or group contacts another person or groups of people with the intention of informing them of a particular incident and or status. Notifications are for information purposes only and may initiate or assist in someone making a decision but in general do not require the immediate attention of the individuals or groups of individuals receiving them.

Examples of notifications would be:

- ♦ A Command Center troubleshooting the same server incident mentioned in the example above realizes there are dependencies on a particular application belonging to a business. A notification is sent to the support staff (Helpdesk, business support team) business representatives, client managers etc with details of the outage including impact, time and ETA to name a few. Notification's are then resent at pre-arranged times or when significant improvements or changes are made in the incident resolution.
- ♦ An earthquake a main office location, notification is sent to ATLC / GTH and other TI Senior Managers as well as COB management outside the impacted region. All parties involved may then decide, based on this information, to inform other parties and in some cases escalate for some decisions on actions to take.

Severity Definitions:

Severity level (also called priority) results from assessing the interaction of incident impact and urgency. Severity sets the right level of action to be taken in incident handling.

Impact is the effect that an incident has on the users of the service or their organization. CTI uses the following Incident Impact definitions:

Impact Classification	Definition
High Impact	- Those incidents that cause disruptions to external or internal users working on critical processes rendering them unavailable to do business, where no suitable workaround is feasible or available close-by to restore service. - Those incidents that cause external customer visibility or regulatory requirements causing a substantial risk to Citigroup's reputation or monetary stability. - Those incidents that make a strategic facility unusable or a smaller facility where there are not close-by alternatives. - Those incidents that are the result of major and/or broad-based external attack on Citigroup technology.
Medium Impact	- Those incidents that cause a disruption to external or internal users where an interim workaround or failover method is available to restore service. - This workaround can include such actions as invoking COB but should not be limited to that. - Those incidents that have minimal external customer impact and no risk to Citigroup's reputation or monetary stability where the business agree the degradation or loss of service is acceptable and non critical. - Those incidents that cause intermittent non-availability or slow response.
Low Impact	- Those incidents that cause a disruption affecting a single end user or non-critical system with no impact to the customer. - Those incidents that cause a disruption with no customer visibility and no risk to Citigroup's reputation or monetary stability.

Urgency is a measure of the effect of the incident on business deadlines. It reflects the time available for service restoration before the impact is felt or worsens significantly for the business. CTI uses the following Incident Urgency definitions:

Urgency Classification	Definition
High Urgency	- It is business hours and a peak transaction period as defined by the impacted business(es) - There is less than 2-hours before a time-sensitive, critical event is scheduled - Agreed availability targets are "high-availability" (i.e., no outages) targets and full redundancy is not operational.
Medium Urgency	It is business hours but not a peak transaction period as defined by the impacted business(es)

	- There are 2-4 hours before a time-sensitive, critical event is scheduled. - Agreed availability targets are less than "high-availability" but more than "best effort". Most SLA's would have availability Service Level Objectives (SLO) that fall in this category.
Low Urgency	- It is non-business hours as defined by the impacted business(es) - For 24x7 operations, it is during a period of very low transactions as defined by the impacted business(es). - There are more than 4 hours before a time-sensitive, critical event is scheduled - Availability targets are "best effort". Normally, this category would only apply to services where the business has made the conscious decision not to have back-ups or readily-available technical support because of either cost constraints or low importance of the service to the business.

After assessing the Incident Impact and Incident urgency (see below for definitions and examples), the following table can be used to calculate the Incident Severity:

Impact / Urgency	High Urgency	Medium Urgency	Low Urgency
High Impact	Severity 1	Severity 1	Severity 2
Medium Impact	Severity 1	Severity 2	Severity 3
Low Impact	Severity 2	Severity 3	Severity 3

For more details on Severity Definitions, please refer to: [Severity Level Assessment Matrix – 2D](#) provided in Appendix A.1.

The Page Express is a system that is used to send messages to alphanumeric pagers and handphones. The Page Express Guide can be found in CS Web Tools in CS Knowledge Management Web: <http://appcweb.citicorp.com/cgti-aspac/appc-units/csweb/>.

In the event where a particular incident requires COB plan activation, then escalation to the Continuity of Business / Disaster Recovery Offices will be required. Please refer to Continuity of Business Level 3 Procedure as documented in "[Continuity Of Business \(COB\) Procedure Manual](#)". (<http://cti.asiapacific.citigroup.net:8800/distops/cob.htm>)**

In the event where the issue constitutes a security risk to Citigroup, then the appropriate Security Incident Response Team (SIRT) process must be used. This will follow the Information Security Level 3 Procedure as documented in "[Information Security Procedure Manual](#)". (<http://cti.asiapacific.citigroup.net:8800/distops/infosec.htm>)

**** Where required, Regulatory Authorities (e.g.: MAS in Singapore) must be notified of occurrence of an incident where business operations are or will be severely disrupted or contingency plans have been invoked. Refer to Appendix C & D for relevant Circulars from Monetary Authority of Singapore and Hong Kong Monetary Authority.**

3.3.1 ESCALATION LIST

The Escalation list should carry the names of the alternate individuals who should be contacted in case the actual stakeholders are not contactable. The entire escalation process should have the contact numbers (Office and Residence), hand phone numbers, email addresses. This is to ensure

that the incident Escalation / Resolution process is not stalled due to the unavailability of the primary resolver group. RPMG has defined the alternate escalation grid up to level 2 only as the actual resolver group resides in between Level 1 and 2, whereas the Level 3 and 4 are for Senior Management awareness, hence alternate escalation for these levels are not applicable. For both BRDC and MRDC, in case the Level 3 and 4 members are not contactable, Problem Management Unit sends Mobile SMS for their awareness of the incident. Distribution Operations' Regional units and Country Heads have defined a similar escalation list for timely** escalation of incidents.

Besides verbal escalation and notification via phone, Page Express and E-Mail are other modes of escalation and notification.

CTI Asia Pacific and Business Aligned Technology Support groups are responsible to notify APPC Customer Service Helpdesk or local datacenters (BRDC / MRDC / In-country CTI support) of any organizational and support staff changes. APPC Customer Service Helpdesk or local datacenters are responsible to maintain their respective contact lists current.

The Escalation and Notification is documented in the "CS Call Management" section of doc. no. QM3/4/86 – Customer Services Guide. Problem Management Unit from BRDC / MRDC is responsible for escalations and notifications for India datacenter incidents. Regional Network Operations command center (formerly known as SINTOC) acts as an interface for CTI Asia Pacific Distributed Operations' incident escalations and notifications.

Refer to Appendix E for Incident Escalation procedure that positively identifies a crisis scenario.

3.3.2 ESCALATION AND NOTIFICATION

In the event of an online incident, the following escalation and notification shall apply. Refer to *Severity Level Assessment Matrix* provided in Appendix A.1 for severity classification for an incident.

- All Severity 1 incidents shall require timely** escalation/notification.
- A subset of Severity 2 incidents managed by CTI RPMG Incident Management Unit shall require timely** escalation / notification.
- Subsequent updates for Severity 1 and selected Severity 2 will be on an hourly basis until incident resolution. These updates can be provided via Conference Bridge assigned for incident resolution.

For the escalation time-lines, refer to [Appendix C Incident Escalation](#) of *CITMP Level 2 Problem Management Process Standards (Version 4.0)*.

****Timely:** Implies that an event occurring at a suitable or opportune time; well timed. (Source: *American Heritage Dictionary*).

RPMG Incident Management Unit escalates all qualifying incidents with known business impact to CTI and respective Business Management. These escalations will be performed anywhere from 15 to 45 minutes from the time incident is reported to RPMG Incident Management Unit. Escalations are performed once all pertinent information is available.

3.3.3 ESCALATION AND NOTIFICATION TO ENGINEERING SUPPORT

In addition to the above escalations, for technology infrastructure incidents (Sev 1/ selected Sev 2), if the resolution can't be determined after 60 minutes, appropriate CTI Engineering support may be contacted for further assistance in incident resolution.

3.3.4 INCIDENT ESCALATION AND NOTIFICATION (SPECIAL SITUATIONS)

There may be times when escalations and notifications need to be performed even though there is no impact to service delivery. Examples include: hot-swap of disk devices, hardware components, manual workarounds to bypass error conditions etc.

Staff working on situations like these (where an infrastructure item is involved) need to escalate immediately via their Unit Manager to their Group Head (2-downs of CTI AP Head), who in turn will make an assessment for further escalations to Regional Problem Management Group as well as respective CTI AP SMT members.

Refer to Appendix F: [Excerpts From Escalation Procedure for CitiGroup Services \(Japan\)](#) on situations that require escalation for CSJ.

3.3.5 NOTIFYING COMPLIANCE ON INCIDENTS REPORTED TO REGULATORS

Singapore CCO, Singapore Country Compliance, Regional Asia Pacific Compliance (CIB and GCG) and CTI Global Compliance and Risk Management (GCRM) Head must be notified of all incidents reported to regulators. The Head of CTI AP Regional Compliance & Risk Management shall communicate all such notifications.

3.3.6 WORK AROUND DURING INCIDENT RESOLUTION

In the course of incident handling and resolution, there may be a need to do a workaround to recover services in a timely manner.

Definition:

A workaround is a method used temporarily for resolving incidents when the usual or planned method isn't working. Once an incident is permanently fixed, the workaround is abandoned.

Work-around process:

When a critical service encounters a disruption and a decision is required between making the service available and a permanent resolution, Support Staff should use the workaround process detailed below.

1. Determine need for work-around

- Support Staff needs to diagnose the incident and determine the various options available, either workarounds or fix.

2. Escalation to supervisor

- Support staff will then escalate to his supervisor and discuss the various options.
- Where other support streams are required, they will be brought into the discussions.

3. Decision Making

- They will perform due diligence risk impact analysis before deciding on the options for incident resolution. The team will determine if an escalation to group Head is necessary. If the escalation is not necessary the concerned group head is be notified in due course.

4. Document workaround

- The workaround steps should be documented in the Incident Ticket.
- The Risk (due diligence) Analysis should also be documented.
- The following information will constitute the documentation:
 - Incident Description
 - Platform/Services Impacted
 - SME/Supervisor Names
 - Options Available
 - What are the options
 - Risk/impact analysis of each option

- Time to recover services/Risk-Impact of actions
- Proposed Workaround/Fix
- Description on proposed normalization
- Validation and signoff by Group Head

5. Update in next business day's Problem Management Meeting.

3.4 INCIDENT HANDLING

The assignee or support group is responsible for the following:

- Investigation and Diagnosis of the cause of incident
- Resolution and Recovery of the incident
- Closure of the incident

The [Incident Management Playbook](#) describes in detail the process flow from the time the incident is reported till the incident is closed.

3.4.1 CLASSIFICATION & INITIAL SUPPORT AND INVESTIGATION & DIAGNOSIS

Support groups must refer to their own "Knowledge Base" which includes past tickets listing, vendor documents and manuals as well as internal websites. Incident Managers when escalated performs Incident Classification to determine the severity level and ensure the correct support groups are engaged to perform Investigation and Diagnosis.

3.4.1.a KNOWN ERROR DATABASE

During the Incident Initial Support or Investigation & Diagnosis process, Incident Managers should attempt to match the database of Known Errors in order to minimize the Mean Time to Repair (MTTR).

The Known Error database is maintained by the Regional Problem Management Group to support this "matching" of incidents that occurred in the past that were either closed with unknown root cause or with a known root cause without a permanent resolution. In either case, the workaround documented would be used if deemed appropriate for an Incident that is under purview.

The typical Known Error list maintained by Regional Problem Management Group contains the archive of all RPMG managed incidents without permanent resolution for which workarounds are known. The columns maintained for each such incident is typically:

- Impacted Country
- Impacted Service
- EMS / VT references
- Date & Time of first Incident Occurrence
- Date & Time of last Incident Occurrence
- Description of the Incident / Problem
- Known Workaround Steps to bypass the incident / problem
- Root cause (if known)
- Permanent Fix (if root cause is known)
- Status of Permanent Fix (if root cause is known)
- Responsible Resolver Group for Permanent Fix (if root cause is known)
- Target Date of Permanent fix (if root cause is known)

The respective Resolver Groups are responsible to provide timely and periodic updates that help Regional Problem Management Group to maintain the steps of known workaround and status of the permanent resolution.

3.4.1.b INVESTIGATION & DIAGNOSIS BY SUPPORT GROUPS

The individual and/or support group assigned with the incident must use the following procedure for incident Investigation and Diagnosis:

- Logon to the VT system and review the pertinent details in the ticket(s).
- Call Customer Services (for APPC incidents) and / or the reporter (for MRDC/BRDC or Distributed Operations) of the incident to get additional information on the incident.
- Logon to the appropriate systems and review system logs and dumps.
- Check with business coordinator whether there are any critical milestones such as business cut-off times.
- Consult appropriate subject matter experts as well as the relevant documentation (including relevant Work Instruction Manuals).
- Record the findings in the ticket once the incident Investigation and Diagnosis is completed.
- Review VT or other documentation if similar incident was previously reported and if there is an existing action plan to address the incident.
- For incidents that cannot be assigned to the appropriate Resolver, the engineer is escalated to the Team Leader(s) for performing next level incident determination.
- The lead engineer(s) are to track the incidents assigned to their group(s); the Duty Incident Manager can escalate to the product / domain manager / Heads of the Resolver group for prompt attention.
- The Resolver shall be responsible for updating the status and necessary information in the ticket on the Ticketing System until the incident is resolved and closed with appropriate root cause and preventive action information.
- If the Resolver assigned cannot resolve the incident due to dependencies with other Resolver Groups or the incident is not within their defined scope (the incident requires another group to resolve the incident), the Resolver can Login to VT to reassign the ticket to another Resolver Group.
- For Virtual Tech ticket reassign - Virtual Tech system will notify Resolver group through email or SMS.

3.4.2 RESOLUTION AND RECOVERY

The assignee or support group shall be responsible for providing the incident resolution. The initial solution provided at this stage could be a system / application recovery, a bypass or a temporary (Temp Fix) solution. The objective is to minimize downtime and to restore Production Services expediently.

The individual and/or support group assigned with the incident must use the following procedure for determining the course of action to take to recover the incident:

- Once the incident investigation and diagnosis is completed, develop appropriate action plan to recover the incident.
- Other stakeholders such as application support personnel, network infrastructure personnel should be involved where necessary to develop the recovery plan.
- Determine whether the recovery will be in the form of a temp-fix or a permanent resolution.
- While determining the recovery options (permanent vs. temp-fix), factors such as business cut-off times, time required to apply the permanent fix, time required to do analysis of system logs / dumps etc. must be considered.
- Execute the recovery plan to recover the services expediently.
- Where the bypass results in disruption of services, guidelines outlined in the above section on "Escalation and Notification" will be adhered.
- A follow-up with the relevant resolver group is done for the permanent fix and restoration to original status.
- All the Severity 1 and selected Severity 2 ageing tickets are discussed in the periodic problem management / review meetings. It will be the responsibility of the Support group to ensure that temporary fix is regularized when the permanent fix is applied.

- Incident notification will be continued where a prolonged degradation in services continues as a result of the bypass. All bypass actions are tracked in VT ticketing system, when the environment is restored to its original state.
- RPMG ensures that permanent fix is applied to a particular incident through an incident tracker reviewed periodically with Resolver Groups.

The RPMG - Incident Management Unit records an incident in Known Error database if the temporary fix / workaround is available but permanent fix is unavailable or not implemented. All active temporary fix / workarounds in the Known Error Database are reviewed and maintained periodically for currency with inputs from respective support teams.

3.4.3 INCIDENT CLOSURE

The individual and/or support group assigned to the incident must use the following procedure for permanently resolving the incident for closure:

- If a temp-fix had been applied earlier, the permanent fix must be applied before the incident is considered closed.
- Once a permanent fix had been applied, the incident resolver needs to check with the business user to review and validate that the reported incident has been fixed permanently.
- Respective resolver groups should update the resolution information in the ticketing system.
- RPMG should ensure the pertinent resolution & root cause information is kept up-to-date in the EMS created for Severity 1 and the subset of Severity 2 incidents managed by RPMG are tracked to closure.

3.4.4 INCIDENT ESCALATION LOGS

Incident Management Unit of Regional Problem Management Group is responsible to maintain an Incident Escalation Log for all Severity 1 incidents that the unit managed.

Incident Escalation Logs (forms) are maintained by the RPMG Duty Incident Manager who managed the incident and reviewed and signed-off by Incident Management Unit Head or RPMG Head. The following information is captured as part of the Incident Escalation Log:

- Incident summary
- Relevant ticket reference numbers (VT / EMS / Infoman)
- Date and Time of the incident start and end time
- Escalation details for various CTI Management, Resolver Teams and relevant Business management. (Person escalated, Time and mode)
- Incident timeline / chronology of events to resolution
- Additional MTTR information (Incident detection)
- Details of manual workarounds that require regularization (if applicable)
- Details of change references (if applicable)

A template for Incident Escalation Log is given in Appendix G.

3.5 PREVENTION AND CONTINUOUS IMPROVEMENT

3.5.1 INCIDENT & PROBLEM MANAGEMENT BY REGIONAL PROBLEM MANAGEMENT GROUP

In order to prevent incidents from recurring again as well as continuously improve the incident management function, Regional Problem Management Group takes the following tracking and control measures:

- Post Mortem for all severity 1 incidents

- Management Reporting
- Service Availability and Reliability (SAR) process for Asia Pacific GCG business (including India)
- Appropriately managing the EMS and VT tickets
- Measuring and managing the MTTR performance
- Management Reviews with CTI Management
- Monthly Scorecard / Trend Analysis reports for APPC Datacenter
- Weekly TI Operations committee meetings O&T / Technology organizations
- Periodic analysis of problem trends with CTI resolver group / domain managers to take appropriate corrective action and improve service availability

RPMG will track all service level deviations and periodically review the issues involved with respective support groups. Corrective action to be instituted based on the reviews, will be documented and tracked.

Refer to Appendix 8 of [Appendixes & Forms for Distributed Operations](#) for Incident & Problem Management forms and report templates specific to CTI Asia Pacific Distributed Operations analysis.

- Aging activity reports should be produced to ensure management oversight of the resolution process.
- Service Level monitoring reports that measure progress continually to reduce incidents and defects for all severity level.
- Periodic performance review of service levels to identify performance gaps and identify and take appropriate corrective actions.

3.5.2 BRDC

In order to prevent incidents from recurring again as well as continuously improve service availability through incident & problem management, BRDC uses a number of mechanisms:

- Post Mortem for all severity 1 incidents
- Weekly Problem Management meetings
- Tracking all the Severity 1 and selected Severity 2 incidents reported in EMS to closure with appropriate root cause and permanent fix
- Publish monthly SLA tracking report which measures all Incident resolutions against the defined SLA for incident resolution for taking actions on any identified trends/gaps
- Publish Weekly Problem Management report and review with management
- Report Monthly Trend Analysis
- Participate in Monthly Incident Review with branches.

3.5.3 MRDC

Following are the key Problem Management Unit functions to improve service availability for services offered in MRDC:

- A process to review unit performance against agreed service levels must be performed at least monthly and must include steps taken when targets are missed.
- MRDC Problem Management Unit keeps a close track of all the chronic incidents in the the unit managed.
- Based on the ageing of the incident, MRDC Problem Management Unit initiates projects with Project Office, Business, Distribution Operations etc. to mitigate the chronic incidents.
- Report to Business and Quality office on a monthly metrics on SLA metrics of MRDC.
- All the Severity Level 1 and selected 2 incidents are reported in the EMS and reviewed with Regional and Global Problem Management review meetings.
- The Post Mortem Reports for Severity 1 incidents are also circulated to the Senior Business Management and related stakeholders.
- Additionally, a daily "Incident Report" is sent to the GCG-CBM and all the stakeholders for awareness.

3.6 POST MORTEM REPORT

All major service disruptions (severity 1 incidents) shall be reported by a Post Mortem Report. In addition, RPMG shall determine service disruptions for which a Post Mortem Report is required (depending on the nature and severity of an incident, business and regulatory requirement e.g. reporting to FSA in Japan).

The Post Mortem Report Owner is generally from the group/unit responsible for the incident resolution identified through the root cause. In cases where root cause is unknown, the Post Mortem Report Owner shall be determined by the RPMG Head in consultation with other Group/Unit/Domain heads. The Post Mortem Report Owner is either the Group Head/designate and shall be responsible for the following:

- Working with other support units to develop an action plan to prevent recurrence of the incident
- Quality and accuracy of the report
- Develop, publish, review and distribute an interim Post Mortem Report, if required
- Obtain concurrence from respective Supervisors if Action Items involve staff from the various groups/units/domains
- Submit final Post Mortem Report as soon as possible i.e. where all pertinent details are available.

The Post Mortem Report Owner shall submit the report to RPMG for validation.

Once approved by the one of the CTI Director or designate, RPMG shall release the Post Mortem Report for external circulation. The interim and final post mortem reports are generated from EMS.

A Post Mortem Report shall contain all the pertinent information related to the incident including the following:

- Name of the Resolver / Senior Manager who reviews and approves the report
- Date the post mortem report is published
- Technology failure start and end date with time
- Customer impact start and end date with time (if applicable)
- Caption / Subject covering the summary line of the incident and respective VT / EMS references
- Description of the incident - Executive Summary covering high-level description of what happened
- Impact of the incident – i.e. countries / services affected
- Resolution – description of the incident was resolved
- Root Cause – the primary reason for the service disruptions
- Corrective Actions – actions taken to bring back the service in operation
- Action Plan – a plan containing short and long-term activities that will prevent the re-occurrence of the incident. The plan should cover the activity description, responsible group/unit as well as target date for implementation
- Detailed Background –Chronological event – narration of events leading to the incident

Upon identification of root cause of the incident and closure of permanent corrective actions by respective support groups, the Known Error Database is updated so that the temporary fix / workaround could be discontinued.

Handling Post-Mortem Reports

- A Post Mortem Report shall be in “Open” status when published.
- The Post Mortem Report Owner in consultation with RPMG shall determine the recipients of the Post Mortem Report.

- A Post Mortem Report shall be "Closed" only when the activities in the action plan are carried out and the incident do not re-occur during the following four weeks especially for severity 1 incidents.
- The RPMG shall act as a repository of all Post Mortem Reports. The RPMG shall keep an up-to-date list of all Post Mortem Reports and their status.
- The RPMG shall perform monthly reviews of all Action Items with respective Group Heads or designate to obtain progress updates for timely closure.
- The RPMG Head shall be responsible for reviewing this procedure once in six months so that the process could be continuously improved.

A Post Mortem Report Tracking is prepared and weekly updated to facilitate the tracking of Post Mortem Reports as well as tracking of action items. It shall contain the following:

- EMS reference no. (*)
- VT reference no. (*)
- Date the Incident happened (*)
- Incident Summary (*)
- Date when the Interim Post Mortem Report was sent to Business (*)
- Interim Post Mortem Report (*)
- No. of days the Post Mortem Report was sent from the date the Incident happened
- Date when the Final Post Mortem Report was sent to Business (*)
- Final Mortem Report (*)
- Expected Date of Action Item/s Closure
- Actual Date of Action Item/s Closure
- Yes or No to indicate if corresponding VT ticket was updated
- Date when the EMS entry was closed
- Average number of days to send Post Mortem Report
- Percentage of Post Mortem Reports, which were sent within the established goal.

The Post Mortem Report Tracking will be published and only information marked with (*) will be made available in the RPMG website.

Maker/Checker Procedure for Post-Mortem Reports

Post mortem reports are published for all Severity 1 incidents recorded and tracked in the Executive Monitoring System (EMS). CTI AP Regional Problem Management Group follows a Maker/Checker procedure to ensure the quality of post-mortem reports published through the EMS meets the Guidelines established. Two standard EMS tasks are raised with standard verbage once the incident is Resolved in the EMS.

- Task 1: Complete post mortem and contact the verifier for approval
 - Assigned to: Resolver Senior Manager OR member of Regional Problem Management Group other than the person who created the EMS entry.
 - Target Completion Date: 3 working days from the time an incident is resolved by CTI. (5 working days for non-CTI resolved incidents)
- Task 2: Review and send Post Mortem Report
 - Assigned to: Resolver Manager (if the Resolver Manager has EMS system write access) OR member of Regional Problem Management Group other than the person who wrote the post-mortem report.
 - Target Completion Date: 3 working days from the time a incident is resolved by CTI. (5 working days for non-CTI resolved incidents)

Refer to the guidelines in [Post-mortem Report Template](http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/csweb/appcpmo/post_mortem_reports/PostMortemReportTemplate.doc) document as referred to in Appendix A.2 (http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/csweb/appcpmo/post_mortem_reports/PostMortemReportTemplate.doc)

Note: For all post-mortem reports related to Japan services, RPMG is responsible to request resolvers to provide necessary evidences when post-mortem action items are completed. These

evidences are centrally filed by RPMG and provided to Japan Business, TI Control and/or Auditors as and when requested. Acceptable evidences include valid request numbers in Infoman, ePJMR and eService Request system. Where the valid request numbers could not be provided, evidences such as procedural updates, email communications will be provided.

3.7 PROBLEM MANAGEMENT METRICS

3.7.1 METRICS REPORTING FOR CTI

Regional Problem Management Group uses the data from VT and EMS to generate metrics and reporting.

In addition to the above, following Management reporting is also performed for Regional Problem Management Group managed incidents:

S/N	REPORT	SOURCE	SUGGESTED TIMINGS	RECIPIENT
1)	Post Mortem Report (for incidents managed by RPMG)	- Subject Matter Experts (SMEs) - VT - EMS	- Interim report – sent within one (1) day after the incident happened (subject to availability of pertinent information) - Final report – sent within five (5) days after the incident happened (subject to availability of pertinent information)	- Business - Workgroup / Domain Head - Concerned Support Staff - EMS Compliance Officer
2)	Weekly Problem Management Scorecard for Datacenter	Virtual Tech	- Interim data extraction / Interim report – done / sent on the 1st working day of the following week - Final data extraction – done one (1) day after Interim report was sent - Final report – sent within two (2) days after the final data extraction	- Workgroup / Domain Heads - Unit Heads - Concerned Staff
3)	Weekly Major Outages Report (for incidents managed by RPMG) Weekly Online Delays Report for Datacenter	- EMS - Daily Operations Report on Batch Issues - Page Express - VT - Service Level Agreement/s	Sent before 1st working day of next week	- TI AP Operations Committee - Workgroup & Domain Heads - GCG O&T, ATO Heads - TI Engineering Managers - APPC Workgroup - EMEA O&T
4)	Weekly Incident & Problem Report for Japan (incidents managed by RPMG)	EMS	Sent before 4th working day of next week	- Japan TI Controllers - CTI Asia Pacific Client Management - CTI Asia Pacific Compliance Management and Japan Management oversight team
5)	Weekly Incident &	EMS	Sent before 1st working day of next	GWM

S/N	REPORT	SOURCE	SUGGESTED TIMINGS	RECIPIENT
	Problem Report for GWM (incidents managed by RPMG)		week	Technology Management - Knowledge Center - CTI Asia Pacific Client Management
6)	Monthly Problem Management Scorecard (APPC) NOTE: Action items identified from Quarterly and Monthly Problem Management Reviews will be tracked and published in the Monthly Scorecard.	- EMS - VT - Post Mortem Report Tracking - SMEs	- Interim data extraction / Interim report – done / sent on the 1st working day of the following month - Final data extraction – done one (1) week after Interim report was sent - Final report for analysis – sent within one (1) week after the final data extraction - Problem Management Review – done every last Thursday of the month	- Workgroup - Unit Heads - Concerned Staff - TI AP Operations Committee - Workgroup - GCG O&T, ATO Heads - TI Engineering Managers
7)	APPC Problem Review meetings during the week	- VT problems notified to Management through Page Express logs - EMS tickets - Online delays	Every week day	APPC Daily Problem Review Meeting group consisting of APPC group heads and Unit heads
8)	Review of Scorecard with CTI Management	- EMS, VT - Weekly scorecards - Analysis from CTI resolver groups	Quarterly	CTI (APPC) group heads and Unit heads

3.7.2 WEEKLY / MONTHLY PROBLEM MANAGEMENT SCORECARD FOR APPC

The Regional Problem Management Group is responsible for conducting monthly reviews with APPC Workgroup together with all APPC units. A weekly and monthly scorecard at unit level will be generated on the following to support the management oversight:

Charts by Root Cause Type

Gives a breakdown of incidents by Root Cause Type and identifies areas which offer the greatest potential for improvement.

Charts by Root Cause Component

Gives a breakdown of incidents by Root Cause Component. This is a more detailed classification of the incident and highlights the actual cause of the incident.

Ageing Ticket

Shows the monthly performance of “Open” Status VT tickets by Resolver Group.

Incident Ownership

The breakdown and assignment of incident by Resolver Groups. The data can be broken down further by Incident Status and Root Cause, if so required.

MTTR Performance

Shows the Work around time for all VT tickets.

The objective of providing scorecard to individual units is to generate management awareness and to accelerate corrective actions to maintain VT.

VT Tickets for Emergency Changes

Shows VT tickets related to Emergency Changes will be included in the Monthly Scorecard. Change Management will provided the VT tickets reference number.

3.7.2.a Generating Weekly / Monthly Problem Management Scorecard for APPC

RPMG uses Virtual Report 2.0 to generate the reporting from VT database which are then exported to Excel.

The period that the reports are generated is from Monday to Sunday of the previous week for the weekly report and from the 1st day to the end of the month for the monthly report. It is sent out to the various APPC Support Groups.

The reports sent out will consist of the following:

- a) All VT tickets closed during the week / month
- b) Root Cause Type / Component breakdown
- c) MTTR for all closed tickets for the week / month
- d) Ageing VT tickets.
- e) List of VT tickets related to Emergency Changes monthly

The data exported to Excel spreadsheet will be used to gather the necessary information for generating the weekly report as well as the Scorecard. A monthly Scorecard is also generated. The process is similar to the weekly but the period selected in the search criteria for the VT extraction is by month.

3.7.3 WEEKLY PROBLEM MANAGEMENT REPORT FOR CTI AP

Regional Problem Management Office will document all significant incidents/major outages and on-line delays for the week. All notifications that were sent out to relevant MANAGEMENT GROUP via Page Express, together with the relevant VT & EMS tickets are reviewed.

The Major Outages report shall include the following information:

Part 1: Highlights and Metrics

- A brief update on Weekly outages and progress on various initiatives undertaken by Regional Problem Management Group.
- Summary of Reporting statistics

Part 2: MTTR Metrics

- A break-down of time to recover each Severity 1 incidents reported for the week

Part 3: Action Items Tracking status

- Summary of Open Action items from Weekly TI Operations committee meeting
- Summary of Closed Action items from Weekly TI Operations committee meeting

Part 4: Summary of Incidents

- Weekly summary of Severity 1 and Severity 2 incidents by week / month

Part 5: Heat charts showing the summary of the week's incidents for Datacenter and Distributed Operations

Part 6: Severity 1 Incidents for the week

- EMS ID
- Start and End Time
- Duration
- Description
- Business Impacted
- Country Impacted
- Service/ Customer Impact
- Customer Impact Begin Date/Time
- Customer Impact End Date/Time
- Customer Impact Duration
- Resolution
- Root Cause Comment
- Long Term Solution
- Resolver Name, Manager

Part 7: Severity 2 Incidents for the week

This list is filtered for Severity 2 incidents for the week like that of columns appears in Part 6.

Part 8: Past Severity 1 incidents without Root cause findings

This updates for past weeks' Severity 1 incidents for which the root cause was Under Investigation is listed. The list has similar columns as in Part 6.

Part 9: Past Severity 2 Incidents without Root cause findings

This updates for past weeks' Severity 2 Incidents for which the root cause was Under Investigation is listed. The list has similar columns as in Part 6.

Part 10: Online SLA Delay reports

The On-line Delays report shall contain the following information:

- Date
- Country
- Service
- Business
- Region
- SLA Time (SST)
- System Uptime (SST)
- Duration
- VT Number
- Reason for Delay.

Part 11: Year to date charts

- Severity 1 YTD chart by Resolver, Root cause, Biz, Region, Change-related and TI/Non-TI resolved incidents.
- Severity 1 YTD chart by Resolver

Part 12: VIP Ticket Analysis

- VIP raised VT tickets are monitored and tracked on a daily basis. The statistics are published as part of the weekly report for CTI Management review.

In addition to the weekly reports mentioned above, a list of outstanding Post Mortem Action Items from EMS would also be published.

3.7.3.a RPMG Website

All reports published by RPMG are uploaded in the RPMG website, which can be accessed at the following URL:

<http://appcweb.citicorp.com/cgti-aspac/appc-units/csweb/appcpmo/index.htm>.

Screen Shot of the RPMG Website:



RPMG Home	The default page.
PMO Projects	Contains RPMG Initiatives/ Special Undertakings.
Post Mortem Reports	Contains Incident Report Summary, and Monthly Post Mortem Report Tracking, which includes the interim and final Post Mortem Reports sent by RPMG to Business. The Incident Report Summary is updated on or before 15 th day of the following month. The Monthly Post Mortem Report Tracking is published within 1 st week of the following month while subsequent updates will be published every Monday.
Scorecards	Contains Weekly and Monthly APPC Scorecards. The Weekly Scorecard is published once it is available, which should be within two (2) days after the final data extraction. The Final Monthly Scorecard (i.e. version containing the final analysis submitted by different groups/units) is published within one (1) week after the Monthly Problem Management review.
On-line Delays Reports	Contains weekly and consolidated reports on On-line Delays. The weekly report and the updated consolidated report are published

	every 1 st working day of the following week.
Major Outages Reports	Contains reports on Major Outages. The report is published every 1 st working day of the following week.
Reports / Metrics	Contains Problem Management Metrics and management review reports.
Reference Documents	Contains links to CITMP Level 2 standards and Level 3 procedures.
Consolidated Japan Online Availability Report	Archive of Japan Daily Health check reports.

3.7.4 SERVICE AVAILABILITY AND RELIABILITY

A monthly SAR Review Meeting for Asia Pacific GCG business is conducted by APPC. The Meeting is attended by representatives of various stakeholder groups responsible for providing technology services to customers. This includes:

Regional Technology Head	Sponsor
APPC Director (or his/her designate)	Chairperson
APPC Representatives	Data Center
ATO Representatives	Application Services
Distributed Operations Regional Team Representatives	Network services (WAN)
Distributed Operations Local Team Representatives	Local Network Services
Country Technology Heads	In-country services

The purpose of the review is to improve service availability and reliability by ensuring all technology service providers regularly and methodically.

- Review levels of service across touchpoints.
- Identify 'root-causes' of reported incidents.
- Identify frequent 'root-causes' and take appropriate action to reduce them.

Refer to the ITO [Service and Reliability Framework](http://ato.citicorp.com/Update/SARFramework2.1.doc) for detailed procedure.
(<http://ato.citicorp.com/Update/SARFramework2.1.doc>)

3.7.5 MANAGING VT TICKETS

All automated VT tickets are created as severity 2. This is necessary for escalation and notification to take place. A majority of these VT created are a result of pro-active monitoring that has been put in place. As a result of this, not all VT tickets created are actual incidents. It is therefore the responsibility of the resolving groups to assign the VT tickets to the correct severity level.

Pro-active monitoring is implemented to ensure that a situation is attended to before it becomes an incident. Some examples of proactive monitoring include system health check, file transfer for Batch Processing and threshold monitoring. CTI Asia Pacific resolver groups use VT tickets as a record for follow up action by the Support staff. As a result of this, a large number of VT tickets created are "Non-problem" tickets.

3.7.5.a Handling "Non-Problem" Tickets

All VT tickets with the following Root Cause Types / Components should be closed as "Non-problem" tickets.

Root Cause Tier 1 (Type)	Root Cause Tier 2 (Component)	Description
Application Software	Alert	This is a pre-defined condition to alert applications before it becomes an incident.
Technology Operations	Data Center Maintenance	This is a scheduled Data Center Maintenance activity.
Technology Operations	Distributed Computing Maintenance	This is a scheduled Distributed Computing Maintenance activity.
Health Check	Health Check	This is a pre-defined monitoring of critical components, which could potentially lead to a incident if not attended to.
Requests	(All Root Cause Tier 2)	This is a client request, which is not an indication of an incident.

Duplicate VT tickets are considered as a “Non-problem” ticket for the purposes of metrics reporting.

3.7.6 MANAGING MTTR PERFORMANCE FOR DATACENTER

3.7.6.a Overview

MTTR (Mean Time to Customer Outage) is an important component in the incident resolution process. This is the time taken for a incident to be “tempfix” or “resolved”. It is calculated from “Tech Failure Begin Time” to “Tech Failure End Time”. The incident resolution timing for all tickets are captured on a weekly and monthly basis. All incidents resolved beyond the standard resolution time are to be reviewed by the respective Unit Managers.

3.7.6.b MTTR Standard

Guidelines for minimum general performance service levels are as follows:

	STANDARD
Severity 1	4 Hours (240 minutes)
Severity 2	8 Hours (480 minutes)
Severity 3	24 hours (working hours*)

* - “Working hours” refers to the normal office hours.

3.7.6.c MTTR Performance

RPMG will review the resolution timing for all VT tickets. A report from VT will be generated and will include the following:

- Number of tickets resolved within MTTR standard
- Number of tickets not resolved within MTTR standard (Over standard)
- Over-standard MTTR for APPC (in percentage)
- Extraction of all over standard VT tickets to be sent to each group.

In order to ensure that the problem management metrics captured and reported on MTTR are accurate, the following must be done to ensure that the correct incident resolution timings are captured in VT:

- Ensure timely resolution of VT tickets by resolver groups
- Ensure that the resolver group maintains the correct severity level is reflected for the incident being resolved.

3.7.7 MANAGEMENT REVIEWS FOR CTI

The CTI Asia Pacific Management actively participates to review the problem management metrics as well as post mortem information of major incidents. The following are the management reviews:

- APPC Workgroup reviews on a monthly basis the Problem Management scorecards.
- The RPMG Head and other CTI Asia Pacific members attend the weekly Technology Operations Review (TOR) meetings and report on major incidents encountered during the previous week.
- The CTI Asia Pacific Management and other key officers participate in the service review meetings with APPC customers wherein the incidents affecting that particular customer group is analyzed and reported.
- Weekly reports and incidents are reviewed with Distributed Operations Country and Domain Heads on a weekly schedule
- Weekly outages, delays and metrics are reviewed with CTI AP Operations Committee members on a weekly basis

3.8 COORDINATION

3.8.1 APPC

The tracking and controlling of all incident status are done within VT. This includes the ownership of the incident at different stages of the resolution process.

The Roles and Responsibilities mentioned in this document, together with the tracking mechanism within VT will ensure that all incidents are moved in a timely fashion from one activity to the next. The RPMG ensures that the VT tickets are properly assigned and review when tickets are not moving in a timely fashion.

3.8.2 BRDC

The tracking and controlling of all incident status are done through VT. This includes the ownership of the incident at different stages of the resolution process. VT has a functionality wherein a incident ticket can be assigned to a particular resolver group and if the incident ticket is incorrectly assigned, that particular resolver group can in turn assign it to the other support group. All these activities get logged on VT. The resolver after proper resolution shall put the appropriate comments in VT and inform the user accordingly.

BRDC Problem Management Unit holds weekly meetings with the resolver group to ascertain the root cause analysis and discuss progress on OPEN issues. Monthly, the Problem Management Unit publishes an overall "Open/Close Issues Report" with long term and short term action plans and probable target dates for resolution to the Senior Management.

3.8.3 MRDC

All groups must monitor their incident queues in a timely manner to ensure proper tracking, control and resolution of incidents. Heightened attention must be applied to Severity 1 and 2 incidents. MRDC Problem Management Unit ensures strict vigil and necessary tracking for incidents pertaining to these two categories. Through EMS, the MRDC Problem Management Unit keeps track of all individual Problems/Incidents to identify and document all incidents and their resolution times within/beyond the agreed timelines as per SLA. The Business is kept informed by mail of the status on a fortnightly basis.

MRDC Problem Management Unit holds monthly meetings with the resolver group / Project Office to ascertain the root cause analysis and discuss progress on OPEN issues. MRDC Problem Management Unit also prepares the incident ageing analysis report to track progress on incident resolution. Weekly, the MRDC Problem Management Unit publishes an overall "Open/Close Issues Report" with long term and short term action plans and probable target dates for resolution to the Senior Management.

3.8.4 DISTRIBUTED OPERATIONS

For all Severity 1 and high-severity 2 tickets, the problem management group shall monitor the trouble tickets status to ensure resolver group resolve the incident in timely manner. The resolver group must ensure swift hand over of the trouble ticket to next resolver group after confirming it has been assigned wrongly.

All Severity 1 incidents must be entered in the EMS (Executive Monitoring System) to identify long-term incident elimination, as well as to report to senior operational and business management.

In addition, for complex incident involving multiple resolver groups, the Problem Management Group shall conference all the necessary resolver groups to jointly investigate and resolve the incidents. Their unit shall act as a facilitator throughout the call and escalate to next level manager, if required

A. APPENDIX – GENERAL GUIDELINES

A.1 SEVERITY LEVEL ASSESSMENT & EMS REPORTING GUIDELINES

Incidents reported in EMS will generally adhere to following guidelines:

All Severity 1 incidents and Severity 2 incidents are reported in EMS. Quick reference guidelines for Severity Level Assessment is provide below. An incident with definition that does not match the SEV1 and SEV2 classification as below is not reported in EMS.

Instructions

Please keep this matrix readily available for reference when incidents occur. This matrix is a reference document and not a form that must be completed. Please note that this matrix does not replace sound professional judgement. For example, if an incident does not appear to be covered, severity levels should be assigned on the side of caution (i.e., higher rather than lower).

Step 1 - Assess Incident Impact

Impact is the effect that an incident has on the users of the IT service or their organization. Read the questions down the left side of the matrix. Then read across and check those answers that most closely apply to the incident. After reading all of the questions, note the highest check mark as the Impact for the incident.

Question	High	Medium	Low	None
What is the impact on external customer touchpoints? <u>Customer Definition</u> - Individuals or businesses external to Citigroup to whom Citigroup provides services <u>Touchpoint Examples</u> : Applications, Services, ATM's, kiosks, branches	☐ Customers <u>cannot use</u> a touchpoint and there is <u>no close-by alternative</u> . <u>Examples</u> : inaccessible Citigroup portals, inaccessible online banking or trading services, multiple ATM's out in an area OR ☐ Customers experience <u>slow</u> touch point response. <u>Examples</u> : slow Statements on Line, slow Citibank on Line, delays in call center services	☐ Customers <u>cannot use</u> a touchpoint but there are <u>close-by alternatives</u> . OR ☐ Customers <u>intermittently cannot use</u> a touchpoint. OR ☐ Customers had to use an alternative touchpoint and failover was not seamless.	☐ Customers have to use an alternative touchpoint and <u>failover was seamless</u> .	☐
What is impact on facilities? <u>Strategic Facilities Examples</u> : data center; trading floor; network operations center; call center; major branches (consumer, private bank or private client), etc.	☐ <u>Cannot use a strategic facility</u> . OR ☐ <u>Cannot use a smaller branch</u> and there is <u>no close-by alternative</u> .	☐ <u>Cannot use part of a strategic facility</u> but mission-critical activities can occur. OR ☐ <u>Cannot fully staff a strategic facility</u> but <u>essential staff have access</u> . OR ☐ <u>Restrictions exist on when</u> staff can enter or leave a strategic facility.	☐ <u>Cannot use a smaller branch</u> but there is a <u>close-by alternative</u> .	☐
What is the impact on internally-used applications / services? <u>Note</u> - Obtain information about mission-critical and non-mission critical application or service from the SLA's for the impacted businesses or during the course of incident handling	☐ <u>Internal users cannot use a mission-critical</u> application or service. <u>Examples</u> : major internal application outage, mail server outage, major site PBX outage, gateway outages, file/print server outages, Internet inaccessibility, International Direct Dialing disruption. OR ☐ Degrades in an application or service <u>visibly impacts</u> the quality of service internal users provide to <u>customers</u> .	☐ <u>Internal users intermittently cannot use a mission-critical</u> application or service. OR ☐ <u>Internal users have slow response on a mission-critical</u> application or service. OR ☐ <u>Internal users had to use a backup to a mission-critical</u> application or service and <u>failover was not seamless</u> . OR ☐ <u>More than 5 internal users cannot use a non-mission-critical</u> application or service	☐ <u>Internal users intermittently cannot use a non-mission critical</u> application or service. OR ☐ <u>Internal users have slow response on a non-mission critical</u> application or service. OR ☐ <u>Internal users had to use a backup to a mission-critical</u> application or service and <u>failover was seamless</u> . OR ☐ <u>1-5 internal users cannot use a non-mission critical</u> application or service	☐
What impact is there on information security?	☐ It is a major and/or broad-based external attack on Citigroup technology <u>Examples</u> : significant virus outbreak, major worm outbreak OR ☐ It results in <u>an enterprise-risk SIRT</u> . OR ☐ It is a firewall-caused Business-to-Business (B2B) link service outage	☐ It results in a <u>less than enterprise-risk SIRT</u>		☐
What impact is there on Citigroup reputation? <u>Example</u> : probproc_v	☐ There is a high probability of significant damage to Citigroup's reputation			☐

Step 2 - Assess Incident Resolution Urgency

Urgency is a measure of the effect of the incident on business deadlines. It reflects the time available for restoral before the impact is felt or worsens significantly for the business. Read the question on the left side of the matrix. Then read across

Question	High	Medium	Low	None
Is it business hours? <u>Business Hours Examples:</u> normal office hours, advertised branch hours, 24x7 for ATM's, 24x7 for Online Banking, etc. <u>Note:</u> Obtain information about business hours and peak periods either from the SLA's for the impacted businesses or	☐ It is <u>business hours</u> and a <u>peak transaction period</u> as defined by the impacted business(es)	☐ It is <u>business hours</u> but not a <u>peak transaction period</u> as defined by the impacted business(es)	☐ It is <u>non-business hours</u> as defined by the impacted business(es) OR ☐ For 24x7 operations, it is during a period of very low transactions as defined by the impacted business(es).	☐
Is there an upcoming critical event that will be impacted by the unresolved incident? <u>Critical Event Examples:</u> trade opening, trade closing, critical financial handoff, critical regulatory handoff, end-of-month processing, end-of-quarter processing, etc	☐ There is <u>less than 2-hours</u> before a time-sensitive, critical event is scheduled	☐ There are <u>2-4 hours</u> before a time-sensitive, critical event is scheduled	☐ There are <u>more than 4 hours</u> before a time-sensitive, critical event is scheduled	☐
What is the agreed availability target for the impacted application or service? <u>High Availability</u> - A "high availability" application or service is one where no unscheduled outage is tolerated. These services are normally fully redundant with hot backup	☐ Agreed availability targets are " <u>high-availability</u> " targets and full redundancy is not operational.	☐ Agreed availability targets are <u>not "high-availability"</u> but more than "best effort".	☐ Availability targets are " <u>best effort</u> ".	☐

Step 3 - Calculate Severity Level

Go across the matrix below with the value for the **Impact** (from Step 1) and then go down the matrix with the value for **Urgency** (from Step 2) to find the Severity Level at the intersection,

Impact \ Urgency	High	Medium	Low
High	1	1	2
Medium	1	2	3
Low	2	3	3

Note: Those circled will be managed by Incident Management Team.

A.2 POST-MORTEM REPORT GUIDELINES

- 1) All post mortems issued by their respective organizations must be approved by either the respective Country TI Head, Distributed Domain Manager or APPC Group Head. A email approval will be required prior to the publication of the post mortem.
- 2) All post mortem reports must be published to external audience only by Regional Problem Management Group.
- 1) Post Mortem reports must be published as soon as the pertinent root cause information is available to RPMG. If root cause is not known after 24 hours of the incident resolution, an interim report must be published.
- 2) Individual groups in APPC and Distributed Operations will be measured in terms of providing necessary inputs for creating quality post mortems as well as timeliness of providing the report to Regional Problem Management Group.

The [Post-mortem Report template & Guidelines](http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/csweb/appcpmo/post_mortem_reports/PostMortemReportTemplate.doc) found in Regional Problem Management Group Website can be used for improving the quality of the Post-Mortem Reports.

(http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/csweb/appcpmo/post_mortem_reports/PostMortemReportTemplate.doc)

Note: For all post-mortem reports related to Japan services, RPMG is responsible to request resolvers to provide necessary evidences when post-mortem action items are completed. These evidences are centrally filed by RPMG and provided to Japan Business, TI Control and/or Auditors as and when requested. Acceptable evidences include valid request numbers in Infoman, ePJMR and eService Request system. Where the valid request numbers could not be provided, evidences such as procedural updates, email communications will be provided.

B. APPENDICES SPECIFIC TO DISTRIBUTED OPERATIONS

Appendices specific to Distributed Operations for reporting templates, Country addresses and metrics templates are provided in the following link:

- [Appendixes & Forms for Distributed Operations](#)

C. MASNET CIRCULAR ON BUSINESS CONTINUITY MANAGEMENT

This procedure references the Monetary Authority of Singapore directive provided on 6 Jan 2006 in the form of Circular (SRD/BCM/01/2006). This procedure has been revised to comply with guidelines with respect to Problem Management and Crisis communication functions.

The link to the MASNET circular communicated to Citigroup on 6 Jan 2006, is provided below:

http://appcweb.citicorp.com/cgti-aspac/appc-units/csweb/appcpmo/citmp_disciplines/MASNET%20CIRCULAR%20-%206%20Jan%202006.doc

D. HKMA INCIDENT REPORTING GUIDELINES

GUIDELINES FOR REPORTING INCIDENTS TO HONG KONG MONETARY AUTHORITY (HKMA)

1. HKMA REQUIREMENTS ON EVENTS REPORTABLE TO HKMA

1.1 EVENTS REPORTABLE TO THE HKMA

Technology-related incidents (including those incurred by Service Providers under an outsourcing arrangement) with business or customer impact

- Any incident, which may reduce the bank's ability to conduct business or impair the bank's services to customers. Such incident should be reported to the HKMA in the first instance (within one hour of the occurrence of system malfunction). The report, either in a verbal or written form, should include:
 - (i) services impact to customers with an estimated duration of the impact;
 - (ii) preliminary assessment of the possible causes of the system problems;
 - (iii) any customer complaints, enquiries so far;
 - (iv) the bank's line to take in case of queries from the press or any outside party; and
 - (v) a copy of press release (if applicable).
- Within 3 days of the incident, the bank should provide the HKMA with a root cause analysis report with detailed information on:
 - (i) possible underlying causes of the incident;
 - (ii) immediate actions taken;
 - (iii) long term remedial actions taken or to be taken (with target dates) to prevent the same problem from recurring;
 - (iv) customer's impact and duration of the impact;
 - (v) customer complaints and claims; and
 - (vi) the bank's estimation of the total compensation to be made to customers.
- Generally, the HKMA expects the bank's Compliance Department as the single point of contact in these reporting requirements. In case of needs, the bank can arrange its technology team to communicate with the HKMA direct to facilitate discussion on technology issues.

2. In line with section on Escalation and Notifications, CTI will advise Hong Kong Business represented by Senior Country Operations Officer (SCOO), Technology Head and/or their deputies as soon as incident occurs but not later than 30 minutes after incident occurring. In this initial notification, all pertinent details such as why the incident occurred, what are the possible causes etc. will be included. Further updates will be provided later to either add to the initial reported details or to make corrections on what was initially reported.
3. Hong Kong Business represented by SCOO, Technology Head etc. will determine whether to notify HKMA upon receiving escalation from CTI.
4. When a decision is made to notify HKMA about an incident, Hong Kong Technology Head and/or his deputy will advise CTI Regional Problem Management Group.
5. When an incident is reported to HKMA, RPMG will work with relevant support teams to develop and publish post mortem reports within 2 working days of incident occurring. Where root cause is

not available within 2 days, an interim report will be published. An updated post mortem report will be published subsequently when all pertinent details are available.

E. CRISIS COMMUNICATION PROCEDURE

E.1 OBJECTIVE

The purpose of Crisis Communication Procedure is to define the procedure to be adopted for communications during a crisis situation. When a crisis happens, rapid escalation to Business and Citigroup Technology Infrastructure (CTI) Senior Management is essential so that appropriate management decisions could be made to minimize the impact of the crisis. Further, a structured communication helps to ensure smooth flow of information between resolver teams, Business and CTI Management.

E.2 SCOPE

Crisis Communication procedure shall apply to all crises situations, which include one or more of the following situations:

- a) An incident situation that severely affects CTI Asia Pacific Production Service delivery to Citigroup businesses and customers
- b) Virus/Worm attacks on Citigroup network
- c) Natural disasters such as Tsunamis, Typhoons etc.
- d) Power Failures affecting data centers, major buildings and/or in-country hub sites
- e) Fire Accidents
- f) Epidemics such as SARS
- g) Fraud or Theft or Hacker Attack resulting in loss of Citigroup Information
- h) Terrorist Attacks
- i) Inadvertent loss of Customer's data
- j) Risk of Life
- k) Legal / Regulatory issues
- l) Any other situation that is considered a crisis by business and/or CTI Asia Pacific.

In situations that can't be readily identified as crises situations, the general rule of thumb is to error on the conservative side and invoke this procedure.

Crisis Communication procedure shall not be used for managing communications for day-to-day incidents. The escalation and notifications for day-to-day incidents are documented in the Problem Management Level 3 procedures.

E.3 ROLES AND RESPONSIBILITIES

1. When a crisis situation is identified, the staff identifying the crisis situation shall immediately notify the respective CTI Senior Manager on the crisis situation. This includes notifying the respective Country TI Head, APPC Group Head and/or Distributed Operations Domain Heads.
2. The CTI Senior Manager shall make a quick analysis of the situation and shall immediately notify the respective CTI Director as well as Regional Problem Management Group Head.
3. The CTI Director and/or Regional Problem Management Group Head shall be responsible to notify CTI Asia Pacific Managing Director as well as CTI Asia Pacific Senior Management within 30 minutes of the crisis situation occurring.
4. The CTI Asia Pacific Managing Director and/or his designate as well as the Regional Problem Management Group Head shall be responsible to notify the members of Asia Technology Leadership Council (ATLC) of the crisis situation within 30 – 45 minutes. Periodic updates shall be provided till the crisis situation is normalized.

5. When crisis situation impacts other region(s), appropriate CTI Regional Head(s), O&T Head(s) and Technology Head(s) shall be notified within 30 – 60 minutes of the crisis situation occurring. In addition, Japan TI controllers shall be notified when a crisis situation impacts Japan. Periodic updates shall be provided till the crisis situation is normalized.
6. When the criticality of a crisis situation warrants, CTI Asia Pacific Managing Director or his designate shall be responsible to notify Business Heads and provide updates on a periodic basis.
7. The Regional Problem Management Group shall be the central point of contact for all communications to businesses and CTI Management on crises situations.
8. Resolver and/or technical teams shall not send out any communications directly to Business and CTI Senior Management.

As timely notification and escalation are essential, staff shall use appropriate means e.g. calling via hand phone. Email shall not be used for notifying crises situations.

E.4 EMAIL UPDATES

1. In consultation with CTI Asia Pacific Managing Director and the respective CTI Director, the Regional Problem Management Group shall publish an initial report to Business and CTI Management. The following shall be notified:
 - Operations & Technology Heads
 - Senior Country Operations Officers
 - Country Technology Heads
 - CTI Senior Management
 - CTI Asia Pacific Management
 - Country CTI Heads
 - Regional Problem Management Group
 - Distributed Operations Domain Managers
 - APPC Management
 - Regional Engineering Domain Managers
 - Asia Pacific Technology Council Members
 - Asia Technology Office (ATO), CitiTech and Citigroup Private Banking (CPB) Management
 - Japan TI controllers (for crisis impacting Japan).
2. When a crisis situation involves information security, appropriate RISO, GISO and BISO are notified.
3. The initial report shall document all pertinent details known at that point in time and shall include a high level overview of the crisis situation, the impact as well as what is being done to recover from the crisis situation. The initial report shall also contain a conference bridge number that will be available for anyone to join and get a status update.
4. Email updates are published every 30 to 60 minutes till the crisis situation is resolved. Updates shall be provided to the same group who are initially notified.
5. When the criticality of a crisis situation warrants, CTI Asia Pacific Managing Director or his designate shall be responsible to notify Business Heads of CIB, CPB and GCG and provide updates on an hourly basis.
6. A sample Email update is show on Appendix A.

E.5 CONFERENCE BRIDGES

1. Upon publishing the initial report, a conference bridge shall be initiated by the Regional Problem Management Group. The conference bridge shall be used to provide periodic updates on the status of a crisis situation.
2. When there are any significant updates, the same shall be communicated to those who are logged onto the conference bridge.
3. When situation warrants, more than one technical bridge could be initiated. However, one of them shall be designated for providing status updates. Other bridges can be used for internal discussions amongst resolver and/or technical teams.
4. The conference bridge for providing status updates shall be available till the crisis situation is resolved.

E.6 POST MORTEM REPORTS

1. The Regional Problem Management Group shall be responsible for ensuring a post mortem report is published for all crises situations.
2. A post mortem report shall be published within 2 working days after the crises situation is resolved. In cases where pertinent information is not available to publish a post mortem report, an interim report shall be published with information available at that point in time. When more information becomes available, an updated post mortem report shall be published.
3. At the minimum, the post mortem report shall contain the following:
 - a. Executive summary
 - b. Business impact
 - c. Actions taken to resolve the crisis situation
 - d. Preventive actions (if applicable)
 - e. Chronology of events.

E.7 SAMPLE EMAIL UPDATES DURING A CRISIS SITUATION

-----Original Message-----

From: Narayanan, Venkat

Sent: Thursday, March 10, 2005 2:21 PM

To: Butcher, Andrew [OPS]; Ng, Peng-Khim [IT]; *GCIB AP Cititech MGT; *GCIB AP Cititech CC; Pamnani, Nanoo G; Sharma, Dk; Chan, Cheow-Hoe; Das, Anup; Chow, Phillip; Kwek, Susan; Yong, Alvin; *GC AP GISO; *APCB AP SCOO; *AP GCIB SCOO

Cc: *TI AP Mgmt Committee; *TI AP COUNTRY HEADS; *GT AP APPC WORKGROUP; *TI AP Prob Mgmt Group; *TI AP BISO; Wong, Mike

Subject: Slammer Virus incident - Update 2

Update 2 as of 10 Mar 02:00 PM

As updated earlier, there are 32 devices that have been identified as vulnerable.

- 23 of these devices have already been patched earlier but were flagged out because of 'Null Password' i.e. no password for the System Admin SQL account. This is being addressed.
- 7 devices from Australia have been identified as vulnerable and appropriate remediation effort is underway to address these 7 devices.
- 2 devices (one in India and one in Taiwan) were suspected to be affected with Slammer virus... they are taken off the network for further assessment/remediation.

As of 2 PM this afternoon, there is no reported outbreak of virus in Asia Pacific region and no reported business impact.

Given that the situation is well under control, I will not be providing regular updates - instead I will provide an update when we complete the remediation of 32 devices.

However, if there is any new development and/or any outbreak reported, I will come back to provide regular updates.

/Signed/

-----Original Message-----

From: Narayanan, Venkat
Sent: Thursday, March 10, 2005 11:20 AM
To: Butcher, Andrew [OPS]; Ng, Peng-Khim [IT]; *GCIB AP Cititech MGT; *GCIB AP Cititech CC; Pamnani, Nanoo G; Sharma, Dk; Chan, Cheow-Hoe; Das, Anup; Chow, Phillip; Kwek, Susan; Yong, Alvin; *GC AP GISO; *APCB AP SCOO; *AP GCIB SCOO
Cc: *TI AP Mgmt Committee; *TI AP COUNTRY HEADS; *GT AP APPC WORKGROUP; *TI AP Prob Mgmt Group; *TI AP BISO; Wong, Mike
Subject: Slammer Virus incident - Update 1
Importance: High

Update 1 as of 10 March 11:00 AM

As of 11 AM this morning, we have identified 32 devices which are vulnerable... 4 of these devices have been patched and work in progress for the remaining 28 devices. 2 devices which are considered to be high risk have been taken out of the network.

At this point in time, there is no reported outbreak of virus in Asia Pacific region and no reported business impact.

I will keep you posted on further developments.

/Signed/

-----Original Message-----

From: Narayanan, Venkat
Sent: Thursday, March 10, 2005 8:23 AM
To: Butcher, Andrew [OPS]; Ng, Peng-Khim [IT]; Sharma, Dk; Chan, Cheow-Hoe; *GCIB AP Cititech MGT; Das, Anup; Chow, Phillip; Kwek, Susan; Pamnani, Nanoo G; Yong, Alvin
Cc: *TI AP Mgmt Committee; *TI AP COUNTRY HEADS; *GT AP APPC WORKGROUP; *TI AP Prob Mgmt Group; Wong, Mike
Subject: Slammer Virus incident - no impact to Asia Pacific

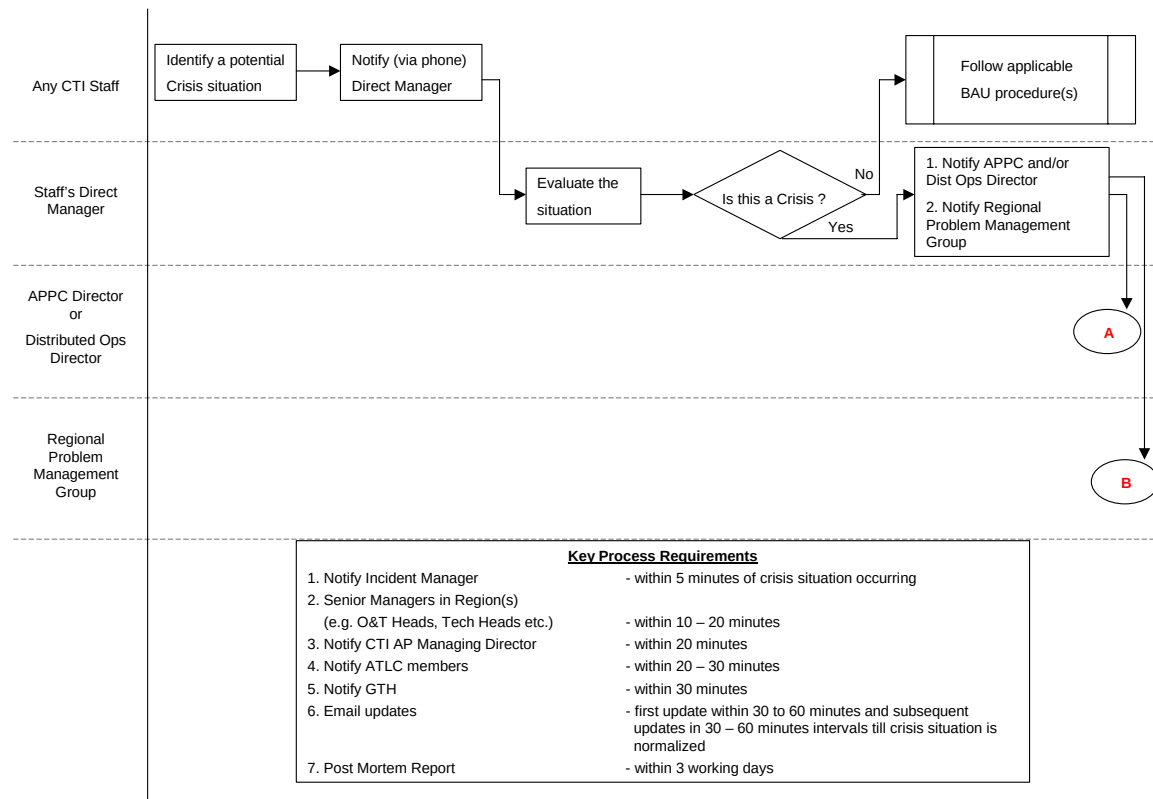
Dear All, there is an outbreak of SQL Slammer virus impacting North America, LATAM and parts of Europe. As of 8 AM this morning, we have not seen any outbreak in Asia Pacific region.

We are closely working with global teams to identify any vulnerability that may exist so that we can quickly take appropriate actions.

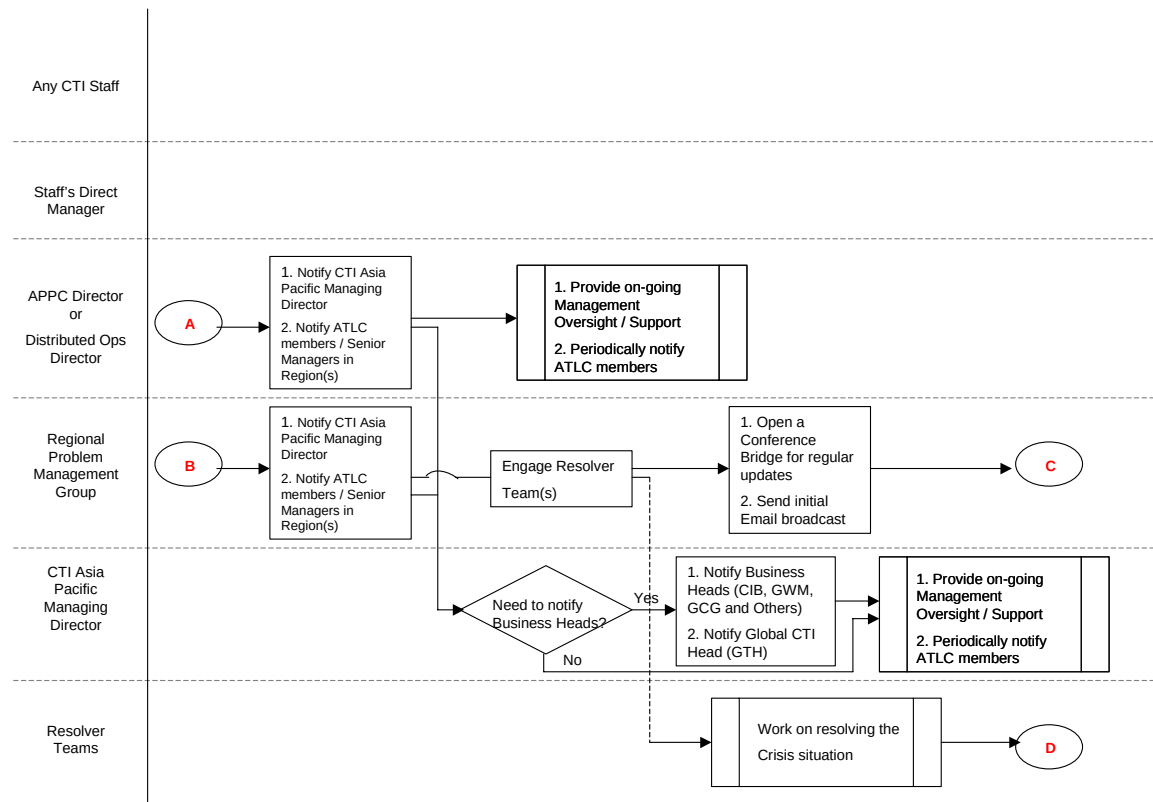
I will keep you posted on further developments.

/Signed/

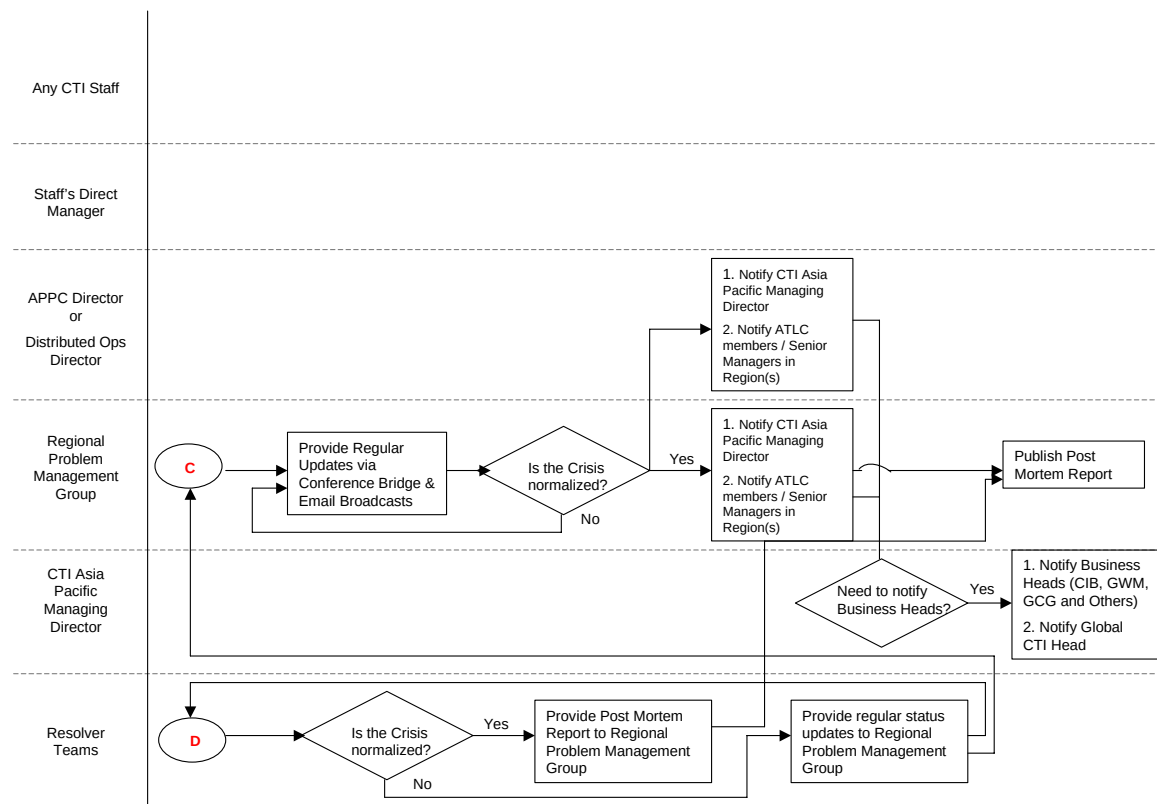
E.8 CRISIS COMMUNICATION - CROSS FUNCTIONAL PROCESS MAP (1 OF 3)



E.9 CRISIS COMMUNICATION - CROSS FUNCTIONAL PROCESS MAP (2 OF 3)



E.10 CRISIS COMMUNICATION - CROSS FUNCTIONAL PROCESS MAP (3 OF 3)



F. EXCERPTS FROM ESCALATION PROCEDURE FOR CITIGROUP SERVICES (JAPAN)

Effective June 01, Citigroup Services (Japan) has published a revision to the *Incidents and Errors Escalation Procedure*. Excerpts on sections that are relevant to this procedure are given below for compliance. For more details, please refer to the Incidents and Errors Escalation Procedure.

Under the Banking Laws in Japan, Citibank N.A., Japan Branch is required to report certain incidents or operational errors to FSA. As a service provider to Citibank Japan, CTI is required to report any incident or error in its operation as defined by the Banking Laws to the Citibank Japan.

It is necessary for CTI AP Management to report incidents or operational errors as defined above including the following:

(a) Computer System Problems

Computer system problems must be reported, regardless of the cause of the problem, where any failure of systems/machines (hardware and software) used/managed.

- Results in or may result in delay or termination of cash withdrawal or remittance and other fund settlement functions of our customer such as Citibank Japan,
- Affects or may affect monitoring fund management/ALM or comprehension of financial status of Citigroup, or
- Is considered to be equivalent to either of the above two categories in carrying out business transactions of our customers.

However, if such system or machine failure is replaced by a back up system/ machine and does not impact on our services or business of customers, then reporting does not become mandatory.

(b) Cyber Terrorism

Reporting is required in the event cyber terrorism is detected against systems/machines (hardware and software) that causes or may cause extensive damage to operations of our customers, or where cyber terrorism is occurred.

(c) Leakage of Customer Information.

Any problem that has Customer Information leakage should follow the CSJ SIRT Process and escalate such problems to in line with SIRT process.

G. INCIDENT ESCALATION LOG TEMPLATE

Please find below the link for the Incident Log template:

http://appcweb.citicorp.com/cgti-aspac/appc-units/csweb/appcpmo/citmp_disciplines/Incident%20Escalation%20Log%20Template.xls