

Citigroup Technology Infrastructure Asia Pacific

Internet Management Procedure Manual

Prepared by: Jonathan Lee
First Published Date: 27/07/2005
Version: 2.1
Published Date: 31/01/2007
Project Reference: N/A
Document #: N/A
Soft Copy Name: CTI-AP-CITMP-L3-InternetManagement-v2.1
Document Classification: INTERNAL USE

Notice of Proprietary Property

Copyright © 2006 by Citigroup. All rights reserved. FOR INTERNAL USE ONLY 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.

DISTRIBUTION LIST

Paul McCarroll	CTI Asia Pacific Managing Director
Anthony Lee	CTI Asia Pacific Distributed Operations
Ramon Karingal	CTI Asia Pacific Processing Center
Mike Chan	CTI Asia Pacific Distributed Operations
Jane Cheung	CTI Asia Pacific Regional Wintel Operations
Soo Kian Sheng	CTI Asia Pacific Regional Voice Operations
Loong Chet Liang	CTI Asia Pacific Regional Unix Operations
Simon Chang	CTI Asia Pacific Distributed Integration
Venkat Narayanan	CTI Asia Pacific Problem Management
Jeffrey Goh	CTI Asia Pacific Change Management
CTI Country Heads Australia Brunei China Guam Hong Kong India Indonesia Korea Malaysia Philippines Singapore Taiwan Thailand Vietnam	
Garry Brown	CTI Project Office / Project Management
Mohsin, Rahim	CTI Asia Pacific Financial Controller
Mustafa Sidek Koh Chong Chiah Felix Lim Ian Le Wee Soon Teng	APPC Group Heads
Guru Venkatachalam Chris Smith Harry Yip Joseph Reyes Koh Jit Soon Lim Wee Joo Philip Kan	CTI Engineering
Raghuram Muthukrishnan	Client Relationship

DOCUMENT APPROVAL

Prepared by:



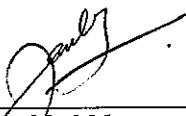
Jonathan Lee
CTI Asia Pacific Regional Internet
Infrastructure and Security Operations

24/01/2007
Date



Edmund Chua
CTI Asia Pacific Wintel Operations

24/01/2007
Date



Tan Koi Yong
CTI AP Business Office

24/01/2007
Date

Reviewed by:



Seow Wee Choon
CTI Asia Pacific Regional Network
Operations

24/1/2007
Date



Pathman Gangesar
CTI AP Business Office

25th Jan 2007

Email Approval

Jane Cheung
CTI AP Wintel Operations

Date

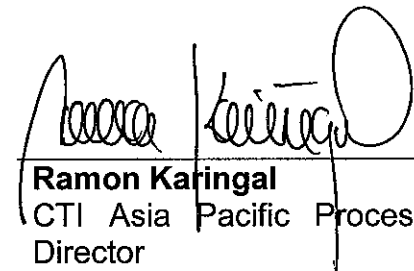
Approved by:



Anthony K C Lee
CTI Asia Regional Distributed
Operations Director

Date

2/27/2007.



Ramon Karingal
CTI Asia Pacific Processing Center
Director

Date

26 Feb 07



Ned Lim
CTI Asia Pacific Information Security &
Compliance Head

Date

Feb 28. 07

Lee, Jonathan [CCC-OT_IT]

From: Cheung, Jane [CCC-OT_IT]
Sent: Monday, February 05, 2007 4:25 PM
To: Lee, Jonathan [CCC-OT_IT]
Cc: Seow, Wee Choon [CCC-OT_IT]; Chua, Edmund Bt [CCC-OT_IT]; Bin Majid, Zakaria [CCC-OT_IT]
Subject: RE: Internet Management L3----- resending for approval

Jonathan,

Sorry for late reply. Here is my approval.

Regards,
Jane

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

From: Lee, Jonathan [CCC-OT_IT]
Sent: Monday, January 29, 2007 3:53 PM
To: Cheung, Jane [CCC-OT_IT]
Cc: Seow, Wee Choon [CCC-OT_IT]; Chua, Edmund Bt [CCC-OT_IT]; Bin Majid, Zakaria [CCC-OT_IT]
Subject: Internet Management L3----- resending for approval
Importance: High

Hi Jane.

Have you had a chance to review? I need your help to approve as I need to upload the document by next week.

thanks
jon

Hi Jane.

Attached is an update to the Internet Management Level 3 procedures prepared by Edmund, Koi Yong (CTI Business Office) and me. Please review and if ok, please provide your sign-off.

Once you sign off, please fax it back to +65 64262100.

thanks
jon

AMENDMENT HISTORY

Version No.	Author	Published Date	Description of changes
1.0	Jonathan Lee	27 July 2005	First Publication of Procedure
2.0	Jonathan Lee	16 January 2006	Updates to Section 4.3.3 on Systems Log Review Updates to Approval Listing

2.1	Jonathan Lee	31 January 2007	Cover page is revised. • Notice of proprietary property box has been revised. Added Distribution List Approval listing is revised. • Approver names and titles are updated • Remove Fincon and Project Office from the Approver listing Changes to Sections: • 1.4 ○ GPMS (deleted) ○ RCSA (added) ○ WES (deleted) • 2.3 ○ 'This will be effected once the exiting staff's SOEID is removed from the APAC domain' (added) • 3 ○ Cacheflow (deleted) ○ ProxySg (added) • 3.1 ○ whitepages.ny.ssmb.com (deleted) ○ ipmgmtm.nsroot.net/dns0/index.php (added) • 3.1.1 ○ 'The external DNS is supported and managed by Web Hosting Group. They will also interface with CDNR to register new Citigroup owned domains on the external DNS's that faces the Internet' (added) • 3.1.2 ○ whitepages.ny.ssmb.com (deleted) ○ ipmgmtm.nsroot.net/dns0/index.php (added) • 4.1.2 ○ 'CTI Regional Internet Infrastructure and Security Operations manage all Netscape tier 1 proxies in Singapore Citiplex and all Volera proxies in the region. (deleted) ○ '...which has their own gateway' added. ○ Korea Cacheflow tier 2 proxy route the Internet traffic to these tier 1 Cacheflow proxies' (deleted) ○ Websense (deleted) ○ Smartfilter (added) • 4.2 ○ http://aptech.ap.ssmb.com:8406/aptech/dti/dtisec.html (removed) ○ http://cti.asiapacific.citigroup.net:8800/cti_citmp.htm (added) • 4.3 ○ 'The SA will perform system administration duties like service change request, OS patching and application patching etc' (modified) • 4.3.4 ○ TECHNOLOGY RISK ASSESSMENT METRIC (TRAM) (removed) ○ 'Applicable technology risk assessment metric (TRAM) should be done annually as part of compliance' (removed) ○ Technical RCSA is also performed quarterly for specific products managed by the respective Operational units (added) • 4.7 (Previously Project Management) deleted ○ Information in this section is not relevant to the purpose
-----	--------------	-----------------	--

			of this document • 4.8 ○ Problem management in CTI follows the procedure in url: http://cti.asiapacific.citigroup.net:8800/distops/stddocs.htm (modified) As for APPC, the problem management procedures can be located at http://appcweb.citicorp.com:8800/cgti-aspac/appc-units/iso/docs/level3/work/problem/toclev3v4prob.htm#P-1_0 (deleted) • 5 ○ Internet Access Registration URL (removed) ○ Windows Secure Configuration Guideline (removed) ○ Firewall form url (removed) ○ CTI Regional Infrastructure and Security operations Problem Management Procedure url (removed) ○ APPC Problem Management Procedure url (removed)
--	--	--	---

TABLE OF CONTENTS

DISTRIBUTION LIST	2
DOCUMENT APPROVAL	3
TABLE OF CONTENTS	8
1. INTRODUCTION	9
1.1 OBJECTIVE	9
1.2 SCOPE	9
1.3 RESPONSIBILITIES	9
1.4 ACRONYMS	9
2. INTERNET ACCESS	11
2.1 INTERNET BROWSER PROXY SETTING	11
2.2 INTERNET ACCESS ENROLLMENT	11
2.3 INTERNET ACCESS TERMINATION	12
2.4 INTERNET ACCESS REVIEW	12
2.5 INTRANET ACCESS	12
3. WEB HOSTING INFRASTRUCTURE MANAGEMENT	13
3.1 DNS	13
3.1.1 EXTERNAL DNS	13
3.1.2 INTERNAL DNS	14
3.1.3 WEB DEVELOPMENT	14
3.2 SERVER AND WAN LOAD BALANCER	14
4. SUPPORT AND MAINTENANCE	15
4.1 INTERNET INFRASTRUCTURE SUPPORT	15
4.1.1 INTERNET SERVICE PROVIDER (ISP)	15
4.1.2 PROXY SERVER SUPPORT	15
4.1.3 REMOTE ACCESS SUPPORT	16
4.1.4 REGIONAL WWDS SUPPORT	16
4.2 SECURITY OPERATIONS SUPPORT	17
4.3 INFORMATION SECURITY MANAGEMENT	17
4.3.1 DMZ AND PORT JUSTIFICATION REGISTRATION	17
4.3.2 BUSINESS RESPONSIBILITIES	18
4.3.3 SYSTEM LOGS REVIEW	18
1.1.1 RISK CONTROL SELF ASSESSMENT (RCSA)	18
4.3.4 DCFC	18
4.4 WEB SITE DEVELOPMENT, OPERATIONS AND MAINTENANCE	19
4.4.1 WEB SERVER OPERATING ENVIRONMENT SETUP	19
4.5 INTRANET WEB SITE MANAGEMENT	20
4.6 CONTINUITY OF BUSINESS (COB)	24
4.6.1 CITIBANK ONLINE	24
4.6.2 CITIVPN	24
4.6.3 INDIA WEBHOSTING COB	24
4.7 CHANGE MANAGEMENT	24
4.8 PROBLEM MANAGEMENT	24
5. APPENDIX A: URL REFERENCES IN THIS DOCUMENT	26
6. APPENDIX B: E-DCFC	27
6.1 Daily Tasks	27
6.2 MONTHLY TASKS	27
6.3 Quarterly TASKS	27

1. INTRODUCTION

1.1 OBJECTIVE

The primary objective of this Internet Management Procedure is to provide the procedure for CTI Asia staff to perform the management of the Internet and Intranet servers and infrastructure in compliance with the Citigroup Information Technology Management Policy (CITMP) on Internet Management and Citigroup Web Site Standard.

1.2 SCOPE

This document covers:

- a) Procedure for internet access for ASPAC employees
- b) Web Hosting Infrastructure Internet Infrastructure, remote access and Web Server operating environment Management, Support and Maintenance
- c) The procedure to perform web hosting servers and infrastructure security review and self-assessment
- d) Intranet website management.

This document complies with CTI CITMP Global Internet Management level2 located in http://www.citigroup.net/ti/compliance/citmp_level2.htm

1.3 RESPONSIBILITIES

CTI Asia is responsible to review and update this document. All CTI Asia functional units are responsible to be compliance with this procedure.

1.4 ACRONYMS

- a) ACL = Access Control List
- b) BISO = Business Information Security Officer
- c) CBOL = Citibank Online
- d) CDNR = Citigroup Domain Names Registrar
- e) CGM = Citigroup Global Market
- f) COB = Continuity of Business
- g) CTI = Citigroup Technology Infrastructure
- h) DC = Data Centre
- i) CWHI = Citigroup Web Hosting Infrastructure
- j) DCFC = Departmental Control Function Checklist
- k) DNS = Domain Name System
- l) DMZ = De-Militarized Zone
- m) DTI = Distributed Technology Infrastructure
- n) EFP = Event Flow Processor
- o) EH = Ethical Hack process
- p) GISO = Group Information Security Officer
- q) GNCC = Global Network Command Center
- r) ISA = Information Security Administrator
- s) ISP = Internet Service Provider
- t) MADD = Move Add Delete and Departure process
- u) NIC = Network Information Center
- v) RNOC = Regional Network Operations Center

- w) RCSA = Risk Control Self Assessment
- x) SA = Systems Administrator
- y) SAID = Security Assigned ID
- z) SDLC = Software Development Life Cycle
- aa) SILC = Standard Infrastructure Life Cycle
- bb) SIRT = Security Incident Response Team
- cc) SOE = Standard Operating Environment
- dd) SOW = Statement Of Work
- ee) SSM = Solaris Security Model
- ff) TIE = Citigroup Technology Infrastructure Engineering
- gg) RCSA=Risk Control Self-Assessment Matrix
- hh) VPN = Virtual Private Network
- ii) VTM = Vulnerability and Threat Management
- jj) VT = VirtualTech
- kk) WHG = Web Hosting Group
- ll) WISE = Web and Internet Security Engineering
- mm) WWDS = World Wide Dial Service

2. INTERNET ACCESS

All the CTI Asia staff workstation should adhere to CTI SOE standard (<http://www.citigroup.net/tie/de/wintel/index.html>)

CTI Regional Internet Infrastructure and Security is responsible for managing network, firewalls and proxy servers to restrict the Internet access. It also manages the remote access service (WWDS, VPN and Corporate Desktop portal).

2.1 INTERNET BROWSER PROXY SETTING

Internet browsers / client / server accessing the Internet must be defined with an authorized proxy in the automatic configuration setting (<http://proxy.citicorp.com/config.pxy>).

Proxy settings for CGM users are pointed to the designated proxy server with bypassing domains for internal sites.

All other access mechanisms are prohibited unless specifically approved by CTI, the Business owner and GISO.

2.2 INTERNET ACCESS ENROLLMENT

- a) Employees who require internet access need to raise a Virtual Request on the Virtual Tech system available via the following website:

<https://virtualtech.eur.nsroot.net/virtualtech/defaulttnt.asp>

Employee's supervisor should:

- b) Then receive an email from the Virtual Tech system for the approval.
- c) Review the request, based on employee's job requirement and dis/approve by approving on the system.
- d) Inform employee that the Citigroup Internet access is for authorized business purposes only and should brief the employee on the following Citigroup Internet practices after the request has been approved.

Employee should not:

- Download any unauthorized software from the Internet sites to the local PC.
- Access / participate in Internet chat rooms.
- Communicate Restricted or Confidential data over the Internet.

Employee should:

- Notify Desktop administrator, if any download required to be installed locally on the Personal Computer.
- Notify Desktop administrator immediately, should he suspect a virus has infected his PC.

- e) For CGM, all employees will have access to public Internet. User must follow the MADD (Modified, Add, Delete and Departure) process. MADD is a CGM application to raise the documentation to list down the things to be done related to any technology request from the business in term of Modify, Add, Delete and Departure. The Technical Team will raise a MADD whenever a

requester from the Business side put up any request. Requester and his Manager have to sign and acknowledge on the MADD for Technology to carry out the task in the MADD. Technology will also have to sign off once the task in the MADD is completed.

- f) For server requiring Internet access, an Internet Access Request form must be filled up detailing the IP address of the server. The request will then be processed and the IP address of the server will be added to the application proxy- it will

2.3 INTERNET ACCESS TERMINATION

Unit supervisor should terminate the staff Internet access upon staff exit within 24 hours or transfer across business departments when change takes effect. This will be effected once the exiting staff's SOEID Id is removed from the APAC domain.

2.4 INTERNET ACCESS REVIEW

Employee's supervisor should:

- a) Perform semi-annual review of the staff Internet access entitlement.
- b) Warn or take appropriate action, if employee is found violating Citigroup Internet Standard usage policies.
- c) CTI Asia Management should inform the staff regarding the Citigroup Information Security Standards and Web Site Standards and remind the staff on the Citigroup Internet practices in section 2.2 (d).

2.5 INTRANET ACCESS

- a) Intranet access does not require approval procedure outlined in 2.2.
- b) Intranet is available to all Citigroup employees, agents, temporary staffs and consultants from internal network and authorized remote access only.

3. WEB HOSTING INFRASTRUCTURE MANAGEMENT

Web servers must be hosted in authorized web hosting environment that's built according to Citigroup Technology Infrastructure Engineering (TIE) standards, such as Singapore Citiplex.

CTI Asia Regional Internet and Security Operations is responsible for managing web hosting infrastructure including ISP link, load balancer, WAN load balancer, firewalls, tier-1 Netscape proxies and all Volera proxies.

CTI Regional Internet Infrastructure and Security Operations will work with US and Asia Pacific Regional counterparts like CDNR, WHG, GNCC, WISE, TIE, CTI Regional Network Operations, CTI Wintel / Unix Regional Operations and other support units. A brief description of these support units is as follows:

- a) CDNR manages the internal and external domain name registration. CTI Regional Internet Infrastructure and Security Operations is the user interface whenever necessary.
- b) Web Hosting Group manages the tier-2 ProxySG proxies in the region, as well as the Singapore tier-1 ProxySG and PAC (proxy automatic configuration) file for ASPAC region.
- c) GNCC monitors the network equipment (routers and switches) as well as managing the legacy Cyberguard firewalls. CTI Regional Network Operations manages all the routers and switches.
- d) WISE is the next level of escalation for Regional Internet Infrastructure and Security Operations and will be the engineering consultant and lead for new deployment.
- e) APPC Wintel and Unix Operations manage all the Windows and Unix OS of the web servers.

Any new access methods or restricted port opening request from the internet to DMZ or from DMZ to internal network or DMZ to DMZ must be reviewed and approved by WISE and BISO.

3.1 DNS

There are two kinds of DNS records:

- External DNS records
- Internal DNS records.

The external DNS records are kept on the root DNS servers in US for Internet urls and address resolution and they are managed by WHG. The internal DNS records are kept on the internal DNS servers distributed across the regions for internal url and address resolution. Whitepages Support maintains these records. They can be contacted at the following url:

<https://ipmgmt.nsroot.net/dns/index.php>

3.1.1 EXTERNAL DNS

The CDNR manages domain names registration and branding. Information and procedure are available at the following URL:

<http://www.citigroup.net/citigroup.net/cdnr>

CTI Regional Internet Infrastructure and Security Operations is the interface to the CDNR in ensuring Internet domain names are being renewed. The procedures are described below:

- CDNR receives notification from the domain name Registrar or the country NIC (Network Information Center) that a domain name is due for renewal.
- CTI Regional Internet Infrastructure and Security Operations will follow up and make sure that the domain names in the AP countries are renewed. Therefore, CTI Regional Internet Infrastructure and Security Operations should have an inventory of all the Domain Names in the AP region with owner and expiration / renewal date. The unit will leverage on CTI country support to liaise with the in-country owner of the Domain Name. The lead-time is 30 days.
- If the domain name has a live web site and it's included in the Corporate Web Hosting Infrastructure inventory – an inventory maintained by CDNR- CDNR will pay the invoice and the listed contact person is notified. If not, the domain name is sent to Trademark Counsel and the line of business for review. Upon receipt of approval, the invoice is paid, if not, the name is allowed to expire.
- The external DNS is supported and managed by Web Hosting Group. They will also interface with CDNR to register new Citigroup owned domains on the external DNS's that faces the Internet.

3.1.2 INTERNAL DNS

For internal DNS record update, requester can go to the following URL:
<https://ipmgmt.nsroot.net/dns/index.php>

3.1.3 WEB DEVELOPMENT

CTI Regional Internet Infrastructure and Security Operations do not develop web application. Therefore, the Citigroup Web Site Standard document does not apply to CTI Regional Internet Infrastructure and Security Operations. However, CTI Regional Internet Infrastructure and Security Operations will support the tasks to be performed by business technology or other requester to comply with the standard in developing web application or migrating web application to Citiplex environment. Such tasks are DNS registration and renewal, processing the firewall port opening, and other related tasks. Refer to the form in this URL:
<http://cti.asiapacific.citigroup.net:8800/distops/intops/formsurl.htm>.

For reference purpose, the CWHI can be found in the following URL:
<http://www.citigroup.net/citigroup.net/cwhi/>.

3.2 SERVER AND WAN LOAD BALANCER

CTI Regional Internet Infrastructure and Security Operations manage the Server and WAN load balancer in Singapore Citiplex as well as Internal load balancers. All requests on for configuration changes on these devices must be sent to Regional Internet Operations. The change implementation must follow the Change Management process.

The request must be completed with Virtual and physical IP address, load balancing method, monitoring type, application URL, and other necessary information. Requester, requester's manager must sign the request. For changes made on the Citiplex Web Hosting environment, BISO approval must be gotten as well.

4. SUPPORT AND MAINTENANCE

4.1 INTERNET INFRASTRUCTURE SUPPORT

4.1.1 INTERNET SERVICE PROVIDER (ISP)

CTI Regional Internet Infrastructure and Security Operations manage the ISP in Singapore Citiplex. CTI India manages the ISP in India Internet Infrastructure.

The link is monitored weekly and reported monthly to management. Capacity planning is done quarterly on these links. Meeting with ISP and Updating escalation contact list is conducted at least every quarter.

4.1.2 PROXY SERVER SUPPORT

All tier-2 proxies in Korea, Hong Kong and Taiwan and China are managed by WHG. All these tier-2 proxies route the Internet traffic to Singapore Citiplex except for Korea, which has their own Internet gateway.

There are two ProxySGs acting as tier-1 proxy in Singapore managed by WHG. Proxy server logs Internet/Intranet usage and blocked certain access in order to ensure that the use of the Internet is for authorized business purposes and to help prevent the introduction of information, which could introduce a virus or create a hostile environment.

Regional Internet Operations Support will publish Detailed Internet Usage reports for the country by the 15th of every month. Some of the information provided by the report is as follows:

- Total number of hits and total size download during each week
- Number of active users each week
- Most active profile and site visited each week
- Top 3 users each week with details like most visited site, profile and total size download.

The report, based on total data size downloaded, highlights the top 3 Internet users and the most active site visited by each of the three users. The Regional Internet Operations Support Engineer review this report for potential misuse or undesired trend, such as the most active site being non-business site, and inform the respective Country Head. The CTI Country Head will conduct the necessary investigation, and if appropriate, inform the relevant parties (e.g. Compliance Unit, HR, Manager of the violate, etc.) for disciplinary action to be taken.

The request for blocking or allowing of websites must be sent to Regional Internet Operations. The blocking will be done through Smartfilter.

4.1.2.a User Subnet Management

All new subnets assigned to the network, either a new one or relocated from other country, should be registered to WHG. The project manager in charge of setting up any new segment/subnet should register the IP subnet to Regional Internet Operations who will check against a list of IP subnet inventory. If it is not in the

inventory, Regional Internet and Security Operations will register it to WHG. Once registered, WHG will push the correct PAC (proxy automatic configuration) file to the users on this new subnet, so that the users will be routed to the nearest proxy server.

Any change in the PAC file is subject to discussion and approval of WHG and global Internet Engineering. Any business or user who wants to make the change must contact Regional Internet Operations first to open a discussion.

4.1.3 REMOTE ACCESS SUPPORT

Remote Access to company network must be using authorized methods only: WWDS (World Wide Dial-up Service), CitiVPN (Virtual Private Network) or Desktop Portal (<http://desktop.asia.citigroup.com>). In supporting remote access, CTI Regional Internet Infrastructure and Security Operations works with Citigroup Mobile Computing, Wintel Engineering and WHG unit in US.

4.1.4 REGIONAL WWDS SUPPORT

For new request or change in remote access service (WWDS/CitiVPN), user must register using form in this URL: <http://remoteaccess.citigroup.net/forms.php>. The turn around time for the service is about 2 weeks. The authentication is through global Safeword/Radius server. Safeword application support in US manages this server.

There are WWDS routers in the countries as well as in Singapore regional for WWDS vendor connectivity such as IBM and Compuserve. GNCC manages these routers.

User first level support for WWDS is the country helpdesk. Regional Internet Operations support is the next escalation for connectivity issues. US CSC helpdesk supports the Safeword card issues.

4.1.4.a Regional CitiVPN Support

CitiVPN is connectivity from Internet to internal network through VPN technology. The components are network, firewalls and VPN gateway. CTI Regional Internet Operations support the VPN gateway. The authentication is through Safeword/Radius and Hong Kong SecureID server. The Safeword server is the same server as WWDS. Hong Kong Unix Operations manages the SecureID server. Most of SecureID users are CGM users. Regional Security Operations supports the firewalls.

User first level support for CitiVPN is the country helpdesk. Regional Internet Operations is the next escalation.

4.1.4.b Regional Desktop Portal Support

Regional Desktop Portal (<http://desktop.asia.citigroup.com>) is connectivity from Internet to internal terminal server through browser / java technology. The components are network, firewalls, Neoteris gateway, web servers, proxy servers and terminal servers. CTI Regional Internet Infrastructure and Security Operations support the Neoteris gateway, proxy servers and terminal server software. The authentication is through Safeword/Radius. The Safeword server is the same server as WWDS. Regional Internet Infrastructure and Security Operations supports the firewalls. Regional Wintel Operations supports the web servers and terminal servers.

User first level support for CitiVPN is the country helpdesk. Regional Internet Operations is the next escalation.

4.2 SECURITY OPERATIONS SUPPORT

All the firewalls are managed by Regional Security Operations. The firewall exceptions or violations logs are reviewed daily. If there's any finding, a report will be sent immediately to management for follow up.

There's IDS in both Singapore Citiplex and India Internet Infrastructure monitoring the inbound and outbound traffic. It consists of IDS sensor and EFP (Event Flow Processor) server. It's managed by US IDS Operations group.

For virus incident, the reporting should be sent by email to "Software, PC Security". For the SIRT procedure, an incident will be defined as a suspected or possible security breach to one or more of our information resources. It is any adverse event whereby some aspect of information security could be threatened, for example loss of data confidentiality, destruction of data, loss of system integrity, loss of data integrity, disruption or denial of service, etc. Regional Security Operations follows the current SIRT process in Information Security Level 3 document which can be found in this URL:

http://cti.asiapacific.citigroup.net:8800/cti_citmp.htm

4.3 INFORMATION SECURITY MANAGEMENT

Regional Internet and Security Operations Support and India DTI Internet support do not manage customer database. In this section, procedures relating to Internet Infrastructure security will be described. For India, the local support will be the contact for business to forward the information to GNCC. The same form will be used for India as well.

4.3.1 DMZ AND PORT JUSTIFICATION REGISTRATION

A typical Internet network set-up will require router connectivity to an ISP link and advertisement of subnets into the ISP. Controls and registration at these 2 points are explained below. For the following sections: 4.3.1.a, 4.3.1.b and 4.3.1.c, user must use the form in the following URL:

<http://cti.asiapacific.citigroup.net:8800/distops/intops/formsurl.htm>

4.3.1.a ISP Open Port Justification

In a typical web-hosting connection, the only TCP ports communication required are http (port 80) and https (port 443) traffic. If there is a need for other ports, an Open Port Justification is required.

GNCC performs periodic port scan checks on all registered DMZs and reports on any un-registered TCP ports. It is expected the TCP ports will be closed within 7 working days if a justification form is not provided.

Access Control Lists (ACLs) on the ISP-facing router are configured to permit only registered ports. Changes on the routers go through the regional change management. Changes that affect the ports communication will not be performed unless a justification form is attached.

4.3.1.b DMZ Registration/De-registration

It is required to register all IP subnets that are being advertised into the ISP. De-registration of any (ISP) IP subnet will also use the same form. This is important information to be used by GNCC to periodically scan the IP subnet for any vulnerability. Completed forms are to be sent to Regional Security Operations Support as per the form instructions.

4.3.1.c Vulnerability Assessment

Vulnerability assessment is the scanning of specific network to identify security weaknesses and/or vulnerabilities. ID/VA team in the US does this scan when open ports are discovered from the port scanning run. The business can request for VA scan prior to deployment of new applications onto the DMZ.

4.3.1.d Ethical Hacking

Ethical Hacking is the most comprehensive tests perform on web hosting environment. This scan is required for any new applications or DMZ infrastructure installed. Business must follow the instruction in the form and submit it to the US fax number as indicated in the form. CTI Asia Regional Internet Infrastructure and Security Operations do not perform ethical hacking.

4.3.2 BUSINESS RESPONSIBILITIES

Business will be responsible for the web content management and compliance to the CITMP. They will be responsible to ensure the servers are properly configured and undergo Ethical Hacking Testing before moving to production environment. As a due-diligence performed by CTI operations for new application setup, business will have to produce the notification or evidence of the EH issues closure and BISO approval before they are allowed into Citiplex Production environment. For UAT setup, EH schedule, SOW and BISO approval is required.

4.3.3 SYSTEM LOGS REVIEW

The duties of the Systems Administrators (SA) must be segregated from the duties of the Information Security Administrator (ISA). The SA will perform system administration duties like perform service change request, OS patching and application patching etc, while the ISA will review the activities of the SA.

ISA will review the system and event logs, including activities done by SA.

For BIGIP and 3DNS, for command line access, in the current version of 4.5 for BIGIP and 3DNS, to view the last login of the users in the command line, type last. For GUI access, there is no log tracking for access.

RISK CONTROL SELF ASSESSMENT (RCSA)

Unit Risk Control Self Assessment is also done quarterly to ensure unit conformity to existing procedures and process.

Technical RCSA is also performed quarterly for specific products managed by the respective Operational units.

4.3.4 DCFC

DCFC (Departmental Control Function Checklist) is carried out daily, monthly, quarterly and annually to control what the supporting unit does to carry business as usual tasks. Unit's supervisor must acknowledge the DCFC.

For those counties and Regional Internet Operations Support engineers, the eDCFC system is used as shown in the following URL:
<http://cti.asiapacific.citigroup.net:8800/e-dcfc/>.

A template of the DCFC to be performed by country operation support can be found in Appendix B of this document.

4.4 WEB SITE DEVELOPMENT, OPERATIONS AND MAINTENANCE

- a) CTI Asia DCs are responsible for ensuring that their own websites conform to Internet Management CITMP Policies and Citigroup Web Site Standards in section 2.4.
- b) Respective Business Unit Sponsor and/or the Application Unit are responsible for ensuring Business Internet/Intranet Web Site conforms to Internet Management CITMP policies and Citigroup web site standards.
- c) CTI Asia DCs are responsible for setting up Web Server operating environment as per Software / Hardware requirement SSM documented in <http://unixeng.ssmb.com>.

4.4.1 WEB SERVER OPERATING ENVIRONMENT SETUP

CTI Asia DCs are responsible for setting up the Internet & Intranet web server operating environments (will be called web server in this document) and should follow the following procedures.

4.4.1.a Unix Operating Environment Web Server SETUP

CTI Asia DCs SA should:

- a) Web Server Build must be Solaris Security Model Build. Refer to section 1.4 (b) and (c).
- b) Web Server SSM Tier classification will be based on Business / Application input on the application information classification.
- c) Apply all patches & fixes on Web Server operating system published on Vulnerability and Threat Management (VTM):
<https://vtmac.ny.ssmb.com/vtmac/defaultN.asp>
- d) Configure all Sun Solaris web servers with RINFO package that communicates to a central server configure with ConfigDB package. ConfigDB is able to generate reports on the servers that are not SSM compliance and reports on VTM patches. These reports can be found at <http://unixeng.ssmb.com> under the Report link.

4.4.1.b Microsoft Windows Operating Environment Web Server SETUP

CTI Asia DCs Systems Administrator should:

- a) Built web servers based on Wintel Engineering guideline and Windows 2000 servers on SOE guideline. Any new web server deployment must conform to the SOE build. SOE Server build details located in the Wintel Engineering web site (<http://www.citigroup.net/tie/de/wintel/index.html>).
- b) The Operating System & Web Server must be patched with all hot fixes published on VTM:
<https://vtmac.ny.ssmb.com/vtmac/defaultN.asp>

- c) Install and setup ISS System Scanner in web servers.

4.4.1.c Audit And Review Of Web Servers

- a) CTI Asia DCs SA / ISA should generate and review the ESM report periodically for production environment for any exceptions/violations. ESM report periodically for production environment for any exceptions/vilations.
- b) CTI Asia DCs SA / ISA / BISO / DC Head should take corrective actions for any exceptions.
- c) If the exceptions cannot be corrected, a Management Awareness Oversight Program or risk acceptance has to be put up with appropriate compensating control in place.
- d) Verisign certificates expiration responsibility lies with the Business / Application Technology group. CTI Asia DCs SA / ISA will assist to monitor the Verisign certification expiration periodically.

4.5 INTRANET WEB SITE MANAGEMENT

- a) Ownership

The CTI Asia Pacific Intranet Portal will be managed and maintained by CTI Asia Pacific Business Office.

- b) Access

Access to the CTI Asia Pacific Intranet Portal will be available to all Citigroup staff and to consultants / contract staff based within Citigroup's firewalls.

Access will not be granted to personnel located outside Citigroup's firewalls without authorization. If vendor personnel require access to the portal via a firewall, the relevant Citigroup vendor manager must request for such access through a Firewall Authorization form (<http://cti.asiapacific.citigroup.net:8800/distops/intops/forms/SystemUserIDRequestForm-v3.1.doc>) authorized by CTI Asia Pacific Business Office prior to submitting to the DTI group.

- c) Branding

Global Intranet branding standards will be adhered to in the CTI Asia Pacific Intranet Portal. Detailed description of the branding standards and resources can be found at <http://www.citigroup.net/brand/intranet.htm>.

The business logo to be used within the CTI Asia Pacific Intranet Portal will be that of Citigroup since CTI Asia Pacific supports multiple business groups.

- d) Domain Names

CTI Asia Pacific Intranet Portal will have the **.Citigroup.net** domain name for the Production environment and a machine specific DNS for the UAT environment.

If the existing domain name for the CTI Asia Pacific Intranet Portal is to be modified:

- * The request must originate from the CTI Asia Pacific Managing Director (or designate), as the business sponsor of the web site
- * The domain name registration procedures as specified at <http://www.citigroup.net/citigroup.net/cdnr/> must be followed.

e) Web Site Registration

CTI Asia Pacific Intranet Portal was launched in 2Q 2000 (previously known as APPC Intranet) and as such is defined as a 'legacy' web site by the Citigroup Website Standards. As per the registration requirements of a legacy web site, the CTI Asia Pacific Intranet Portal (APPC Intranet) site has been registered with the Citigroup Web Hosting Infrastructure (CWHI) representative.

If and when an additional Intranet website is to be launched for TI Asia Pacific, the new site should conform to Section 5 of the Citigroup Web Site Standards and follow the registration procedures given at <http://www.citigroup.net/citigroup.net/cwhi/register.htm>.

f) Periodic Review for Compliance, Obsolescence and Dormancy

It will be the responsibility of the CTI Asia Pacific Business Office to review the currency of the overall CTI Asia Pacific Intranet Portal on a semi-annual basis. However, for web pages specific to CTI Asia Pacific units, it will be the responsibility of the unit manager to ensure currency and compliance of content.

- * The review will be conducted by accessing web pages under the following sections of the portal:
 - Tools and Applications
 - Datacenters
 - Distributed Operations
 - Human Resources
 - Financial Control
 - People and Workplace
 - Engineering Services
 - IS and Compliance.
 - Project Management Office

Web pages and links appearing under the Useful Links section are not subject to the review procedure since they are owned and managed by non-CTI Asia Pacific entities.

- * The review procedure will examine web pages to ensure that:
 - Citigroup Intranet Branding Standards as specified at <http://www.citigroup.net/brand/intranet.htm> are conformed to.
 - Section 10 of the Citigroup Web Site Standards is adhered to.
- * It will be the responsibility of the respective web page owners to ensure the currency of unit level practices, procedures and documentation published on the portal.
- * Any evidence of obsolescence or non-conformance will be notified to the owner of the web page via e-mail and followed through to corrective action.

g) Web Site Content Maintenance and Changes

CTI Asia Pacific will not develop or launch new web sites. However, as and when necessary CTI Asia Pacific will implement small-scale tools within the existing portal infrastructure. In implementing such tools:

- * The Automation team will ensure that the implementation will benefit TI Asia Pacific by yielding one or more of: cost savings, productivity gains, paper usage savings or process improvements.
- * System Development Lifecycle (SDLC) steps as listed in the Intranet Modification Request form will be followed. Send an email to "gt ap appc auto" for a copy of the request form.

Additions, deletions and other changes to static web page content (e.g. html pages, word documents and spreadsheets available on CTI Asia Pacific Intranet Portal) will be carried out at the discretion of the respective unit, and will not be subject to the steps outlined in the Intranet Modification Request form.

h) Restricted Technologies and Content Types

CTI Asia Pacific Intranet Portal will conform to Section 11 of the Citigroup Web Site Standards.

- * Any use of technology components defined as 'Restricted Technologies' by CWHI (refer to <http://www.citigroup.net/citigroup.net/cwhi/ths.htm#restricted> and Appendix E of the Citigroup Web Site Standards) will require the appropriate Restricted Technology Permit Request form to be submitted. This form can be downloaded from: <http://www.citigroup.net/citigroup.net/cwhi/downloads.htm>.
- * The information contained in the TI Asia Pacific Intranet Portal is classified as 'Internal'. Any information classified as 'Restricted' or 'Confidential' will not be published on the TI Asia Pacific Intranet Portal.

i) Corporate Technology Requirements and Compliance

CITMP will be complied with in maintaining and operating the CTI Asia Pacific Intranet Portal. Citigroup Website Standards (Section 18: Minimum Requirements for Intranet Web Sites) will also be conformed to:

- Section 6: "Domain Names;"
- Section 7: "Centralized Web Site Registration;"
- Section 10: "Periodic Review for Compliance, Obsolescence and Dormancy;"
- Section 11: "Restricted Technologies and Content Types;"
- Section 12: "Use of External Vendors or Servers and Links to Third Party Sites;"
- Section 17: "Corporate Technology Requirements".
- Import and export of technology, software, and data – In accordance with the Citigroup Web Site Standards, the use or distribution of software (including encryption software) that requires licensing or export controls must be approved by the CWHI Group. It is the

responsibility of the Sponsor Business for a web application utilizing this technology to: (1) Obtain the necessary CWHI approvals and (2) Ensure compliance with the applicable import and export laws.

- Use of telecommunications technology and encryption - The use of telecommunications and encryption must also be compliant with applicable laws and regulations. It is the responsibility of the Sponsor Business to consult with their Legal Counsel and Compliance Officer to ensure all applicable laws are addressed. The GISO for the Business Sponsor must ensure that the data is encrypted in accordance with the Citigroup Information Security Standards except where prohibited by local law.
- Transmission of personal data across national borders – It is the responsibility of the Business Sponsor to consult with its Legal Counsel and Compliance Officers regarding the applicable laws relating to the transmission of data across national borders based on the functionality of their web site.
- Protection of privacy - All applications must comply with the Citigroup Privacy Promise (<http://www.citigroup.com/citigroup/privacy/index.htm>). It is the responsibility of the Sponsor Business working with their Legal Counsel and Compliance Officer to ensure that non-public information from an applicant or customer is used only as permitted by customer notice, consent and applicable law. Further, all Web applications owned or managed by the Sponsor Business must be operated in conformity with and conspicuously display the Citigroup Privacy for Consumers (i.e., displayed intact as a free-standing document) if applicable, the Business Unit Sponsor's own privacy policy and any other legally mandated privacy disclosures.
- Further, the use of certain technologies that use data models (e.g., Cookies or local storage of confidential information even temporarily be made known to the customer) on the Citigroup web sites must comply with Citigroup's privacy promise. In addition, Internet customer-facing applications must review and comply with the Citigroup Platform for Privacy Preferences (P3P) toolkit document (<http://www.citigroup.net/internet/p3p.doc>) to ensure customers using P3P equipped browsers are able to access Citigroup sites. Because legal requirements regarding the permissibility and disclosure of the use of cookies is dynamic and evolving, the Sponsor Business is responsible, with the support of the application developer, for consulting with their Legal Counsel and Compliance Officer with regard to use and disclosure of cookies.
- Protection of copyrights (including messages, other written materials, iconography, and software) and intellectual property in general - The Business Unit Sponsor is responsible for consulting with their Legal Counsel and Compliance Officer as it applies to Trademark and Intellectual Property issues. Business Legal must consult with the appropriate Trademark and Intellectual Property Counsel in advance of publication. It is the Business Unit Sponsor's responsibility to ensure that it owns or has the rights to the intellectual property used in the development and operation of its web site, e.g., product or service names; logos, trade and service marks; iconography; music; images; text and quotes.

Any non-compliance will be raised as a control issue and tracked until closure.

4.6 CONTINUITY OF BUSINESS (COB)

Citiplex is a true COB (Continuity of Business) infrastructure. It employs two interconnected data centers, connected to the Internet by two different ISP carrier providers. It is also provisioned with fully redundant components from front to back, including dynamic load balancing and a full mesh of switches, routers and firewalls. Collectively, these data centers provide Business Units with continuous Web Hosting services, even in the event of the loss of an ISP, an ISP's carrier or a complete Data Center due to some localized event.

The only impact is when the country proxy is down. The user browser will be routed to US proxies. The user will experience slower response time for Internet access.

During COB drill, default route settings in the external routers of Telepark and Cintech II have to be changed for some dedicated business applications that directly connected to external segment of Citiplex by Cyberguard firewall.

4.6.1 CITIBANK ONLINE

For Citibank Online (CBOL) application, the arrangement had been made so the webserver (DA home) will access COB Bafes in case of production Bafes site is down. The necessary ports are already opened for all country's CBOL that's already in Citiplex Web Hosting Pod. In COB test, Regional Internet Operations Support Engineer will disable the testing site Pool in the 3DNS so it's not available to users. Business COB tester will connect to the server using a direct static DNS name of the DA home server. External firewalls will be configured to allow only this testing user during COB drill.

4.6.2 CITIVPN

For CitiVPN, the infrastructure in place transparently fails over to the surviving site should there be a catastrophic failure at any one site. The COB test is conducted annually. Regional Internet Operations is responsible to maintain the CitiVPN COB procedure and conduct the COB test.

4.6.3 INDIA WEBHOSTING COB

For India Internet web hosting infrastructure, India Data Center maintains the COB plan. TI India will support this COB plan.

4.7 CHANGE MANAGEMENT

Change management in CTI Asia follows the procedure in this URL:
<http://cti.asiapacific.citigroup.net:8800/distops/stdocs.htm>

4.8 PROBLEM MANAGEMENT

Problem management in CTI follows the procedure in this URL:
http://cti.asiapacific.citigroup.net:8800/cti_citmp.htm

Virtualtech (<https://virtualtech.eur.nsroot.net/virtualtech/defaultnt.asp>) is used to log and monitor problems within Citigroup.

All faults should be logged to VirtualTech or into the Country Helpdesk (including India), whereby a trouble ticket will be opened and assigned. Faults could be also reported into APPC Customer Service Helpdesk. If the problem needs to be resolved by CRI Internet and Security Operations, APPC will assign the GPMS to Regional TOC who will then open a VirtualTech for Regional Internet Operations. The group id is ASPAC Regional Internet Operations.

For other Internet-related problems, such as DNS problem, Web Enrollment problem, proxy cache problem, etc., see the following table:

PROBLEM TYPES	REPORTING TO	PHONE NO.
DNS, proxy server, Web enrolment	CSC Helpdesk	1-212-809-9361
Firewall (Cyberguard)	CTAC Helpdesk	1-212-723-4480

For vendor support, Regional Internet Operations Support maintains and updates the escalation list quarterly.

5. APPENDIX A: URL REFERENCES IN THIS DOCUMENT

- a) Unix SOE URL:
<http://unixeng.ssmb.com/>
- b) Unix SOE Global Deployment Services URL:
<http://gdsunix.ny.ssmb.com/>
- c) Windows 2000 SOE URL:
<http://www.citigroup.net/tie/de/wintel/index.html>
- d) CITMP URL:
<http://www.citigroup.net/citmp/>
- e) Citigroup Information Security Standards URL:
<http://www.citigroup.net/ciso/doc/standards.doc>
- f) Citigroup Web Hosting Infrastructure URL:
<http://www.citigroup.net/citigroup.net/cwhi/>
- g) Citigroup Information Security Services URL:
<http://www.citigroup.net/informationsecurityservices/>
- h) CTI CITMP Level2 – Internet Management
http://www.citigroup.net/ti/compliance/citmp_level2.htm
- i) Asia Desktop Portal URL:
<http://desktop.asia.citigroup.com/>
- j) CDNR URL:
<http://www.citigroup.net/citigroup.net/cdnr>
- k) Internal DNS update URL:
<https://ip03rut.nam.nsroot.net/webreq/>
- l) EDCFC URL:
<http://appcweb.citicorp.com/e-dcfc/>
- m) VTM URL:
<https://vtmac.ny.ssmb.com/vtmac/defaultN.asp>
- n) Citigroup Branding URL:
<http://www.citigroup.net/brand/intranet.htm>
- o) Project Management procedure URL:
<http://cti.asiapacific.citigroup.net:8800/eis/pmo/>
- p) Change Management procedure URL:
<http://cti.asiapacific.citigroup.net:8800/distops/change.htm>
- q) VirtualTech URL:
<https://virtualtech.eur.nsroot.net/virtualtech/defaultnt.asp>
- r) WWDS URL:
<http://remoteaccess.citigroup.net/forms.php>

6. APPENDIX B: E-DCFC

6.1 DAILY TASKS

Task Description	Applicability
Ensure Security incidents are to be reported to unit Head and BISO with a CISO SIRT reporting for next step	Countries with Citiplex Infrastructure

6.2 MONTHLY TASKS

Task Description	Applicability
Check validity of business- sponsored urls are renewed based on CDNR records.	All countries
Analyze Detailed Internet Usage report for any Internet misuse	All countries

6.3 QUARTERLY TASKS

Task Description	Applicability
Update Internet Management section on Process Control Manual.	Countries with Citiplex Infrastructure