For discussion
on 14 April 2008

Legislative Council Panel on Information Technology and Broadcasting

Enhancing Preparedness for Telecommunications Contingencies

Background

At the Panel meeting held on 15 January 2007, the Office of the Telecommunications Authority ("OFTA") briefed Members on the impact of the earthquake which occurred in the Luzon Strait on 26 and 27 December 2006 (the "Incident") on the external telecommunications services of Hong Kong. OFTA further briefed Members at the Panel meeting held on 17 April 2007 on the actions taken by OFTA in the aftermath of the Incident. At that meeting, Members asked for further information on:

(a) OFTA's contingency plan in response to such emergency incidents and the dissemination of information to the public in the event of disruptions to IDD and Internet services, etc;
(b) the damages and losses suffered by the Small and Medium Enterprises ("SMEs") as a result of the Incident; and
(c) any specific measures which would be taken by the Administration to help SMEs impacted by the Internet outage during the Incident and in future.

2. This paper addresses the specific questions raised by Members, and briefs Members on the latest development of the telecommunications and Internet infrastructure of Hong Kong and the additional measures that have been implemented to further improve the preparedness of Hong Kong to cope with similar incidents in future.

Enhanced Network Outage Reporting Mechanism

3. To facilitate the coordination of contingency actions with the telecommunications operators in respect of major incidents or disasters that may adversely affect the normal operation of the telecommunications services, it is important for OFTA to obtain accurate and timely information from the operators so as to assess the impact of such incidents or disasters. OFTA has long established an Emergency Response System under which an emergency response team will stand by round the clock and 365 days a year (including public holiday) which will keep in close contact with its counterparts (including operators, relevant Government agencies and overseas administrations) to obtain first hand information about emergency incidents. Operators are also required to report outage of the public telephone networks. In the light of the Incident, OFTA issued a new set of guidelines (Annex A) on 28 February 2007 with a view to enhancing the reporting mechanism by requiring the concerned operators to report outages of submarine cable systems, external telecommunications services and Internet services within the prescribed timeframe.

4. As reported in the Panel Paper No. CB(1)1298/06-07(10) submitted on 17 April 2007, in the event of outage of the major submarine cable systems, etc, the concerned operators are required to report to OFTA within 2 hours from the confirmation of the incident or within 4 hours from the happening of the incident. In the event of a major outage of the public telephone network, the operator concerned is required to report to OFTA within one hour after the reporting criteria are met[1].

5. Since the promulgation of the guidelines, OFTA issued nine alerts related to earthquakes to the operators (Annex B). Three network fault reports due to damage of submarine cable system by an earthquake

[1] "Guidelines for Fixed and Mobile Network Operators for Reporting Network Outage".

near Taiwan in September 2007 were received. In this incident, the concerned operators were able to duly comply with the guidelines by reporting the network outage within the prescribed timeframe, thus proving that the enhanced reporting mechanism works and functions smoothly. In addition, by re-routing the communications traffic through contingency routes, IDD and Internet services of Hong Kong were not affected. It proved that the contingency plans and measures of the operators are generally effective to maintain Hong Kong's external telecommunications services during such emergency incidents.

6. Separately, OFTA receives and handles enquiries and complaints from the general public about telecommunications services in Hong Kong. If a large number of enquiries/complaints are received within a short period of time against a particular operator, there may be ground to believe that faults have developed in the network of the concerned operator. In such case, OFTA will proactively contact the operator concerned to confirm whether a fault has indeed occurred. Although normally such faults would be confined to the network of a single operator, OFTA will nonetheless closely monitor the situation in respect of other operators.

Issuance of Public Alert

7. OFTA fully appreciates Members' concern about the need for the provision of timely information to the general public in relation to telecommunications network congestion or disruption. Therefore, if the Director-General of Telecommunications (Director-General) is of the view that a critical incident such as serious network congestion or outage has severely affected or has the potential of severely affecting the public telecommunications services[2], the Director-General will alert the public through making public warning messages on TV and radio within one

[2] Examples of critical incidents that may severely affect the public telecommunications services are complete failure of critical network facilities (such as public telephone exchange and mobile switching centre), or simultaneous failure of more than half of all the major submarine cables.

hour or so after receipt of the report submitted by the operator between 0900 and 1700 on a weekday (except for public holiday). For reports received outside this window, while more time may be needed to confirm details and arrange for the appropriate announcement to alert the public, OFTA will seek to follow the foregoing arrangement as far as practical. After such warning is issued, OFTA will keep the public informed of the latest status of the incident and the progress on the recovery of the affected services until the incident is cleared.

Impact on SMEs Caused by the Incident

8. The Incident had reduced the usable capacity of the submarine cable systems passing through the Luzon Strait to only 10% of its normal level. The public Internet service was seriously affected and businesses that relied on the public Internet for external communications were adversely affected. Following the implementation of contingency measures by the telecommunications service operators (including using satellites and overland cables passing through the Mainland and Europe to re-route the traffic), the communication and Internet services between Hong Kong and other places resumed within a short period of time. IDD and roaming services to all countries/territories (except Taiwan and South Korea) also resumed within two days after the earthquake, while about 80% of the international connection capacity of the Internet service was recovered by 2 January 2007, the first business day after the Christmas and New Year holidays following the Incident. During the normal business hours on 2 January 2007, the quality of the Internet services for business users was basically in order.

9. As reported in the Panel Paper No. CB(1)1298/06-07(10), OFTA attended the industry forum organized by the Professional Information Security Association in January 2007 and the meeting of the Small and Medium Enterprises Committee ("SMEC") held by the Trade and Industry Department in February 2007 to discuss matters concerning the Incident and the impact on SMEs. While representatives of SMEs

had not provided specific information in respect of the impact on them arising from the Incident, they requested OFTA to:

(a) draw up guidelines on contingency plans for the operators concerned to follow;
(b) advise the submarine cable operators to avoid laying cables in the earthquake regions; and
(c) request the Internet Service Providers to provide SMEs with backup and diversity services.

Actions required in respect of (a) had already been completed and were reported in the Panel Paper No. CB(1)1298/06-07(10). Details regarding (b) and (c) are provided in paragraphs 10 to 12 below.

Updates on Hong Kong's Telecommunications and Internet Infrastructure

10. Hong Kong needs a reliable telecommunications infrastructure to ensure that it can withstand future incidents that may be caused by failure of multiple submarine/overland cable systems on a scale similar to the Incident. After the Incident, the operators concerned have taken various initiatives to enhance their capacity. The total activated capacity of external facilities has increased from 698 Gbps in December 2006 to 1 323 Gbps in December 2007, an increase of almost 90%. The capacity of submarine cable and land cable over the Mainland of China has increased by 464 Gbps and 161 Gbps respectively (which represent an increase of 99.7% and 70.2% respectively). All these have been achieved through commercial initiatives. The availability of additional overland cable capacity means that more cable capacity is now available on land for diversion of traffic in case we encounter another major disruption to the submarine cable systems. The enhanced capacity of external facilities as a whole has boosted Hong Kong's position as a telecommunications hub in the region.

11. As revealed by some of the deputations at the Panel meeting held on 15 January 2007, local websites which deployed overseas domain names ending with ".com" or ".net" and the like were inaccessible during the Incident. This is because the authoritative root name servers associated with these domain names are mostly situated overseas which were unreachable during the Incident. With the communications links to these authoritative root name servers disconnected during the Incident, users could not access the relevant servers to get the associated Internet Protocol address for proper data routing. To overcome this shortfall, the Hong Kong Internet Exchange ("HKIX"), which is managed by the Chinese University of Hong Kong, has collaborated with Verisign, Inc.[3] and established a Regional Internet Resolution ("RIR") Site in Hong Kong and this has been brought into operation since February 2008. With the establishment of the RIR Site in Hong Kong, end customers (including the business community and SMEs) will no longer have to rely solely on overseas authoritative root name servers to access web sites with ".com" and ".net" domain names. The establishment of the RIR Site in Hong Kong has therefore improved the resilience of our Internet services and should further enhance our position as the telecommunications and Internet hub in the region.

12. It was widely reported that the Incident had affected many countries in the region. Hong Kong cannot therefore work on its own to reduce the threat of potential service outage due to disruption of the submarine cable systems. The telecommunications operators in the region have joined hands to further improve the reliability of the regional submarine cable infrastructure as follows-

(a) a number of Asia-Pacific economies have proposed new submarine cable systems with route diversity to bypass the earthquake zone in the Luzon Strait. The consortia concerned have approached OFTA with a view to connecting these new cable systems to Hong Kong. OFTA will offer assistance to

[3] VeriSign, Inc. is the authoritative directory provider of all .com, .net, .cc, and .tv domain names.

facilitate the projects; and

(b) a total of 14 telecommunications companies in the Asia-Pacific region, including one telecommunications operator in Hong Kong, have signed a memorandum of agreement to pursue cooperation initiative that will pool all available resources at their disposal to deal with major cable failures that may occur in future.

All these will serve to improve the reliability and resilience of our telecommunications infrastructure and the services provided to end customers.

Updates on Hong Kong's Preparedness to Handle Similar Incidents in Future

13. Further measures that have been implemented to improve the preparedness of Hong Kong to cope with similar network outage in future include-

(a) Cooperation with Counterpart Administration

OFTA has made arrangements with its counterpart in Singapore, the Info-communications Development Authority, on information exchange relating to failure of major submarine cable systems that link up Hong Kong and Singapore. Notification mechanism of such a nature will help secure early warning and first hand information about incidents that may adversely affect our telecommunications services.

(b) Issuance of Guidelines to SMEs

The Government issued through its one-stop information security portal (http://www.infosec.gov.hk/english/promotion/files/sme_guide_2007_eng.pdf) the "Information Security Guide for Small Businesses" (Third Edition) in September 2007, including a new section on disaster recovery and business

continuity planning for the SMEs' reference in planning for adverse conditions in future. (An extract of this new section is at Annex C.)

Conclusion

14. OFTA fully appreciates public concern for the issue of early warning in respect of serious network congestion or outage of the telecommunications services. The telecommunications and Internet infrastructure have been strengthened and various improvement measures have been put in place. OFTA will maintain its vigilance and stands ready to disseminate the necessary information in a timely manner to the public in the event of disruption to public telecommunications services.

Commerce and Economic Development Bureau
Office of the Telecommunications Authority
April 2008

Annex A

Guidelines for Cable-based External Fixed Telecommunications Network Services Operators and Internet Service Providers for Reporting Network and Service Outages

Office of the Telecommunications Authority

Issue 2
29 January 2008

CONTENTS

1 Introduction

1.1 Public telecommunications networks and services form a critical part of the information infrastructure in Hong Kong. The information on public telecommunications network and service outages is essential to maintain and improve the infrastructure reliability as it provides the basis for the Office of the Telecommunications Authority ("OFTA") to determine whether the patterns of outages justify government interventions or industry cooperation initiatives to prevent the recurrence of similar outages. The critical need for rapid and accurate information is also recognized in times of outages to assess their impacts and to determine whether immediate responses are required to contain or minimise the impacts.

1.2 Under their respective licences, public telecommunications operators are obliged to provide their services in a manner satisfactory to the Telecommunications Authority ("TA") at all times. To fulfill his functions and responsibilities in respect of overseeing the operators' compliance with the licensing condition, the TA issues this document entitled "Guidelines for Cable-based External Fixed Telecommunications Network Services Operators and Internet Service Providers for Reporting Network and Service Outages" ("the Guidelines").

1.3 The Guidelines should be observed by the cable-based external fixed telecommunications network services operators and Internet service providers (collectively called the operators). In the event of network or service outages, the operators should report the outages to OFTA in accordance with the criteria and timeframes set out in the Guidelines.

1.4 Both the operators and OFTA should play their respective roles in advising the users and the public. The operators, having the first-hand information about the operational status of their networks and services, should be responsible for providing prompt information and advice to their customers on outages or degradation. Where the outage or degradation falls within the reporting criteria, the operator concerned should, in addition to providing information and advice to its customers, report to OFTA within the specified timeframe. OFTA, upon receiving such information, should promptly inform the public and provide guidance where necessary if the outage or degradation is assessed to have significant and territory-wide implications.

1.5 The commercial sensitive information contained in the outage reports submitted by the operators should be treated as confidential and should not be disclosed without consent from the operators concerned.

1.6 The Guidelines should be subject to continuous review to keep pace with the technological and market changes in order to safeguard the public interest.

2 Reportable Outage

2.1 An outage is defined as a loss of or a significant degradation in the ability of the customer to establish and/or maintain a channel of communication as a result of failure or degradation in the performance of an operator's network or service.

2.2 In addition to incidents of software or hardware outage, significant degradation occurs when traffic produces excessive demands on available system resources, resulting in switch congestion or system overload.

2.3 The criteria for determining whether an outage event is reportable and the reporting procedures are given in Appendices A, B and C for submarine cable system outage, external telecommunications services ("ETS") outage and Internet service outage respectively. Submarine cable system operators[1], cable-based external fixed telecommunications network services operators other than submarine cable system operators, and Internet service providers are required to comply with Appendices A, B and C respectively.

2.4 The reportable events given in the Appendices A, B and C are by no means exhaustive. Operators should, whenever necessary, report to OFTA on other events that may have significant impact on their network operation or services.

[1] For the purpose of the Guidelines, the term "submarine cable system operators" refers to the cable-based external fixed telecommunications network services operators who operate submarine cable systems.

3 Information to be Provided by the Operator when Reporting an Outage

3.1 When reporting an outage to OFTA, the operator concerned should provide OFTA with the following information, whenever possible :-

(a) name of operator;
(b) description of incident;
(c) date and time of onset of the incident;
(d) types and estimated number of customers/end-users affected;
(e) affected areas;
(f) actions taken; and
(g) contact information: name of contact person as well as the person's fixed and mobile telephone numbers and email address.

4 Updates on Network and Service Status

4.1 During the recovery stage, the operator concerned should inform OFTA of the status of the affected network/service. Under critical circumstances, OFTA may specify the update frequency and the information to be provided by the operator concerned to facilitate the assessment on the impact of the outage and the progress of recovery of the affected network/service.

5 Incident Report

5.1 A preliminary report should be submitted to OFTA within 3 working days from the happening of the incident. The preliminary report should give a detailed account of the incident, the events which lead to the occurrence of the outage and the remedial actions taken.

5.2 Where requested by OFTA, a full report should be submitted to OFTA within 14 working days from the happening of the incident or other deadline as specified by OFTA. The full report should give a detailed account of the measures which have been taken (or will be taken) in order to prevent similar incidents from happening again.

6 Contact Points

6.1 OFTA's contact points for reporting outage are as follows :-

[Intentionally Left Blank]

6.2 Each operator is required to provide OFTA with the contact information of its focal point responsible for reporting outage to OFTA, including the names, fixed and mobile telephone numbers and email addresses of the first and second contact persons. Whenever, there is any update on the contact information, the operator should inform OFTA of the change at least 5 days before the effective date.

Appendix A

Submarine Cable System Outage

The reporting criteria are given in Section A1. In the event of a submarine cable system outage, the submarine cable system operator should report the outage to OFTA within the timeframe set out in Section A2. Sections A3 and A4 show the examples of submarine cable system outage and the main steps for reporting the outage respectively.

Section A1 Events of Submarine Cable System Outage

	Event	Duration of outage (minutes)
Fishbone/linear submarine cable systems	Dual failures in two fishbone/linear submarine cable systems causing Hong Kong to be unable to communicate with other places by means of these two systems	> 30
Ring or other types of submarine cable systems	Failure in a ring or other type of submarine cable system causing Hong Kong to be unable to communicate with other places by means of that system	> 30
Backhauls	A loss of more than 50 % of the backhaul capacity of a submarine cable system within Hong Kong	> 30

Section A2 Timeframe for Reporting Submarine Cable System Outage

Occurrence Time	Initial Report	System Normalization
Between 00:00 and 24:00 of each day	The operator concerned should report the submarine cable system outage to OFTA within 2 hours from the confirmation of the outage or within 4 hours from the happening of the outage, whichever is earlier. Under critical circumstances, OFTA may request the operator concerned to submit the initial report within a shorter period of time.	The operator concerned should report to OFTA within 1 day from the completion of system normalization. Under critical circumstances, OFTA may request the operator concerned to report to OFTA within a shorter period of time.

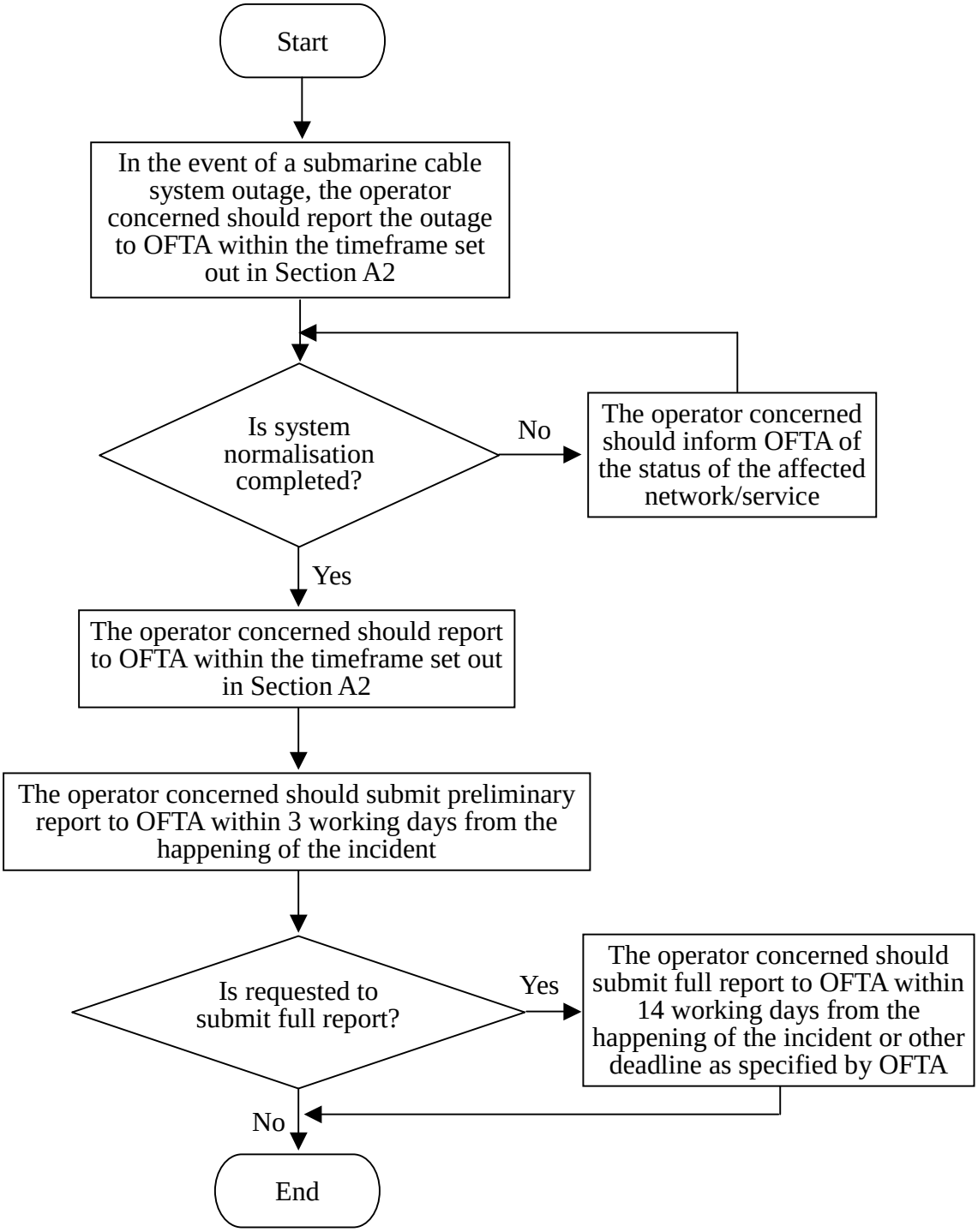
Section A3 Examples of Submarine Cable System Outage

- Incidents of submarine cables such as submarine cables being damaged by anchors dropped from ships, dredging fishing nets, earthquakes or other unknown reasons.

- Multiple failures in the backhaul links leading to a loss of more than 50 % of the backhaul capacity of a submarine cable system within Hong Kong.

Note: The list above is by no means exhaustive. Operators should report other submarine cable system outage that is not covered in the list, if deemed necessary.

Section A4 Flowchart Showing the Main Steps for Reporting Submarine Cable System Outage



Appendix B

External Telecommunications Services Outage

The reporting criteria are given in Section B1. In the event of an ETS outage, the cable-based external fixed telecommunications network services operator (other than submarine cable system operator) should report the outage to OFTA within the timeframe set out in Section B2. Sections B3 and B4 show the examples of ETS outage and the main steps for reporting the outage respectively.

Section B1 Event of ETS Outage

Event	Duration of outage (minutes)
A loss of more than 50% of the activated capacity between Hong Kong and another place	> 30

Section B2 Timeframe for Reporting ETS Outage

Occurrence Time	Initial Report	Restoration of Service
Between 00:00 and 24:00 of each day	The operator concerned should report the ETS outage to OFTA within 2 hours from the confirmation of the outage or within 4 hours from the happening of the outage, whichever is earlier. Under critical circumstances, OFTA may request the operator concerned to submit the initial report within a shorter period of time.	The operator concerned should report to OFTA within 1 day from the restoration of network/service. Under critical circumstances, OFTA may request the operator concerned to report to OFTA within a shorter period of time.

Section B3 Examples of ETS Outage

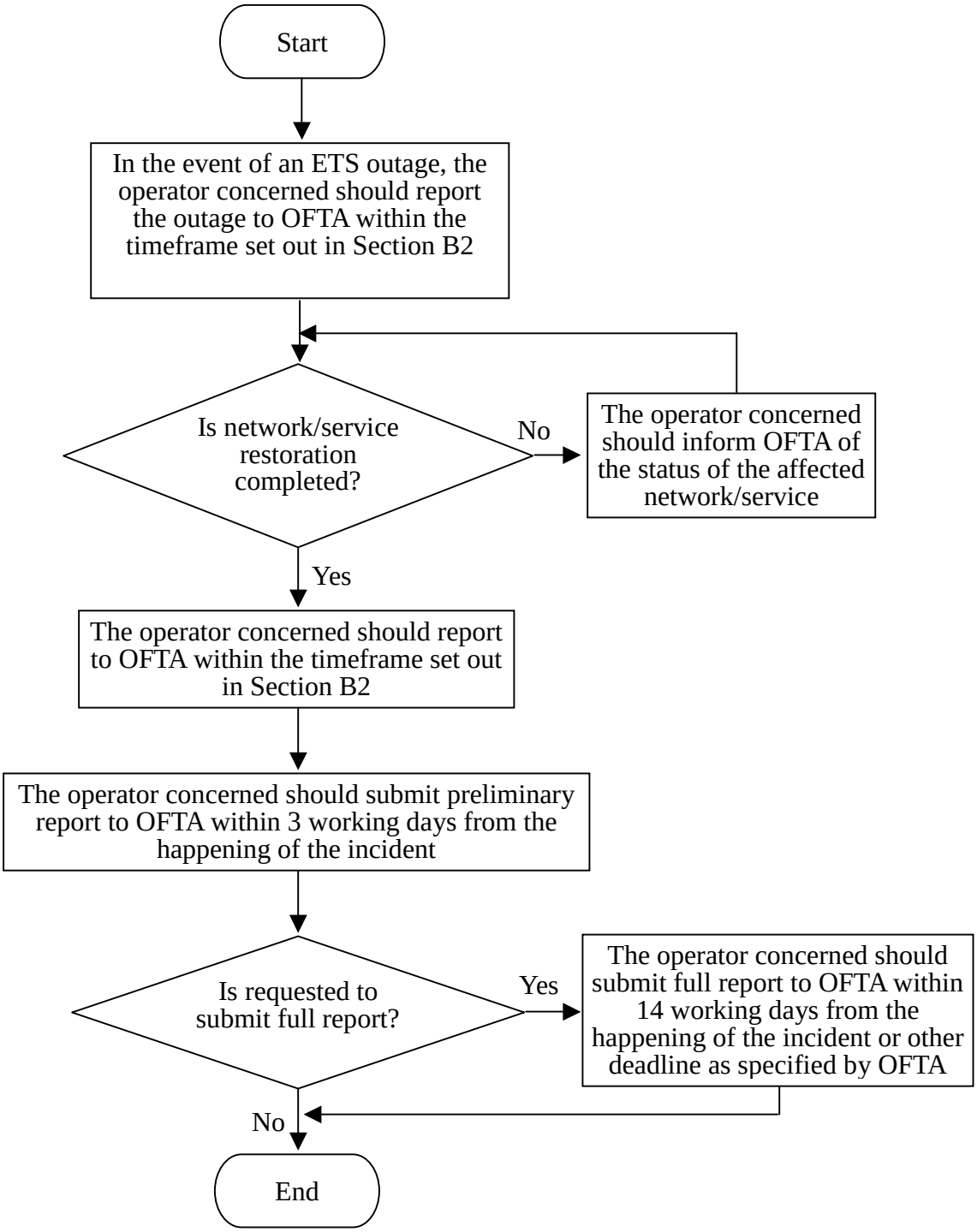
- Failure(s) in submarine cable system(s) or overland cable system(s) leading to a loss of more than 50 % of activated capacity between Hong Kong and another place.

- Multiple failures in the backhaul links leading to a loss of more than 50 % of backhaul capacity.

- Total failure in the main switch and the standby switch.

Note: The list above is by no means exhaustive. Operators should report other ETS outage that is not covered in the list, if deemed necessary.

Section B4 Flowchart Showing the Main Steps for Reporting ETS Outage



Appendix C

Internet Service Outage

The reporting criteria are given in Section C1. In the event of an Internet service outage, the Internet service provider should report the outage to OFTA within the timeframe set out in Section C2. Sections C3 and C4 show the examples of Internet service outage and the main steps for reporting the outage respectively.

Section C1 Events of Internet Service Outage

	Event	Duration of outage (minutes)
External Connectivity	A loss of 50 % or more of the total bandwidth to HKIX	> 30
	A loss of 50 % or more of the total bandwidth to local peers	> 30
	A loss of 50 % or more of the total bandwidth to any one of the following destinations :- • USA/North America • Mainland China • Asia Pacific countries • UK/Europe	> 30
	Total bandwidth utilization to any one of the following destinations reaching or exceeding 95 % :- • HKIX • Local Peers • USA/North America • Mainland China • Asia Pacific countries • UK/Europe or	> 30

	Event	Duration of outage (minutes)
External Connectivity	Total bandwidth utilization to any one of the following destinations dropping to 50 % or below (with reference to the date/time of the previous week) :- • HKIX • Local Peers • USA/North America • Mainland China • Asia Pacific countries • UK/Europe	> 30
Core Network	Degradation of service or failure of critical components including, but not limited to, DNS, routers or switches that would affect/potentially affect 10,000 or more users	> 30
User Connectivity	Degradation of service or failure of critical components including, but not limited to, DHCP, or authentication servers that would affect 10,000 or more users	> 45

Section C2 Timeframe for Reporting Internet Service Outage

Occurrence Time	Initial Report	Restoration of Service
Time Zone 1 (Between 08:30 and 01:00 of next day)	The operator concerned should report the Internet service outage to OFTA within 1 hour from the happening of the outage	The operator concerned should report to OFTA within 2 hours from the restoration of the network/service
Time Zone 2 (Between 01:00 and 08:30)	The operator concerned should report the Internet service outage to OFTA within 1 hour from the happening of the outage or by 08:30, whichever is later	The operator concerned should report to OFTA within 2 hours from the restoration of the network/service or by 08:30, whichever is later

Section C3 Examples of Internet Service Outage

- A loss of 50 % or more of the total connection bandwidth to HKIX.

- A loss of 50 % or more of the total bandwidth to any one of the following destinations :-

  - Mainland China
  - US
  - UK/Europe
  - Asia Pacific countries.

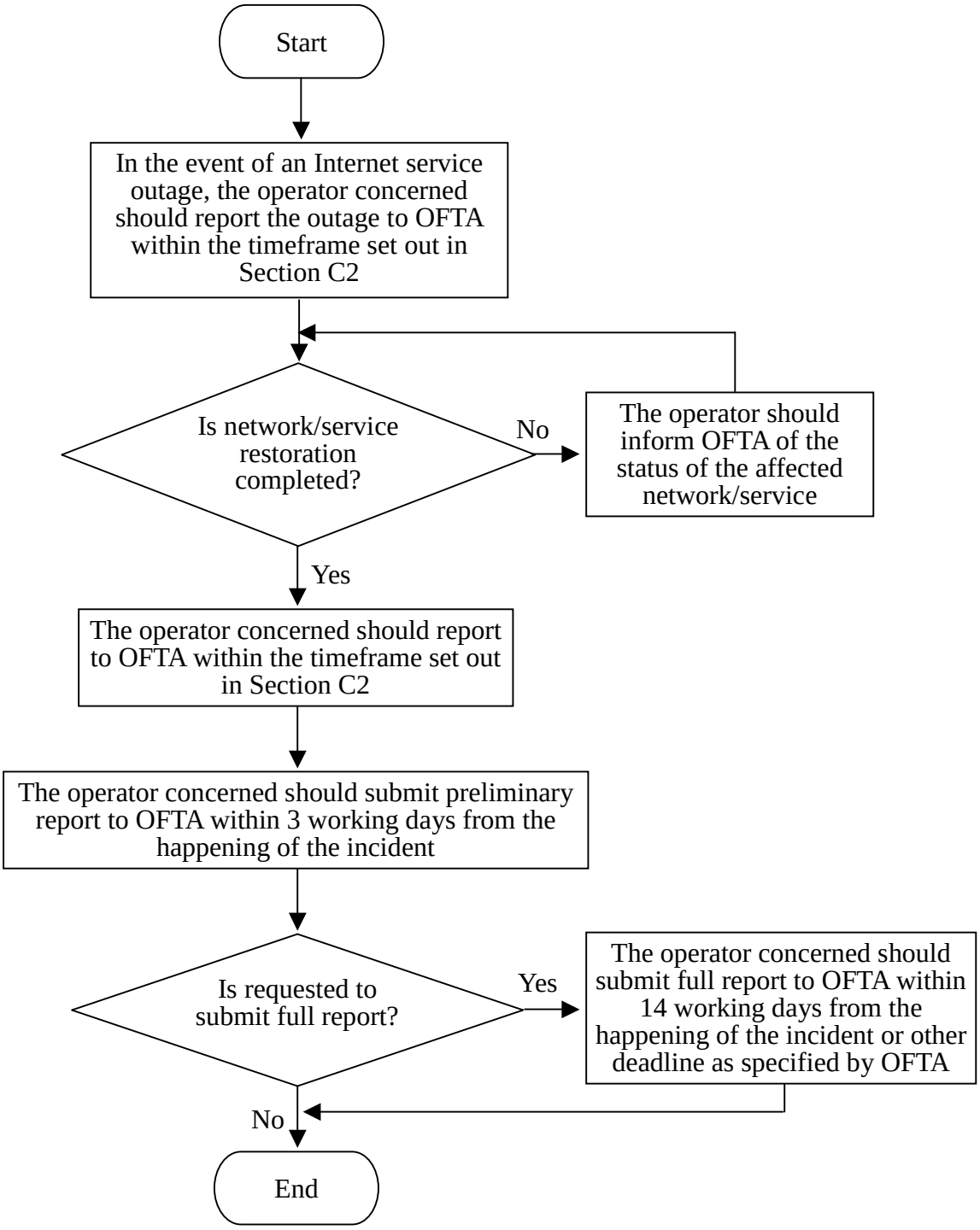
- 95 % or more of the total bandwidth utilization of connections to HKIX is constantly reached for 30 minutes.

- 10,000 or more users are unable to connect to the Internet.

- Failure of core routers/switches causing 10,000 or more users to be unable to access to the Internet.

Note: The list above is by no means exhaustive. Operators should report other Internet service outage that is not covered in the list, if deemed necessary.

Section C4 Flowchart Showing the Main Steps for Reporting Internet Service Outage



Annex B

Alerts Related to Earthquakes Issued by OFTA and Impacts on Hong Kong External Telecommunications Services Caused by the Earthquakes (Since 28 February 2007)

Date	Location	Impact on Submarine Cables	Impact on Hong Kong External Telecommunications Services	Outage Report within Prescribed Timeframe
20.4.2007	Luzon Strait	No	No	Not applicable
7.9.2007	Near Su-ao, Taiwan	Three submarine cables were damaged	Traffic re-routed. Internet and IDD services of Hong Kong were not affected.	Yes
12.9.2007	Sumatra, Indonesia	No	No	Not applicable
18.2.2008	Near Taitung, Taiwan	No	No	Not applicable
20.2.2008	Philippine Islands Region	No	No	Not applicable
3.3.2008	Luzon Strait	No	No	Not applicable
5.3.2008	Near Taitung, Taiwan	No	No	Not applicable
29.3.2008	Philippine Islands Region	No	No	Not applicable
1.4.2008	Luzon Strait	No	No	Not applicable

Annex C

Extract of Information Security Guide for Small Businesses (Third Edition)

3.2 Contingency Management

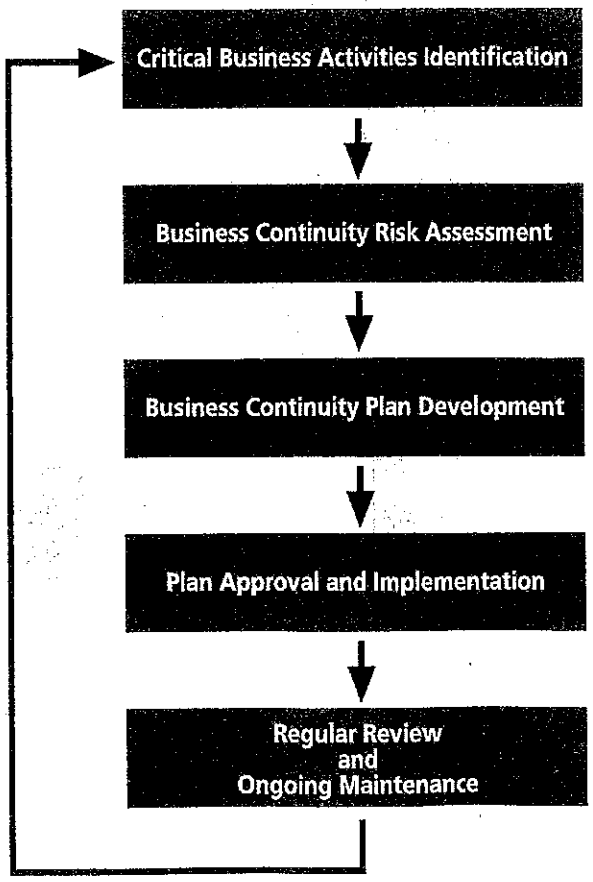
Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, disk drive failure) to severe disruptions (e.g. equipment destruction, fire, natural disasters). Many of these vulnerabilities and impact may be minimized or eliminated through management, operational and technical controls. A contingency plan should be developed to enable sustained execution of mission critical business activities and information systems in the event of a disastrous disruption.

There are different types of contingency plans. The two most common ones are Business Continuity Plan and Disaster Recovery Plan. Business continuity plan focuses on sustaining an organization's critical business activities during and after a disruption, whereas disaster recovery plan provides detailed procedures to facilitate recovery of IT capabilities.

3.2.1 Business Continuity Planning

Business continuity planning involves the development of a Business Continuity Plan (BCP) to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimizing the loss impact to the organization. Implementing a BCP is essential to every business.

Business continuity planning involves following five major processes:



3.2.1.1 Critical Business Activities Identification

It is crucial to understand where a company needs to focus on in order to recover in case of an incident. The first step in business continuity planning is to identify the most critical business activities to your company's survival. You need to have a good understanding of your business, including its objective, products, services, resources, facilities, suppliers, customers, and their interdependencies.

Critical business activities are those that must be present to sustain the continuity of business, where failing to performing them would lead to:

- Major revenue losses;
- Failure to meet regulatory or contractual requirements;
- Compromise of operational efficiency, or
- Loss of customer / damage of reputation.

Once the critical activities are identified, you should perform analysis on each of them to determine the priority and objective on the recovery of critical business activities based on their importance to the company's achievement of strategic goals. Typical questions to be considered include:

- What are the operational, financial and other competitive impacts to the company if the activities are not functioned?
- How quickly do the activities need to be back in production for your company to survive?
- How much data and financial losses can you afford?

For each of the critical business activity identified, it is also necessary to find out all the supporting resources needed to perform the activity and the effect on the business of the unavailability of the resources. Listed below are the areas of resources you should consider:

- People;
- Information technology (service, application, network, data);
- Data and voice communication;
- Paper-based documents and records;
- Physical infrastructure, key equipment and facilities; and
- External services / products dependencies.

3.2.1.2 Business Continuity Risk Assessment

A disaster could happen to any company – no matter the business size. Risk assessment on critical business activities should be conducted, identifying possible risks and assessing the likelihood and impact of disruptive events. It is vital that you understand the disruptions that would be disastrous to the running of your business. Different disaster scenarios should be considered, some common threats include:

- Natural disaster, such as earthquake, fire, typhoon, flood;
- Loss of key equipment / information system / facility;
- Disruption of external telecommunications services;
- Utility outage, such as failure of power supply;
- Loss of life, disease, health & safety issues; and
- Terrorism & cyber attack.

Risk assessment against different threats may result in different outcomes. Some may require no action, while some require continuity planning to be developed and supported with additional resources. This will help a company to explore the possible effects of disaster incidents. After that, risks can be prioritized against objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

3.2.1.3 Business Continuity Plan Development

BCP allows you to prepare for the worst situation that would keep your business from being operational and to minimize service disruption as well as financial loss. The plan only needs to include the business activities that are most critical to keep your company up and running.

Based on the results from the analysis made on critical business activities and possible risks, you can start developing business continuity and recovery strategies. The selection of strategy may depend upon the criticality of business activities, cost, time for recovery and security.

Listed below are the typical items included in a BCP:

- Individual roles and responsibilities;
- Conditions for its activation;
- Processes to be followed;
- Escalation plan;
- Emergency procedure to handle incident;
- Temporary operational procedure;
- Resumption procedure;
- Fallback procedure; and
- Maintenance schedule and process for testing the plan.

For a small company, a BCP may be simply a printed manual stored safely away from main working location, with emergency contact information, location of offsite data backup storage media, copies of insurance contracts, and other critical material necessary for survival of the business.

The purchase of suitable insurance may be considered as part of the overall business continuity process to recoup losses from risks that cannot be completely prevented or controlled. The decision to obtain insurance should be based on the likelihood and degree of loss identified. Please note that insurance should not be treated as a substitute for an effective BCP since it does not deal with the recovery of business.

Before the plan is put into practice, testing should be conducted to ensure it is effective. Testing may include simulations, business process test, technical recovery and resumption testing, recovery processes testing at alternate site, supplier facilities and services testing etc.

3.2.1.4 Plan Approval and Implementation

Once a BCP is developed, it is important that endorsement should be sought for approval and support.

Points to note during the implementation of BCP:

- BCP should be documented and disseminated to all staff to follow before, during and after disruptive event occurred.
- Awareness training and education for staff should be conducted to help them understanding the business continuity processes and their individual responsibilities and actions to be taken when the plan is invoked. This is to ensure the processes would be carried out effectively.
- Copies of BCP should be stored at remote location and kept updated with the same level of security protection as at the main site.
- Other material necessary to execute the BCP and for organizational survival should also be stored at the remote location, such as offsite data backup storage media and copies of insurance contracts.
- A company may also need to have pre-arrangement with external parties to ensure timely resumption of operations, such as facilities access and telecommunication systems.

3.2.1.5 Regular Review and Ongoing Maintenance

In order to validate the business continuity arrangements, testing, review and ongoing maintenance should be conducted regularly to ensure they are up-to-date and effective.

- Regular review, testing & verification of documented BCP and the technical solutions should be conducted regularly, say annually.
- When any new or major change in business requirements / environment are identified, the existing procedures should be updated as appropriate.
- Procedures should be included within the organization's change management programme to ensure that business continuity matters are always addressed appropriately.
- BCP and the test results should also be subjected to independent audit and review.

3.2.2 Disaster Recovery Planning

Disaster recovery planning is a process to create a disaster recovery plan (DRP) for an information system for the recovery of IT processing facilities. DRP includes a well-planned document to deal with situations when a disaster occurs to an information system and/or its primary site, whereby the systems and data are totally lost.

DRP should include detailed backup procedure of the information system, the recovery procedure of the information system, say to an alternate site, and the procedure to resume data back to the primary site when the site is restored after the disaster. Refer to "Section 3.6 Backup and Recovery" for details on backup and recovery procedures.

Consideration should be given to the possibility that the primary site of the information system may not be available for a prolonged period of time after the disaster, and that the information system at the alternate site will not be run at an optimal performance level (e.g. the performance degradation may be supplemented by manual procedures). There are various means of alternate backup and processing services, such as hot / warm / cold sites subscription service run by third-party, providing different level of supporting facilities.

A detailed and well-tested procedure for data recovery and verification should be included to increase the accuracy and effectiveness of the procedure. In addition, all necessary materials and documents in recovering the data should be prepared beforehand, such as the arrangement of telecommunication network services at the alternate site.

Proper security protection should also be put in place and incorporated in the DRP. Security best practices should be followed and not ignored so that security level could be maintained after the recovery process (e.g. check and avoid restoring from unauthorized backup media which may contain malicious code). Security areas to ponder include perimeter defense, intrusion detection system, virus protection, system patching and configurations.

Similar to BCP, DRP should be maintained with updated information, especially when there are changes to the information system. Scheduled disaster recovery drill should be performed to test for the accuracy and effectiveness of DRP. But since carrying out a disaster recovery can be time-consuming and may affect normal operations, the frequency of conducting drills would be determined according to business environment and needs.