For information

Legislative Council
Panel on Economic Services

Airport Authority Year 2000 Compliance Programme

PURPOSE

This paper reports on the position and progress of the Authority's Year 2000 (Y2K) Programme as at 31 March 1999. It also covers the Authority's efforts in co-ordinating the activities of its key business partners.

BACKGROUND

Contractual Position

2. The Y2K problem was not unknown when the airport's systems contracts were concluded in the earlier part of the decade. However an explicit requirement for Y2K compliance was not included in the contracts, because at that time it was intended that the various provisions, including the fitness for purpose clause, provided safeguards to ensure that equipment supplied would either be Y2K compliant on installation or would subsequently be modified by the contractor to enable compliance. This has proved to be the case. Through these requirements, the Authority is working with the contractors and vendors on its Y2K Programme. The current focus is on the practicalities of getting the work done and adhering to the schedule.

3. The British Standards Institution (BSI) published the document defining Y2K compliance in 1997. This BSI definition was adopted as a standard by the Authority in 1998.

THE PROGRAMME

4. The Authority started working on the Y2K issue in early 1998 when it began building up the Y2K inventory and asking contractors and vendors for compliance statements on the equipment and systems they provided. In September 1998, after the initial airport system problems were resolved, the Authority instituted a comprehensive Y2K Programme. The mission of the Authority's Y2K Programme is to minimise the risks of the Y2K problem on the Authority's operations, to safeguard the continuity and normal operations of the

airport and the provision of a safe and effective service to the public before, during and after the transition to the millennium.

5. The Authority recognises that the Y2K problem is not simply an IT problem since it threatens the overall operational and business continuity. It is a management challenge and a corporate-wide concern. Tackling the issue demands the greatest possible commitment and a concerted effort throughout the Authority. Accordingly the highest priority is accorded to the Y2K Programme, and the Authority has a commitment to make necessary financial and other resources available to the Programme.

6. In order to ensure that the problem is clearly understood at all levels, a Board workshop was conducted for members in November 1998. A number of workshops have been organised since October 1998 for the Y2K Project Managers, System Owners and operations staff on Y2K compliance testing and verification, and contingency planning. A presentation on the Programme was given in January at the Quarterly Staff Briefing, targetting all staff of the Authority. There is also a regular column in the Staff Newsletter to update all staff on progress.

7. Since the establishment of the comprehensive Programme, and in view of the intricate and complicated interface the operation of the airport has with other operators, the Authority has been working closely with its business partners to ensure that all possible preparations are being made to minimise any Y2K impact.

8. The Authority also reports to the Information Technology and Broadcasting Bureau through Civil Aviation Department on the status of its Programme, including that of the contingency planning aspects.

Management Structure

9. The Board appointed a Y2K Steering Committee in September 1998 to direct and steer the Programme. The Steering Committee is chaired by the Chief Executive Officer, and comprises, among others, senior management like Airport Management Director, Project Director, Finance & Commercial Director, Management and Operations Consultant, Head of System Services and the Authority's Y2K consultant.

10. A Y2K Central Programme Office and Contingency Planning Project Office with 27 full-time staff and secondees have been set up to manage and co-ordinate the day-to-day Y2K compliance effort. ***In addition to their normal day-to-day duties,*** a total of 41 managers from various technical departments have been nominated as Y2K Project Managers. Their responsibility is to manage the verification of individual systems, together with any necessary rectification work required.

11. Users are closely involved in the process. The Authority has identified for each system in its Y2K inventory a System Owner. System Owners are user representatives. They are accountable for ensuring the continuity of business operations, signing off Y2K verification, as well as developing, testing and implementing contingency measures, under their respective function areas. Teamwork between users and technical staff is strongly emphasised to all concerned as a key success factor.

12. The Authority has also employed a Y2K consultant to provide guidance and assistance, particularly in the areas of programme methodology, strategy and organisation, and contingency planning. External technical resources have also been acquired for testing and rectification work, as well as contingency planning.

13. For the engineering systems, e.g. lifts, escalators, aircraft loading bridges, etc., the Authority has a team of 13 staff from Government's Electrical and Mechanical Department to work on Y2K verification testing and contingency planning.

14. The Programme is overseen by the Head of System Services and assisted by two managers, respectively looking after the progress of the Authority's own compliance efforts and the liaison with business partners. They are IT professionals with over 20 years of experience. The contingency planning aspects of the Programme are taken care of by a manager with over 20 years of airport planning and operational experience.

Annex 1

15. The organisation chart at Annex 1 illustrates the management structure of the Programme. (Please refer to paragraph 32 on the role of the Millennium Task Force.) The Authority regularly reviews the progress of the Programme and the demands imposed to ensure that adequate resources are available in good time.

Size of the Problem

16. The Authority's Y2K inventory, which is substantially complete, shows a total of 124 systems. These include both IT and non-IT systems and consist of about 4 000 different components.

17. Many of the Authority's systems interface with systems belonging to its business partners and other third parties. As a result, the Authority can be affected should any of these external systems fails to function in the Y2K environment. For example, the 12 airline departure control systems (DCS's) in use in the Terminal Building are connected to the Authority's Baggage Handling System through the SITA network and equipment. These DCS's are located offshore and clearly it is difficult for the Authority to control their compliance.

While SITA has Clauned its network and equipment to be compliant, the Authority will verify the compliance status of such systems up to the direct interface point between SITA's and the Authority's and will formulate contingency measures to protect the operation of its own systems. Such aspects create further dimensions to the Authority's Y2K problem.

18. There are another nine systems related to the North Runway and the Northwest Concourse extension projects. While these nine systems have not yet been commissioned, they will be Y2K compliant when the North Runway and the Northwest Concourse are brought into full service.

PROGRESS TO DATE

19. The process to establish Y2K compliance involves -

(a) determining from the contractor or the vendor the compliance of a specific system;

(b) taking rectification action to upgrade non-compliant hardware and/ or software;

(c) testing and verifying that it performs correctly under different date case scenarios, e.g. 31.12.1999, 1.1.2000, 29.2.2000, even if it is claimed to be compliant by the contractor or the vendor.

20. The Authority has classified the 124 systems into three categories, high, medium and low criticality, based on the potential impact on airport operations should they fail. The criteria used in determining the criticality status of the systems are tabulated in Table 1.

Table 1 : Criteria used in Ranking of System Criticality

Category	***Failure of which would result in any of the following***
High	• intolerable financial loss • major operational disruption, perhaps even suspension of airport operations • an impact on safety and security standards • severe damage to public image and media exposure • likely expensive and extended litigation

Table 1 : Criteria used in Ranking of System Criticality (cont'd)

Category	*Failure of which would result in any of the following*
Medium	• tolerable financial loss • localised operational disruption • damage to public image and media exposure • litigation
Low	• minor financial loss • minimal operational disruption • minimal damage to public image • unlikely litigation

Annex 2

The criticality of the systems and their compliance status, based on representations from the contractors and vendors, is summarised in Table 2. (Annex 2 sets out details of the high criticality systems.) The ranking system ensures that high criticality systems are given precedence in compliance efforts should there be any conflicts of competing priority in resources.

Table 2 : Compliance Status by Criticality as declared by contractors and vendors

Status		***Criticality***			***Total***	***%***
		High	***Medium***	***Low***		
Compliant or no date impact to operations		35	21	19	75	60.5%
Non-compliant	Rectification Complete	4	12	9	25	20.2%
	Rectification in Progress	14	5	5	24	19.3%
	Total	53	38	33	124	
	%	43%	31%	26%		

- As a single large system may well comprises over 100 component elements, the Authority has adopted a prudent policy to declare the ENTIRE system as non-compliant if just ONE of its component parts is non-compliant, unless the non-compliant component does not affect the functioning of the system or airport operations.

Compliance Verification Progress

21. According to the contractors and vendors, 60.5% of the systems are Y2K compliant or will have no Y2K impact on operations. However, the

Authority's policy is to verify each and every system's compliance status, even if it is claimed to be compliant by the contractor or the vendor. Verification tests on other systems would also start once a "non-compliant" system is rectified. In this regard, the Authority has adopted a parallel processing approach in respect of rectification and verification.

22. Many of the systems claimed to be compliant by the contractors and vendors are now undergoing the Authority's own testing and verification. The Authority has a comprehensive test strategy based on internationally accepted standards. The strategy specifies several phases of Y2K compliance work as follows -

(a) rectification;

(b) verification testing on each system or embedded process;

(c) integration testing of data flows between various internal systems and with external systems; and

(d) once a system has been verified as compliant, a stringent change control mechanism on any subsequent changes is imposed to ensure its compliant status is maintained.

The Authority's Y2K compliance testing includes the testing of data interface between the Authority's systems, and with external systems. The principal group of external systems where data exchange occurs is the flight information and passenger and baggage check-in processes. Comprehensive Y2K compliance testing is underway between key external systems.

23. As targetted, the Authority has completed verification of 43 systems or about 35% of the total 124 by end March. These include 21 high, 11 medium and 11 low criticality systems. Of these 43 systems, 17 have been verified as compliant and 18 not affected by the Y2K problem. The remaining eight have been verified as not fully conforming to the BSI Y2K compliance definition but any non-compliant component in them does not affect the useful functioning of the system or airport operations. The Authority expects the number of verified systems to rise sharply in the next three months. Please see Table 3.

Table 3 : Progress to-date (as at 31 March 1999)

	Target				***Actual***			
Date	*No, of Systems*	*Cum Total*	*%*	*Cum %*	*No, of Systems*	*Cum Total*	*%*	*Cum. %*
Nov-98	6	6	4.8%	4.8%	10	10	8.1%	8.1%
Dec-98	6	12	4.8%	9.7%	2	12	1.6%	9.7%
Jan-99	2	14	1.6%	11.3%	4	16	3.2%	12.9%
Feb-99	6	20	4.8%	16.1%	6	22	4.8%	17.7%
Mar-99	23	43	18.5%	34.7%	21	43	16.9%	34.7%
Apr-99	32	75	25.8%	60.5%				
May-99	10	85	8.1%	68.5%				
Jun-99	35	120	28.2%	96.8%				
Jul-99	1	121	0.8%	97.6%				
Aug-99	2	123	1.6%	99.2%				
Sep-99	1	124	0.8%	100.0%				
Total	***124***				***43***			

- The table above shows the number of systems and the cumulative total with compliance verification completed or to be completed by each month. Although the numbers appear high through the period April to June, a large amount of work, including compliance determination, necessary rectification and verification testing, has been performed, or is being performed, to bring the systems to the state ready for verification testing which is the last phase.

- Due to the dynamic nature, the above numbers may be subject to change as verification work progresses.

Target Compliance Date

24. The Authority has used its best endeavours to accelerate the Y2K Programme. The target date for completing compliance verification for all 124 existing systems is June 1999 except -

(a) the Supervisory Control and Data Acquisition/ Building Management System;

(b) the Human Resources Management System;

(c) the Access Control System; and

(d) the Baggage Handling System.

25. (a) and (b) above are systems of low criticality. Workarounds are available through manual procedures and airport operations will not be affected by their compliance status.

26. (c) and (d) above are stated to be compliant by the relevant contractors. The Authority plans to complete verification tests of the key components of these two systems in a simulated environment by June 1999. However, given the significance of these two systems to the operation of the airport, the Authority has also scheduled some on-site tests or tests in a live environment for further assurance. These tests can only commence in July when the related contingency plans have been fully tested; on-site verification is expected to be completed by August 1999.

CONTINGENCY PLANNING

27. Given the uncertainties surrounding the Y2K problem, there is no guarantee that a system will be "problem-free" even if it has successfully undergone the Y2K compliance verification process. Furthermore, because many of the Authority's systems interface with other external systems, there is always a risk of disruption through interface points. Contingency plans are therefore being developed and refined to ensure critical operations can continue in the event that one or more technical systems should suffer a Y2K related failure. To underline the importance of contingency planning, a Y2K Contingency Planning Project Office has also been set up to take up the overall responsibility for this part of the Programme.

28. The Authority started focusing on contingency planning in December 1998. The scope of the Contingency Planning Initiative includes -

(a) development of workable contingency plans, which will be predominantly manual, for critical operational processes; and

(b) identification of failure scenarios for the technical systems that provide infrastructure support to airport operation and development of corresponding fallback measures to ensure continuity of operation.

In other words, during the contingency planning process individual systems are mapped to the Authority's various operational processes and steps. This mapping, together with analysis of the operational processes and steps, will provide a clear picture of how the failures of individual system will have on airport operations.

29. With the assistance of the consultant, analyses to identify the critical operational processes on the following five key airport operational areas were carried out at the beginning of the year, these are -

(a) Arriving passengers and baggage movement

(b) Departing passengers and baggage movement

(c) Transfer and transit passengers and baggage movement

(d) Aircraft ground movement and ground servicing

(e) Cargo and mail movement

With inputs from the line management of the Authority and business partners, the Authority has identified within each of the above activities key operational steps which are critical to the continuity of airport operations. Contingency plans for each of these critical operational steps will be drilled and tested in May and June.

30. Contingency plans are being developed on the assumption that a system or multiple systems cease to function completely. However, some systems can be operated in a semi-manual or reduced functionality mode. Systems are being analysed to determine these reduced functionality fallback scenarios.

31. Workshops with Project Managers and System Owners to review risk and to facilitate incorporation of fallback measures into the overall operational contingency planning effort are being conducted in April and will continue into May.

BUSINESS PARTNERS

32. While the Authority cannot take responsibility for contingency measures which are clearly within the franchisees' or the business partners' own operation, e.g. the Community System for Air Cargo of HACTL, the Authority has taken up the role of co-ordinator. The Authority has grouped its business partners into high, medium and low criticality. The high criticality business partners (totalled 26) have been invited to be members of the Millennium Task Force in order to -

(a) facilitate the exchange of information and sharing of experience related to Y2K compliance among its members;

(b) review the progress of work related to Y2K compliance for those systems required by airport operations;

(c) identify the interfaces of their operation with the Authority's; and

(d) identify any problems or delay in implementing Y2K compliance and to facilitate the formulation of contingency plans that require co-ordination between members.

The Authority will synchronise its own contingency plans with those of its business partners. Co-ordinated trials of the Authority's contingency measures and those of its operationally critical business partners' will be carried out as far as possible. The task force has been meeting on a monthly basis since January 1999.

33. Business partners who are in the high and the medium criticality categories (totalled 40) have also been requested to provide monthly progress reports. As at 31 March, half of them reported that they have achieved Y2K compliance. The others have targetted to achieve compliance by June 1999 except for three who are in the medium criticality category. The target compliance dates of these three business partners are respectively August 1999 (for one) and September 1999 (for the other two).

HACTL

34. HACTL has attended all the meetings of the Authority's Millennium Task Force. In the most recent Task Force meeting held on 1 April, when members were individually asked about their progress and issues, HACTL's representative confirmed that its Y2K programme is on schedule and that she could not foreseen any critical issue which could hinder progress towards Y2K compliance.

35. In the light of the significance of HACTL's operation to the cargo processing function of the airport, a separate report from HACTL on its Y2K programme is at Annex 3.

Annex 3

LOOKING AHEAD

Rectification, Testing and Verification

36. While rectification, testing and verification work on individual systems is now underway, due to the dynamic nature of the Y2K projects, there is a possibility that new problems may be discovered during testing, thus impacting the project progress. The Authority continues to closely monitor progress and to ensure that target dates are adhered to.

Contingency Planning

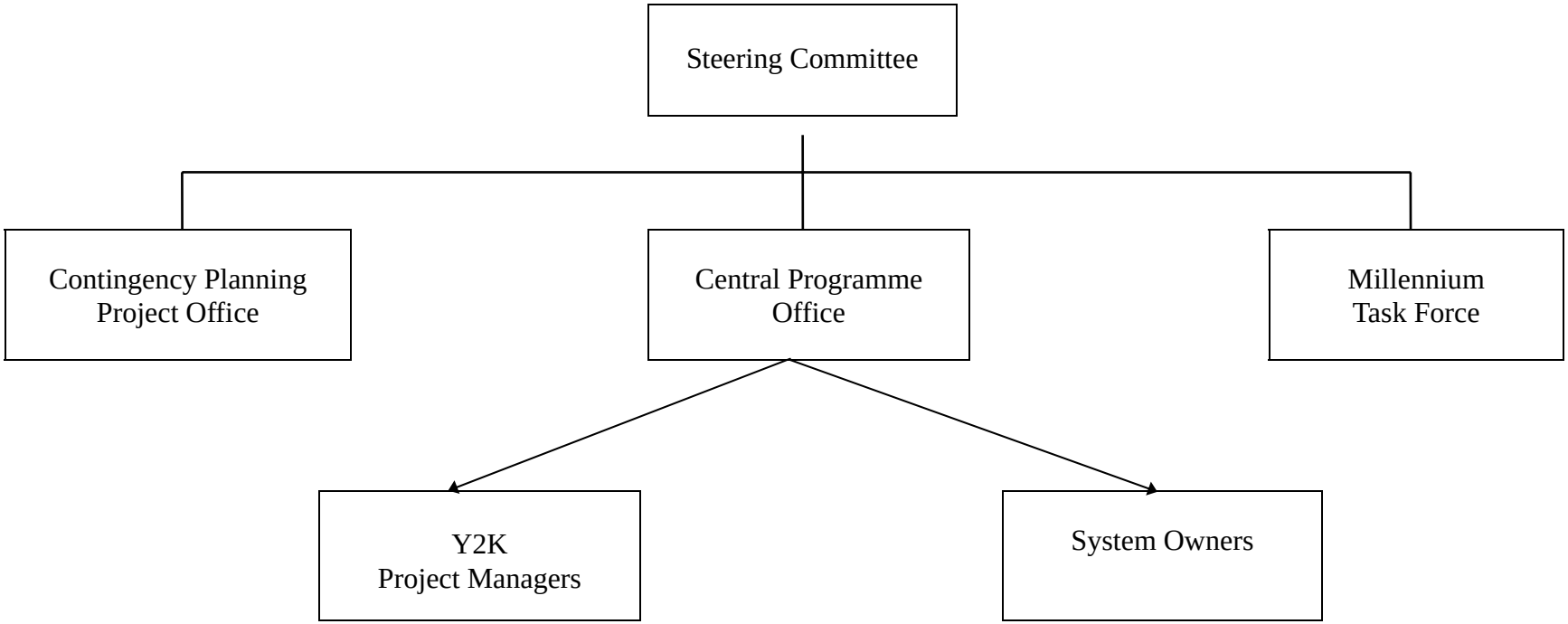
37. Contingency planning is progressing on schedule. Five workshops have so far been organised and a further 11 are planned for April and May, involving both technical and operational staff of the Authority and personnel from relevant business partners. The aim of these workshops is to revise and enhance the contingency measures, and to consolidate them into a coherent plan. Co-ordinated test/drills of contingency plans supporting the critical airport operations will be substantially complete by September 1999.

38. Work is also progressing on establishing a Command and Control framework involving senior airport management. This management framework, which includes the establishment of a Command and Control Centre, will be in place before, during and after the transition period to the new millennium and will be responsible for implementation and co-ordination of contingency measures.

Airport Authority
20 April 1999

Annex 1

The Programme Structure



List of Mission Critical Computer and Embedded Systems

Annex 2

stem/ Equipment Name	Abbrev.	Description
xcess Control System	ACS	The system provides controlled access to restricted areas both in the terminal and in the airfield. It works in conjunction with CCTV in providing intrusion detection around the airfield perimeter. The system includes facilities in access card production.
'craft Loading Bridges		The airbridge connects the fixed link bridge and the aircraft to allow passenger boarding and unboarding.
rcraft Parking Aid	APA	This system provides main centerline, azimuth guidance, distance-to-run and stopping guidance, and stand number indicator to aircraft arriving and departing at 38 aircraft stands and 27remote stands.
rfield Fire Stations and Control Centre		The system includes fire protection, electrical distribution, air conditioning and other building services inside Northern and Southern Airside Fire Stations, Civil Work Depot, Airfield Operation Centre, Refuse Compaction Centre, and also a simulation control system at Fire Training Pit.
rfield Ground Lighting (South Runway)		Lighting System installed along the South Runway.
rport Operational Data Base	AODB	AODB acts as a data repository and information hub enabling data exchange of commonly used Airport data among airport and external systems. It also provides online flight information enquiry and certain data entry functions.
rport PABX		The PABX system installed by the Authority serves two roles. One is to provide a single telephone service to the Authority across the entire airport. The other role is to provide direct telephone hotline facilitate for selected user groups.
'M Network Management System	ATM NMS	Asynchronous Transfer Mode Network (ATM) NMS provides network management for all Newbridge network products. Functions include configuration, connection, maintenance, performance monitoring, as well as, Virtual Local Area Network management.
ıtomated People Mover System	APM	This system transfers departure passengers from East Hall to West Hall and arrival passengers from West Hall to East Hall.
ggage Handling System	BHS	This system consists of conveyors transferring hold baggage between Baggage Hall, Departures Hall and Arrivals Hall.
ıilding Systems Integration	BSI	The BSI system brings together major airport operations systems into a single common operator workstation to enable structured monitoring of the status of various facilities such as fire services, CCTV, public addressing, etc.
ılding Systems Integration - Network		The BSI dedicated network that connects all BSI users, devices and external systems.
ntral Backup		To provide central backup servers for all office automation file servers.
osed Circuit Television System	CCTV	The system provides visual surveillance of the terminal building and airfields. Camera control can be effected from the various control centres including the airport police station. Images from cameras at fixed locations are time-lapse recorded.
ectrical Equipment & Distribution		The system involves cables, switchboards, busbars , etc.
nergency Power Plant		Generators installed at various locations on the airport platform for emergency backup of normal power supply.
nance System		To provide an effective tool to record, control & report on financial operations of AA using General Ledger, Billing System, Accounts Receivable System, Purchase Order Control, Accounts Payable & Budgeting System.
re Fighting & Rescue Vehicles		These are Fire fighting and rescue vehicles for the Airside areas.
re Fighting & Rescue Vessels		To provide sea rescue and fire fighting within the 5 Km zone of airport.
xed Communications System	FCS	The Fixed Communications System (FCS) is an airport wide communication network . It provides support for data, video and voice traffic. A three tier structure is used to move traffic from one point to another point.
ight Information Display System - etwork	FIDS Network	The FIDS dedicated network that connects all FIDS users, devices and external systems to the FIDS central servers.
ight Information Display System - NMS	FIDS - NMS	It provides network management for all 3Com network devices, functions include configuration, connection, maintenance and performance monitoring. It also monitor status of system/application, and LCD hardware.
ight Information Display System - SW HW	FIDS	FIDS provides flight information to all users including passengers, ramp handlers within the terminal building and it also provides resources allocation function for gates, stands and check-in desks.
round Transportation Centre - Fire arm Systems		They are automatic fire detection systems installed inside the Ground Transportation Centre (GTC)
gh Mast Lighting		They are high mast lights installed in the apron areas.
ost LAN	HLAN	The Host Local Area Network (Host LAN) provides the connectivity between the Airport Operational Database (AODB) and other host computer systems throughout the airport. The Host LAN is located in the Passenger Terminal Building (PTB).
formation Network	IN	Information Network is a common network providing access from the Information Network Workstations to AODB or other host computers in the airport.
' Addr. Mgmt System		To manage IP network addresses allocation and assignment within the Authority's network

List of Mission Critical Computer and Embedded Systems

Annex 2

Item/ Equipment Name	Abbrev.	Description
Level 3 Trace Detection Equipment		This system is used to perform Level 3 security screening to detect any explosive in hold baggage. The equipment is adopting the trace detection technology.
Level 3 X-Ray Baggage Security Screening Systems		This system is used to perform Level 3 security screening to detect any explosive in hold baggage. The equipment is adopting the computed tomography scanner technology
Machine Automated Explosive Detection System		This system is integrated with the baggage handling conveyors for Level 1/2 security screening of all hold baggage.
Major Fire Fighting and Rescue Eqpmt & Consumables		Additional fire fighting, communications and rescue equipment on the fire fighting vehicles.
Network Management System		The Network Management System manages network equipment and user workstations in AA's various networks (FCS, HLAN and IN systems). In addition, the NMS also re-route ATM network data.
Open Channel Radio System		This radio system is used by AA Airport Fire Contingent (AFC). Users are fire appliance, fire vessels, airside fire stations, rescue piers. The system also links to AA's Trunked Mobile Radio system, Civil Aviation Department (CAD), HK Fire Service HQ for
Operational Vehicles and Equipment		Normal operational vehicles, special purpose vehicles and equipment for airport maintenance & operations.
Out-of-gauge Baggage Screening System		This system is used to perform security screening for the out-of-gauge hold baggage.
Passenger & Hand Baggage Security Screening		This system is used to scan hand carried baggage entering the airside.
Passenger Terminal Building - Public Address		This system provides public address functions in Passenger Terminal Building. The voice sources include: live messages from microphones, pre-recorded fire evacuation messages, preprogrammed reminder messages.
Primary Substation A		Concrete structure and normal building services to house China Light & Power power distribution equipment.
Primary Substation B		Concrete structure and normal building services to house China Light & Power power distribution equipment.
Project Cost Control Systems		This system monitors contract status, budgets-costs progress and payment.
PTB Building Serv. - High Voltage SCADA		The system monitors and controls the 11kV networks status in the Passenger Terminal Building.
PTB Building Serv. - Thorn Addressable Fire Alarm		These are automatic fire detection systems installed inside the Passenger Terminal Building.
PTB Building Services		This system includes lighting, air-conditioning, hydraulic and sprinklers systems installed inside the Passenger Terminal Building.
PTB Lifts		This system includes lifts inside the Passenger Terminal Building and Ground Transportation Centre.
Sea Rescue Facilities		The system includes air conditioning, fire protection, electrical distribution, standby generator, lifting gear and other building services inside four Sea Rescues Facilities.
Seawater Pumping Station Equipment (North)		To supply filtered and chlorinated seawater for cooling and toilet flushing to PTB, GTC, Air Traffic Control Centre, AA's Maintenance HQ, Airport Hotel and other ancillary buildings in the northern part of the airport.
Seawater Pumping Station Equipment (South)		To supply filtered and chlorinated seawater for cooling and toilet flushing to buildings of the government and franchisees in the southern part of the airport.
Stand Allocation System		Stand-alone Stand Allocation system is the backup system to be used if the Terminal Management sub-system (TMS) of the Flight Information Display System is not operational.
Standby FIDS		Stand-alone Display Control System is the back up system to be used at the PTB if the main FIDS display component and check-in desk control are not operational.
Time of Day Clock	TODC	The Time of Day Clock system provides a single, common source of correct time to the systems and devices within the PTB. The system under normal conditions synchronises to Global Positioning System (GPS) satellites to produce the time of day which is then
Trunked Mobile Radio (Hitachi)	TMR	This radio system is used by all AA departments, except the Airport Fire Contingent, and Government departments. Coverage includes whole Chek Lap Kok, PTB plant rooms, PTB & airfield service tunnels, airfield vehicle tunnels.
VHF System		This radio system enables radio holders to listen to (and join if necessary) conversations between aeroplane pilots and CAD control centres.

Annex 3

HACTL Year-2000 compliance Programme
An Update for the Legco Economic Services Panel

Executive Summary

1. Misunderstanding over the state of Y2K readiness at HACTL appears to have arisen due to the simplified way in which data on Y2K compliance progress was recorded in documents submitted to Legco. In reality, HACTL has had comprehensive plans in place since October 1998, and progress on implementation has been satisfactory and on schedule.

2. HACTL began implementation of its Y2K compliance plan in October 1998, led by an 10-member Year-2000 Progress Review Committee chaired by HACTL Managing Director. Detailed plans were formulated by a Year-2000 Working Group which includes representatives from all related functional areas of HACTL. Reports on progress were made to the Progress Review Committee monthly. The company's Y2K compliance plan has been progressing smoothly and on schedule. The company is confident ST1 will be fully compliant ahead of its own deadline of June 1999.

3. By compliant, the company adopts the relevant British Standards Institute Committee definition for compliance, requiring that the company identifies all equipment and processes in any way reliant on or likely to be affected by the Y2K transition, examines these to ensure they are compliant, replaces any hard or software found not be fully compliant, comprehensively tests all systems after any replacements have been made, and has business contingency plans in place to apply in the event of any disruptions caused by systems or equipment failure or third party compliance.

4. HACTL has 28 mission-critical systems, of which 16 are computer systems and 12 are electronic systems. As of April 19 1999, 22 are already fully Y2K-compliant. Of the remaining 6 systems, system remediation and testing has already been satisfactorily completed, and full compliance is likely to be achieved during the course of May, ahead of the company's own deadline of June 1999.

5. An audit of supplier compliance has been in progress at HACTL, and is due to be completed with HACTL's critical suppliers by June.

6. Comprehensive contingency plans have been prepared which are intended to anticipate all external challenges to smooth operation through the Y2K transition. These plans were completed and signed off in March 1999. HACTL will "walk through" these plans with customers and business partners in May, and will complete training and drilling in July and August.

19 April 1999

HACTL Year-2000 compliance Programme
An Update for the Legco Economic Services Panel

1. PURPOSE

1.1 In response to LegCo's request through the Airport Authority, HACTL welcomes the opportunity to provide this brief which serves to update Panel Members on the position and progress of HACTL's Year-2000 Compliance Programme as at 19 April 1999. Members may wish to note that HACTL successfully achieved "Y2K READINESS" for its critical computer and electronic systems on 20th February 1999 and is currently on schedule towards achieving full "Y2K COMPLIANCE" by end June 1999.

2. BACKGROUND

2.1 HACTL has been preparing for the Year-2000 transition since early 1997. The modification process for Year-2000 compliance of our computerized community system for air cargo, COSAC, commenced as early as March 1997. Newly developed computer systems, such as the Logistics Control System and Resource Management System, had Year- 2000 compliance requirements in place throughout the design and development phases.

2.2 With the migration to Chek Lep Kok completed and most of the airport opening enquiries over, HACTL management began in October 1998 to consolidate all Year-2000 activities into an integrated company-wide project. At the same time, the company also monitored the various Year- 2000 project methodologies launched by HACTL shareholders as it was necessary to enable shareholders to be updated on progress in spite of the fact that different definitions on "compliance", "readiness" and methodologies have been adopted and reporting on progress to interested parties could have misleading results if there was not absolute clarity on definitions and methodologies being used.

2.3 To ensure greater consistency in formulating and tracking its Year-2000 programme, in October 1998 management recommended, and the HACTL Board approved, the use of external consultants including the services of the Y2K Programme Office of John Swire & Sons (HK) Ltd. As a result, consistent standards and definitions have been adopted for HACTL's Y2K project in terms of reporting to interested parties. HACTL has also benefitted from a tightly structured framework of

regular independent quality assessments and progress monitoring of its overall Year-2000 programme. This enables a consistent standard of progress monitoring and a standard set of definitions that have henceforth been adopted for HACTL's Y2K project in terms of reporting to interested parties. This recommendation was unanimously supported by the HACTL board, and implemented from October 1998.

3. The Y2K Transition at HACTL

3.1 The Year-2000 compliance definition as applied to the performance of HACTL systems is based on that established by the British Standards Institute Committee (BSI) and is as follows:

Rule 1: No value for current date will cause any interruption in operation.

Rule 2: Date-based functionality must behave consistently for dates prior to, during and after Year-2000.

Rule 3: In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or interfacing rules.

Rule 4: Year-2000 must be recognized as a leap year.

3.2 HACTL has identified 28 mission-critical systems, of which 16 are computer systems and 12 are electronic systems. These systems are essential to the HACTL business and are potentially Year-2000 relevant.

YEAR-2000 READINESS of HACTL is achieved when :

1. An *inventory* of all relevant equipment & systems (that is all business-critical IT systems & equipment relying on embedded electronic chips failure of which to operate in a manner unaffected to a material extent by the date change at YEAR-2000 would have a material adverse effect on the business or operations of HACTL) has been made;

2. Such equipment and systems have been *assessed & tested* for potential YEAR-2000 problems identified by the relevant project team & a *course of action* relating to any identified problems has been decided upon & the *equipment* or *services required* to implement this have been ordered or arranged.

3. HACTL will have business contingency plans in place to apply in the event of any disruptions caused by systems or equipment failure or third party non-compliance.

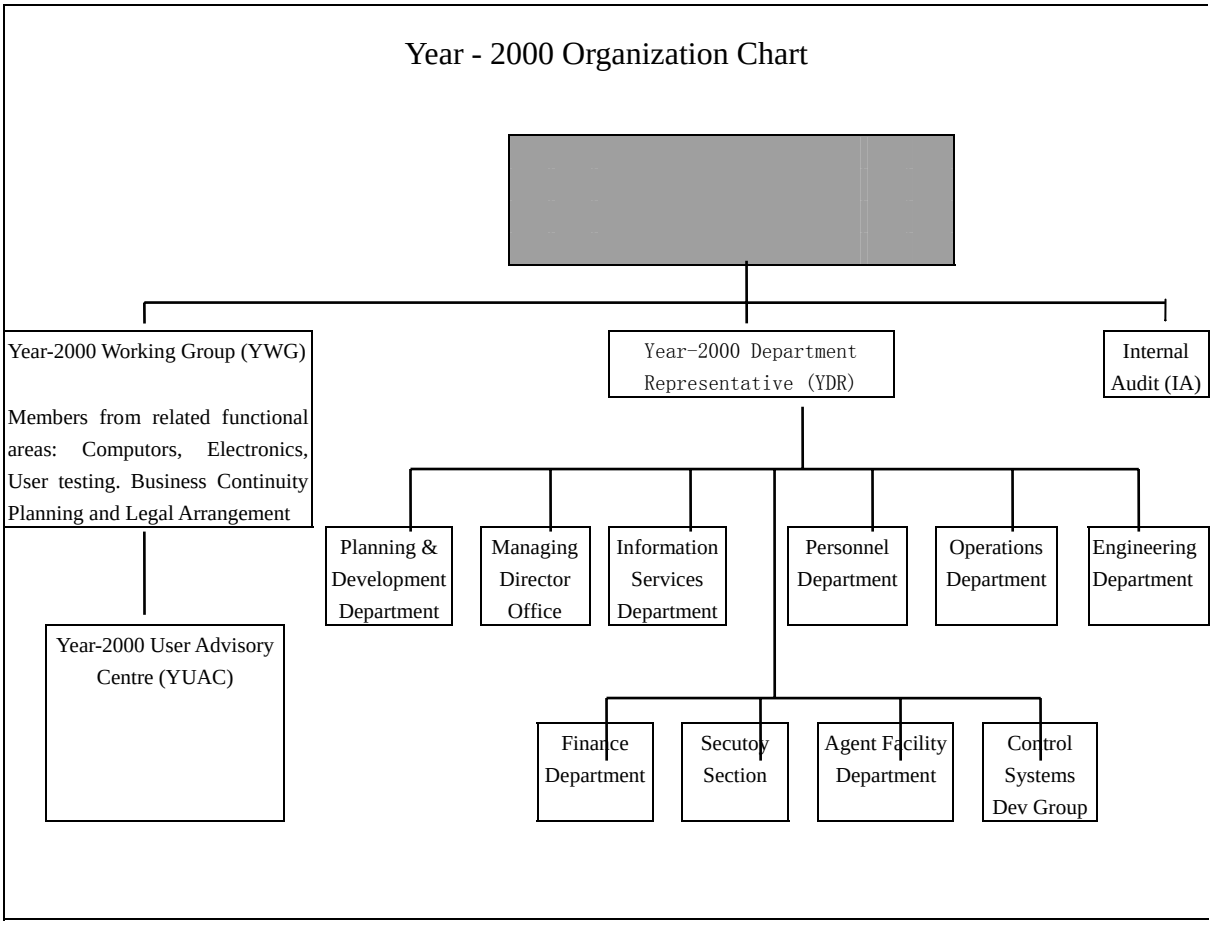
YEAR-2000 COMPLIANCE of HACTL :

4. means in relation to our own relevant equipment & systems, the modification or replacement of all such equipment & systems that fail our YEAR-2000 compliance test and, in respect of suppliers of such equipment and systems, we mean all critical suppliers, will *have passed* our YEAR-2000 *compliance audit,* or have been *replaced* by those that have.

5. Critical *suppliers* of such equipment & systems will have been *audited* for YEAR-2000 compliance & compliant *alternates* identified for those product suppliers that are deemed unlikely to achieve YEAR-2000 compliance in time.

4. Year-2000 Organization Structure in HACTL

4.1 The implementation of the HACTL Year-2000 compliance effort is a responsibility of the HACTL management under the leadership of the Managing Director. The company compliance effort is made up of the respective compliance programmes undertaken by HACTL Departments/Sections/Units under the direction of respective department heads and designated section heads i.e. HACIS Manager/Agent Facility Manager (HM/AFM), Project Manager- Control (PMS) and Security Manager (SCM) in respective of Agent facility Department (AFD), Control Systems Development Group (CDG) and Security Section (SEC). For Year-2000 Compliance, HACTL has established a compliance project organization:



4.2 A Year-2000 Progress Review Committee (YPRC) formed to direct the Year-2000 project progress is led by the HACTL Managing Director Members of YPRC are made up of all department heads of HACTL as well as section heads who have direct reporting lines to the Managing Director. The YPRC conducts monthly meetings during which reports are made to attending department heads on progress and decisions taken in order that problems/obstacles encountered or anticipated in the course of the project will be resolved. Compliance in accordance with time- tables as set out in the HACTL Year-2000 Project Plan and as agreed from time to time in YPRC meetings will remain the personal responsibility of department heads and the designated section heads.

4.3 A Year-2000 Working Group (YWG) is formed to develop the HACTL Year-2000 compliance project plan and subsequent progress reports. These YWG members report to YPRC on their respective areas of responsibility on a monthly basis. Endorsed reports are circulated to Swire's Year-2000 Program Office and will be available also to HACTL Executive Committee and Board Members to facilitate their monitoring

over progress on HACTL Y2K compliance.

4.4 In addition, the Year-2000 Departmental Representatives will represent respective departments for ensuring Year-2000 compliance, user testing and Contingency Planning on a departmental level. Departmental representatives may be invited to report to the YPRC to make a direct report from time to time.

4.5 A Year-2000 User Advisory Centre (YUAC) is formed to provide technical advice, hot line services and workshop training for all user representatives. The YUAC is made up of specialists from Information Services Department, Engineering Department and Planning & Development Department.

5. Current Position

We have been able to achieve the following status according to the Five Building Blocks structure in John Swire & Sons Year-2000 scheme. An update on HACTL'S Y2K progress report (*in the format required by the Airport Authority*) is attached (Appendix 1)

5.1 Computers (IT systems)

A company-wide *inventory* as at 20 February 1999 for computer systems and equipment was made and published. All critical computer systems and equipment had been *assessed, remediated* and *tested* by technical departments (ISD and CDG) for potential Year-2000 problems. End user departments (OPS, ENG, AFD, SEC and PER) had successfully completed the *user acceptance tests* on the critical computer systems with positive results on 20 February 1999. These systems would be ready for *implementation* in the production environment between March and June 1999 in order to achieve Year-2000 compliance.

5.2 Electronics (Embedded Chip)

A company-wide *inventory* as at 20 February 1999 for electronic systems and equipment was made and published. All critical electronic systems and equipment had been *assessed* and *tested* by Engineering departments for potential Year-2000 problems. Related end user departments of the critical electronic systems had confirmed the *user tests* with positive results on 20 February 1999. As all critical electronic equipment passed our Year-2000 assessment and tests, there would be no need for Year-2000 enhancement to existing critical electronic systems and equipment.

5.3 Business Contingency/Continuity Plan (BCP)

Totally 12 system *failure scenarios* have been identified, 8 for single point of failure and 4 for multiple points of failure. The first version of the HACTL Year-2000 Business Continuity and Contingency Plan ("the Plan") was prepared and signed off in early March 1999. Its aim is to provide business continuation in the event of any interruptions due to failure of multiple critical systems or suppliers.

It is envisaged that a *Transition Control Centre* will be set up, consisting of two Transition Control Teams, one dealing with internal transition issues while the other interfaces with external parties who would be affected.

The contingency planning process covers 3 areas: first a *walkthrough* with customer airlines and business partners to demonstrate Plan viability, then *training* and finally *drilling*. The first one is being undertaken and will be completed by mid-May 1999. The latter two are to commence by phases in July and August 1999.

5.4 Suppliers

The completion for supplier compliance is targeted in June 1999. *Face- to-face meetings* are being held to audit the Year-2000 compliance status of the most critical suppliers and these are progressing satisfactorily.

For the remaining critical suppliers, HACTL has sent *detailed questionnaires* to enquire about Y2K compliance status. Follow-up face- to-face meetings with the critical suppliers are scheduled by the responsible department of HACTL between April and June 1999.

5.5 Customers

The completion for customer compliance was targeted in June 1999. A strategy for assessing customers' Year-2000 compliance was formulated. *Interviews* with key customers are being held progressively.

5.6 Legal

The completion for legal arrangement is scheduled to June 1999. A relevant contract *inventory* has been drawn up and is being reviewed internally.

HACTL
19 April 1999

Year 2000 Compliance Situation and Progress--Monthly report (Cut off date : 19 April 1999) Attachment 1

Organization name : Hong Kong Air Cargo Terminals Ltd.

Item no	System / Equipment Name	Already Y2K compliant	Current Systems Status	Target date to achieve Y2K compliance				Cannol achieve compliance by 1/1/2000	Start date of rectification work	Start date of preparing the Y2K contingency plan	Decision date to exercise the Y2K contingency plan
				99/03	99/06	99/09	99/12				
1	COSAC	N	R		X				1-Nov-98	Dec-98	Sep-99
2	Logistic Control System - Container storage system	N	R		X				4-Nov-98	Dec-98	Sep-99
3	Logistic Control System - Bulk storage system	N	R		X				4-Nov-98	Dec-98	Sep-99
4	Bulk cargo distribution system	N	R		X				4-Nov-98	Dec-98	Sep-99
5	Staff clocking system	Y	C						1-Nov-98	Dec-98	Sep-99
6	Maintenance Management system	Y	C						1-Nov-98	Dec-98	Sep-99
7	Onboard courier system	Y	C						1-Nov-98	Dec-98	Sep-99
8	Vehicle Information System	Y	C						1-Nov-98	Dec-98	Sep-99
9	AFD Cargo inventory control system	N	R		X				1-Nov-98	Dec-98	Sep-99
10	Attendance System (Rostering)	Y	C						1-Nov-98	Dec-98	Sep-99
11	COSAC on INTERNET (COIN2)	Y	C						1-Nov-98	Dec-98	Sep-99
12	Gobal Security System	Y	C						1-Nov-98	Dec-98	Sep-99
13	Smartcard reader	N	R		X				1-Nov-98	Dec-98	Sep-99
14	SuperLINDA	Y	C						1-Nov-98	Dec-98	Sep-99
15	CCmail	Y	C						15-Oct-98	Dec-98	Sep-99
16	Spreadsheet	Y	C						15-Oct-98	Dec-98	Sep-99
17	Bulk storage system	Y	C						1-Oct-98	Dec-98	Sep-99
18	Container storage system	Y	C						1-Oct-98	Dec-98	Sep-99
19	CCTV system	Y	C						1-Oct-98	Dec-98	Sep-99
20	Integrated Radio Telephone and Paging System	Y	C						1-Oct-98	Dec-98	Sep-99
21	Overview Display System	Y	C						1-Oct-98	Dec-98	Sep-99
22	PABX	Y	C						1-Oct-98	Dec-98	Sep-99
23	Weighing System	Y	C						1-Oct-98	Dec-98	Sep-99
24	X-ray screening system	Y	C						1-Oct-98	Dec-98	Sep-99
25	MVAC for computer rooms	Y	C						1-Oct-98	Dec-98	Sep-99
26	Uninterrupted Power System for computer rooms	Y	C						1-Oct-98	Dec-98	Sep-99
27	Lift system - cargo lifts	Y	C						1-Oct-98	Dec-98	Sep-99
28	Lift system - dolly lifts	Y	C						1-Oct-98	Dec-98	Sep-99

The list includes all Mission Critical systems which are operated by HACTL. Mission Critical systems are those system which HACTL cannot do business without.

N: Not compliant as at the date of report

Y: Compliant already

X: Target compliant date

R: System remediation/testing already completed System implementation is planned for completion before June 1999.

C: System in Y2K Compliant status