



## ACI WORLD FACILITATION AND SERVICES STANDING COMMITTEE

### BEST PRACTICE PAPER: BUSINESS CONTINUITY MANAGEMENT FRAMEWORK AND CASE STUDIES FOR HEALTH-RELATED DISRUPTIONS AT AIRPORTS

DRAFTED BY ACI WORLD SECRETARIAT

---

## Executive Summary

In response to the SARS and Avian Flu outbreaks in 2003-2005, the industry has established contingency measures for public health events of international concern. Aviation stakeholders have put in place several measures, such as arrival and departure screening processes, health declaration forms and contingency plans for inbound aircraft with suspected cases on board.

However, aviation industry partners have not achieved the same level of preparedness for protracted, long disruptions to civil aviation operations that could arise from an infectious disease pandemic or health related emergencies.

ACI recommends that an airport establishes one Business Continuity Management System to cover the range of operational safety risks that it faces.

ACI's approach to this project is to define a Business Continuity Management System framework and development process and to build onto it best practice examples from airports that have mature systems in place.

## Table of Contents

Executive Summary .....	1
1. Definitions:.....	3
2. Business Continuity Management Systems (BCMS) framework:.....	4
2.1. Business Continuity Timeline.....	4
3. The BCMS Development Process.....	5
3.1. Establish the BCMS Project Oversight structure.....	6
3.2. Map the core processes.....	6
3.3. Conduct Operational Impact Analysis.....	7
3.4. Develop / Review the adequacy of Preventive measures (Maintenance Plans and System Fallback Plans).....	8
3.5. Develop / Review adequacy of Post-Event Plans (IT Recovery Plans, Operational Continuity Plans and Business Recovery Plans) .....	9
3.6. Develop / Review Crisis Management Capabilities.....	13
3.7. Preparedness / Quality Assurance (Monitoring & Corrective Action) .....	17
3.8. Management Review .....	18
4. BCMS – Best Practices for Infectious Disease Pandemics .....	19
Planning template.....	19
Operational checklists .....	20
Using Existing Infrastructure .....	22
5. Acknowledgements .....	24

## 1. Definitions:

The Business Continuity Management System (BCMS) used in this document is a simple, response driven model that makes use of basic business continuity first principles. As such, it is very much compatible with other types of BCMS that are currently in vogue (e.g. continuity of operations planning (COOP), disaster management planning/program (DMP), enterprise risk management planning (ERMP), incident response planning/program (IRP), continuity of business planning (COBP), plan-centric BCM (PBCM), risk-centric BCM (RBCM), enterprise resiliency planning (ERR), sustainable organizational resilience planning (SORP), etc.). The terms used may be different and the implementation progression may be dissimilar though the underlying business continuity first principles are the same.

**‘Business Continuity Management System’ (BCMS):** An integrated, multi-layered, business driven, process based approach to plan for and manage business disruptions and crises.

**‘Incident’:** An event which causes an impact or has the potential to cause an impact or disruption to the normal operational flows at an airport.

**‘Crisis’ or ‘Critical Event’:** Any event requiring an immediate, proactive response in order to minimize its negative impacts to the airport operator’s operations, reputation and profitability.

As a further explanation, an *incident* which is not properly managed and resolved could give rise to a *crisis*. *Incidents* occur every day in the course of an airport’s operations and most have a limited impact in terms of scope, scale and duration.

The concept of operational flows is important as managing an airport is in essence, managing flows of aircraft, vehicles, people, baggage, cargo, mail and information.

Airports manage these flows through **‘processes’**, **‘people’** and **‘systems’**. Therefore, an incident will have a detriment effect on the process output or service delivered because of the impact on these factors.

## 2. Business Continuity Management Systems (BCMS) framework:

### 2.1. Business Continuity Timeline

To understand the Business Continuity Management Systems better, it is important to show the component parts of the system in the context of a time line.

Figure 1 shows a critical event in its time context. From a management perspective, it is possible to differentiate between the **Pre** and **Post** event actions.

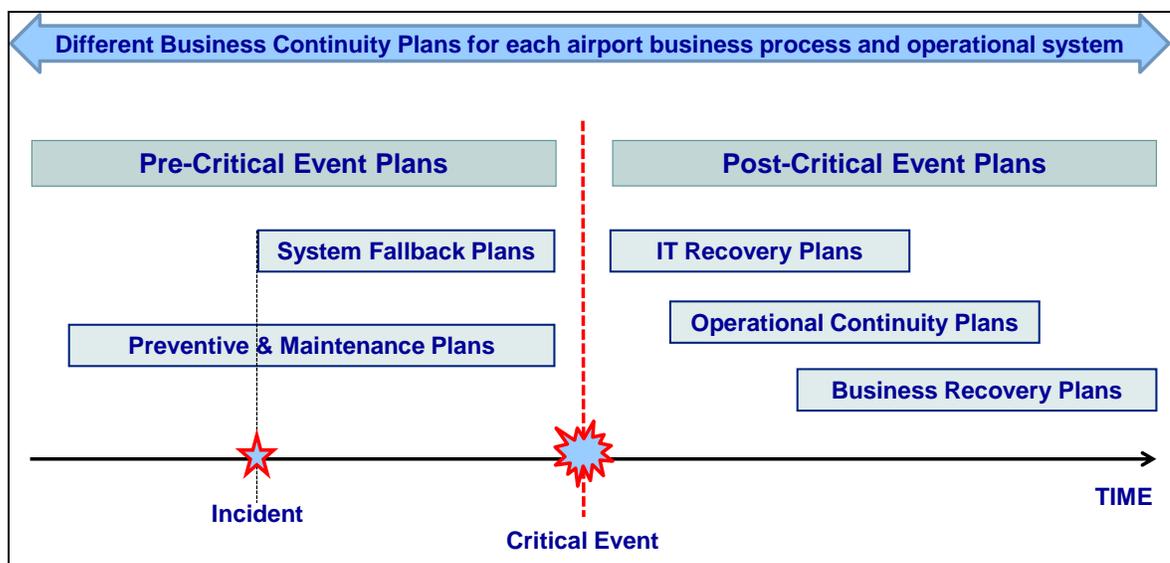


Figure 1: Critical event in its time context. (Courtesy of AAHK)

The pre-event actions can be termed **Pre-Critical Event Plans** and include:

- **Preventive & Maintenance Plans.** Good preventive management practices and well implemented maintenance plans help to prevent system failures and other avoidable incidents.
- **System Fallback Plans** are designed to maintain system operations and service delivery, when problems occur. Well designed and implemented system fallback plans help to prevent an incident from escalating into a critical event or failure.

The **Post-Critical Event Plans** include:

- **IT Recovery Plans:** where a system has failed and service has been disrupted.
- **Operational Continuity Plans:** outlining how the essential operations and services are maintained, achieved either by establishing deeper layers of resiliency to essential operations and services or through alternative arrangements.
- **Business Recovery Plans:** to restore normal operations.

Example: In a failure to the baggage handling system, the **Operational Continuity Plans** might include manually taking bags on trolleys from the check-in area down to the baggage make-up area.

Example: In the case of the baggage handling system failure, the **Business Recovery Plans** might provide for operations to be restored in steps, gradually increasing the load on the system and monitoring the system performance.

This is the BCMS framework. The above mentioned plans will be described in detail following the different steps of the BCMS Development Process.

### 3. The BCMS Development Process

Figure 2 shows the process map to identify the key steps that an airport will need to go through to develop and implement a BCMS.

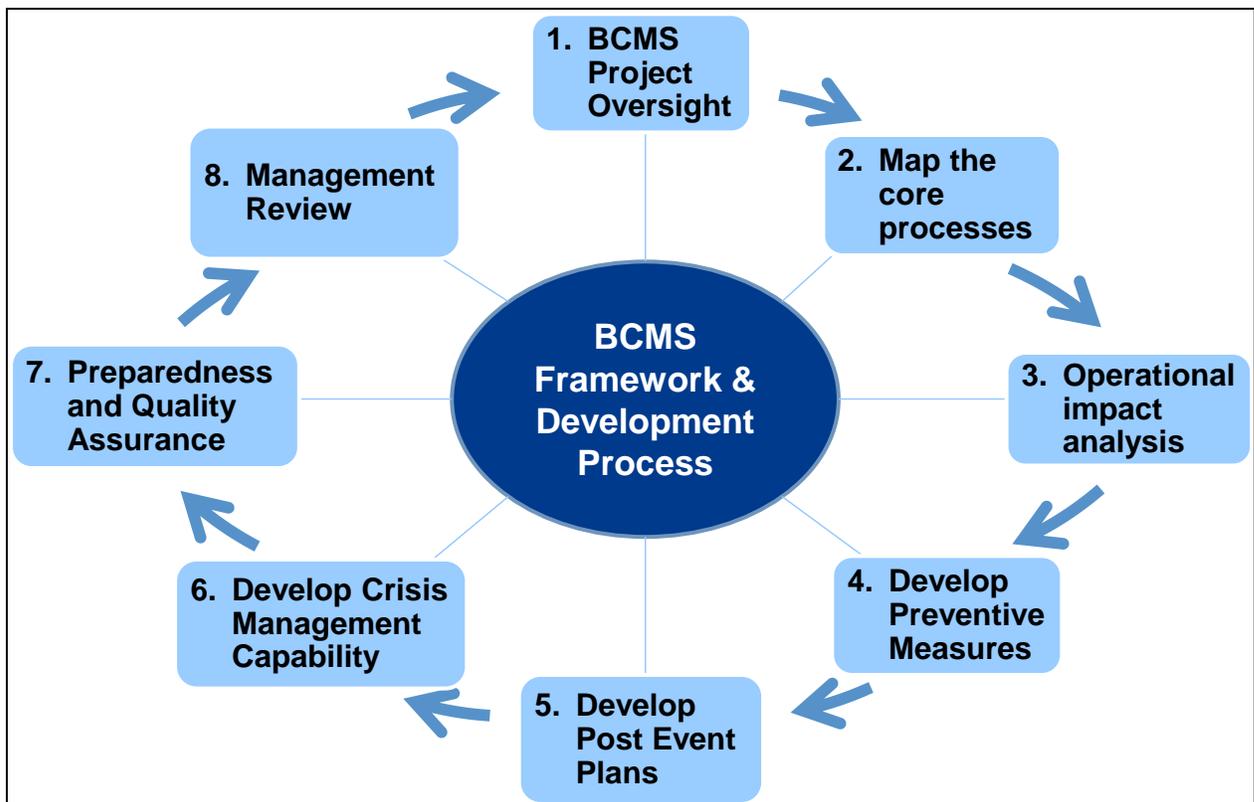


Figure 2: BCMS Development Process

### 3.1. Establish the BCMS Project Oversight structure

A BCMS is not easy to develop or implement. There needs to be a dedicated effort, driven by the top management team, with a specific team and dedicated resources to define the BCMS structure and oversee its implementation.

The BCMS Project Oversight Team should have at least the following participants

- From the Airport Operator:
  - o Director of Operations or Senior Operations Manager, with operations experience
  - o Engineering and maintenance Senior Manager
  - o Business process owners
  - o Senior Safety and Security Managers
  - o Administration and HR Manager
- Possible representatives from Business Partner and External participants
  - o Civil Aviation Authorities
  - o Health Authorities
  - o Emergency Services
  - o Airlines and aircraft operators
  - o Customs
  - o Border police
  - o Local police
  - o Air catering operators
  - o ATM and ANSP (please explain the shortenings.....)
  - o Local Station Managers
  - o Ground and Ramp Handlers
  - o Line and base maintenance operators
  - o Fuel Suppliers
  - o ATS
  - o Utilities and supplies (water, electricity, ICT, etc...)

The BCMS Project Oversight Team will be responsible for:

- The publication and maintenance of BCPs for the airport
- Coordinating the BCP process with airlines and Business Partners
- Communicating the development process and the results to the airport community

The BCMS Project Oversight Team will establish a face to face meeting or teleconference calendar, and should keep a documented work plan, deliverables, and milestones programme.

### 3.2. Map the core processes

It is crucial to have a deep understanding of the processes and sub-processes at the airport, especially those that are critical for the continuity of the operations. It is necessary to know the relationship between processes, and how the value chain is affected when a process or sub-process' outputs are degraded.

Figure 3 shows the typical processes at an airport with two terminals. Each of these should be mapped with all the sub-processes documented. These would identify the system and people resources needed, as well as the minimum service-level inputs and outputs.

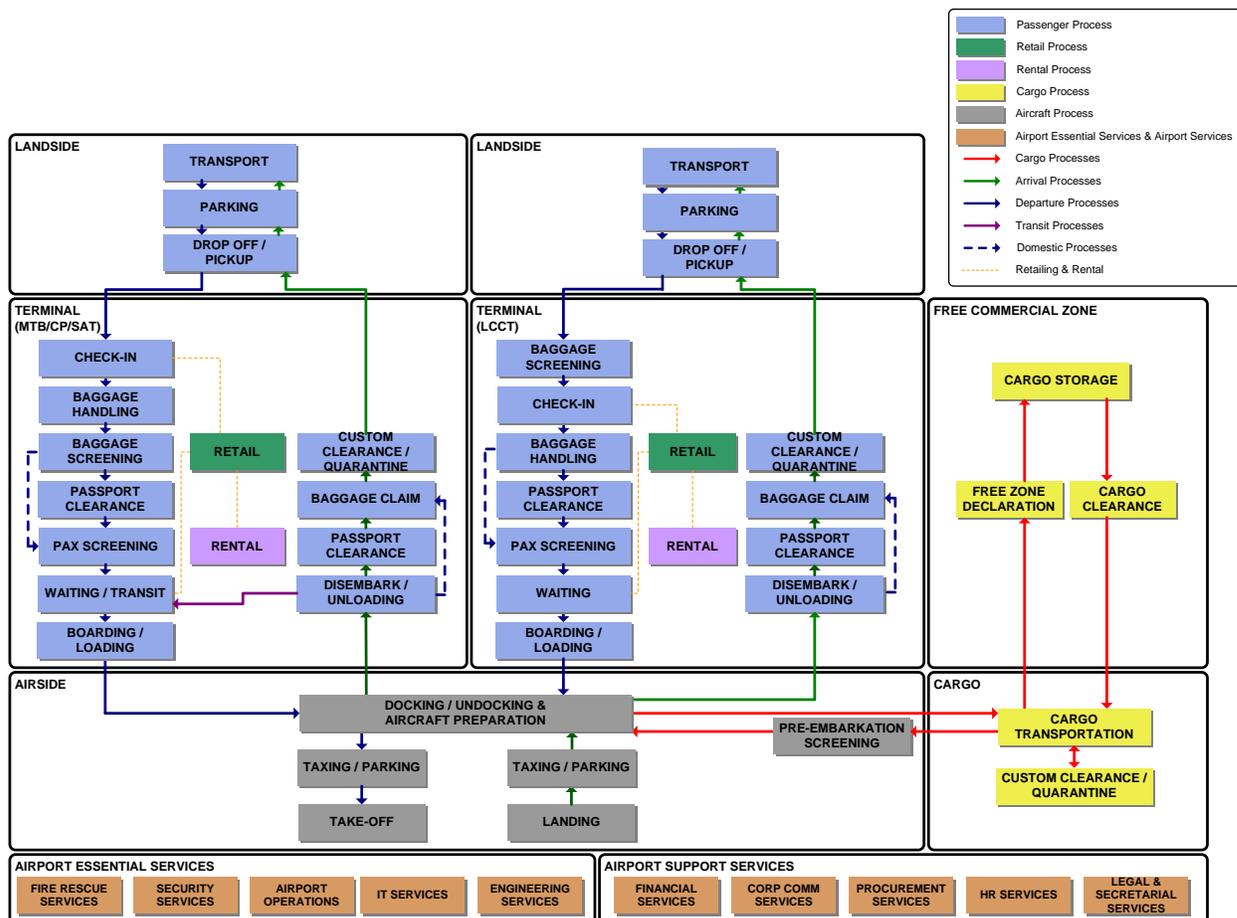


Figure 3: Typical airport processes (Courtesy of KLIA)

### 3.3. Conduct Operational Impact Analysis

In this step, it is necessary to identify the effects of a degraded service from the proceeding step in the process, as well as failures or service degradation in this step of the process. A three or four tiered categorization could be adopted:

- Normal operations = 100% of agreed Service Delivery Standards
- Degraded (Impact) Level 1 = XX% of agreed Service Delivery Standards
- Degraded (Impact) Level 2 = YY% of agreed Service Delivery Standards

It is fundamental to define the output capabilities at degraded levels of operation and the minimum resource requirements, particularly in terms of staff and equipment. After this study, it is necessary to assess the effect of degraded service on this process and other integrated processes.

Example: If it is possible to achieve only 50% of the Baggage handling system service delivery standards, it will be necessary to calculate the cumulative effect on the aircraft turn around process, flight delays and the possible knock-on effect on the aircraft movement schedules, passenger check-in delays, passenger bag pick-up delays, etc...

### **3.4. Develop / Review the adequacy of Preventive measures (Maintenance Plans and System Fallback Plans)**

The analysis in step 3.3 should identify critical issues and the adequacy of existing preventive measures should be assessed in comparison with these. Enhanced arrangements might be required, for example cross training and qualifying staff in specific activities (e.g., driving specialist equipment) to ensure that service delivery standards can be maintained if the normal staff levels are degraded.

#### **3.4.1. Preventive and Maintenance Plans**

##### Definition

Preventive and maintenance plans are those programmed actions that are undertaken to warrantee the normal operation of a system or process without failure. May include predictive maintenance regimes whereby parts or whole systems are replaced upon reaching projected lifespan due dates and prior to catastrophic breakdowns.

##### Objective

The objective of these plans is to prevent any possible incident to appear.

##### Measures of success

- Zero incidents due to equipment aging or system malfunction from poor maintenance

##### Who's involved in putting the plan together?

- Business Process owner (could be department head)
- Technical owner/expert or system owner/manager
- Main user(s) (stakeholders and business partners)

##### What needs to be done?

- Document all maintenance protocols from equipment manufacturers
- Plan to deliver all maintenance actions accordingly
- Program regular inspections of critical systems and processes to detect potential incidents before they happen.
- Coordinate with the maintenance department as needed.

#### **3.4.2. System Fallback Plans**

##### Definition

These plans ensure that, when an incident occurs, those specific business process elements affected are either fixed, or in the case of systems that may fail with only minor, non-operational effects, there is a workaround or a backup. May include strengthening system resiliency by redundancies (e.g. server mirroring), back-ups (e.g. standby generators), rerouting (e.g. power grid interweaving from different power sources), etc.

### Objective

To ensure that all elements of the business process (**systems, equipment and personnel**) that are affected by an incident are fixed and function normally through the period. If there are known problems with any elements, they are fixed. If they cannot be fixed, there is a working method put in place that bypasses the non-functioning element.

### Measures of success

- Minimal disruption of the business due to elements of the process failing.
- All critical business processes have a fallback plan in place, signed off by the BCMS leadership.

### Who's involved in putting the plan together?

- Business Process owner (could be department head)
- Technical owner/expert or system owner/manager
- Main user(s) (stakeholders and business partners)
- Public Health Authorities

### What needs to be done?

- Ensure the process map and inventory of systems is up to date and systems' status are known.
- From the process flows, determine weaknesses/failure spots
- Propose fixes and workarounds
- Determine the resource requirements for each part
- Document the Plan
- Validate the Plan by regular drills and exercises

## **3.5. Develop / Review adequacy of Post-Event Plans (IT Recovery Plans, Operational Continuity Plans and Business Recovery Plans)**

The objectives of these plans need to be defined in terms of Process Recovery Times. It is important to define the maximum length of time in which each critical service need to be restored. An important corollary to this is a clear understanding of the maximum allowable downtime of each critical service; in other words, how long can you operate without that service keeping in mind the interdependencies with other services?

A holistic view of the whole airport's operations needs to be achieved. Core business processes need to be identified, process vulnerabilities determined and critical paths highlighted.

These objectives will help to shape the Recovery Strategy. Where there has been a protracted and widespread disruption to airport operations, defining priorities in restoring operations is a fundamental step. Normally, priority will be accorded to restoring the essential services first. As far as possible, these strategies need to be planned in advance.

Example: Passenger operations might take priority over cargo operations, wide-body operations over narrow; regional flights over long haul, etc.

### 3.5.1. ICT Contingency and Recovery Plans

The Post-Event Plans should start by addressing the importance of Information and Communication Technologies (ICT) as a basic enabler of aviation operational business continuity. Priority should be given to manage and recover any possible disruption in the basic ICT services (phone, internet) and its power sources.

#### Definition

- An ICT Contingency plan enables the operation of an ICT related service to continue in the event of a failed system. This may involve a degraded standard of service.
- An ICT Recovery plan details the means by which ICT systems are brought back into service after failure or back into normal operation from contingency mode.
- Includes the ICT disaster recovery plans for ICT applications / servers / main frames.

#### Objective

To ensure that, should an ICT element of a process fail, action can be taken to reinstate the function of the process and enable the business to bring those failed elements back into service.

#### Measures of success

During the ICT contingency period, any failure which does occur is dealt with adequately, and causes little or no disruption. The ICT service is brought back into operation in an effective, efficient and economical manner.

#### Who's involved in putting the plan together?

For each process:

- The ICT department (ICT business process owner)
- System owners/technical experts
- Main users/operators of the critical ICT services

#### What needs to be done?

For each process:

- Develop the ICT Contingency Plan:
  - o Assess the risk and the impact of failure on critical elements of the process.
  - o Evaluate the preventive measures to ensure they adequately address the risks identified.
  - o If these measures do not adequately address the risks, then a contingency plan needs to be developed, trigger points identified and operational roles assigned.
  - o Provide ICT tools and procedures to work remotely, for those staff members that cannot work physically at the airport campus.
  - o Contingency planning is a common exercise and as such will not be dealt with directly in these guidelines.
- Develop the ICT Recovery Plans:
  - o For each ICT related contingency plan, assess the status of the process once it is in operation (airport and business partner operational status)
  - o Determine the impact going into contingency mode will have on the service levels
  - o Document the steps required to proceed from contingency mode to normal operational mode
- Implement the ICT Contingency and Recovery Plans:
  - o A series of validation drills and exercises to ensure efficacies of the Plans

### 3.5.2. Operational Continuity Plans

#### Definition

An Operational Continuity plan enables the operation of a business process to continue in the event of a failed system or piece of equipment, or lack of supplies or human resources. This may involve a degraded level of service. These plans can be divided in material continuity plans and staff continuity plans.

#### Objective

To ensure that, during the time of the disruption effect and before recovery, action can be taken to maintain the outputs of the disrupted process as per accepted level of service.

#### Measures of success

During the contingency period, any failure which does occur is dealt with adequately, and causes little or no disruption to agreed levels of service.

#### Who's involved in putting the plan together?

For each process:

- The Business Process Owner
- System owners/technical experts
- Main users/operators of the process

#### What needs to be done?

For each process:

- Develop an Operational Materials and Supplies Continuity Plan:
  - o Assess the risk and the impact of failure on the supply chain for critical elements of the process.
  - o Identify the amount of supplies required to maintain operations at an agreed service level.
  - o Ensure stock of those minimum supplies that are critical for operations.
  - o Evaluate the preventive measures to ensure they adequately address the risks identified relative to reduction of supplies.
  - o Review prioritisation of Business Processes and balance against supply numbers required.
  
- Develop an Operational Staff Continuity Plan
  - o Identify the number of staff required to maintain operations at a predetermined service level (minus 10 %,30%,50% of staff) over the disruption period.
  - o Ensure that adequate additional staff are available to be called upon to manage the operation if necessary.
  - o Monitor the number of staff affected by the disruption.
  - o Involve Airport Human Resources/Personnel department; Business Process owners; Staffing Representatives (Unions) and Airport Operational Management
  - o Gather input from Business Partners on their contingency plans and the demands they may place upon the airport's staffing plans.
  - o Include operational personnel, security staff, engineering and maintenance operatives and contractors. Senior managers required for crisis management roles.
  - o Study legislation to address remuneration levels and extra time workload for individuals and groups (specific to operating company) to guarantee required staff numbers over the disruption period.
  - o Collate total staff numbers required by function/department eliminating duplication and double counting.
  - o Think about back up staff (ex-employees, retired people, students.....)
  - o Reduce staff in the hot phase as employees from administration e.g. (as back up system if needed)
  - o Implement crisis intervention team if needed
  - o Implement care team for employees
  - o Implement telephone hotline for employees
  - o Implement medical care for your employees
  - o Review prioritisation of Business Processes and balance against staff numbers required.
  
- Implement the Operational Continuity Plans
  - o Conduct series of validation drills and exercises to ensure efficacies of these plans in close cooperation with public health authorities.
  - o Establish a regular schedule of drills and exercises to train all parties to the plans as well as ensure the plans' continued viability over time.

### 3.5.3. Business Recovery Plans

#### Definition

A Business Recovery plan details the means by which the systems, processes or equipment are brought back into service after failure or back into normal operation from contingency mode.

#### Objective

To ensure that action is taken to reinstate the business process normal status and enable the business to bring those failed elements back into service.

#### Measures of success

The element is brought back into operation in an effective, efficient and economical manner.

#### Who's involved in putting the plan together?

For each process:

- The Business Process Owner
- System owners/technical experts
- Main users/operators of the process

#### What needs to be done?

For each process:

- Develop the Business Recovery Plans:
  - o For each contingency/continuity plan, assess the status of the process once it is in operation (airport and business partner operational status)
  - o Determine the impact going into contingency/continuity mode will have on the individual elements within the process
  - o Document the steps required to proceed from contingency/continuity mode to normal operational mode
- Implement the Business Recovery Plans:
  - o Establish a reasonable timeline to gradually implement subsequent steps identified in the plan.
  - o Establish a regular schedule of drills and exercises to train all parties to the plans as well as ensure the plans' continued viability over time.

### 3.6. Develop / Review Crisis Management Capabilities

The response to a crisis requires **communication, coordination and control**. This requires a crisis management strategy, properly trained competent people and adequate equipment. Normally, a dedicated crisis management centre is needed, separate from the facilities used to monitor and manage normal operations. While the tactical response to a critical event on the

ground will differ, the crisis management approach should be similar. Its role is to minimize the scope, scale and duration of the crisis and to restore normal operations as quickly as possible.

### **3.6.1. Crisis Management strategy**

#### Definition

This plan shows how to effectively and efficiently manage the response to any major disruption.

#### Objectives

- To assign roles and responsibilities to all relevant management and staff to enable them to react quickly to any crisis situation that arises.
- To enable fast and effective communication between key parties within the airport community.
- To ensure all relevant staff and business partners are prepared and able to instigate the recovery of processes or systems that may fail due to a critical event and its related effects.

#### Measure of success

The Crisis management team is able to lead and drive effectively the response measures.

#### Who's involved in putting the plan together?

- Airport Senior Management
- Business Partners
- Process Owners/Systems Managers
- Key Staff members

#### What needs to be done?

- Evaluate existing Crisis Management Strategies and Plans, and update where necessary.
- Ensure that the following elements are included:
  - o Decision making processes
  - o The process for recording decisions taken
  - o The communications approach and mechanisms
  - o The escalation process
  - o The instigation process and trigger mechanism
  - o Cooperation with public health authorities
- Determine the availability of a Crisis Management Centre or a Communications Centre.

### 3.6.2. Training Plans

#### Definition

A structured plan which details the special staff training needs over the disruption period. These duties will have changed due to the business continuity plans and contingency plans.

#### Objective

To ensure that all staff members receive appropriate training required to allow them to fulfill the roles they might be assigned when contingency measures are activated.

#### Measures of success

All staff members involved in business continuity actions are adequately:

- trained as per their specific roles in the BCMS
- cross-trained to fulfill adequate level of staff for critical functions and roles

#### Who's involved in putting the plan together?

- Airport Human Resources/Personnel department
- Business Process owners
- Staffing Representatives (Unions)
- Airport Operational Management
- Input from Business Partners (as PHA....) on their contingency plans and the demands they may place upon the airport's staffing plans.

#### What needs to be done?

- All Business Continuity Plans need to be analysed for their staffing requirements (numbers) and for the changes to working practices that they need.
- Line management, Human Resources (Personnel) and Process Owners have to match staff numbers and capabilities to the roles required and draw up the training requirements matched against the actual staff members.
- Timing of the training must also be taken into account to ensure that the instruction remains in the minds of the trainees as close to the time of activation of the specific Continuity Plan as possible.
- Organisations must negotiate with unions to agree to changes in working practices to address the additional resources needed to face the disruption.

### 3.6.3. Communications Plans

#### Definition

This plan details how communications, both internal, external and with the press and other media are to be handled over the disruption period.

### Objective

To provide a robust communications matrix that defines the content and level of communications between all parties involved in the operation of the airport over the disruption period.

### Measures of success

There is a constant flow of information to and from all the individuals, teams and aviation stakeholders involved in the BCMS, and the travelling public and media are adequately informed.

### Who's involved in putting the plan together?

- Airport, Government, Regulatory Authorities and business partners Senior Management
- Public Relations/Media department
- Operational management
- Process Owners/Systems Managers
- Key Staff members

### What needs to be done?

- A communications matrix needs to be drawn up detailing all the relevant parties that may be involved in the operation, including senior management and public relations, airlines and business partners, the press and public. It should be tested in a variety of scenarios to ensure that relevant information is received at all levels to enable swift management decisions to be made and action taken in response.
- Consideration should be given to the establishment of a communications centre to assist in the control and dissemination of information for the period.
- Alternative means of communication should be investigated to ensure back-up systems are available.
- Consideration should be given to the effect of electricity loss as well as service provider loss.

### 3.7. Preparedness / Quality Assurance (Monitoring & Corrective Action)

With any management system, there needs to be a quality assurance process. The quality assurance of the BCMS can be divided into two: Quality assuring the preventive measures and quality assuring the post-event response plans.

Quality assuring the preventive measures would include the continual measuring and monitoring the performance of processes (and their systems) against service delivery standards and auditing the maintenance and system fall-back plans. Where non-conformance occurs corrective action should be taken.

The effectiveness of the post-event response will be depend on the quality of the plans, the competence of the staff implementing them; and the availability and serviceability of the equipment needed. This will involve briefing staff on the plans (knowledge), training them in how to operate equipment (skills) and validating this through drills and exercises. Drills typically focus on one aspect of a plan, while an exercise tests the whole plan.

#### 3.7.1. Scenario Testing

##### Definition

The means by which any element of the overall business continuity plan is tested to prove it is able to protect the business. This is achieved through a series of levels, including:

- Desktop exercises
- Process level testing
- Full, end to end testing involving all aviation stakeholders.

##### Objective

To implement a Testing Programme to show that the Business Continuity Plans are adequate for the main risk areas identified, with an appropriate level of confidence.

##### Measures of success

Testing is conducted and lessons learned are applied for all areas of the business and cover all levels previously mentioned within the operation.

Who's involved in putting the plan together?

- Airport, Government, Regulatory Authorities and business partners Senior Management
- Process Owners/Systems Managers
- Key Staff members

### What needs to be done?

- It will be impossible to fully test every single scenario. Main target areas and plans dealing with mission critical processes should be tested. These will come from risk and impact analysis of the airport's most vulnerable or critical processes.
- Test Scenarios need to be developed and agreed. These include, for example, single and multiple system failures within a process as well as combinations of both these within multiple processes.
- Periodic review of plans and re-running of scenario tests should be programmed as appropriate.

### **3.8. Management Review**

Given the strategic importance of the continuity of operations to an airport, the top management team, together with the BCMS oversight team, should satisfy that the BCMS is fit for purpose and that it is being properly implemented and maintained. This should be a regular activity, embedded into the corporate management approach, and will be subject to the reports from drills and exercises, and the implementation of corrective actions following a closed loop, continuous improvement approach.

## 4. BCMS – Best Practices for Infectious Disease Pandemics

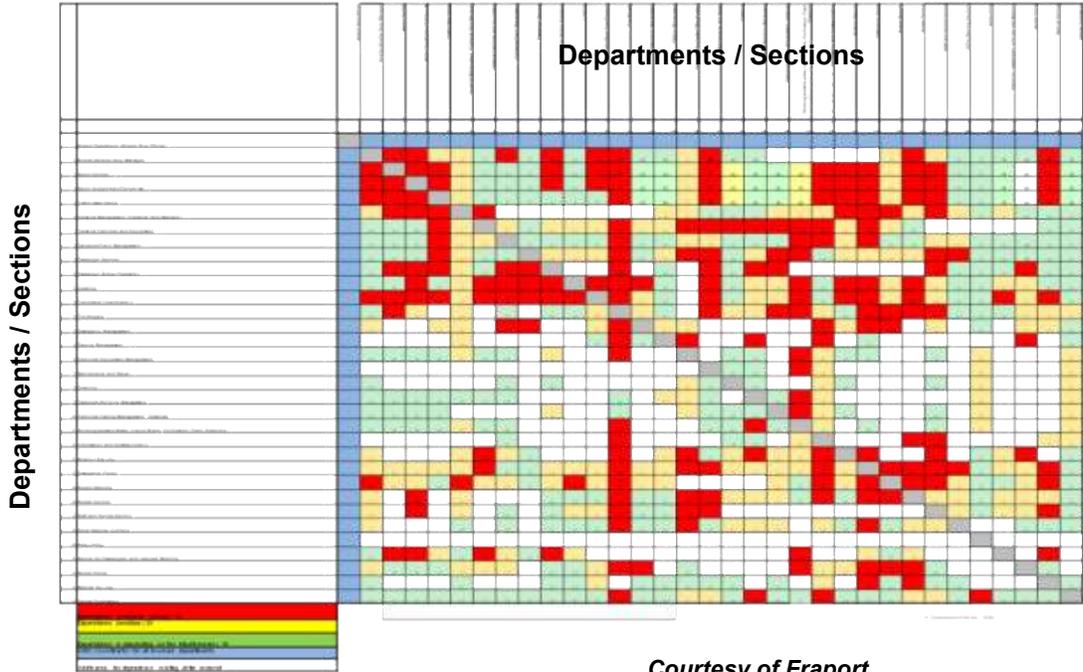
Our research into existing practices in the industry have identified a number of tools or best practice approaches, which could assist airports that are establishing a BCMS. Here are some examples:

### Planning template (HKIA)

1. This planning template is to assist you in writing new procedures wherever your existing processes are missing such procedures.
2. This is a planning process in itself; it will take you step by step to write out new contingency plans.
3. First thing you need to do is to state the Business Deliverable.
4. Next is to write out the agreed service delivery standards in measurable, quantifiable terms.
5. Next is to list out all the resources needed (Staff, Premises, IT & Engineering Systems) to maintain and/or recover this Business Deliverable to the stated service delivery standards.
6. Once you have decided on the resources you will need, next step is to write out and document the operational procedures.
7. Ensure that other stakeholders in your Business Deliverable are consulted for their inputs.
8. Some service disruptions or crises will involve a possible lowering of service standards; as such, you may wish to add to the table one or two levels of acceptable/agreed upon service degradation(s) with their corresponding resources and operational procedures.

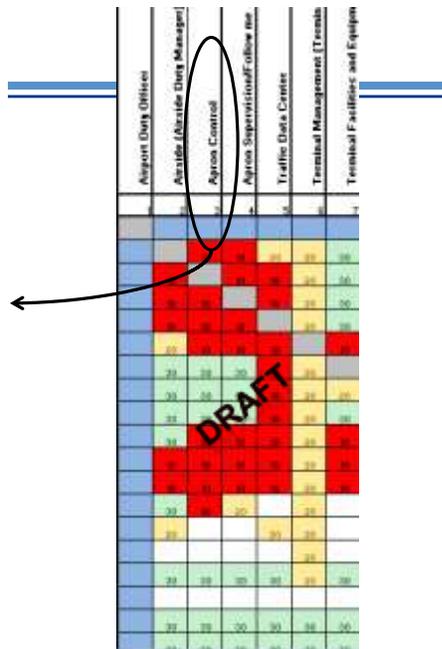
Business Deliverables Planning Template														
Department / Section : _____														
Business Deliverables (BD)	Staff	Premises			IT / Telecommunications / Engineering Systems & Equipment								Operating Procedures (Referenced in which document?)	Others Involved (Internal / External parties)
		Area (m <sup>2</sup> )	Work Stations	Others	IT Systems / Applications	Engineering Systems	PC Internet Enabled	Printer	Fax	Phone / TMR	Others			
BD 1 – Quantify with measurable criteria														
Agreed Service Delivery Standards														
Degraded Level 1 Service Delivery Standard (if applicable)														
Degraded Level 2 Service Delivery Standard (if applicable)														
BD 2 – Quantify with measurable criteria														
Agreed Service Delivery Standards														
Degraded Level 1 Service Delivery Standard (if applicable)														
Degraded Level 2 Service Delivery Standard														

Operational checklists (courtesy of Fraport)



© 2012 Airports Council International

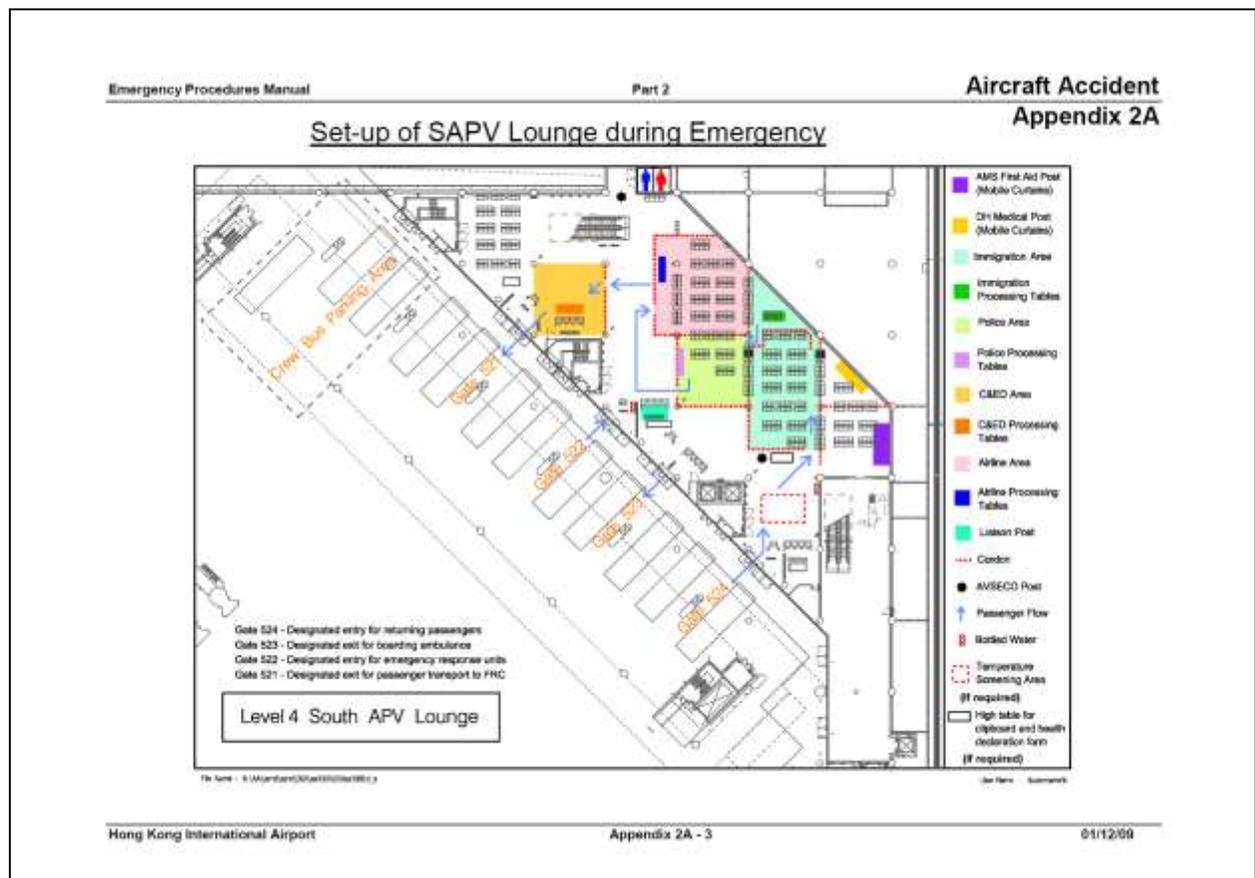
Courtesy of Fraport





## Using Existing Infrastructure (HKIA)

1. Planning for new and emerging risks may include using existing response infrastructure as much as possible.
2. Resources are limited at the airport and making use of existing infrastructure is good practice in maximizing limited resources.
3. Adapting and adopting existing response infrastructure will help responders transition easier to new procedures as they are already familiar with existing environment.
4. Temporary Holding Area (THA) is part of the public health response plan to an aircraft with passenger(s) suspected of having an infectious disease.
  - a. The THA may be used to accommodate passengers and crews while waiting for laboratory test results on whether it is or is not an infectious disease.
  - b. This holding function is similar to that of the aircraft accident response’s Passenger Reception Center (PRC) for uninjured passengers (see diagram below).
  - c. As such, the PRC is adapted for use as the THA in a public health response (see diagram on following page).



Emergency Procedures Manual      Part 13
   
**Public Health Emergencies**
  
 Appendix 13-B

**Temporary Holding Area Set Up at SAPV**



## 5. Acknowledgements

ACI World would like to recognise the input from the following companies and entities in drafting and reviewing these Guidelines:

- Hong Kong International Airport
- Fraport AG
- Malaysia Airports Holding Berhad
- ACI World Facilitation and Services Standing Committee

End of v.1 – 31 December 2012