'QH-04'

(1)

Queensland Government
Queensland Health

AUDIT REPORT

OPERATIONAL AUDIT OF

EMERGENCY PREPAREDNESS, DISASTER MANAGEMENT AND BUSINESS CONTINUITY PLANNING –

CORPORATE MANAGEMENT

DOCUMENT CLASSIFICATION

THIS REPORT HAS BEEN PREPARED BY THE AUDIT AND OPERATIONAL REVIEW UNIT, QUEENSLAND HEALTH.

THIS DOCUMENT IS CLASSIFIED AS "CONFIDENTIAL" UNDER THE QUEENSLAND HEALTH INFORMATION CLASSIFICATION POLICY (QHEPS DOCUMENT IDENTIFIER 25959) AND SHOULD BE APPROPRIATELY SECURED.

THE UNAUTHORISED POSSESSION, REPRODUCTION, AND/OR DISCUSSION OF THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROHIBITED AND MAY RESULT IN PROSECUTION.

IF IN DOUBT AS TO THE DEALING WITH INFORMATION ARISING OUT OF THIS DOCUMENT, PLEASE CONTACT THE DIRECTOR, AUDIT AND OPERATIONAL REVIEW UNIT, QUEENSLAND HEALTH ON (07) 323 40815 OR FAX (07) 323 41967.

TABLE OF CONTENTS

Page No.

BACKGROUND

PRIOR REVIEW 2006 – HEALTH SERVICE DISTRICTS

During the period April – May 2006 the Audit and Operational Review Unit performed a detailed review of Emergency Preparedness, Disaster Recovery and Business Continuity Plans as prepared by a sample of Health Service Districts.

The overall objective of the review was to ensure Queensland Health Executives were managing, (through the establishment and implementation of adequate and effective frameworks, strategies, plans, policies and procedures) the risks associated with emergency, disaster, security, contingency, asset protection and resilience management in accordance with applicable frameworks to enable effective response and service continuity in the event of an incident.

The Framework Forming the Basis of Prior Review

Queensland Health has established its Emergency Preparedness and Continuity Management Policy, Guidelines and Program to support its preparedness and capability to prevent, respond to, and recover from an emergency event such as:

- A cyclone, earthquake, flood, storm, storm tide, tornado, tsunami, volcanic eruption or other natural happening;
- An explosion or fire, a chemical, fuel or oil spill, or gas leak;
- An infestation, plague or epidemic;
- A failure of, or disruption to, an essential service or infrastructure;
- An attack against the State (eg terrorism);
- Medical emergency;
- Accident, a bus or aircraft crash or major industrial accident;
- Threat to or on a person;
- A release of a chemical, biological or radiological agent; and/or
- Any other similar event.

Queensland Health's Emergency Preparedness and Continuity Management Policy, Guidelines and Program ("the Framework") include, et al:

- Queensland Health Disaster Plan 2002;
- Queensland Health Policy Statement 28028 – Emergency Preparedness and Continuity Management;
- Queensland Health Integrated Risk Management Framework (QHEPS 15232);
- Queensland Health Information Security Policy (QHEPS 3485); and
- Queensland Health Information Security Standard 9 – Business Continuity Management (QHEPS 23724).

This Framework is part of, and in support of, the Queensland Government's project for the safety and security of Queensland in:

- The preparation for, prevention of, response to and recovery from terrorism related incidents, as set out in the Queensland Government Counter-Terrorism Strategy 2005-2007, and consistent with the National Counter-Terrorism Framework;
- The protection and resilience of infrastructure; and
- The protection of critical infrastructure from terrorism.

The Framework is also based on, and supports compliance with and implementation of, relevant Legislation, Policies, Standards and key documents including:

- Disaster Management Act 2003;
- State Counter Disaster Plan 2001;
- Queensland Government Counter Terrorism Strategy 2005-2007
- Queensland Government Infrastructure Protection and Resilience Framework;
- Queensland Government Plan for the Protection of Critical Infrastructure from Terrorism
- Standards Australia and New Zealand - AS/NZS 4360 - 2004 – Risk Management
- Standards Australia and New Zealand- HB 221:2004 Business Continuity Management;
- Australian Standard – AS 4083-1997 Planning for Emergencies – Health Care Facilities; and
- Queensland Government Information Standard 18 – Information Security.

Health Service Districts Subject to Prior Review

Review was performed on a sample basis across the following (then) Health Service Districts:

- Southern Area Health Service - Princess Alexandra Hospital Health Service District
- Southern Area Health Service - Gold Coast Health Service District
- Northern Area Health Service - Cairns Health Service District
- Northern Area Health Service - Innisfail Health Service District
- Central Area Health Service - Gladstone Health Service District
- Central Area Health Service - Central Highlands Health Service District

Scope and Nature of Prior Review Procedures

Prior review procedures took the form of:

- Discussions with key officers at hospital based facilities and inter-agency representatives; and
- High-level review of plans, policies, procedures and related documentation as presented to us.

Outcomes and Conclusions of Prior Review

Overall, the review highlighted ***significant issues and progress limitations relating to inadequate capacity and resources*** for facilities to develop, implement, review, test and maintain frameworks for emergency, disaster, security, contingency, asset protection and resilience management within current skill sets and resources allocations. This observation is particularly impacting smaller and medium size operations.

In summary, areas of weakness related to:

- Progress to date in establishing and implementing appropriate/formal Governance structures;
- Progress to date in performing and maintaining a formal all-hazards / whole-of-business approach to risk assessment for the development of adequate strategic and operational contingency and continuity plans;
- Progress to date in performing and maintaining formal security risk assessments and related general security strategies and plans to support infrastructure protection and resilience; and
- Progress to date in developing and maintaining specific incident emergency response plans.

Matters arising from the review indicated, at a Health Service District and facility level, a perceived lack of leadership, role and responsibility clarity and resource support from Corporate Office in respect of planning requirements. As a result, this audit has been performed over Corporate Office functions as they relate to same. The Terms of Reference for this audit are attached at Appendix A.

EXECUTIVE SUMMARY

The following provides an overview of key observations for each area subject to audit, as well as specific matters for consideration in undertaking further necessary development work.

Overall, the audit has highlighted that a significant amount of work is required to continue to progress development of plans and procedures in accordance with established frameworks for emergency, disaster, security, contingency, asset protection and resilience management.

An overall summary of progress evaluation is as outlined below, noting that in all instances, further development work to some extent is required:

	Mature Leadership, Responsibility, Governance, Control and Accountability Frameworks	Mature Structures, Frameworks, Procedures, Protocols and Supporting Tools	Section Reference
Corporate Services Unit	Further development required	Further development required	Section 1
Corporate Services – Business Policy and Strategy Unit	Further development required	Further development required	Sections 2 and 3
Shared Service Provider – Availability of Emergency Medical Supplies	*Note 1*	Further development required	Section 4
Shared Service Provider – Finance and Payroll Systems	*Note 1*	Further development required	Section 5
Shared Service Provider – Business Continuity Plan with CorpTech	*Note 1*	Further development required	Section 6
IT Systems – QGIS 18 – Information Business Continuity and Disaster Recovery Planning	*Note 1*	Further development required	Section 7

	Mature Leadership, Responsibility, Governance, Control and Accountability Frameworks	Mature Structures, Frameworks, Procedures, Protocols and Supporting Tools	Matter Reference
IT Systems – Enterprise IT Applications Backup and Disaster Recovery	*Note 1*	Further development required	Section 8
Area Health Services and Clinical and Statewide Services	Further development required	Further development required	Section 9

Note 1: Our observation and evaluation is specific to matter subject to audit. Overall high level evaluation of this broad scope element was not within the scope of this audit and therefore comment is not made.

INTRODUCTION

The objective of the current audit has been to:

- Identify key areas of leadership, responsibility and accountability for Emergency Preparedness, Disaster Management and Business Continuity Management, at Corporate Office and other key service delivery units;
- Seek feedback on their progress in developing and implementing appropriate structures, frameworks, policies, procedures, protocols and supporting tools in the planning for their area of responsibility/accountability and supporting integration throughout the Agency; and
- Identify and communicate matters perceived as continuing to hinder progress in developing, implementing and managing same for further consideration and resolution by Queensland Health.

Areas subject to review, and key personnel consulted during review, included:

UNIT	KEY PERSONNEL
Corporate Office	• Chief Health Officer
Emergency Management Unit	• Director, Emergency Management Unit (also in capacity of delegate of the Chief Health Officer)
Corporate Services Unit	• Executive Director, Corporate Services
Shared Service Provider	• Executive Director SSP
Business, Policy and Strategy Unit	• Director Business Policy and Strategy Unit • Acting Team Leader Property and Facilities Management, Business Policy and Strategy Unit
**** Policy, Planning and Resourcing Unit***	• Executive Director, Policy, Planning & Resourcing
**** Reform and Development Unit***	• Executive Director, Reform and Development

UNIT	KEY PERSONNEL
Information Division	• Chief Information Officer • Acting Senior Director, InfoInvestment • Director Operations Consulting, InfoOperations • A/Director Information Security and Risk Unit, InfoInvestment Branch • Manager, Enterprise Data Centres, InfoOperations
Clinical and Statewide Services	• Delegate of Executive Director, Clinical and Statewide Services
Southern Health Area Service	• General Manager
Central Health Area Service	• Assistant General Manager (as delegate of the General Manager)
Northern Health Area Service	• General Manager

Our report herein sets out status and feedback from the above.

Units noting * advised they have no direct line responsibility/accountability for Emergency Preparedness, Disaster Management and Business Continuity Planning.

AUDIT FINDINGS

1. CORPORATE SERVICES UNIT

Background

Corporate Services functional areas of responsibility include: Finance, Human Resources, Capital Works and Asset Management, and Business Policy.

The context for its responsibility and accountability is in respect of policy setting only (with the exception of operational/business analyst functions, ie monitoring, assessment and reporting performance at a high level). The Corporate Services Unit provides high level support for strategic issues across these functional areas, with Health Service Districts responsible and accountable for managing specific and direct delivery issues.

In relation to corporate systems relied upon in delivery of functional areas of responsibility and accountability, Queensland Health's Shared Service Provider (QH SSP) owns and implements Finance and Human Resource Systems, which are in turn maintained by Queensland Health.

Issues

Audit were advised that the only key role in Emergency Preparedness, Disaster Recovery and Business Continuity Planning and Management is in respect of the coordination of Corporate Office building issues in the event of an emergency or disaster incident (eg fire evacuation, managing security staff, building relation etc). Again, districts are responsible for these issues in respect of their own areas of responsibility.

For these matters, refer Sections 2 and 3 below.

Audit were advised that, in respect of Emergency Preparedness, Disaster Recovery and Business Continuity Planning and Management as it relates to corporate systems, the Corporate Services Unit's only responsibility is to ensure that Disaster Recovery and Business Continuity Management Plans are maintained by its SSP in accordance with established Operating Level Agreements (OLA).

Audit were advised that requirements in this respect are discussed with the SSP through the annual OLA negotiation process, with reliance on Internal Audit to ensure plans are adequately maintained. No further management actions are taken to ensure the adequacy and effectiveness of plans developed and maintained by the SSP.

Implication

The role of Internal Audit is to provide assurances as to the adequacy and effectiveness of management controls, and should not be relied upon as the first line of management control, responsibility and accountability.

Further to reliance on Internal Audit for ensuring the adequacy and effectiveness of plans developed and maintained by the SSP, no action is taken by the Corporate Services Unit in this regard.

Risk Assessment		
Likelihood	Impact	Risk
Possible	Moderate	High

Recommendation 1

It is recommended that the Executive Director Corporate Services, establishes control processes for the confirmation, on an annual basis, that SSP roles and responsibilities for emergency preparedness, disaster recovery and business continuity planning have been met.

Management Response			
☐ Accept	☐ Reject	/ /	
Please select		Implementation Date	Action Officer
Comments:-			

2. CORPORATE SERVICES - BUSINESS POLICY AND STRATEGY UNIT

Background

The Corporate Office Services Unit Building Infrastructure Business Continuity Plan (the Plan) was prepared in August 2003, with latest revision February 2006. The Plan relates primarily to buildings and does not take into consideration other corporate services infrastructure, including:

- Records Management Systems (Corporate Office – SSP; all others Agency Responsibility through Health Service District's BCP) (Edocs to be implemented and BCP will form part of this roll out process);
- Fleet Management Systems; and
- Travel Management Systems.

Issues

Management recognises, the Corporate Office Services Unit Building Infrastructure Business Continuity Plan as requiring significant revision to comply with Agency and State Policy requirements for Emergency Preparedness, Disaster Recovery and Business Continuity.

Going forward, the Unit plans to establish and operate an Emergency Preparedness Group to address the Emergency Preparedness, Disaster Recovery and Business Continuity aspects (from a policy setting perspective) of:

- Records Management Systems (Corporate Office – SSP; all others Agency Responsibility through Health Service District's BCP) (Edocs to be implemented and BCP will form part of this roll out process);
- Fleet Management Systems;
- Travel Management Systems; and
- Property and Facilities.

At the time of audit, the Emergency Preparedness Group was yet to finalise its membership and establish Terms of Reference/Charter, and was seeking to establish guidelines on what is required from the Unit's perspective regarding Emergency Preparedness, Disaster Recovery and Business Continuity Planning.

Other matters noted:

- Queensland Health is in the process of moving premises for a number of Units. This will impact the currency and appropriateness of existing Building Infrastructure Business Continuity Plans, which will require revision to be location specific. It is intended that this will be actioned under the Emergency Preparedness Group.

- Yet to progress Pandemic Planning for business continuity as it relates to management of areas of responsibility. It is intended that this will be actioned under the Emergency Preparedness Group.

    - Yet to progress Pandemic Planning as it relates to BCP.
    - Seeking to establish EP Committee for QH Building (Charlotte St) to coordinate all Units as appropriate for respective impacts and management planning.

Implication

Lack of direction, co-ordination and responsiveness in the event of a disaster or emergency.

Risk Assessment		
Likelihood	*Impact*	*Risk*
Possible	Moderate	High

Recommendation 2

It is recommended that the Executive Director Corporate Services ensures the Business Policy and Strategy Unit, in forming the Emergency Preparedness Group as planned:

(i) establishes a formal Terms of Reference / Charter to govern its purpose, authority and responsibility. This Terms of Reference / Charter should address, as a minimum:

- ***The Group's Purpose:*** **This may be, for example, to:**

    - **Develop an emergency response framework to comply with the Queensland Health's Emergency Preparedness and Continuity Management Policy; and**
    - **To optimise and coordinate all functions for which the Business Policy and Strategy Unit is responsible and relied upon as they relate to policy, planning, preparedness, response and recovery activities.**

- ***The Group's Scope and Function:*** **This may include, for example:**

    - **Development, maintenance and testing of strategies, plans, manuals and processes as they relate to Emergency Preparedness, Disaster Recovery and Business Continuity and the Unit;**
    - **Respond to emergencies (including directions of external agencies) as they relate to the Unit and other stakeholders reliant on the Unit in this regard;**

- **Minimise risk from emergencies;**
- **Ensure compliance with relevant policies, standards and legislation;**
- **Maintain adequate training of staff in cooperation with Queensland Health's training and education functions;**
- **Liaise with external agencies to ensure responses are optimised both to external and internal emergencies, including planning and coordination exercises; and**
- **Ensure resolution of issues referred to the Committee.**

- ***The Group's Composition:*** **This should be multidisciplinary and representative of all areas of Unit responsibility and other key internal stakeholders.**

- ***Meetings protocols:*** **For example, meetings may be held monthly for 6 – 12 months (during development phase), then quarterly. Meetings should be minuted with action plans established for implementation monitoring at each meeting.**

- ***Reporting and accountability structures*** **as they relate to reporting from the Committee.**

(ii) addresses all matters required for the development, maintenance and testing of strategies, plans/sub plans, manuals and processes as they relate to Emergency Preparedness, Disaster Recovery and Business Continuity and the Unit across the following minimum areas of responsibility:

- **Records Management;**
- **Fleet Management;**
- **Travel Management; and**
- **Property and Facilities Management.**

Appendix B sets out in detail matters to be addressed in comprehensive planning to meet the minimum requirements of Queensland Government and Queensland Health Frameworks, as well as matters noted in applicable recognised standards.

Management Response				
2 (i)	☐ Accept	☐ Reject	/ /	
2 (ii)	☐ Accept	☐ Reject	/ /	
Please select			Implementation Date	Action Officer
Comments:-				

3. CORPORATE SERVICES - BUSINESS POLICY AND STRATEGY UNIT - BUILDING AND INFRASTRUCTURE BUSINESS CONTINUITY PLAN

Background

The Corporate Office Services Unit Building Infrastructure Business Continuity Plan was established in August 2003 and has seen several revisions to February 2006. The purpose of the Plan is provided as being to detail the key people (positions) and the responses and actions needed to enable Corporate Office business units to recover from an emergency situation.

In summary, the Plan appropriately addresses the following key minimum requirements:

- Detailed roles and responsibilities of BCP Implementation Personnel/ Incident Recovery Team. These have been reviewed and are consistent with recognised standards for Emergency Management and Business Continuity Management.
- Process for identification and assessment of critical activities that need to continue to be undertaken immediately after a disaster in order for the business to continue operating. This includes establishing expected/maximum outage periods for prioritisation of recovery
- 'All hazards' in the identification of exposures that may threaten business continuity. These have been reviewed and are consistent with Queensland Government frameworks.

Issues

On high level review of this Plan, it is noted that:

Matter Noted	Gaps / Recommendations
The Business Continuity Plan is prepared as the third stage of a three stage planning process involving: • Security Planning (including Incident Preparedness); • Emergency Response Planning; and • Business Continuity/Disaster Recovery Planning.	Security Plans (including Incident Preparedness) and Emergency Response Plans to be reviewed / prepared in accordance with summary of Queensland Government requirements set out at Appendix B. All Plans should be cross referenced as appropriate to represent interdependencies and necessary escalations/de-escalations.

Matter Noted	Gaps / Recommendations
The Corporate Office Services Unit has the operational, tactical and strategic responsibility for all Corporate Office sites. These are identified in the Plan as including: **Leased Buildings:** • Queensland Health Building; • Forestry House; • Level 1-4, Citilink Business Centre; • 307 Queen Street; • 55 Little Edward Street; • Level 5, 160 Ann Street; and • 104 Melbourne Street. **Owned by Queensland Health:** • PA Hospital (TAFE Building); • 51 Herschel Street.	Plan to be updated to reflect application to revised locations. Each location's plan should be tailored for specific requirements and referenced to the Corporate Office Services Unit – Corporate Office – Building Infrastructure Business Continuity Plan for interdependences and necessary escalations/de-escalations.
The Plan Implementation Personnel / Incident Recovery Team membership by position.	Updated contact lists to be prepared and maintained to support membership, roles and responsibilities as set out in the Plan.

Implication

Lack of direction, co-ordination and responsiveness in the event of a disaster or emergency.

Risk Assessment		
Likelihood	Impact	Risk
Possible	Moderate	High

Recommendation 3

It is recommended that the Executive Director Corporate Services addresses Corporate Office Services Unit Building Infrastructure Business Continuity Plan gaps and recommendations as identified above.

Management Response			
☐ Accept	☐ Reject	/ /	
Please select		Implementation Date	Action Officer
Comments:-			

4. QUEENSLAND HEALTH SHARED SERVICE PROVIDER – MEDICAL SUPPLIES AVAILABILITY IN THE EVENT OF AN EMERGENCY

Background

In discussions with the Executive Director, Queensland Health Shared Service Provider, a number of matters were raised that are relevant in the context of emergency preparedness for Queensland Health. The medical supply issues outlined below are known to management and are highlighted in this report to provide focus within the scope of this audit.

Issues

Currently most of the medical inventory is extracted out of a number of decentralised stock locations and into the wards, leaving about half of the inventory managed by manual systems. It was noted that while this offers some challenges in efficiency and in estimating the value of inventory on hand for financial statement purposes, it offered an element of reduced risk in the event of disaster or emergency due to the availability of supply in a large number of locations.

There are plans to begin to rationalise warehousing (beginning approximately in July 2007), resulting in possibly two large more centrally located warehouses.

Implication

While the warehouse project has sound efficiency and effectiveness objectives, it will inevitably have an impact of placing a higher risk on the availability of medical supplies in the event of a disaster or emergency. The impact of this would depend on the timeliness of transporting medical supplies to areas where it is needed and how long the current inventory levels would last in the event of a disaster of emergency (which may vary depending on the scenario).

Risk Assessment

Likelihood	*Impact*	*Risk*
Unlikely	Moderate	Medium

Recommendation 4

It is recommended that the Executive Director, Queensland Health Shared Service Provider:

(i) acknowledges the importance of medical supplies in the event of disaster recovery or emergency; and

(ii) ensures that the project to rationalise the warehousing requirements for medical supplies considers the impact on disaster recovery and emergency preparedness in relation to the critical inventory requirements at decentralised locations.

Management Response			
4 (i) ☐ Accept	☐ Reject	/ /	
4 (ii) ☐ Accept	☐ Reject	/ /	
Please select		Implementation Date	Action Officer
Comments:-			

5. QUEENSLAND HEALTH SHARED SERVICE PROVIDER – FINANCE AND PAYROLL SYSTEMS

Background

In discussions with the Executive Director, Queensland Health Shared Service Provider, a number of matters were raised that are relevant in the context of emergency preparedness for Queensland Health. The Financial and Management Information System (FAMIS), that runs on SAP R3 (V4.6B), and the payroll (LATTICE) systems issues outlined below are known to management and are highlighted in this report to provide focus within the scope of this audit.

Issues

There are plans to replace LATTICE by July 2008. There are however concerns about this timeline, with discussions occurring at the Director-General and the Under Treasurer level.

LATTICE was down for nine days before Christmas 2006 and it was uncertain if the cause was identified. LATTICE is an old system. It is considered unlikely that LATTICE will extend support past 1/7/08 (after already extending it for several years). The standard process in the event of an emergency is to pay the last pay (with a focus on critical adjustments such as joiners and leavers and follow up on adjustments in the next pay run). It is uncertain if these procedures are up to date.

There has been schedule slippage by CorpTech (which manages the SAP financial system as part of an Operating Level Agreement with Queensland Health) in delivering the SAP finance needs of other agencies which has impacted on CorpTech's ability to deliver within QH requirements.

There is a State Wide Co-ordinator for Payroll and Supply, with a State Wide Co-ordinator for Finance planned for July. It is uncertain if the emergency preparedness plans are up to date.

Implication

It is understood that the criticality for emergency preparedness of the LATTICE and FAMIS systems is "in the red zone".

While these systems are support systems for Queensland Health operations, their unavailability in the event of a disaster or emergency will impact on the ability to respond in an efficient manner.

Risk Assessment		
Likelihood	*Impact*	*Risk*
Unlikely	Moderate	Medium

Recommendation 5

It is recommended that the Executive Director, Queensland Health Shared Service Provider:

(i) confirms that the procedures for undertaking an emergency pay run are up to date, ensuring that appropriate adjustments and controls are in place; and

(ii) ensures the State Wide Co-ordinators for Payroll, Supply and Finance (when appointed in July) review and update a strategy and plan for emergency preparedness for the respective systems.

Management Response				
5 (i)	☐ Accept	☐ Reject	/ /	
5 (ii)	☐ Accept	☐ Reject	/ /	
Please select			Implementation Date	Action Officer
Comments:-				

6. QUEENSLAND HEALTH SHARED SERVICE PROVIDER – BUSINESS CONTINUITY PLAN WITH CORPTECH

Background

Under the Queensland Government Shared Service Initiative, providers and their clients are required to develop partnering and Operating Level Agreements that formalise the service delivery arrangements. Such an agreement (Version 2) is in place between CorpTech and Queensland Health - SSP for the provision of services. Outlined below are extracts that relate to business continuity:

> ***A 3.4 Loss of Business Continuity***
> *The Provider is responsible for ensuring continuity in the delivery of services under the Agreement and, in consultation with the Client, must develop an IT Service Continuity Plan which will underpin and form a component of the Client's Business Continuity Plan. Details of the service elements associated with IT Service Continuity Management are described in Schedule 1, Section 0 S1.3.3 IT Service Continuity Management* ***(SVM.SA-3)***
>
> *Specific activities which will be invoked following loss of business continuity will be identified, tested, documented and agreed with the Client as part of the IT Service Continuity Plan.*
>
> *In the event of a severe disruption to business continuity, the Provider and Client will work together to minimise the impact of the disruption, to re-establish normal business operations and to determine and apportion costs having regard to Pricing and Costs as outlined in Section A4.1*

S1.3.3 IT Service Continuity Management (SVM.SA-3)	
CorpTech	**Queensland Health SSP**
• *Business Impact analysis and risk assessment.* • *Determine and agree risk reduction measures and recovery options to support those requirements in consultation with Queensland Health SSP and Agencies.* • *Analyse and Develop IT Service Continuity Deliverables.* • *Develop information technology service continuity management plans and procedures.*	• *Business Impact analysis and risk assessment for Queensland Health SSP.* • *Determine and agree risk reduction measures and recovery options to support those requirements in consultation with CorpTech and Agencies.* • *Define IT Service Continuity requirements in conjunction with CorpTech.* • *Acceptance of information technology service continuity management plan.*

S1.3.3 IT Service Continuity Management (SVM.SA-3)	
CorpTech	**Queensland Health SSP**
• *Implement information technology service continuity management plans and procedures.* • *Manage IT Service Continuity.* • *Testing, change control and assurance.*	• *Queensland Health SSP business continuity planning.* • *Education and review*

SVM.SA-3 IT Continuity Management	
PROVIDER RESPONSIBILITY	**CLIENT RESPONSIBILITY**
• *Provide suitable contingency strategies via maintaining the Human Resource Management Information Systems (HRMISU) Unit Business Continuity Plan.* • *Liaison with the client in relation to undertaking business impact assessments relating to contingency management planning.* • *Provision of advice in relation to the application of contingency plans.*	• *Adhere to client responsibilities as per the HRMISU Business Continuity Management Plan.* • *Advise the provider in relation to business impacts associated with contingency management.* • *Develop local continuity plans in line with the HRMISU Business Continuity Plan.*

Issues

While the focus of the Operating Level Agreement is on business continuity, there is uncertainty that there is sufficient clarity in the event of a disaster or emergency.

Implication

Lack of co-ordination and responsiveness in the event of a disaster or emergency.

Risk Assessment		
Likelihood	Impact	Risk
Unlikely	Moderate	Medium

Recommendation 6

It is recommended that the Executive Director, Queensland Health Shared Service Provider reviews the Operating Level Agreement with CorpTech to ensure that there is sufficient clarity relating to activities required in the event of a disaster or emergency.

Management Response			
☐ Accept	☐ Reject	/ /	
Please select		Implementation Date	Action Officer
Comments:-			

7. QUEENSLAND HEALTH IT SYSTEMS – QUEENSLAND GOVERNMENT INFORMATION STANDARD 18 – INFORMATION SECURITY - PRINCIPLE 9 - INFORMATION BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Background

This objective of this audit relates to identifying "key areas of leadership, responsibility and accountability for Emergency Preparedness, Disaster Management and Business Continuity Management, at Corporate Office and other key service delivery units". This section of the report relates to the extent of compliance with Principle 9 of Queensland Government Information Standard (QGIS) 18 Information Security relating to Business Continuity Management. There has recently been an enhancement (from Version V2 to Version V3) to the existing mandatory requirements of Queensland Government Information Standard (QGIS) 18 relating to Information security.

The authority to "apply the mandatory principles of the information standards" is derived from Section 56(2)(a) of the Financial Management Standard 1997.

The current V2 - Principle 9 - Business Continuity Management of QGIS 18 states:

> *"A managed process that includes documented plans, must be in place to enable the information environment to be restored or recovered in the event of a disaster or security failure. Plans must include Agency methods for reducing known risks to business continuity and identifying actions for the continuation of business activities in the event of unforeseen failures or disasters."*

The amended V3 - Principle 9 - Business Continuity and Disaster Recovery Management of QGIS 18 states:

> *"A managed process including documented plans must be in place to enable the information environment to be restored or recovered in the event of a disaster or major security failure. At a minimum, agencies must:*
>
> - *Establish processes to assess the risk and impact of the loss of information or systems on agency business in the event of a disaster or security failure;*
> - *Develop methods for reducing known risks to agency information or systems; and*
> - *Ensure business continuity and disaster recovery plans are maintained and tested to ensure systems and information are available and consistent with agency business and service level requirements."*

V3 provides these comments in relation to Disaster Recovery Plans:

> *"The Queensland Government Chief Information Office is currently developing Business Continuity and Disaster Recovery Frameworks. These frameworks were expected to be available for consultation in early 2007.*
>
> *In the interim, when developing business continuity management plans, agencies should consider adapting the Australian Standards HB:221:2004 Business Continuity Management available through the Australian Standards*

website. Further detailed information on both Business Continuity and Disaster Recovery Plans can be found in the Information Risk Management Best Practice Guide located on the Information Standards website."

These new requirements of V3 states that the "new requirements must be implemented based on the following dates:

- High-level risk assessment: Completion by June 2007; and
- High risk principles implementation: Completion by December 2007".

A Draft Business Case is being developed by the Information Security and Risk Unit that supports the Information Security Strategic Plan 2006-2011. It is understood that this plan is being significantly enhanced for the period 2007-2012 and now incorporates Information risk and continuity issues. The draft document is proactive and makes reference to "establish crises management capability for major incidents affecting Enterprise applications and infrastructure (by December 2007)" and "Establish an information continuity management system encompassing Enterprise information continuity risks and site information continuity/disaster recovery plans (by June 2008)".

In November 2005, the Information Security & Risk Unit (ISRU) undertook the responsibility for Information continuity and risk - in addition to existing Information Security role. In October 2006 additional resources were approved in relation to these new responsibilities. This unit is presently reviewing how to leverage existing, relatively mature, Information Security governance arrangements to fast-track the emerging (and less mature) Information continuity and risk disciplines, which are a key focus area in the new QGIS 18 V3.

In October 2006 a report ("The Progress Report on the Overall Compliance of Implementation Status of QGIS 18 in Queensland Health") was sighted on the status of implementing the QGIS 18 (which was subsequently confirmed as taking into consideration the expected changes in QGIS 18 V3), the Queensland Health Information Security and Risk Unit identified three "Very High" residual risks associated with QGIS 18 Principle 9 (as outlined above). The maturity rating for compliance with Principle 9 was rated as 0% for "Maturity Level 2 – Repeatable or better". Each of the three topics identified for Principle 9 were rated with a Current Residual Risk rating of "Very High" (in a scale that included rating options of Low Risks, Medium Risks, High Risks Very High Risks, or Extreme Risks).

A recently developed draft Crisis Management Plan Maintenance Process document (Version 1.1, dated 12 April 2007) was sighted and while still in draft, it is evidence of recent positive developments and risk mitigation actions in the context of the scope of this audit relating to Emergency Preparedness, Disaster Management and Business Continuity Management. We were further advised that most sites have a level of local Information Continuity and/or Disaster Recovery plans in place already, but there are opportunities to improve their quality, consistency and to enhance alignment to wider business continuity plans.

Issues

While there is significant proactive effort in the context of crises management and Information Security within Queensland Health, there was recognition that there is

significant effort required to reduce the three topics relating to Principle 9 - Business Continuity Management of QGIS 18 from a "Very High" current residual risk and to ensure business continuity and disaster recovery plans are maintained and tested (as required by the current QGIS 18).

Key actions that need to be performed to minimise the risks in the context of this audit include the adoption of the Crisis Management Plan Maintenance Process, the Information Security Strategic Plan 2007 – 2012, and the testing of information continuity/disaster recovery plans.

It is important that there is an appropriate level of involvement of the Information Security & Risk Unit (ISRU) in activities undertaken by various organisational units across Queensland Health and that appropriate leverage is obtained from the already mature information security governance environment and framework.

Implication

Queensland Health needs to acquit its accountabilities through approval of key documents (as mentioned above under "Issues").

Missed opportunities through not aligning information security, risk and continuity across Queensland Health. Projects that target operational aspects of information management e.g. IT architecture, telecommunications, etc, may not optimise security, risk and governance outcomes.

Risk Assessment		
Likelihood	Impact	Risk
Possible	Moderate	High

Recommendation 7

It is recommended that the Chief Information Officer:

i) **reports on the timetable for adoption or completion of the Crisis Management Plan Maintenance Process, the Information Security Strategic Plan 2007 – 2012, and the adoption and testing of disaster recovery plans; and**

ii) **considers the benefits of a consolidated Information Security, Risk and Continuity Program/portfolio - aligned to ISRU's governance responsibilities.**

Management Response				
8 (i)	☐ Accept	☐ Reject	/ /	
8 (ii)	☐ Accept	☐ Reject	/ /	

Please select	Implementation Date	Action Officer
Comments:-		

8. QUEENSLAND HEALTH IT SYSTEMS – ENTERPRISE IT APPLICATIONS BACKUP AND DISASTER RECOVERY

Background

Forty-eight Enterprise IT systems have been identified within Queensland Health. While the audit of the back up process was not able to be undertaken (given the scope of this audit), it was established that there are two Enterprise Data Centres for production and off-site facility.

It is understood that the off-site facility is on a different electricity grid (which is important for business continuity in the event of a disaster or emergency).

The off-site facility is less than fifteen kilometres from the main production site. A project has already been approved by the Queensland Government ICT Governance Peer Review Panel with funding available to relocate the ICT Infrastructure to a distance greater than fifteen kilometres from the main production site. However, this project will commence in June 2007 for completion by October 2007.

Audit was advised that "No document has been identified or is currently available that includes an overview of the disaster recover status of these enterprise applications from an IT infrastructure perspective. However a disaster recovery plan encompassing all enterprise infrastructure, which supports enterprise applications is currently being developed."

The back up generators used as part of the main production facility are managed by RBWH Engineering Services with audit advised that they are "generally tested (under load) quarterly". Audit was advised that the off site back up generator is "understood to be tested month with no load, and quarterly with load". The InfoOperations Information Division does not obtain acquaintance that the key testing of back up generators is undertaken to the level required in the event of a disaster or emergency. Audit has not verified that procedures or service level agreements are in place.

The enterprise AUSLAB system is managed by Clinical & Statewide Services. Internal audit was advised that:

- Backup tapes are sent to offsite storage (usually available within ninety minutes) with both the main server and the backup server co-located.
- The hardware replacement cycle is due Quarter 3 2008, but this may be brought forward with potential changes in QH data centre operations.
- The new system, yet to be designed, is envisaged to have two discreet servers located at two separate QH data centres.

It is understood that a Business Continuity Plan exists for AUSLAB but this was neither sighted nor reviewed by Audit.

Issues

It is considered that with the distance between the off site facility and the main production site being less than fifteen kilometres, Queensland Health business continuity risks increase significantly. While this assessment is not based on a "standard" that specifies this distance or requires Queensland Health to adhere to, it is an indicator of high risk.

As guidance, we have provided extracts (in footnotes 1, 2 and 3) from other industry standards and reports undertaken of like organisations.

These include the *Business Continuity Management GOOD PRACTICE GUIDELINES 2007.* [1], the *Australian National Audit Office Report No.9 2003-04 Business Continuity Management and Emergency Management in Centrelink - Loss of both data centres and off-site backup storage* [2] and the *Prudential Standard APS 232 Business Continuity Management: Guidance Note AGN 232.1 Risk Assessment and Business Continuity Management* [3].

While a disaster recovery plan for the forty-eight Queensland Health enterprise systems is currently being developed by Queensland Health, it has not been completed and tested.

The AUSLAB system, managed by Clinical & Statewide Services is exposed in the timeliness of restoration of services in the event of the main computer facility encountering a disaster, as both the main server and the backup server are co-located.

Implication

The proximity risk associated with the off-site facility being less than fifteen kilometres (distance used as guidance only) from the main production site will remain until the completion of the alternate site.

The absence of a Disaster Recovery Plan for Enterprise systems exposes Queensland Health to an inability to adequately respond to disasters or emergencies in the total devastation of both the main production data centre and the off-site backup storage facility.

---

[1] *Business Continuity Management GOOD PRACTICE GUIDELINES 2007 Version 2007.2 15th March 2007 © The Business Continuity Institute 2007:*

> Whilst it is self-evident that greater geographical separation decreases the likelihood of two sites being affected by the same incident, there is no 'minimum' or 'correct' distance for separation as the ability of worldwide infections and computer viruses to cause concurrent incidents demonstrates. However a few hundred metres is likely to provide little protection even in localised incidents because of the way that emergency services use cordons and the likely disruption to transport.

[2] *Australian National Audit Office Report No.9 2003-04 Business Continuity Management and Emergency Management in Centrelink - Loss of both data centres and off-site backup storage*

> 5.58 The 2003 ACT firestorm highlighted the possibility of total devastation of both data centres and its off-site backup storage facility in Canberra as real risks to be considered by Centrelink.

[3] *Prudential Standard APS 232 Business Continuity Management: Guidance Note AGN 232.1 Risk Assessment and Business Continuity Management*

> 17. Where an ADI has its primary operations in the Central Business District (CBD) of a major capital city, APRA would normally expect the alternate site to be located outside that CBD in order to minimise the risk of both sites being impacted by a wide area disruption. Where the two sites are located in the same CBD, the ADI will need to demonstrate to APRA that it has adequate arrangements in place to manage the potential risk of both sites being impacted simultaneously.

It is important that the InfoOperations Information Division obtain clear understanding that agreed testing of back up generators at the main production site and off site facility is undertaken to levels required to minimise the risks relating to disaster or emergency.

It is important that the impact of the loss of the AUSLAB system is taken into consideration in assessing the ability to respond in a disaster.

Risk Assessment		
Likelihood	Impact	Risk
Possible	Moderate	High

Recommendation 8

It is recommended that the Chief Information Officer ensures a further review is performed of the disaster preparedness of all key applications, including confirmation that procedures or service level agreements are in place to ensure clarity and sufficiency of testing of off site facilities and back up generators.

Management Response			
☐ Accept	☐ Reject	/ /	
Please select		Implementation Date	Action Officer
Comments:-			

9. AREA HEALTH SERVICES AND CLINICAL AND STATEWIDE SERVICES

Background

Southern AHS	Central AHS	Northern AHS
Gold Coast HSD	Central Queensland HSD	Cairns and Hinterland HSD
Mater Hospital and HSD	Central West HSD	Cape York HSD
Princess Alexandra Hospital HSD	Fraser Coast HSD	Mackay HSD
Southside HSD	Northside HSD	Mt Isa HSD
South West HSD	Royal Brisbane and Women's Hospital and HSD	Torres Strait HSD
Toowoomba and Darling Downs HSD	Royal Children's Hospital and HSD	Townsville HSD
West Moreton South Burnett HSD	Sunshine Coast and Cooloola HSD	
	Wide Bay HSD	

Emergency Preparedness, Disaster Management and Business Continuity Planning – Scenario Specific – Pandemic Influenza Planning

Audit was advised across Area Health Services and Clinical and Statewide Services that Pandemic Plans have progressed to at least draft stage (in some cases finalised) and have been scenario tested. Each District/Service has a plan and District/Service plans are being integrated for flow effectiveness and efficiency within Area Health Services/Clinical and Statewide Services.

General Managers have performed reviews of plans and consider these appropriate and prepared in accordance with Queensland Health and National requirements.

Area Health Services/Clinical and Statewide Services participated in National Testing Exercise – "Cumstum" and plans were revised for matters arising on practical application.

Committees have been established to govern the preparation and maintenance of Pandemic Plans, including the oversight of testing and incorporation of results into Plan revisions.

Issues

Area Health Services/Clinical and Statewide Services noted that, further to Pandemic Planning, progress on Emergency Preparedness, Disaster Recovery and Business Continuity Plan on the basis of an "all hazards approach" may be limited. No formal structures had been established at Area Health Service/Clinical and Statewide Services Levels for monitoring and reporting Health Service District/Unit Planning in this regard.

It was considered and agreed that the frameworks, procedures, protocols and practical tools developed and applied for Pandemic Planning exercises may form a strong basis for development of Emergency Preparedness, Disaster Recovery and Business Continuity Plans for the management of other, all threats scenario, planning.

Implication

While Districts and Units have achieved varying degrees of progress in the development and ongoing maintenance of "all hazards" Emergency Preparedness, Disaster Management and Business Continuity Planning, there is uncertainty that there are adequate foundations in place to manage incidents in a coordinated, efficient and effective manner.

Risk Assessment

Likelihood	Impact	Risk
Possible	Moderate	High

Recommendation 9

It is recommended that the respective Area Health Service General Managers/ Executive Director Clinical and Statewide Services implement the following:

(i) **To gauge the level of preparedness and adequacy of plans prepared by District Health Services/Clinical and Statewide Services in respect of Emergency Preparedness, Disaster Recovery and Business Continuity, a comprehensive self assessment (for example using the pro forma attached at Appendix B as a guide) be performed by Managers for facilities for which they are responsible and accountable and reported to respective General Managers/Executive Director;**

(ii) **Where significant progress gaps are noted, detailed actions plans should be reported to General Managers/Executive Director for monitoring and follow up accountability; and**

(iii) A similar self assessment should be performed and reported by Managers to General Managers/Executive Director on an annual basis to ensure plans are reviewed and maintained on a frequent and timely basis in accordance with Queensland Health requirements.

Management Response				
9 (i)	☐ Accept	☐ Reject	/ /	
9 (ii)	☐ Accept	☐ Reject	/ /	
9 (iii)	☐ Accept	☐ Reject	/ /	
Please select			Implementation Date	Action Officer
Comments:-				

10. OTHER MATTERS

During discussions with Area Health Service representatives, a number of matters were raised which, although outside the scope of this review, are brought to the attention of the Chief Health Officer for further consideration.

In discussing experiences learned from the 2006 Cumstum, and 2007 Emergo Train test exercises, the following were considered as needing to be addressed in order for effective roles, responsibilities and accountabilities to be carried out at Area Health Service and District Health Service levels:

- Staff are not trained in managing the specific skills requirements, roles and responsibilities required in managing disaster scenarios (specifically, training for trauma/incident specific requirements, and maintenance of skill set profiles for future reference);

- Queensland Health's direction on relationships with other agencies and District Disaster Managements Groups is not always clear to Area Health Services for authority, communication and chain of command in the event of a disaster incident.

  For example, Queensland Police and Queensland Ambulance Service usually act as lead agencies, when in some cases (such as a Pandemic incident), Queensland Health may be better placed as the lead agency. Direction from Corporate Office's on chain of command is not considered clear in current communications and chains of command.

- Other incident examples were provided as follows:

  Indonesian Plane Crash and Cyclone Larry: not clear on chain of command. Instructions from Corporate Office were going direct to hospital staff and not through Management, who are ultimately responsible and accountable for service delivery during disaster.

- Disaster management continues to be seen as the function of the Chief Health Officer. Area Health Services do not consider their District facility staff always appropriately trained and resourced to take responsibility for disaster management.

  In this regard, Area Health Services are seeking:

  - Frameworks, guidelines, standards and expectations regarding roles and responsibilities of Area Health Services in Disaster Management.

  - More centralised training and development from Corporate Office's Emergency Management Unit (from a management and clinical specific perspective).

  - Clear coordination and connection between Area Health Service General Managers and the Corporate Office Disaster Group (chaired by the Chief

APPENDIX A

TERMS OF REFERENCE

AUDIT TITLE:

Operational Audit of Emergency Preparedness and Continuity Management Planning

AUDIT OBJECTIVE:

The objective of the audit is to assess the adequacy of Queensland Health's Corporate Office ability to respond and support a Health Service District in the event of an emergency occurring.

The audit will be required to –

i) Assess the adequacy of current policies and guidelines relevant to the Emergency Preparedness and Continuity Management Plan;
ii) Identify those areas of Corporate Office which are expected to play a role in supporting and coordinating a local emergency;
iii) Assess the capacity of each area to deliver the support required;
iv) Identify those areas of Corporate Office which are expected to have continuity management plans in place to sustain critical Corporate Office functions should the Queensland Health Building facility be compromised itself; and
v) Assess the capacity of each of the identified business functions in (iv) above, to give effect to their respective continuity management plans.

AUDIT SCOPE:

The audit will include all areas of Corporate Office including the Area Health Services which should legitimately contribute to an emergency situation or be compromised by the Queensland Health Building facility being compromised consequent to an emergency incident.

It should be noted that as a result of the recent Queensland Health restructure, Area Health Services may still be developing their plans in this area. In that case, this audit should acknowledge their current status and provide an opinion on the proposed direction and timeframes.

DESIRED OUTCOMES:

Provide assurance to the Executive Management Team of Queensland Health, that Corporate Office is adequately prepared to provide the leadership and support required to assist any Health Service District and/or other services in the event of an emergency occurring.

BACKGROUND INFORMATION:

As part of the Whole-of-Government strategy for Government Agency Preparedness, Queensland Health has developed policies and guidelines to ensure it has the capacity to respond to an emergency occurring.

Recently, the Audit and Operational Review Unit, Assurance and Risk Advisory Services conducted an operational audit within a number of Health Service Districts to assess their maturity in relation to their development of Emergency Preparedness and Continuity Management Plans.

While recommendations have been provided to further develop the local requirements there is a complementary role required at the corporate level to coordinate activities in a responsive and timely manner.

AUDIT PLAN:

It is intended that the audit process be undertaken utilising the following methodology -

Phase	Process
1	Develop an audit program consistent with legislative and policy requirements to address the audit objectives.
2	Interview key stakeholders.
3	Evaluate audit findings.
4	Debrief client on findings and recommendations.
5	Prepare audit report.

COMMUNICATION PLAN:

Regular updates will be provided to the Manager, Operational Audits and/or the Audit Sponsor (as determined) at key milestones during the course of the audit. All communication protocols will be clarified prior to the audit commencing.

RESOURCING:

The audit will be undertaken by Ms Marita Luxton of BDO Kendalls on behalf of the Audit and Operational Review Unit.

REPORTING ARRANGEMENTS:

A written report will be provided to the Manager, Operational Audits as soon as possible following the conclusion of the audit activity but not later than four (4) weeks. The report format and standard will be as determined by the Manager, Operational Audits.

TIMEFRAME:

The audit will commence on 4 April 2007 and is expected to be completed by 25 May 2007.

REFERENCE MATERIAL:

Queensland Health Policy 28028: *Emergency Preparedness and Continuity Management Policy – June 2005*

Australian Standard: *Planning for Emergencies – Health Care Facilities AS 4083:1997*

Australian and New Zealand Standard: *Business Continuity Management HB 221:2004*

Queensland Health Operational Audit Reports: *Emergency Preparedness and Continuity Management 2006*

APPENDIX B

EMERGENCY PREPAREDNESS, DISASTER MANAGEMENT AND BUSINESS CONTINUITY

PLAN DEVELOPMENT / SELF ASSESSMENT CHECKLIST

The following is provided as a guide to the development of Emergency Preparedness Plans, or alternatively, as a self assessment tool for detailed review of the adequacy and effectiveness of developed plans.

It draws on Queensland Health's Emergency Preparedness and Continuity Management Policy, Guidelines and Program ("the Framework") including, et al:

- Queensland Health Disaster Plan 2002;
- Queensland Health Policy Statement 28028 – Emergency Preparedness and Continuity Management;
- Queensland Health Integrated Risk Management Framework (QHEPS 15232);
- Queensland Health Information Security Policy (QHEPS 3485); and
- Queensland Health Information Security Standard 9 – Business Continuity Management (QHEPS 23724).

This Framework is part of, and in support of, the Queensland Government's project for the safety and security of Queensland in:

- The preparation for, prevention of, response to and recovery from terrorism related incidents, as set out in the Queensland Government Counter-Terrorism Strategy 2005-2007, and consistent with the National Counter-Terrorism Framework;
- The protection and resilience of infrastructure; and
- The protection of critical infrastructure from terrorism.

The Framework is also based on, and supports compliance with and implementation of, relevant Legislation, Policies, Standards and key documents including:

- Disaster Management Act 2003;
- State Counter Disaster Plan 2001;
- Queensland Government Counter Terrorism Strategy 2005-2007
- Queensland Government Infrastructure Protection and Resilience Framework;
- Queensland Government Plan for the Protection of Critical Infrastructure from Terrorism
- Standards Australia and New Zealand - AS/NZS 4360 – 2004 Risk Management
- Standards Australia and New Zealand- HB 221:2004 Business Continuity Management;
- Australian Standard – AS 4083-1997 Planning for Emergencies – Health Care Facilities; and
- Queensland Government Information Standard 18 – Information Security.
- HB231:2000 Information Security Risk Management Guidelines,

Note: this guide / self assessment tool is an outline summary of key matters to be addressed in preparing, testing and maintaining emergency, disaster recovery and business continuity plans. It is not, and should not be relied upon as being, a comprehensive checklist of all matters to be considered and addressed in preparing, testing and maintaining emergency, disaster recovery and business continuity plans. It does not, and is note intended to, replace the need for full review and understanding of source authoritative documents.

	YES	PART	NO
Critical Infrastructure			
Has the facility been identified and classified (and advised of identification and classification) as a critical infrastructure? If so, what is its rating: • Vital; • Major; • Significant; and • Limited.			
Is the facility fully and solely owned and operated by Queensland Health? If not, provide details of occupancy arrangements, including any arrangements regarding responsibility for Emergency Preparedness, Disaster Recovery and Business Continuity Planning: .... Identify any other tenants within premises owned and/or operated by Queensland Health: • ..... • ..... •			
Risk Identification, Assessment and Management			
Has Queensland Health Integrated Risk Management Policy and Framework for Clinical and Corporate Services been applied in identifying and assessing risk (where this framework is based on AS/NZS 4360 Risk Management).			
All Hazards Approach to Risk Assessment			
Has an "all hazards approach" been taken to the identification and assessment of risk?			
Has the risk identification and assessment approach considered, for example: • Identification of essential or key elements within the asset (critical nodes); • Consideration of whether the infrastructure is a producer of products that could be used by, or are of interest to a terrorist; • Identification of possible threats, including threat of vulnerability to terrorism; • Determination of risks that require/do not require treatment; • Means by which an attack could be mounted; • Vulnerability assessment covering personnel and the site; • Levels of consequential impact; • Off-site interdependencies.			

	YES	PART	NO
Have arrangements, within the facility, been established with Qld Police Service and other government agencies as appropriate, for the provision of information and guidance in relation to the conduct of risk assessments, including the provision of relevant information, in accordance with Queensland arrangements? Briefly describe or provide Plan reference:			
What other "tools' have been utilised in identifying and assessing the level of risk for infrastructure, for example: • National Counter Terrorism Alerts; • Individual asset and industry sector threat assessments, risk context statements and security intelligence; • Others: ..... • ..... •			
Have processes, forums and reporting structures been established for ongoing monitoring and review of risk assessments, in particular when: • There has been a change in the threat or strategic context; • The nature of the asset has changed; • A major risk treatment has been applied (ie an event has occurred and been treated). Briefly describe or provide Plan reference:			
How frequently is a full review of the risk assessment(s) (including counter-terrorism context) performed? • ..... If the facility has been identified and classified (and advised of identification and classification) as a critical infrastructure rated: • 'Vital' or 'Major': has full review been conducted annually unless otherwise regulated; • 'Significant' or 'Limited': has full review been conducted every 2 years unless otherwise regulated. When was the last full review performed? ..... When is the next scheduled full review?			

	YES	PART	NO
Security Plans			
Have security risk assessments and plans been developed, including in the context of counter terrorism?			
Do Security Plans address matters such as: • Location and nature of the facility; • Key systems and processes; • Personnel and other resources; • Existing counter-terrorism alert levels; • Risk mitigation strategies; • Deterrence, detection, media management and response arrangements.			
Do security plans address: ***Personnel Security*** - considering for example: • Access of personnel to facilities; • Personal identification requirements; • Visitor/contractor escort requirements; • Increased access restriction/identification requirements under increased National Alert Level			
Vehicle Access - considering for example: • Controlling or limited access to underground or proximate car parts, loading docks, and vehicle access points; • Increased control requirements under increased National Alert Level.			
Incident Reporting - addressing communication and reporting protocols and procedures for reporting suspicious activity to nominated personnel and/or the Queensland Police Service (as necessary).			
Mail/Parcel Receipting Arrangements - addressing procedures for accepting and opening mail and parcels (including courier deliveries), and considering links to relevant procedures included in on-site emergency response plans in relation to mail (eg 'white powder' incidents/letter bombs).			
Utilities/Services - addressing security arrangements for utility services and supplies to hospital facilities, for example, potential impacts on supply of electricity, water, telecommunications and the security of air conditioning systems (including accessibility to inlet ducts etc).			

	YES	PART	NO
Staff Awareness and Training - increasing staff vigilance for effective and cost effective way to improve security. Security plans to address strategies to ensure staff awareness of counter-terrorism issues and department procedures (eg include security briefings in staff induction and awareness programs).			
Roles and Responsibilities - nomination of key security personnel within areas and within each key asset, allocation of clear roles and responsibilities, contact details, command and control structures?			
Is the facility in a multi-tenanted building? If so, have general security plans been developed in consultation with the building owner and other tenants?			
Do Security Plans take account of arrangements and procedures for each national counter-terrorism alert level?			
Has/does the facility consult with relevant government agencies and the Queensland Policy Service to ensure that their security plans and arrangements are able to respond to changes in the threat level and/or National Counter-Terrorism Alert Level?			
Have standard operating procedures been formally established and communicated to staff for actions and responsibilities in the event of a security related incident? When were these established?			
Are standard operating procedures regularly reviewed and tested to ensure they provide comprehensive guidelines for staff? How often? ..... When was the last review and testing performed?..... When is the next review and testing scheduled to be performed?..... Are details and results of each testing documented for future planned testing and review?			

	YES	PART	NO
On – Site Emergency Response Plans			
Are separate plans maintained/considered necessary for different parts of infrastructure/different emergencies? Identify and respond for each emergency type: • ***Internal Emergency*** (eg failure or threat to essential services or hazardous substance incident; illegal occupancy); • ***Personal Threat*** (eg armed or unarmed person/s threatening injury to others/s or themselves); • ***Fire/Smoke Emergency;*** • ***Bomb/Arson Threat;*** • ***Evacuation;*** • ***External Emergency*** (eg natural disasters). Identify and respond for terrorist threats: • ***Arson*** (eg aimed at diverting attention from more sinister attack); • ***Bombs or explosive devices*** (eg parcel/package – post or courier, human – backpack); • ***Ground vehicle, waterborne vehicle or aircraft;*** • ***Cyber*** (eg hacking info information systems); • ***Firearm or weapons;*** • ***Hijack*** (eg transport vehicles or vessels carrying hazardous materials); • ***Kidnapping*** (eg kidnapping of key personnel / taking hostages – staff and/or patients); • ***Scare tactics*** (hoax phone calls, suspicious mail / packages, threatening graffiti etc to undermine the confidence of security arrangements); Identify and respond for each part of infrastructure type: • ..... • ..... • ..... • ..... • ..... • ..... •			

	YES	PART	NO
Do plans address, for example: • Hazard identification; • Personnel safety; • Site safety; • Emergency notification procedures; • On-site emergency equipment; • Media management; • Roles, responsibilities and contacts of key staff.			
Do plans outline reporting and command and control structures?			
Do on-site emergency response plans include additional mitigating arrangements for terrorism threats (with inputs from other relevant agencies – as noted above)?			
Are internal on-site emergency response plans reviewed/tested at least annually? Frequency of testing ..... Date of last testing ..... Scheduled timing of next testing ..... Are details and results of each testing documented for future planned testing and review?			
Are evacuation exercises conducted at least annually? Frequency of evacuation exercise ..... Date of last evacuation exercise..... Scheduled timing of evacuation exercise ..... Are details and results of each evacuation exercise documented for future planned testing and review?			
Have plans been linked to local arrangements to address the threats (including terrorism) within an all-hazards approach?			

	YES	PART	NO
External Emergency Response Plans			
Have External Emergency Response arrangements and plans been developed to outline response strategies for any potential emergencies, including potential terrorist incidents or risks, as identified in the risk assessment process?			
Do plans address the following specific emergencies: • ***External Emergency*** (eg Major Incident/State Disaster Plans); • ***Medical Emergency***			
Do plans consider arrangements for: • ***State Disaster arrangements*** (Queensland Health Disaster Plans) • ***Major Incident*** arrangements • ***Public Health*** Incidents • ***Infection or communicable disease*** incidents • ***Biological*** incidents • ***Radiological*** incidents • ***Chemical*** incidents • ***Medical evacuation and transfer*** arrangements			
Are plans based on consideration of emergency scenarios related to the following terrorist threats: • ***Biological and radiological*** - eg releasing radiological or biological material (eg anthrax) • ***Ground vehicle, waterborne vehicle or aircraft*** • ***Chemical*** - eg release of chemical materials (eg cyanide) • ***Hijack*** - eg transport vehicles or vessels carrying hazardous materials			
Do plans outline roles, responsibilities, contact details of key staff, command and control structures?			
Are external emergency response plans reviewed/tested at least annually? Frequency of testing ..... Date of last testing ..... Scheduled timing of next testing ..... Are details and results of each testing documented for future planned testing and review?			

	YES	PART	NO
Business Continuity Planning			
Have Business Continuity Plans been developed within the context of the already established high-level arrangements outlined in the State Counter Disaster Plan?			
Have Business Continuity Plans Pandemic threats been prepared?			
Has planning considered: • Identification and prioritisation of ***key business processes/deliverables*** (including the processes associated with producing/delivering these key deliverables, and the resources needed to support the key processes); • ***Hazard identification***; • Establishment of ***maximum acceptable outage periods*** for key business processes/deliverables and resources • ***Identification of business impacts*** of key process/deliverable interruption, including the impact if outages are exceeded; • ***Continuity and resumption*** of operations and/or supply (including how and where resources and infrastructure essential to the running of the key processes, will be sourced); and • Identification of ***recovery procedures*** for key business processes/deliverables; • Identification of ***recovery arrangements for staff***, if required (eg staff counselling); • Establishment of ***key staff roles/responsibilities, contact details, command and control structures***; • Notification and management of stakeholders, including community and media liaison strategies?			
Are plans reviewed/tested at least annually? When was the last review/testing? ..... When is the next scheduled review/testing? ..... What is the format of review/testing (ie 'desktop' discussion exercises, or through simulated scenarios (such as emergency evacuation testing).? .... Are details and results of each testing documented for future planned testing and review?			

	YES	PART	NO
Communication Protocols			
Are all Plans formally documented and distributed in authorised version control format to appropriate staff and locations?			
Have protocols and procedures for communication of roles, responsibilities and contact details of key staff been established and implemented for activation and safe deactivation of plans.			
Have appropriate communication strategies, protocols and procedures been established to ensure effective communication and engagement arrangements within the facility and between the facility and other forums and arrangements that support the facility (eg Queensland Health, Queensland Police Service, Dept Emergency Services, Critical Infrastructure Protection Coordination Group, Media Liaison)? Briefly outline or provide Plan reference:			
Do communication protocols incorporate procedures for informing organisational personnel and relevant authorities such as emergency responders? Other key stakeholders eg patients, shared-occupancy dwellers, contractors, suppliers, media?			
Have adequate protocols and procedures been established to report any incidents or suspicious activity to the Queensland Police Service?			
Have adequate protocols and procedures been established to identify and maintain points of contact within the hospital for urgent communication of terrorist related threat information and normal communication of security related information?			
Have adequate protocols and procedures been established to advise the Queensland Police Service, Counter Terrorism Coordination Unit, and the Department of Premier and Cabinet - Security Planning and Coordination of changes in emergency contact information to enable prompt communication of threat information to the correct recipient?			
Have communication protocols been established to receive advice regarding changes in alerts, whole-of-government, inter-agency status and other intelligence is effectively communicated for consideration in planning and action?			

	YES	PART	NO
Implementation			
Have Emergency Preparedness Plans been implemented through the following: • Provision of information and guidance material; • Conduct of workshops/forums; • Establishment of governance structures (eg Emergency Planning and Mgt Committees); • Conduct of reviews and audits; • Other			
Review and Evaluation			
Have timelines been established for review, evaluation, testing and revising Emergency Preparedness Plans? When were Plans established ..... What is the review/testing frequency ..... What was the last date of review/testing			
Has/does the facility participate in any exercises to test plans conducted by government authorities? When was participation ..... What is participation frequency ..... When is the next scheduled participation.....			
If the facility has been identified and classified (and advised of identification and classification) as a critical infrastructure, has/does the hospital participate in any state level CIP exercises, in accordance with the following frequency requirements: • If rated 'Vital' or 'Major' - at least once annually; • If rated 'Significant' or 'Limited' - at least once every two years.			

	YES	PART	NO
Assurances			
Where the facility has been identified and classified as a critical infrastructure, has the head of the facility (eg Hospital CEO) provided a signed annual statement to the Department of Premier and Cabinet - Security Planning and Coordination, addressing the validation and audit requirements set out in the National Guidelines? That is: • Date of the most recent risk assessment, which includes the counter-terrorism context; • Date of current plans (security, on-site emergency response and business continuity); • Current plans signed off by (name and position); • Date of last test and/or exercise of plans; • Date of last audit or plans (internal or external); • Audit performed by (name, company and position); and • Audit results (including recommended actions and those implemented).			
Risk Management Governance and Management Structure			
Have appropriate governance, accountability, reporting and escalation structures been established to manage risks within area of accountability and delegation?			
Have management groups/committees established adequate and appropriate Terms of Reference of Risk Management function?			
Does the facility have a role in Local Disaster Management Groups? Ie is it integrated into existing local disaster management arrangements through the application of the Local Government Counter-Terrorism Risk Management Guidelines?			
Does the facility have a role in Local Security Committees? (Have Committees been established locally?)			

	YES	PART	NO
Information Security and Disaster Recovery			
Has QGIA 18 - confidentiality, integrity and availability of information assets been complied with as it related to information security?			
Information Disaster Recovery			
Have information disaster recovery plans been established to include: • Continuity treatments for key information technology processes; • Recovery procedures for key information technology processes; • Key staff roles, responsibilities and contact details.			
Do these plans appropriately consider: • Data recovery arrangements; • Application recovery arrangements; • Communication alternatives; • Alternative hardware availability; • Alternative site arrangements.			
Are Information Security and Disaster Recovery Plans tested at least annually? What is the frequency and nature of testing:			

APPENDIX C

TERMS OF REFERENCE

AUDIT TITLE:

Operational Audit of Emergency Preparedness and Continuity Management Planning

AUDIT OBJECTIVE:

The objective of the audit is to assess the adequacy of Queensland Health's Corporate Office ability to respond and support a Health Service District in the event of an emergency occurring.

The audit will be required to –

vi) Assess the adequacy of current policies and guidelines relevant to the Emergency Preparedness and Continuity Management Plan;
vii) Identify those areas of Corporate Office which are expected to play a role in supporting and coordinating a local emergency;
viii) Assess the capacity of each area to deliver the support required;
ix) Identify those areas of Corporate Office which are expected to have continuity management plans in place to sustain critical Corporate Office functions should the Queensland Health Building facility be compromised itself; and
x) Assess the capacity of each of the identified business functions in (iv) above, to give effect to their respective continuity management plans.

AUDIT SCOPE:

The audit will include all areas of Corporate Office including the Area Health Services which should legitimately contribute to an emergency situation or be compromised by the Queensland Health Building facility being compromised consequent to an emergency incident.

It should be noted that as a result of the recent Queensland Health restructure, Area Health Services may still be developing their plans in this area. In that case, this audit should acknowledge their current status and provide an opinion on the proposed direction and timeframes.

DESIRED OUTCOMES:

Provide assurance to the Executive Management Team of Queensland Health, that Corporate Office is adequately prepared to provide the leadership and support required to assist any Health Service District and/or other services in the event of an emergency occurring.

APPENDIX C

MANAGEMENT ACTION PLAN SUMMARY

NO.	RECOMMENDATION	AGREE OR DISAGREE	OFFICER RESPONSIBLE FOR IMPLEMENTATION	REQUIRED DATE FOR IMPLEMENTATION	COMMENTS
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Health Office). In this respect, Area Health Services are not always clear on:

- Group's role in management of disaster emergencies, and how this interfaces with Area Health Services responsibilities and accountabilities; and
- Group's role in monitoring whole of State and reporting objectives to the Group and its Area Health Service representatives.

Risk Assessment		
Likelihood	*Impact*	*Risk*
Likely	Moderate	Very High

Recommendation 10

It is recommended that the Chief Health Officer ensures –

i) **roles, responsibilities and accountabilities are clear at all levels of management including Area Health Services;**

ii) **command and coordination networks between Area Health Services and Corporate Office are clear;**

iii) **relationships with external agencies are clear at all levels; and**

iv) **training and development responsibilities are clear between the Area Health Services and the Emergency Management Unit.**

Management Response				
10 (i)	☐ Accept	☐ Reject	/ /	
10 (ii)	☐ Accept	☐ Reject	/ /	
10 (iii)	☐ Accept	☐ Reject	/ /	
10 (iv)	☐ Accept	☐ Reject	/ /	
Please select			Implementation Date	Action Officer

Comments:-

APPENDIX A

TERMS OF REFERENCE

AUDIT TITLE:

Operational Audit of Emergency Preparedness and Continuity Management Planning

AUDIT OBJECTIVE:

The objective of the audit is to assess the adequacy of Queensland Health's Corporate Office ability to respond and support a Health Service District in the event of an emergency occurring.

The audit will be required to –

i) Assess the adequacy of current policies and guidelines relevant to the Emergency Preparedness and Continuity Management Plan;
ii) Identify those areas of Corporate Office which are expected to play a role in supporting and coordinating a local emergency;
iii) Assess the capacity of each area to deliver the support required;
iv) Identify those areas of Corporate Office which are expected to have continuity management plans in place to sustain critical Corporate Office functions should the Queensland Health Building facility be compromised itself; and
v) Assess the capacity of each of the identified business functions in (iv) above, to give effect to their respective continuity management plans.

AUDIT SCOPE:

The audit will include all areas of Corporate Office including the Area Health Services which should legitimately contribute to an emergency situation or be compromised by the Queensland Health Building facility being compromised consequent to an emergency incident.

It should be noted that as a result of the recent Queensland Health restructure, Area Health Services may still be developing their plans in this area. In that case, this audit should acknowledge their current status and provide an opinion on the proposed direction and timeframes.

DESIRED OUTCOMES:

Provide assurance to the Executive Management Team of Queensland Health, that Corporate Office is adequately prepared to provide the leadership and support required to assist any Health Service District and/or other services in the event of an emergency occurring.

(3)

QH Operational Audit of EPCM – Corporate Management (June 2007)

Recommendations

1. The Executive Director Corporate Services establishes control processes for the confirmation, on an annual basis, that SSP roles and responsibilities for emergency preparedness, disaster recovery and business continuity planning have been met.

2. The Executive Director Corporate Services ensures the Business Policy and Strategy Unit, in forming the Emergency Preparedness Group as planned:
    a. Establishes a formal Terms Of Reference/Charter to govern its purpose, authority and responsibility. This Terms Of Reference/Charter should address as a minimum:
        i. The Group's Purpose
        ii. The group's scope and function
        iii. The groups composition
        iv. Meetings protocols
        v. Reporting and accountability structures
    b. Addresses all matters for the development, maintenance and testing of strategies, plans, manuals and processes as they relate to EPCM in the Unit across the following minimum areas of responsibility:
        i. Records management
        ii. Fleet management
        iii. Travel management
        iv. Property and facilities management

3. The Executive Director Corporate Services addresses Corporate office Services Unit Building Infrastructure Business Continuity Plan gaps and recommendations as identified

4. The Executive Director Queensland Health Shared Service Provider:
    a. Acknowledges the importance of medical supplies in the event of disaster recovery or emergency
    b. Ensures that the project to rationalise the warehousing requirements for medical supplies considers the impact on disaster recovery and emergency preparedness in relation to the critical inventory requirements at decentralised locations

5. The Executive Director Queensland Health Shared Service Provider:
    a. Confirms that the procedures for undertaking an emergency pay run are up to date, ensuring that appropriate adjustments and controls are in place
    b. Ensures the State Wide Coordinators for payroll, Supply and Finance (when appointed in July) review and update a strategy and plan for emergency preparedness for the respective systems

6. The Executive Director Queensland Health Shared Service Provider reviews the Operating Level Agreement with CorpTech to ensure that there is sufficient clarity relating to activities required in the event of a disaster or emergency

7. The Chief Information Officer:
    a. Reports on the timetable for adoption or completion of the Crisis Management Plan Maintenance Process, the Information Security Strategic Plan 2007-2012 and the adoption and testing of disaster recovery plans
    b. Considers the benefits of a consolidated Information Security, Risk and Continuity program/portfolio – aligned to ISRU's governance responsibilities

8. The Chief Information Officer ensures a further review is performed of the disaster preparedness of all key applications, including confirmation that procedures or service level agreements are in place to ensure clarity and sufficiency of testing of off site facilities and back up generators

9. The respective AHS GMs and the Executive Director Clinical and Statewide Services implement the following:
    a. To gauge the level of preparedness and adequacy of plans prepared by Districts/CASS in respect of EPCM, a comprehensive self assessment (using the audit report proposed pro forma as a guide) be performed by managers for facilities which they are responsible and accountable and reported to the respective GM/CASS ED
    b. Where significant progress gaps are noted, detailed actions plans should be reported to the respective GM/CASS ED for monitoring and follow up accountability
    c. A similar self assessment should be performed and reported by managers to the respective GM/CASS ED on an annual basis to ensure plans are reviewed and maintained on a frequent and timely basis in accordance with QH requirements and follow up accountability

10. The Chief Health Officer ensures:
    a. Roles, responsibilities and accountabilities are clear at all levels of management including AHS
    b. Command and coordination networks between AHS and Corporate Office are clear
    c. Relationships with external agencies are clear at all levels
    d. Training and development responsibilities are clear between the AHS and the Corporate Office Emergency Management Unit

EMT agreed action (3 September 2007)

EMT noted:

1. Receipt of the report and the urgency for preparation of a response to recommendations

2. That there would be urgent resource implications

Agreed action:

1. CHO to take carriage of organising a corporate response, acknowledging that each AHS/Division would need to develop an internal response plan

2. AHS contacts for consultation in terms of responding on internal service issues are:
    a. Central - Susan Mahon
    b. Northern - Alison Faiginez
    c. Southern - Martin Jarman

3. CHO in consultation with CIO sand ED/CASS to prepare a response to each audit recommendation within 2 weeks (17 Sept) with a project plan to be completed within 6 weeks (12 Oct)

---

(4)

Queensland Government
Queensland Health

MEMORANDUM

To: Ms Roxanne Ramsey, General Manager, Northern Area Health Service

Copies to: Mr Ken Whelan, A/Manager, Cairns Health Service District
Dr Jeannette Young, Chief Health Officer

From: Uschi Schreiber, Director-General **Contact No:** [redacted]
Fax No:

Subject: **FINAL AUDIT REPORT OPERATIONA/EFFICIENCY AUDIT – EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT – CAIRNS HEALTH SERVICE DISTRICT**

File Ref: 0652003/06046131

I wish to draw to your attention the attached Final Audit Report prepared for the Operational/Efficiency Audit of Emergency Preparedness and Continuity Management which was completed by the Audit and Operational Review Unit recently at the Cairns Health Service District.

The District has given a target date of July 2007 as a timeframe for the implementation of the recommendations. I would be pleased if you could provide an update of the status of the implementation progress, using the attached Action Plan, to Mr Pat Culpan, A/Director, Audit and Operational Review by 24 November 2006.

If you should have any enquiries regarding this matter, please do not hesitate to contact Mr Culpan on [redacted]

US 2/11

Uschi Shreiber
Director-General
/ /

Queensland Government
Queensland Health

FINAL AUDIT REPORT

OPERATIONAL/EFFICIENCY AUDIT

EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT

CAIRNS HEALTH SERVICE DISTRICT

SEPTEMBER 2006

Audit and Operational Review Unit

QUEENSLAND HEALTH
OPERATIONAL AND EFFICIENCY AUDIT
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT

EXECUTIVE SUMMARY

BACKGROUND AND FRAMEWORK OF REVIEW

Queensland Health has established its Emergency Preparedness and Continuity Management Policy, Guidelines and Program to support its preparedness and capability to prevent, respond to, and recover from an emergency event such as:

- A cyclone, earthquake, flood, storm, storm tide, tornado, tsunami, volcanic eruption or other natural happening;
- An explosion or fire, a chemical, fuel or oil spill, or gas leak;
- An infestation, plague or epidemic;
- A failure of, or disruption to, an essential service or infrastructure;
- An attack against the State (eg terrorism);
- Medical emergency;
- Accident, a bus or aircraft crash or major industrial accident;
- Threat to or on a person;
- A release of a chemical, biological or radiological agent; and/or
- Any other similar event.

Queensland Health's Emergency Preparedness and Continuity Management Policy, Guidelines and Program ("the Framework") include, et al:

- Queensland Health Disaster Plan 2002;
- Queensland Health Policy Statement 28028 – Emergency Preparedness and Continuity Management;
- Queensland Health Integrated Risk Management Framework (QHEPS 15232);
- Queensland Health Information Security Policy (QHEPS 3485); and
- Queensland Health Information Security Standard 9 – Business Continuity Management (QHEPS 23724).

This Framework is part of, and in support of, the Queensland Government's project for the safety and security of Queensland in:

- The preparation for, prevention of, response to and recovery from terrorism related incidents, as set out in the Queensland Government Counter-Terrorism Strategy 2005-2007, and consistent with the National Counter-Terrorism Framework;
- The protection and resilience of infrastructure; and
- The protection of critical infrastructure from terrorism.

The Framework is also based on, and supports compliance with and implementation of, relevant Legislation, Policies, Standards and key documents including:

- Disaster Management Act 2003;
- State Counter Disaster Plan 2001;
- Queensland Government Counter Terrorism Strategy 2005-2007
- Queensland Government Infrastructure Protection and Resilience Framework;
- Queensland Government Plan for the Protection of Critical Infrastructure from Terrorism
- Standards Australia and New Zealand - AS/NZS 4360 - 2004 – Risk Management
- Standards Australia and New Zealand- HB 221:2004 Business Continuity Management;
- Australian Standard – AS 4083-1997 Planning for Emergencies – Health Care Facilities; and
- Queensland Government Information Standard 18 – Information Security.

QUEENSLAND HEALTH
OPERATIONAL AND EFFICIENCY AUDIT
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT

EXECUTIVE SUMMARY

OBJECTIVE OF REVIEW

The overall objective of the review has been to ensure Queensland Health Executives are managing, (through the establishment and implementation of adequate and effective frameworks, strategies, plans, policies and procedures) the risks associated with emergency, disaster, security, contingency, asset protection and resilience management in accordance with the Framework to enable effective response and service continuity.

SCOPE AND NATURE OF REVIEW PROCEDURES

Review has been performed on a sample basis across the following Health Service Districts:

- Southern Area Health Service - Princess Alexandra Hospital Health Service District
- Southern Area Health Service - Gold Coast Health Service District
- Northern Area Health Service - Cairns Health Service District
- Northern Area Health Service - Innisfail Health Service District
- Central Area Health Service - Gladstone Health Service District
- Central Area Health Service - Central Highlands Health Service District

Our review was a high-level desktop review for the purposes of gauging implementation progress and identifying areas for further focus and development.

Our review procedures took the form of:

- Discussions with key officers at hospital based facilities and inter-agency representatives; and
- High-level review of plans, policies, procedures and related documentation as presented to us.

Our review procedures have not, and should not be relied upon by any parties as having, sought to test or provide validations or assurances in relation to:

- Completeness for all matters that may be identified and/or require further focus and development;
- Detailed compliance with all and/or specific legislation, standards, policies and/or guidelines; and/or
- Practical ability for plans, policies and procedures to successfully deter, mitigate, respond to and/or recover from disaster emergencies in test exercise or actual incident situations.

Review has been performed by BDO Kendalls as a party independent to Queensland Health. Review has been performed under the direction of, and for, Queensland Health and the Acting Senior Director, Assurance and Risk Advisory Services and should not be released to or relied upon by any other party without BDO Kendalls' prior knowledge and express consent, unless under obligation and direction at law.

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

SUMMARY OBSERVATIONS

The Cairns Health Service District (CHSD) comprises the hospital facilities at Cairns (356 beds), Cooktown (14 beds), Gordonvale (14 beds), Mossman (24 beds) and Yarrabah (8 beds). The Cairns Hospital is one of three tertiary level facilities in Queensland, providing care in all major adult specialities, including Hospital, Surgical, Medical, Clinics, Allied Health, Outreach, Aged Care and other services. The Health Service District employs more than 2,500 staff.

The CHSD has performed an all-hazards security risk identification, assessment and treatment planning exercise for the development of its overall hospital facility Security Strategy and Emergency Preparedness and Continuity Management Project.

It has also prepared and Emergency Plan, supported by specific incident Emergency Response Plans in accordance with Australian Standard AS 4083-1997 – Planning for Emergencies in Health Care Facilities. Plans are appropriately supported by related policies and procedures as required.

The CHSD has not however formally performed an all-hazards whole-of-business risk assessment process to collectively identify existing contingency and continuity arrangements and gaps, although contingency and continuity arrangements are addressed in the context of specific emergency responses through existing Security Risk Assessment and Treatment Plans, Emergency Plans and incident specific Emergency Response Plans.

The following provides high-level and specific matters for consideration by the Disaster Planning Committee in undertaking further plan development and maintenance work in relation to:

- All-hazards whole-of-business approach to contingency and business continuity planning;
- Actioning recommendations arising from Counter Terrorism Security Risk Assessment For Cairns Base Hospital (June 2005) – Emergency Preparedness And Continuity Management Project;
- Further Emergency Plan development; and
- Review and Assurance.

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

1. ALL-HAZARDS WHOLE-OF-BUSINESS APPROACH TO CONTINGENCY AND BUSINESS CONTINUITY PLANNING

Matter Noted ***Risk/Action Priority – High***

The aim of business contingency and continuity planning in an asset protection and resilience, emergency planning and continuity management context is to enable the restoration of normal business operations as soon as feasible following a critical incident. The plans serve to enable the hospital to establish disaster recovery and business resumption strategies to support its business in the event of any critical incident, regardless of its nature and source.

To a large extent, asset protection and resilience, contingency and continuity arrangements are addressed in the context of specific emergency responses through existing Security Risk Assessment and Treatment Plans, Emergency Plans and incident specific Emergency Response Plans. Similarly, work currently being performed in the preparation of Pandemic Influenza Plans are also expected to identify contingency and continuity risks equally applicable to whole-of-business risk and planning scenarios.

To date however, the CHSD has not performed a high-level, all-hazards continuity risk identification and assessment process to form the basis of preparation of *whole-of-business* asset protection and resilience, contingency and continuity plans, in accordance with applicable Queensland Government and Queensland Health Frameworks, Policies and Guidelines and other recognised best practice standards.

Recommendation

It is recommended that an all-hazards whole-of-business process be undertaken, considering and being based on requirements and best practice standards established by the following:

- Queensland Health Policy 28028: Emergency Preparedness and Continuity Management Policy (June 2005);
- Queensland Government Infrastructure Protection and Resilience Framework;
- Australian and New Standard AS/NZS 4360:2004 – Risk Management; and
- Australian and New Zealand Standard HB 221:2004 – Business Continuity Management.

Other relevant references include:

- HB231:2000 Information Security Risk Management Guidelines (for information security);
- National Guidelines for the Protection of Critical Infrastructure From Terrorism (for critical infrastructure); and
- Business Continuity Management: Keeping the Wheels in Motion – A Guide to Effective Control (Australian National Audit Office).

Based on the above, the framework and process should incorporate:

- Identification of essential or key elements within the asset (tangible and intangible);
- Identification and assessment of possible all-hazard continuity threats and risks and levels of consequential impact;
- Off-site interdependencies and other contingency and continuity strategies, plans, controls and procedures; and
- Determination of risks that require/do not require treatment, and development of treatment plans for unacceptable risk exposures.

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

Management Response

Recommendations Accepted: **YES**

Management Action Plan

Responsible Officer	*Target Date*
Steven Tresidder – Acting District Director of Corporate Services	July 2007

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

2. COUNTER TERRORISM SECURITY RISK ASSESSMENT FOR CAIRNS BASE HOSPITAL (JUNE 2005) – EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT PROJECT

Background

The CHSD has performed a security risk assessment to ensure its security measures are adequate and consistent with the standards defined in the Department of Premier and Cabinet – Government Agency Preparedness Document. Assessment has been preformed based on recognised best practice standard tools and appropriately identifies and considers critical assets, premises, essential elements and services, location and geography, capacity, site vulnerabilities, and national security threat levels.

Security risks assessed by scenario analysis appropriately include:

- Arson
- CBR Incidents
- Bombs/explosives
- Firm arm or weapon vulnerability
- Cyber attacks
- Utilities security
- Emergency power capability
- Security planning

Existing hospital security regimes provide:

- Security Field Officer Structure;
- 35 CCTV throughout campus with constant surveillance within the Security Control Station;
- Duress alarms in designated areas; and
- Electronic Access Control system throughout the campus in key areas. Staff ID cards (proximity cards) facilitate access to authorised locations. Other areas controlled by a key system.

Matter Noted ***Risk/Action Priority – High***

We were advised that the report of risk assessment, and self-assessed recommendations was provided to Queensland Health Corporate Office for consideration and incorporation into whole-of-agency counter terrorism security planning processes. The report included self-assessed recommendations, identifying progress in implementation of mitigation strategy enhancements as outlined below.

Self Assessed Recommendation	Progress and Status Since Reporting
1. Document role of emergency officers within core position descriptions.	Complete.
2. Emergency Response Equipment (CBR suits, filters, shower etc) to be stored in reality accessible and secure location.	Complete for reasonable risk mitigation.
3. Provide capacity to "positively pressurise" the Emergency Department (ED) area to minimise contamination.	***Identified as a control/mitigation strategy, however unlikely to be actioned on a cost/benefit basis. This matter has been raised to the attention of QH Corporate.***
4. Provide suitable equipment for crowd control and management such as barricades, signage, privacy screens, met tags, property tags, disposable clothing and industrial quality bags.	Complete for reasonable risk mitigation.

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

Self Assessed Recommendation	Progress and Status Since Reporting
5. Establish a central delivery location to receive courier deliveries and minimise uncontrolled access of couriers to many parts of the campus.	Complete for reasonable risk mitigation.
6. Educate staff, including cleaners and maintenance staff, to be alert of suspicious parcels in their area of work, and their response procedures.	Complete for reasonable mitigation.
7. Consider the possibility of a policy for lawful search of patients/visitors that includes clearly articulated procedures, comprehensive staff training and appropriate back up.	Complete for reasonable mitigation.
8. Security Officer's training to include counter-terrorism awareness.	Complete for reasonable mitigation.
9. Provide security of identified utilities in the event of changes to the National Alert Level. Additional security many include security locking to inspection pits, physical barriers to supply links, increased security presence, physical access controls and increased staff awareness and training.	***Not yet established. Preparation outstanding to priority resource allocation.***
10. Assess emergency power capability to support campus expansion requirements and sustain critical services. The expansion may include a field hospital environment in front of the hospital.	Complete for reasonable mitigation.
11. Include in staff orientation education to ensure staff awareness of terrorism issues, including: • Information security – prevention through vigilance • Key managers educated in the current procedures for building key management • Procedures relating to use of proximity cards • Staff alert to suspicious behaviour, vehicles and notification procedures.	Complete for reasonable mitigation.
12. Develop security sub plans for identified areas which require specific plans eg dangerous goods stores, generation stations, pathologies etc.	Addressed in Emergency Response Plans, specific roles and responsibilities, sub plans for ED etc. Not currently able to provide Queensland Fire and Rescue Service with a list of dangerous goods without a knowledgeable person to advise. Implementing database system to provide listing of all goods at any time.
13. Develop campus security plan to cover each of the four levels of National Alert to enable rapid escalation/de-escalation of security arrangements as required.	***Not yet established. Preparation outstanding to priority resource allocation.***

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

Recommendation

It is recommended that:

- Security Plans be developed and formalised to address the chain of command, engagement and communication procedures and protocols for receiving/communicating advice of changes in National Alert Levels (for example, with Queensland Health, Health Services Directorate, Internal Emergency Response and General Security Unit, and Queensland Police Services).

- Security Plans be further developed for procedures and protocols to be actioned on escalation/de-escalation of National Alert Levels. Requirements should be determined on guidance from Queensland Health, Health Services Directorate, Internal Emergency Response and General Security Unit.

Management Response

Recommendations Accepted: **YES**

Management Action Plan

Responsible Officer	*Target Date*
Steven Tresidder – Acting District Director of Corporate Services	July 2007

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

3. CAIRNS HEALTH SERVICE DISTRICT – EMERGENCY PLAN

Matter Noted ***Risk/Action Priority - High***

An Emergency Plan including a high-level Emergency Plan for application in all disaster emergency incidents, has been appropriately prepared. A number of matters noted for further development of the Emergency Plan and/or specific Emergency Response Plans are as outlined below.

Observation	Recommendation
The Emergency Plan and specific Emergency Response Plans appropriately address both internal and external emergencies, with reference to coordination with Far North Queensland's Emergency Medical System Plan and the Queensland Health Disaster Plan as required.	The CHSD is represented in Local and District Disaster Management Groups and Plans for inter agency engagement and coordination in managing a disaster emergency incident. It is recommended that the Emergency Plan – Code Brown – External Disaster Plan provide further reference/link to the Local Disaster Management Plan and the District Disaster Manual Plan for access as required.
The Emergency Plan appropriately establishes Command Post operations and procedures, including detailed role references for members. As appropriate, role references for specific emergency incidents address protocols for media and public relations responses.	It is recommended that the Emergency Plan address, at a high level for reference by all staff, the chain of command and authority for media and public relations responses. This should be in accordance with *Queensland Health Media Policy and Contact Guidelines.*
Specific incident Emergency Response Plan for Internal Emergencies (Code Yellow) has been established in accordance with AS 4083-1997 – Planning for Emergencies in Health Care Facilities.	It is recommended that the Code Yellow Emergency Response Plan provide further reference/link to: • Established procedures and treatment plans for hazardous substances; and • Contingency plans for continuity in operations and essential services.
The Emergency Plan provides authority for all emergency response plan activation phases, including the declaration of 'all clear' for re-entry and occupation.	It is recommended that Emergency Response Plan for Evacuation (Code Orange) specifically provide response procedure for declaration and communication of 'all clear' by the Emergency Controller (consistent with the Emergency Plan).
Specific incident Emergency Response Plan for Smoke/Fire (Code Red) has been established in accordance with AS 4083-1997 – Planning for Emergencies in Health Care Facilities.	It is recommended that the Emergency Response Plan for Smoke/Fire (Code Red) specifically provide for post incident checking, testing and replacement of equipment as necessary.
Specific incident Emergency Response Plan for Personal Threat (Code Purple) has been established in accordance with AS 4083-1997 – Planning for Emergencies in Health Care Facilities.	It is recommended that plans provide guidance and include recording templates for any identifying characteristics of the perpetrator including location, identity, age, sex, accent or speech impediment, background sounds etc.

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

Management Response

Recommendations Accepted: **YES**

Management Action Plan

Responsible Officer	***Target Date***
Steven Tresidder – Acting District Director of Corporate Services	July 2007

APPENDIX 3

QUEENSLAND HEALTH
EMERGENCY PREPAREDNESS AND CONTINUITY MANAGEMENT
CAIRNS HEALTH SERVICE DISTRICT

4. REVIEW AND ASSURANCE

Matter Noted ***Risk/Action Priority - High***

Under the Queensland Government's Infrastructure Protection and Resilience Framework, the CHSD has been classified as a Critical Infrastructure Asset of 'Significance'.

The Framework recommends, for significant assets, review and audit of all protection plans be performed on an annual basis.

In addition, the Framework recommends that the Chief Executive Officer of the Hospital provide an annual statement to the Department of Parliament and Cabinet (Security Planning and Coordination) to address the validation and audit requirements including:

- Date of the most recent risk assessment, which includes the counter-terrorism context;
- Date of current plans (security, on-site emergency response and business continuity);
- Current plans signed off by (name and position);
- Date of last test and/or exercise of plans;
- Date of last audit or plans (internal or external);
- Audit performed by (name, company and position); and
- Audit results (including recommended actions and those implemented).

In practice, the CHSD performs reviews on regular basis as resource permit. The CHSD was not aware of its classification as a 'Significant' Critical Infrastructure Asset and the associated review and assurance requirements of this classification.

Recommendation

As a 'Significant' Critical Infrastructure Asset, it is recommended that risk profiles and plans associated with the CHSD's Emergency Preparedness and Continuity Management Framework (including those relating to infrastructure resilience and protection from terrorist threats and activities) be reviewed on an annual basis, or more frequently for changing internal and external circumstances. Furthermore, underlying risk profiles should be re-assessment in detail every two years.

Based on review and assurance activities undertaken, it is recommended that quality procedures include the issue of certification as set out above to the Department of Parliament and Cabinet (Security Planning and Coordination) on an annual basis.

Management Response

Recommendations Accepted: **YES**

Management Action Plan

Responsible Officer	*Target Date*
Steven Tresidder – Acting District Director of Corporate Services	July 2007