Submission No 3

FOLLOW UP OF THE AUDITOR GENERAL'S 2012 FINANCIAL AUDIT REPORT

Organisation: Department of Premier and Cabinet

Name: Mr Chris Eccles

Position: Director General

Date Received: 17/06/2013



2013-187383

1 3 JUN 2013

Jonathan O'Dea MP
Chair
Legislative Assembly
Public Accounts Committee
Parliament of New South Wales
Macquarie Street
SYDNEY NSW 2000

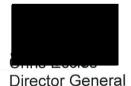
Dear Mr O'Dea

I write in response to your letter of 17 May 2013 requesting a submission from the Department of Premier and Cabinet to recommendations of the Auditor-General's 2012 Financial Audits.

Attached is the Department's response which includes actions taken.

If you require any further information, please contact Mr John Clark, Assistant Director General, Corporate Services on

Yours sincerely



2012 Financial Audits – Implementation of repeat recommendations

RESPONSIBILITY (Section of agency responsible for implementation)		Corporate Services	ServiceFirst
STATUS (completed, on track, delayed) and COMMENT		Completed	Completed
DUE DATE		The Business Recovery Plan has been implemented. It is reviewed annually.	A Disaster Recovery Plan has been implemented and is reviewed annually.
ACTIONS TAKEN		a) DPC has an approved Business Recovery Plan for its in-house financial systems. The plan includes: details of the required recovery activity to be undertaken; the position responsible for each activity; contact details of the position; the time required for each activity to be completed; and resources required to ensure effective	b) Financial systems are provided to DPC by ServiceFirst, a third party provider. To ensure the appropriateness of the ServiceFirst Disaster Recovery Plan, ServiceFirst subjects the Plan to an annual review by a consultant in conjunction with the
ACCEPTED OR REJECTED		Accepted	
RECOMMENDATION	All agencies should:	1 Define their recovery requirements and ensure these are reflected in disaster recovery plans for financial systems.	

Accepted and Services. Accepted an DPC's Business Recovery Plan is tested annually and updated where necessary. DPC's Business Continuity Program including the ServiceFirst Disaster Recovery Plan was also reviewed by Deloitte during 2012. b) ServiceFirst subjects its Disaster Recovery Plan to an annual review by a consultant in conjunction with the Department of Finance and Services. ServiceFirst has provided an assurance letter to DPC advising that the annual review and testing confirmed the effectiveness of the Disaster Recovery Plan. Accepted an Information Security Management System framework and is in the process of implementing this system across the			
Accepted and Services. Accepted a) DPC's Business Recovery Plan is rested annually and updated where necessary. DPC's Business Continuity Program including the ServiceFirst Disaster Recovery Plan was also reviewed by Deloitte during 2012. b) ServiceFirst subjects The Disaster its Disaster Recovery Plan was also reviewed by Deloitte during 2012. b) ServiceFirst subjects The Disaster Recovery Plan to an annual Plan is tested review by a consultant annually. In conjunction with the Department of Finance and Services. ServiceFirst has provided an assurance letter to DPC advising that the annual review and testing confirmed the effectiveness of the Disaster Recovery Plan. Accepted DPC has developed 17 st. DPC has developed 18 security Management Progress System framework report to the and is in the process of implementing this system across the 1 January	Corporate Services	ServiceFirst	Corporate Services
Department of Finance and Services. Accepted a) DPC's Business Recovery Plan is tested annually and updated where necessary. DPC's Business Continuity Program including the ServiceFirst Disaster Recovery Plan was also reviewed by Deloitte during 2012. b) ServiceFirst subjects its Disaster Recovery Plan to an annual review by a consultant in conjunction with the Department of Finance and Services. ServiceFirst has provided an assurance letter to DPC advising that the annual review and testing confirmed the effectiveness of the DPC has developed an Information Security Management System framework and is in the process of implementing this system across the	Completed	Completed	In Progress
Accepted a) b)	The Business Recovery Plan is tested annually.	The Disaster Recovery Plan is tested annually.	31 July 2013 – 1 st Progress report to the ICT Board.
	Department of Finance and Services. a) DPC's Business Recovery Plan is tested annually and updated where necessary. DPC's Business Continuity Program including the ServiceFirst Disaster Recovery Plan was also reviewed by Deloitte during 2012.	1	DPC has developed an Information Security Management System framework and is in the process of implementing this system across the
insure disaster recovery plans are ested periodically. Revise their information security nanagement framework to align with Premier's Memorandum AZ012-15 Digital Information security Policy.	Accepted		Accepted
ω Πħ	Ensure disaster recovery plans are tested periodically.		Revise their information security management framework to align with Premier's Memorandum M2012-15 Digital Information Security Policy.

Corporate Services
In Progress
December 2013
and records management system. An initial risk assessment and information has been undertaken of all DPC information assets and work commenced on assessing the controls for these assets. DPC has a number of policies / controls to define user access requirements and segmentation of duties
Accepted
Enhance agency compliance with information security procedures and guidelines to focus on appropriate user access

vith the ces viceFirst, t these	012 an It was of IT	rking ion of the ations.	IT project 30 June 2014 In progress Corporate t	I which security,	iity s.		within the second secon	t System	ion of
DPC works with the shared services provider, ServiceFirst, to implement these controls.	In October 2012 an Internal Audit was undertaken of IT Security. The Department is	currently working through the implementation of the recommendations.	Accepted DPC has an IT project management framework	implemented which incorporates security,	risk and quality requirements.	This will be	incorporated within the Department's Information Security	Management System	implementation of
of duties and security configurations.			Consider information security requirements during new system	process changes.					