ATTACHMENT C

STATE OF COLORADO

Colorado Department of Human Services
people who help people

1575 Sherman Street
Denver, Colorado 80203-1714
Phone 303-866-5700
www.cdhs.state.co.us

Bill Ritter, Jr.
Governor

Karen L. Beye
Executive Director

Sally Symanski, CPA
Office of the State Auditor
200 East 14th Avenue
Denver, CO 80203

September 28, 2007

Dear Ms. Symanski:

In response to your request received September 19th, Human Services provides the following status report regarding the audit recommendations from the Mainframe Disaster Recovery Audit of January 2007.

Recommendation #2:

The Departments of Human Services, Labor and Employment, Personnel and Administration, and Revenue should take immediate steps to adopt disaster recovery plans that adhere to the requirements of the Information Management Commission's Contingency Planning/Disaster Recovery Policy for their respective critical systems housed on the state mainframe. The plans should be submitted to the Office of Information Technology no later than the June 2007 deadline specified in the 2006 Information and Technology Strategic Plan.

Department response status to recommendation #2:

- The implementation status for this recommendation is completed.
- The department acquired the services of a contractor specializing in disaster recovery/business continuity services to help complete the disaster recovery plans for our critical mainframe systems. Disaster recovery plans for the Automated Child Support Enforcement System (ACSES), Low-income Energy Assistance Program (LEAP), State Identification Module (SIDMOD) and Electronic Benefits Transfer (EBT) system were completed by June 2007 and have been forwarded to the Governor's Office of Information Technology (OIT).
- There are no other factors that impacted the implementation of this recommendation.

Recommendation #4:

a. Identifying and testing their respective critical mainframe systems.

b. Identifying and testing all components of non-mainframe systems that the critical mainframe systems interface with.

c. Developing comprehensive test plans that adequately test the disaster recovery plans developed for critical systems and actively coordinating with the Division of Information Technologies.

d. Assigning testing responsibilities to all appropriate personnel, including system administrators as well as end users, and ensuring all necessary activities and transactions are tested.

Department response status to recommendation #4:

- The implementation status for items a, b, c, and d is completed.

- Item a: The department examined all of CDHS mainframe applications to determine those that were critical in nature. As a result of the examination, Automated Child Support Enforcement System (ACSES), Low-income Energy Assistance Program (LEAP), State Identification Module (SIDMOD) and Electronic Benefits Transfer (EBT) were identified as critical systems and were tested in this year's Mainframe Disaster Recovery Test in August.

  Item b: The SIDMOD application interfaces with several non-mainframe applications. These non-mainframe applications were identified and were tested in this year's Mainframe Disaster Recovery Test.

  Item c: Comprehensive test plans were developed for these four critical systems. Testing responsibilities were assigned and coordinated with the Department of Personnel Administration (DPA) Division of Information Technologies (DoIT).

  Item d: In readying for participation in this years annual Mainframe Disaster Recovery Test, meetings were held to determine testing objectives, pass/fail criteria, end-user participation and required transactions, tasks and procedures.

- There are no other factors that impacted the implementation of this recommendation.

If you have any questions, please contact Stephen Swanson, Chief Technology Officer, at (303) 866-5521 or by e-mail at Stephen.swanson@state.co.us.

Sincerely,

Karen L. Beye

Karen L. Beye
Executive Director, Colorado Department of Human Services

Cc: Ron Huston, Chief Information Officer, Colorado Department of Human Services
Ron Ozga, Deputy Chief Information Officer, Colorado Department of Human Services
Steve Swanson, Chief Technology Officer, Colorado Department of Human Services

BILL RITTER, JR.
Governor

DONALD J. MARES
Executive Director

DEPARTMENT OF LABOR AND EMPLOYMENT
OFFICE OF THE EXECUTIVE DIRECTOR

633 17th Street, Suite 1200
Denver, Colorado 80202-3660

September 25, 2007

Sally Symanski, CPA
Office of the State Auditor
200 E. 14th Ave.
Denver, CO 80203

Dear Ms. Symanski:

To update the responses of the Department of Labor and Employment to the Mainframe Disaster Recovery Audit, we report that all actions prescribed are **IN PROGRESS.**

The Department of Labor and Employment has completed the 2006 statewide Continuity of Operations (COOP) Plan and completed a successful "table top" exercise of the plan on January 11, 2007. A new fully developed COOP plan for Unemployment Insurance is now in the internal approval process. This will be provided to OIT by October, 2007. A similar plan for Workers' Compensation special funds will be modeled on the UI plan. A decision item has been submitted for the acquisition of hardware and communication between sites which will allow complete DR abilities as well as failover abilities in the event of single site failures.

Critical mainframe systems have been identified. The mainframe backup test of August 20, 2007 was successfully applied to Unemployment applications (CATS and CUBS). The next test will include critical Workers' Compensation applications (Special Funds).

Critical non-mainframe interfacing systems have been identified (IIC, ICC, and Special Funds). DR plans and related test plans are being developed subject to the approval of the decision item for backup hardware and communications.

We will be glad to provide any additional you may require and appreciate your attention to these important matters.

Very truly yours,

Donald J. Mares
Executive Director
Colorado Department of Labor & Employment

STATE OF COLORADO

DEPARTMENT OF REVENUE
State Capitol Annex
1375 Sherman Street
Denver, Colorado 80203

Bill Ritter, Jr.
Governor

Roxanne Huber
Executive Director

September 10, 2007

Sally Symanski, CPA
Office of the State Auditor
200 East 14th Avenue
Denver, Colorado 80203

Dear Ms. Symanski:

Attached please find the Department's response to the follow-up on the State Auditor's recommendations to the Department of Revenue contained in the Mainframe Disaster Recovery audit report dated January 2007.

If you have any questions regarding these documents or the Department's implementation of the recommendations, please contact me at (303) 866-5610.

Sincerely,

Roxanne Huber
Executive Director

Attachment

Office of the State Auditor

FORMAT FOR PROGRESS REPORT
IMPLEMENTATION OF AUDIT RECOMMENDATIONS

Name of Audit: Mainframe Disaster Recovery Performance Audit
Department of Revenue Responses
September, 2007

Recommendation #__2_

The Departments of Human Services, Labor and Employment, Personnel and Administration, and Revenue should take immediate steps to adopt disaster recovery plans that adhere to the requirements of the Information Management Commission's Contingency Planning/Disaster Recovery Policy for their respective critical systems housed on the state mainframe. The plans should be submitted to the Office of Information Technology no later than the June 2007 deadline specified in the 2006 Information and Technology Strategic Plan.

Department of Revenue Reported Implementation Status:

1. Implemented __X_ In Progress _____ Not Implemented ____(Check one.)

2. The Department completed the actions in Recommendation #2 in June, 2007. In accordance with Statewide cyber security polices and rules as set forth previously by the Governors Office of Information Technology, Cyber Security Office, Information and Technology Strategic Plan, the Department completed and submitted via the Executive Director's Office, the Department's Cyber Security Plan. This plan included a Critical Systems Inventory and outlined disaster recovery plans for critical mainframe systems that adhere to the prior Information Management Commission's Contingency Planning/Disaster Recovery Policy.

Recommendation #__4__: (for multi-part recommendations)

The Departments of Human Services, Labor and Employment, Personnel and Administration, and Revenue should improve their disaster recovery testing for critical mainframe systems by:

a. Identifying and testing their respective critical mainframe systems.
b. Identifying and testing all components of non-mainframe systems that the critical mainframe systems interface with.
c. Developing comprehensive test plans that adequately test the disaster recovery plans developed for critical systems and actively coordinating with the

Division of Information Technologies.
d. Assigning testing responsibilities to all appropriate personnel, including system administrators as well as end users, and ensuring all necessary activities and transactions are tested.

Department of Revenue Reported Implementation Status:

1. Implemented _X__ In Progress _____ Not Implemented ____ (Check one.)

2.

a. Recommendation #4a was considered to be not applicable to the Department of Revenue. This part of the recommendation to the Department of Revenue, because it previously identified its critical systems and those systems were tested in the annual mainframe disaster recovery test.

REVISED RESPONSE 10/9/07

b. This was implemented in August, 2007. In the annual mainframe disaster recovery test, this plan was successfully tested. The Department will continue to monitor and update the disaster recovery plan and testing plan as needed to incorporate any and all systems that interface with the mainframe in the future.

c. The Department completed these tasks and finished implementation in August, 2007. The Department developed test plans to adequately test the disaster recovery plan and coordinated with the Division of Information Technology in the utilization and testing of these plans.

d. The Department completed these tasks in August, 2007. The Department developed plans that assigned testing responsibilities to all appropriate personnel, including administrators, as well as end users such as Taxation, Motor Vehicle and 24 hour Communications Center team members. All necessary transactions were identified and these plans were tested successfully in August, 2007.

State of Colorado

Bill Ritter Jr.
Governor

Rich Gonzales
Executive Director

Jennifer Okes
Deputy Executive Director

Todd E. Olson
Division Director

DPA

Department of Personnel & Administration

Division of Information Technologies
690 Kipling Street
Lakewood, Colorado 80215
Phone (303) 239-4313
Fax (303) 239-4383

September 25, 2007

Sally Symanski, CPA
State Auditor
Office of the State Auditor
200 E. 14th Ave.,
Denver, Colorado 80203

Dear Ms. Symanski,

Enclosed, you will find the Department of Personnel & Administration's response to the January 2007 Mainframe Disaster Recovery Performance Audit recommendations.

The responses address the recommendations made in of the January 2007 Mainframe Disaster Recovery Performance Audit report, specifically the Recommendation Locator beginning on page 3 of the report.

If you have further questions or comments regarding the response, please call me at 303-866-6559.

Sincerely,

Rich Gonzales
Executive Director

h:Michelle/Correspondence/07/RG/Ltr to S Symanski re Response to Jan 07 Mainframe Disaster Recovery Perf Audit Recommendations

Enclosures - 3

Recommendation 2 21

Adopt disaster recovery plans that adhere to the requirements of the IMC's Contingency Planning/Disaster Recovery Policy for their respective critical systems housed on the state mainframe. The plans should be submitted to the Office of Information Technology no later than the June 2007 deadline specified in the 2006 Information and Technology Strategic Plan.

1) Implemented X Not Implemented In Progress

2) Please provide a brief response (nor more than 15 lines) discussing how you intend to implement the recommendation.

Individual COFRS and CPPS disaster recovery plans were sent to OIT June 2007.

3) Implementation Date: June 2007 (Please provide the month and year by which you intend to fully implement the recommendation.

4) Factual Changes: If you believe that there are facts in the narrative that need to be updated, changed, or developed further, please indicate those changes here.

No Changes.

Recommendation 3 27

Strengthen the effectiveness of the annual mainframe disaster recovery test by (a) providing adequate formal notification to the chief information officers at all of the agencies with critical systems on the mainframe and notification to the Office of Information Technology, and (b) defining the scope, timing, and purpose of the test in coordination with the participating agencies.

1) Implemented X Not Implemented In Progress

2) Please provide a brief response (nor more than 15 lines) discussing how you intend to implement the recommendation.

a) 2007 Annual Mainframe Disaster Recovery Test was announced at both the February 2007 and July 2007 CIO Forums. OIT is represented at these forums. Copies of the announcement circulated at these meetings is available upon request.

b) Each customer agency defines their own test scope; the DoIT DR Coordinator requests customers to provide a list of any special needs. For the 2007 test, the DoIT DR Coordinator conducted individual and group customer meetings beginning in April 2007 for the August 2007 test.

3) Implementation Date: Spring / Summer 2007 (Please provide the month and year by which you intend to fully implement the recommendation.

4) Factual Changes: If you believe that there are facts in the narrative that need to be updated, changed, or developed further, please indicate those changes here.

No changes.

Recommendation 4 28

Improve disaster recovery testing for critical mainframe systems by (a) identifying and testing their respective critical mainframe systems; (b) Identifying and testing all components of non-mainframe systems that the critical mainframe systems interface with; (c) developing comprehensive test plans that adequately test the disaster recovery plans developed for critical systems and actively coordinating with the Division of Information Technologies; and (d) assigning testing responsibilities to all appropriate personnel, including system administrators as well as end users, and ensuring all necessary activities and transactions are tested.

1)

Implemented	X	Not Implemented	In Progress

2) Please provide a brief response (nor more than 15 lines) discussing how you intend to implement the recommendation.

COFRS and CPPS disaster recovery test plans have been created. The respective plans were submitted to OIT in June 2007. Maintenance plans were included as recommended in 2 21.

3) Implementation Date: June 2007 (Please provide the month and year by which you intend to fully implement the recommendation.

4) Factual Changes: If you believe that there are facts in the narrative that need to be updated, changed, or developed further, please indicate those changes here.

No Changes.

STATE OF COLORADO

OFFICE OF INFORMATION TECHNOLOGY (OIT)
Office of the Governor

1580 Logan, Suite 200
Denver, Colorado 80203
Phone: 303-866-6060
FAX: 303-866-6454

Bill Ritter, Jr.
Governor

Michael Locatis
State Chief Information Officer

Office of the State Auditor
200 East 14th Avenue
Denver, CO 80203

Dear Ms. Symanski

In response to your request for action taken on the recommendations contained in the January 2007 *Mainframe Disaster Recovery Audit* I am pleased to provide you with the following.

Recommendation No 1.

a. *Agree. Implementation date: July 2007.*

The OIT will develop mechanisms to track and plan submissions and follow up with agencies that do not submit plans as prescribed.

Implemented. The OIT has developed an Excel spreadsheet that is used to track submissions and follow-ups with agencies that do not submit their plans. (Attachment 1)

b. *Agree. Implementation date: September 2007.*

The OIT will review all agency disaster recovery plans to ensure compliance with state information technology policies and rules, including the Contingency Planning/Disaster Recovery Policy.

In progress. The OIT is in the process of receiving and reviewing all of the disaster recovery plans to ensure compliance with state information technology policies and rules.

c. *Agree. Implementation date: September 2007.*

The OIT will develop a formalized process in which feed back will be given to state agencies regarding their disaster recovery plans. This process will also include a mechanism for state agencies to request assistance in developing and refining their plans.

In progress. The OIT is developing a formalized process to allow for feed back of the agency's disaster recovery plans. Currently, the OIT is considering using the Executive Governance Committees that were formed after SB07-254 abolished the Commission of Information Management. (Attachment 2)

Recommendation No. 5

Agree. Implementation date: January 2008.

The OIT will develop procedures for:

a. *Reviewing agencies' disaster recovery test plans.*

b. *Verifying tests were completed.*

c. *Determining if the test meet the requirements of the Disaster Recovery Policy.*

d. *Performing any follow-up.*

In progress. The OIT is developing these procedures and is working with other agencies to determine the best way to implement them. Once the disaster recovery plans are tested The OIT will identify areas for improvement and update the plan accordingly.

Recommendation No. 6

Agree. Implementation date: July 2007.

The state Chief Information Security Officer (CISO) has developed a new policy that specifically addresses the four Disaster Recovery requirements outlined in this recommendation. The OIT will adopt this new policy and enforce its requirements.

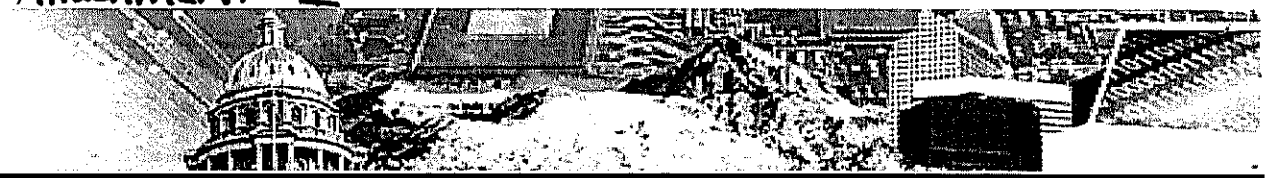
Implemented. The OIT has reviewed the CISO's plan and has begun the necessary steps to formally adopt this policy. (Attachment 3)

Sincerely,

John D. Conley
Deputy Director

Attachment 1

OIT Governor's Office of Information Technology

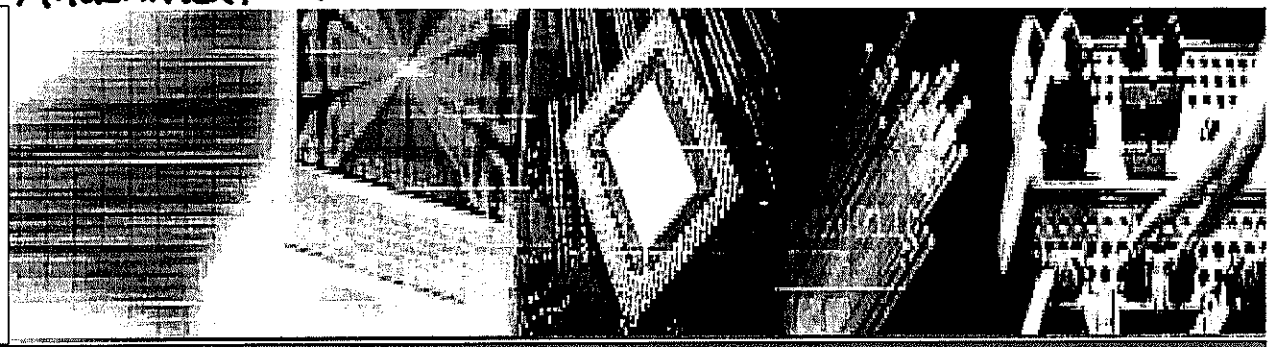


DIASTER RECOVERY PLAN SUBMISSION

Agency	Plan Submitted by deadline	Deadline Given	Follow-up initiatiated on	Deadline for Follow-up	Follow-up deadline met	Compliance Letter Sent	Date sent	File Name of Compliance Letter
Department of XYZ	*Yes*	*10/10/2005*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	
Department of 123	*No*	*10/10/2005*	*12/10/2005*	*12/20/2005*	*No*	*Yes*	*12/22/2005*	*Dpt. 123 DR Compliance Letter*

Attachment 2

Office of the State Chief Information Officer



Understanding the Executive Governance Committee

Prepared for:

Department Leadership and Staff

September 12th, 2007

Defining the Executive Governance Committee

The EGC will provide senior-level enterprise oversight of active and certified IT projects. Specifically, it will:

- Ensures cross-departmental cooperation across the State.
- Provide communication to Executive Management (Governor, Executive Directors), as well as to the Legislature and the general public about the state of IT projects across the State.
- Acts as the escalation point for the project steering committees.
- Resolves major issues that need escalation beyond the project steering committees.
- Reviews Independent Verification & Validation (IV&V) reports and helps mitigate risks and issues with the project teams.
- Helps leverage IT and business resources across Departments.
- Helps identify projects and systems that can be used more effectively across the enterprise.

Executive Governance Committee Staffing

Office of the State Chief Information Officer

The following organizational structure is recommended to oversee the major projects across the State:

Agriculture and Natural Resources

- OIT Chair
- Dept of Agriculture (3)
- Dept of Natural Resources (3)
- OIT PMO Director (Non-Voting)

Public Safety

- OIT Chair
- Dept of Corrections (2)
- Dept of Public Safety (2)
- Dept of Military / Veterans Affairs
- Dept of Local Affairs
- OIT PMO Director (Non-Voting)

Finance

- OIT Chair
- Dept of Revenue (3)
- Dept of Reg Agencies
- Dept of State
- DOLA
- Treasury
- State Controller (Non Voting)
- OIT PMO Director (Non-Voting)

Personnel and Labor

- OIT Chair
- DPA (3)
- CDLE (3)
- OIT PMO Director (Non-Voting)

Health Care and Human Services

- OIT Chair
- Dept of Human Services (2)
- Dept of Health Care Policy and Financing (2)
- Dept of Public Health and Environment (2)
- OIT PMO Director (Non-Voting)

Education

- OIT Chair
- Dept of Education (2)
- Dept of Higher Ed (3)
- Historical Society
- OIT PMO Director (Non-Voting)

Transportation

- OIT Chair
- Dept of Transportation (4)
- DPA
- Dept of Revenue
- OIT PMO Director (Non-Voting)

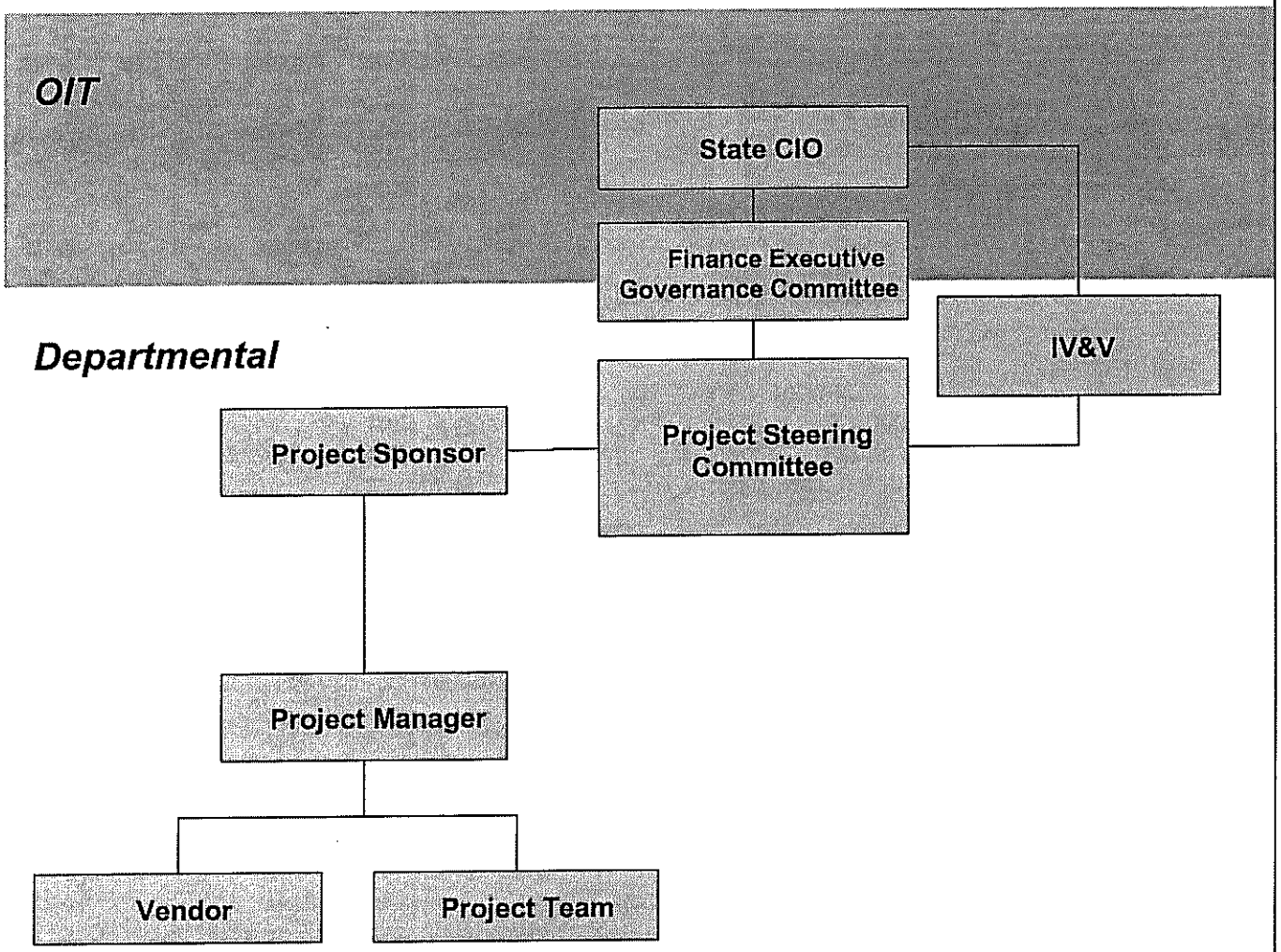
Summary

- There will be seven EGC committees that will provide oversight for logically grouped Departments.
- Each EGC has 7 advisory members. Each group will be chaired by OIT.
- EGC will not convene if the represented partners do not have any active, major projects.
- The other six seats will be staffed by represented departments and/or relevant subject matter expertise.
- Meetings will be held monthly.
- Project steering committees will provide summary reports on a regular basis to OIT.
- OIT will prepare a monthly summary report for the EGC and the EGC will focus on higher priority issues and risks.
- This body provides input for OIT to make critical enterprise decisions.

Understanding the Structure of the EGC

Office of the State Chief Information Officer

The following outlines the project governance model:



Structural Summary

- The example on the left is for the Colorado Integrated Tax Architecture (CITA) project within the Department of Revenue but represents the model for all large IT projects.
- Departments manage the Project Steering Committees and projects.
- Project Steering Committees will report summary project status – including issues and risks -- to the EGC.
- IV&V will report out at the Project Steering Committee and to the EGC to ensure visibility.
- A dedicated business centric project sponsor is highly recommended.

Certified Projects and EGC Scope

Office of the State Chief Information Officer

Within the EGC structure, OIT has identified the following projects which have been certified:

Public Safety

- CCIS Replacement

Finance

- CSTARS
- CITA
- DOS/HAVA SCORE II

Health Care and Human Services

- MPSC-WIC Replacement
- CBMS Re-procurement
- CHATS Replacement
- DVR RISE

Personnel and Labor

- VoIP Convergence
- Digital Trunk Radio (DTRS)

Focus Areas

- Business and policy constraints and issues
- Major issues that have been escalated from the project steering committee
- Budgetary issues
- Schedule issues
- Cross-departmental / jurisdictional issues
- Resource utilization / sharing across departments
- Issues from the IV&V report
- Enterprise Architecture / Shared Services

Out of EGC Scope

- Minor issues with schedule, budget, staffing, or other project level concerns
- Procurement of services and products
- Lower level project governance
- Approval of change and scope requests
- Review of specific quality assurance metrics and requirements
- Contractual issues

EGC Action Plan

Office of the State Chief Information Officer

Here is what OIT requires from the Departments for the following schedule. OIT will ask for Executive Directors to assign respective members for 1 year.

Planning

Communicate expectations for the EGC and make sure participants and project representatives are identified.

- Identification of the EGC participant (s).
- Identification of the project sponsor and project representatives.
- Identification of IV&V reporting.
- Project information from the project sponsor.

October Meeting

Kick-off the EGC meetings, introduce roles, and assign responsibilities.

- Overview of the certified project (s).
- EGC participation to understand roles, responsibilities, and expectations.

November Meeting

Begin execution of the EGCs to govern certified projects.

- Project sponsors and representatives with OIT assistance will complete the EGC reports.
- EGC participation to begin reviewing projects and providing oversight.

Next Steps

- OIT will work with project sponsors to share the reporting requirements.
- During the October EGC kick-off meeting, OIT will explain roles and responsibilities. This meeting will set EGC member expectations and how the meetings will be conducted.
- OIT will identity the IV&V vendors for the projects and coordinate reporting to OIT.
- OIT will assist the project teams in preparing reports for the EGC meetings.

Attachment 3

TITLE:	STATEWIDE DISASTER RECOVERY		
POLICY #:		EFFECTIVE DATE:	AUGUST 1st, 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	

State of Colorado

IT Disaster Recovery

Overview

This policy document is part of the Governor's Office of Information Technology policies, created to support the State of Colorado Chief Information Officer (CIO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Public Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance are outlined in a separate Guidelines document which is designed to help Public Agencies achieve the objective of this Policy.

For the purposes of this document, a "Public Agency" includes organizations as defined in C.R.S. 24-37.5-102(5).

Policy

It is the policy of the State of Colorado that all State Public Agencies and associated departments prepare and test IT Disaster Recovery Plans that will be maintained and used in the event of an impact to the IT Operational Infrastructure . This may be in the form of a localized power outage or fire to a major incident either man made or natural.

Authority

C.R.S. 24-37.5-103 (1.5), C.R.S. 24-37.5-106

Scope

This policy document applies to every State Public Agency ("Agency") as defined in C.R.S 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include state-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Applies to IT Infrastructure of a State Public Agency. Business operations of the Agency are covered in the Agency Continuity of Operations Plan (COOP) of which the plan developed as directed by this policy is a part of.

Roles and Responsibilities

Agency Executive Director – is responsible for:

- Supporting Disaster Recovery planning and testing needs.

State CIO – is responsible for:

- Review and approval of Public Agency Disaster Recovery Plans.
- Verification of Disaster Recovery test completion.
- Ensuring tests meet the requirements of the Disaster Recovery Policy

State CISO - is responsible for:

- Review of Public Agency Disaster Recovery Plans.
- Review of test results as part of the Cyber Security Program Plan approval process.

Agency Chief Information Officer (CIO) – is responsible for:

- Leading the development of the Public Agency Disaster Recovery Plan.
- Coordinating testing of the Disaster Recovery Plan
- Ensuring that Agency IT staff are maintaining the Disaster Recovery Plan and performing the tasks identified in the plan on a day-to-day basis.

Agency Information Security Officer (ISO) – is responsible for:

- Monitoring the effectiveness of the disaster recovery planning and preparation process.
- Ensuring required security controls are implemented during Disaster Recovery operations.

Agency IT Staff – is responsible for:

- Completing disaster recovery training.
- Participating as required in disaster recovery testing.
- Maintaining the Disaster Recovery plan when the IT environment changes
- Carrying out day-to-day activities that allow the plan to be put into operation if necessary, i.e. storing backup tapes off-site as specified in the plan.

Requirements

To ensure adherence to best practices and industry standards, this policy requires that all Public Agencies develop a Disaster Recovery Plan and comply with the following:

Planning

A Disaster Recovery Team shall be established with a designated Coordinator. Team members and key user personnel shall be identified, along with work location, work phone, home phone, mobile phone, pager and home address and their responsibilities defined. Plans shall be developed to provide for the rotation of team members both within and on and off the team in order to ensure that knowledge is transferred among team members and that back-ups to tasks are available in case of emergency.

Development of the Disaster Recovery Plan

IT Disaster Recovery Plans are to be developed and designed to reduce the impact of a major disruption on key business functions and processes. The Disaster Recovery Plans must address requirements for alternative processing and recovery capability of all critical IT services. Plans shall be developed for each system using the same Recovery Time Objectives for the business function that the IT system supports. Disaster Recovery Plans shall also include usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach. The systems, applications, and resources identified as the most critical should be the focus in the IT Disaster Recovery Plan. This will establish the priorities

in recovery situations and to keep costs at an acceptable level while complying with regulatory and contractual requirements.

Continuity Of Operations Planning (COOP)
The COOP Plan should include a detailed information technology continuity framework including the procedures for documenting, testing and executing the plans. This plan should include guidelines for identifying and updating the list of all critical IT systems on a periodic basis and monitoring and reporting on the availability of crucial resources, alternative processing, and the schedule of system back-ups performed.

Operations

Maintenance of the IT Disaster Recovery Plan
The IT Disaster Recovery Plan maintenance procedures will be defined to ensure that the Plan is kept up to date with respect to dynamic changes, such as personnel changes, new hardware and software systems deployment, documentation updates, and to ensure it continually reflects business requirements. The Disaster Recovery Plan shall also contain instruction to notify stakeholders of changes to the plan.

Testing of the IT Disaster Recovery Plan
The IT Disaster Recovery Plans shall be tested on a yearly basis, or after a significant change to the environment, to ensure that IT systems can be effectively recovered and shortcomings can be addressed. Disaster Recovery Plan testing must identify testing procedures and contain instruction how the public agency will approve updates to the IT Environment based on test results.

Training on the IT Disaster Recovery Plan
All concerned parties are to receive regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. The IT Disaster Recovery Plan must contain instruction on how training is enhanced or distributed in the event of new Plan requirements, roles, responsibilities, or communication processes.

Logistics

Distribution of the IT Disaster Recovery Plan
A defined and managed distribution strategy must be outlined in the IT Disaster Recovery Plan to ensure that the Plans are properly and securely distributed and available to appropriately authorized interested parties when and where needed. This distribution strategy must take into account all disaster scenarios that the Plan is intended to address.

Offsite Backup Storage
All backup media, documentation and other IT resources necessary to recover or resume IT processing must be stored off-site. Backup procedures and rotation schemes must be adequate to provide the necessary data for recovery while minimizing data loss. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Backup media and the hardware used to restore from backup must be tested as part of the Disaster Recovery Plan testing strategy.

Recovery

IT Services Recovery and Resumption

The IT Disaster Recovery Plan must include step-by-step instructions for recovery and resumption of services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, resumption procedures, etc.

Post-Resumption Review

A post-resumption review shall occur after successful resumption of the IT functions following a disaster. The purpose of this review is to assess the adequacy of the Disaster Recover Plan and procedures, and to subsequently update the Plan accordingly.

References

- ISO 17799-2005 Section 10 Business Continuity/Disaster Recovery
- National Institute of Standards and Technology (NIST) Special Publication (SP)-800-34, "Contingency Planning Guide for Information Technology Systems"
- Guidelines for State of Colorado IT Disaster Recovery Plans (September 2007)

IT Disaster Recovery Guidelines

Overview

This document describes recommended practices for meeting the objective of the IT Disaster Recovery policy. Note that these are recommended practices and guidelines only and further research, study, implementation and lessons learned in the field of IT Disaster Recovery should be utilized instead of using these guidelines as the level of capability an Agency should see as achieving.

Disaster Recovery Plan Development

Public Agencies should perform a Business Impact Assessment to identify IT systems that would have the greatest negative impact to the Public Agency in the event of a disaster. Such systems should be used to prioritize the recovery scope and schedules.

A Threat and Vulnerability Analysis should be conducted to identify the most probable disaster scenarios. The most probable scenarios should be used to guide the development of the Disaster Recovery Plan strategy.

Contact Information

The IT Disaster Recovery Plan should address roles, responsibilities, and identify both primary and secondary individuals with contact information, and activities associated for both primary and secondary individuals in executing the disaster recovery plan.

The IT Disaster Recovery Plan should be reviewed and updated if necessary on a quarterly basis to address changes in systems and organizations.

IT Disaster Recovery Plan Training

Public Agencies should keep auditable records of disaster recovery training and validate that the team members have received training prior to each disaster recovery test (or more frequently). Training should be delivered to all individuals that are assigned roles in the Disaster Recovery Plan.

End-user training should address expectations of the user in the event of a disaster and should be delivered on initiation of employment with refresher training administered periodically thereafter.

Enhanced Disaster Recovery Plan Testing

Testing of the IT Disaster Recovery Plan shall be included in Agency or Department level Drills, Table Top Exercises, Functional Exercises and Full Scale Exercises as determined by the Agency COOP Planner. The depth and rigor of testing is balanced against the potential impacts to on-going operations. At a minimum, operational testing of the IT Disaster Recovery Plan is performed for critical systems.

Maintenance of IT Disaster Recovery Plan

Maintenance of the plan and the use of a sustainment team around IT Disaster Recovery is necessary to keep the plan current, to ensure that staff are assigned to review and update the plan as part of their job role responsibilities and to also test the plan on a regular basis. The main items to look for in a quarterly plan review is the turnover of staff through new hires, attrition and promotion and the addition or deletion of applications or services that is support by the agency.

Recovery and Resumption

Alternate Storage, Processing, and Operations

An alternate processing site should be geographically separated from the primary processing site so as not to be susceptible to the same hazards. A rule of thumb to be used is to locate the alternate processing site 200 to 300 miles away from the primary processing facility.

The alternate processing site should be configured to facilitate timely and effective recovery operations and maintain the appropriate security controls for critical systems.

A Public Agency identifying an alternate processing site should initiate the necessary agreements to permit the resumption of operations for critical functions within a specifically defined period of time when the primary processing capabilities are unavailable.

Equipment and supplies required to resume operations should be available at the alternate site or there should be contracts are in place to support immediate delivery to the site.

The alternate processing site should be fully configured to support the minimum required operational capability and be ready to use as the operational site with little or no notice and no intervention by Public Agency IT staff.

The alternate processing site may optionally be used as the business operations alternate site to reduce cost and impact to the public agency. In this configuration, however, care should be taken to uphold reasonable physical security controls.

Telecommunications Support

The Public Agency should identify primary and alternate telecommunications services and initiate necessary agreements to permit the resumption of system operations for critical functions when the primary telecommunications capabilities are unavailable.

Ubiquitous use of cellular phones may help defray some of the costs involved in setting up voice telecommunications, but care should be taken to ensure reception at the alternate facility is adequate for operational needs.

Offsite System Backups

The Public Agency should conduct backups of user-level and system-level information and protect backup information from loss, theft, or modification while in transit and at the backup media offsite storage location. The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) shall be consistent with the public agency's recovery time objectives.

Configuration of the hardware environment, operating system, database management system, system software, network infrastructure, etc is equally important to record and rebuild in a disaster scenario.

At a minimum, the Public Agency backup plan includes:

- Daily incremental backups of all critical systems
- Weekly full backups of all critical systems and off-premise media rotation.
- Monthly full backups and off-premise storage for disaster recovery purposes.
- Labeling of backup media to indicate its data classification level.

The public agency should test backup information frequently to ensure media reliability and information integrity.

Post-resumption

Lessons learned workshops should be held immediately following recovery and the results of this lessons learned should add to the public agency's Plan of Action and Milestones (POA&M).

Threats

While this is not a definitive list of the possible threats that exist for IT infrastructure, or a State Agency, it is difficult to prepare a plan to address issues without some thought to the threats that exist today.

- Prolonged Power Outage, more than 1 day, all systems on UPS
- UPS failure/outage, risk of regular system outages due to reliance on mains power
- Flooding in basement impacting Telecom and Power, 7 day outage, complete building evacuation
- Hostage situation, greater than 1 day, complete building evacuation
- Biological situation, complete building evacuation, 7 days
- HVAC failure, partial building evacuation, Data Center Shutdown, 2 day outage
- Telecom failure (Cable cut), 2-3 day outage
- Water supply interruption, partial building evacuation, 2 days
- Fire in building, complete building evacuation, water damage, 1-2 month restoration
- Fire in Data Center, complete building evacuation, water damage, 1-2 month restoration
- Server failure, 1-2 day outage
- Storage Area Network failure, 1-2 day outage
- Denial of Service attack, 1-2 day outage to repair, no remote access
- Virus, 3-5 day outage to repair, no remote access
- Data integrity issue caused by software bug, 3-5 days to repair and re-validate data
- Backup data loss, Systems unavailable while full backup takes place, 4 hours
- Mass Staff Illness, 5-10 days on skeleton staff, potentially all IT staff.