Backup/ Recovery/Contingency Network Server Data

Audit Report # 16-04

August 25, 2016

The University of Texas at El Paso
Institutional Audit Office

"Committed to Service, Independence and Quality"

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UTEP Institutional Audit Office
500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU
WWW.UTSYSTEM.EDU

August 25, 2016

Dr. Diana Natalicio
President, University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited- scope audit of Backup/ Recovery/Contingency Network Server Data. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by Enterprise Computing and Information Security Office staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Dr. Stephen Riter, Vice President for Information Resources and Planning
Mr. Luis E. Hernandez, Director Enterprise Computing
Mr. Gerard Cochrane, Jr, Chief Information Security Officer
Mr. Lethick Leon Cruz, Manager of Systems Support
Ms. Sandy Vasquez, Assistant Vice President for Compliance Services

University of Texas System (UT System):
UT System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

Audit Committee Members:
Mr. David Lindau
Mr. Steele Jones
Mr. Fernando Ortega
Dr. Roberto Osegueda
Dr. Gary Edens

Auditors Assigned to the Audit:
Ms. Victoria Morrison, IT Auditor
Ms. Courtney Rios, Audit Manager

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services (OACS) has completed an audit of the Continuity Planning and Backup/Recovery Operations of the network servers housed at Centralized IT, and managed by the Enterprise Computing Department. The source of the audit criteria is the Texas Department of Information Resources (Texas DIR): "*Security Controls Standards Catalog Version 1.3*" (Texas Administrative Code Chapter 202.76 Security Control Standards Catalog).

The Enterprise Computing Department (EC) performs backups for over 520 servers. Based on the work performed, OACS found that backup/recovery operations generally met the security controls. The Texas DIR set required dates for the implementation of each security control. EC has implemented 100% of the group Media Protection and five out of nine of the group Contingency Planning.

In addition:

- A continuity plan has been developed, but there are some requirements to be met before it is complete.

- An alternate processing site located away from the UTEP's main campus has not been established. UTEP does store the magnetic media (tapes) at an alternate storage site, off campus. The location meets the safeguards to secure the tapes.

- There has been no annual continuity testing or training, to include business users and users with contingency plan roles. The required date of completion was February 2016.

BACKGROUND

Effective March 2015, Texas Administrative Code (TAC) 202 was revised by The Texas Department of information Resources (DIR) to align with the Federal Information Security Management Act (FISMA) rules. The result of this revision was the development of TAC §202.76 "Security Control Standards Catalog," which defines risk statement, APPENDIX A: Security Controls Structure and Family Names (NIST) Control Groups minimum security requirements and implementation guidance for 26 control groups. See

APPENDIX A: Security Controls Structure and Family Names (NIST) Control Groups

This audit covers control group CP-Contingency Planning and MP-Media Protection (See Appendix B: Texas DIR Controls Required by Dates), The report outlines the audit results for contingency planning procedures and policies, alternate sites for processing and storage, backup and recovery of business systems and testing of backup and recovery, and the overall review of the backup/recovery operations.

AUDIT OBJECTIVES

1. To obtain an understanding of UTEP's Disaster Recovery/Contingency plan, policies, and procedures.

2. To determine if mission critical resources have been identified, ranked, have a recovery time objective (RTO) and recovery point objective (RPO) in agreement with business system owners/stakeholders.

3. To determine if UTEP's has an Alternate-Site to continue to process critical mission systems after a threat or disaster has occurred.

4. To determine if UTEP performs Contingency Plan testing and exercises at a scheduled time in accordance with the regulations and information and security policies.

5. To determine if the UTEP operations backup and restore systems are in accordance with the regulations.

SCOPE AND METHODOLOGY

- The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors (IIA).

- The audit addresses the high risk areas identified in the campus wide risk assessments for Fiscal Year (FY) 2015: "Back-up Recovery of Network Servers" and "Alternate Processing Site".

- The audit was limited to network servers running business systems and infrastructure systems managed by UTEP's Centralized IT "Enterprise Computing" located in Union West.

- The criteria used for the audit is Security Control Standards Catalog control groups Contingency Planning with the exception of CP-8, CP11 (communications), and Media Protection, which address the required implementations by February 2016, according to Texas Department of Information Resources (DIR), regulations.

- The audit period was December 2015-May 2016, for any documentation, software and hardware elements.

- Audit procedures included:

  interviewing key personnel,
  reviewing applicable laws, regulations, policies and procedures,
  verifying the existence of appropriate institutional policies and procedures,
  requesting information from key personnel, and
  limited testing.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority - an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

AUDIT RESULTS

1. Disaster/Recovery/Business Continuity Plan

Requirements/Controls

The current requirements governing business/disaster continuity plans are the following:

- Texas (DIR) Security Controls Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog):
  CP-1 Contingency Planning Policy and Procedures… Required by February 2016
  CP-2 Contingency Plan… Required by February 2015

- The University of Texas System Information Resources Use and Security- Policy 165:
  Sec. 9 Backup Recovery of Network Servers and Data.
  "9.1 Backup Requirement. All U. T. System Data, including Data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner (see Section 14).
  9.2 Backup and Recovery Plan. All Data Owners with each Entity shall adopt a backup and recovery plan commensurate with the risk and value of the computer system and Data.

Observations:

- Based on our review of the Continuity of Operations Plan (COOP), we found items that need to be implemented or completed in order to be prepared for internal and external threats. See Appendix C: Threats for list of possible threats.

Recommendation:

UTEP has developed a Continuity of Operations Plan (COOP) for the recovery of mission essential functions. Below are some areas that are still outstanding. For a complete list, see Texas DIR: "*Security Controls Standards Catalog Version 1.3*" (TAC 202.76 Security Control Standards Catalog), sections "*CP-Contingency Planning*".

- The mission critical resources list should be included in the plan itself or referenced to external document(s), (See Appendix D: Mission Critical Resources).
- The written COOP should be approved by management and communicated to key personnel.
- The COOP and all of its external documents should be stored in a safe off-site location.
- Personnel listed in the plan and the University community should be trained on tasks/roles/responsibilities.
- Include in the COOP a list of software and hardware within the plan itself or referenced to external document(s).
- The plan should include "*Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan*".
- Include in the plan itself or reference to external document(s) a list of what would be kept running with limited power or reduced communication bandwidth.
- Include in the COOP references to documentation required for restoration of recovery of mission essential functions.

Both documents, NIST-SP 800-84 and NIST-SP 800-34, can be used as references to create a well-defined COOP.

Level: This finding is considered **Medium,** because the plan has not yet been tested, users have not been trained and the plan has not been communicated to the University community. Failure to process mission critical systems could result in the loss of income or/and reputation to the University.

Management Response:

COOP and all supporting documentation will be compiled on two (2) USB drives. One will be stored in the safe in the Student Business Services office located in the Mike Loya Academic Services building. Once final edits are completed on the COOP, it will be reviewed by the Dr. Riter, the Vice President for Information Resources and Planning. Once approved by him, it will be shared with senior leadership on campus.

All personnel will be trained on their roles and a mock emergency will be scheduled in order to test the plan and its execution.

Responsible Party:

Luis E. Hernandez, Director Enterprise Computing.

Implementation Date:

1/31/2017

2. Alternate Processing Site

Requirements/Controls

The current requirements governing an alternative processing site are the following:

Texas Security Control Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog):

CP-7 Alternate Processing Site (required implementation date: not provided)

> *"a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;*
> *b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and*
> *c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site."*

Observations

UTEP has not established an alternate processing site that permits the restoration of all mission critical resources in a location away from the UTEP campus (primary site). An alternate processing site (secondary site) would not be subject to the same threats or disaster as the primary site. See Appendix C: Threats for list of possible threats.

The funding for the site was obtained in 2016, and UTEP is in the analysis phase of establishing an alternate processing site with the same safeguards as the primary site.

Recommendation:

Identify an alternate site for restoration of all mission or business essential functions away from the UTEP campus (primary site). The alternate site should conform to regulation requirements and best practices.

Alternate site requirement processes are:

- Include necessary agreements to permit the transfer and restoration of UTEP's essential missions/business functions within the defined/agreed recovery time and recovery point objectives, separate from the primary processing site, to reduce susceptibility to the same threats,

- ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site, or contracts/agreements are in place to support delivery to the site within the organization-defined time period for transfer/resumption,
- ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site,
- ensure that the alternate processing site contains all the procedures and documentation needed to recover with little or no loss, and
- ensure that the program includes a strategy to recover and perform full system operations at the alternate facility for an extended period of time.

Level: This finding is considered **Medium** because failure to process mission critical systems could result in the loss of income or/and reputation to the University.

Management Response:

Funding for an alternate site has been secured and options for that site are being evaluated. Part of the criteria for evaluation is balancing the impact of hypothetical disasters with the probability of those disasters occurring and balancing costs of operations and implementation against costs associated with probable disasters. Our goal is to have a cost effective solution identified which meets DIR requirements operational by 1/31/2018.

Responsible Party:

Luis E. Hernandez, Director Enterprise Computing

Implementation Date:

1/31/2018

3. Disaster Recovery/Continuity Testing and Training

Requirements/Controls

The current requirements for disaster recovery/continuity testing are the following:

- Texas Security Controls Standards Catalog Version 1.3 (TAC 202.76 Security Control Standards Catalog):

  CP-4 Contingency Plan Testing (required by February 2015)

  a. "Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

  b. Reviews the contingency plan test results; and

  c. Initiates corrective actions, if needed.

  Implementation: Each state organization's written disaster recovery plan will include provisions for annual testing."

- CP-3 Contingency Training (required by February 2017)

  "The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

  a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
  b. When required by information system changes; and
  c. [Assignment: organization-defined frequency] thereafter."

- The University of Texas System Information Resources Use and Security- Policy 165:

  Sec. 9 Backup Recovery of Network Servers and Data...

  9.2 Backup and Recovery Plan...

  (e) testing backup and recovery procedures

Observations:

IT has successfully performed restores which tested the effectiveness of the backup media and the restore process. For example, in December 2015, the Banner Student Information System was restored using backup media into the original servers. The incident and the process was documented from the initial request to final email notification. Another example was the moving of a server to a new server using backup media.

Based the security control requirements for contingency testing and training, the IT auditor found the following items that still need attention:

- Restore procedures should be written and stored off site to include but not limited to:
  - restore procedures to recover a server,
  - restore procedures for each mission critical resource, and
  - restore procedures for creating another environment.

- Contingency training by testing simulated events, with business user(s) and assigned user(s with Contingency Plan roles/responsibility.

- Schedule annual continuity testing and document the test results that have not been performed.

Recommendation:

OACS recommends the following:

- Create written restore procedures and store them off site. The detail should be sufficient so that a new junior system administrator could perform the restore steps. Written missing procedures to include: recover a server, restore mission critical resources, and how to create another environment. The written procedures should be reviewed yearly.

- Perform a scheduled annual continuity test in order to test and train with business user(s) and assigned users with contingency plan roles/responsibility. Additionally, both the test and test results should be documented.

Level: This finding is considered **Medium** because failure to test recovery of mission critical systems could result in the loss of income and/or reputation to the University.

Management Response:

Restore procedures for critical systems will be included as part of the COOP documentation and tested regularly as part of normal operations.

Responsible Party:

Luis E. Hernandez, Director Enterprise Computing.

Implementation Date:

1/31/2017

CONCLUSION

Based on the work performed, OACS found that backup/recovery operations generally met the security controls. We believe that the University needs some improvement in order to be 100% complaint with Security Control Standards Catalog control group Contingency Planning.

We wish to thank the management and staff of Enterprise Computing and the Information Security Office for their assistance and cooperation provided throughout the audit.

APPENDIX A: SECURITY CONTROLS STRUCTURE AND FAMILY NAMES (NIST) CONTROL GROUPS

Security Control Structure Identifiers and Family Names (National Institute of Standards and Technology (NIST) CONTROL GROUPS/ABBREVIATIONS)

AC Access Control	MA Maintenance
AP Authority and Purpose	MP Media Protection
AR Accountability, Audit, Risk Management	PE Physical and Environmental Protection
AT Awareness and Training	PL Planning
AU Audit and Accountability	PM Program Management
CA Security Assessment and Authorization	PS Personnel Security
CM Configuration Management	RA Risk Assessment
CP Contingency Planning	SA System and Services Acquisition
DI Data Quality and Integrity	SC System and Communications Protection
DM Data Minimization and Retention	SE Security
IA Identification and Authentication	SI System and Information Integrity
IP Individual Participation and Redress	TR Transparency
IR Incident Response	UL Use Limitation

APPENDIX B: TEXAS DIR CONTROLS REQUIRED BY DATE:

Contingency Planning Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	LEGACY TAC 202	REQUIRED BY	Y/N
CP-1	Contingency Planning Policy and Procedures	P1		Feb-2016	Y
CP-2	Contingency Plan	P1	202.24 (a)	Feb-2015	Y
CP-3	Contingency Training	P2		Feb-2017	N
CP-4	Contingency Plan Testing	P2	202.20 (6)	Feb-2015	N
~~CP-5~~	~~Contingency Plan Update~~	~~withdrawn~~			~~n/a~~
CP-6	Alternate Storage Site	P1	202.24 (b)	Feb-2015	Y
CP-7	Alternate Processing Site	P1			N
~~CP-8~~	~~Telecommunications Services~~	~~P1~~			~~n/a~~
CP-9	Information System Backup	P1		Feb-2016	Y
CP-10	Information System Recovery and Reconstitution	P1		Feb-2016	Y
~~CP-11~~	~~Alternate Communications Protocols~~	~~P0~~			~~n/a~~
CP-12	Safe Mode *(list of what is kept running with limited resources)*	P0			N

Y = security controls met

N = security controls not met

n/a = not applicable or not included in this audit.

Media Protection Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	LEGACY TAC 202	REQUIRED BY	Y/N
MP-1	Media Protection Policy and Procedures	P1		Feb-2016	Y
MP-2	Media Access	P1		Feb-2016	Y
MP-3	Media Marking *(labeling)*	P2			Y
MP-4	Media Storage	P1			Y
MP-5	Media Transport	P1			Y
MP-6	Media Sanitization *(disposal of media)*	P1	§202.28	Feb-2015	Y
MP-7	Media Use	P1		Feb-2016	Y
MP-8	Media Downgrading *(removal of data)*	P0			Y

APPENDIX C: THREATS

General IT threats *General threats to IT systems and data include:*	hardware and software failure malware viruses spam, scams and phishing human error cyber attacks
Criminal IT threats *Specific or targeted criminal threats to IT systems and data include:*	hackers fraud passwords theft denial-of-service security breaches staff dishonesty
Natural disasters and IT systems *Damage to buildings and computer hardware can result in loss or corruption of customer records/transactions.*	fire tornado floods winds broken water pipe electrical issues
Services *Damage to utilities or loss of services*	electric gas water phone internet contraction

APPENDIX D: MISSION CRITICAL RESOURCES

Please note that we have given the System Name generic names for reporting purposes and the order was determine by the page sizing. The information below was provided by the IT Systems Support Manager. Note: h=hour, d=day, n/a=not available

System Name	Function	Stakeholder/Owners	Max Tolerable Downtime (MTD)	Recovery Time Objective (RTO)	Work Recovery Time (WRT)	Recovery Point Objective (RPO)
Network Infrastructure	Connectivity of all systems	Students, Faculty, Staff, External Customers	2d	1d	1d	n/a
Business System 01	Student Registration Grade Changes Course additions Financial Aid Web reports	Enrollment Services, Advisors, Graduate School, Cashiering, Int's Students, Students Registrar's Financial Aid Faculty/Staff	3d	1d	2d	1d
Directory Services	Directory Services	Students, Faculty & Staff	2d	1d	1d	1d
Business System 03	Assignment Management	Students & Faculty	1d	8h	16h	1d
Business System 04	Marketplace Bill/Pay Suite Cashiering Payment Gateway	Students, Faculty, Staff & External Customers, Student Business Services Students, Faculty	4d	1d	3d	1d
Exchange Mail System	Mail	Faculty & Staff	1d	8h	16h	1d

System Name	Function	Stakeholder/Owners	Max Tolerable Downtime (MTD)	Recovery Time Objective (RTO)	Work Recovery Time (WRT)	Recovery Point Objective (RPO)
Persons	MIIS - Account creation, activation, provisioning Door Access Identipass\IVIS - Goldcard Parking Decal Sales Access to Swimming and Fitness 9 month appointment Extensions Doctoral Student Extensions OAMS	Faculty, Staff, Students Faculty, Staff, Students, Parking, Key shop, COBA, Biosciences, Miner Village Faculty, Staff, Students, Miner Gold Card office, Ticket Center Parking Swimming and Fitness Faculty Doctoral Students HR, CAOs	3d	1d	2d	1d
Business System 02	Registration Grades/Rosters Advising Transcripts 1098's	Students, Staff Faculty Advisors Students, Alumni Students	3d	1d	2d	1d
Data Warehouse	State Reporting Course Evaluations Cognos Reports Download of active students eligible for Library services Testing Red Flag Appointment Letters	CIERP Faculty, Students Financial Services, VPBA, HR Library Testing Security, VPBA, Compliance Faculty, Staff, Budget	4d	1d	3d	1d

APPENDIX E: DEFINITIONS

Business Continuity Plan (BCP)	A collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster."
Continuity Of Operations Plan (COOP)	Continuity of Operations (COOP), as defined in the National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20), is an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies.
Disaster Recovery Plan (DRP)	is a documented process or set of procedures to **recover** and protect a business IT infrastructure in the event of a **disaster**. Such a **plan**, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a **disaster**.
Business Resumption Plan (BRP)	The business resumption plan addresses restoration of your business after an emergency. Different from the disaster recovery plan and business contingency plan, the BRP does not contain continuity procedures used during an emergency; instead it focuses on preventative measures and after the dust settles. The BRP helps you get your business back into full running order.
Back-Up Recovery Plan:	Backing up data into media for the purpose of recovery data
TAC 202	Texas Administrative Code
Texas DIR	Texas Department of Information Resources
IT Continuity Planning	The process that ensures continuous operations of business applications and supporting IT systems (i.e., desktops, printers, network devices). IT continuity planning is a subset of enterprise business continuity planning. A business continuity plan is an enterprise wide group of processes and instructions to ensure the continuation of business processes in the event of an interruption.