Chief Information Office

IT General Controls Assessment
NetPlus

Internal Audit Report
19-101

April 2019

Department of Information Resources

Internal Audit Mission Statement

To collaborate with DIR leadership to fulfill the agency's core mission by providing independent and objective audit services designed to add value and improve the effectiveness of risk management, control, and governance processes.

DIR Internal Audit Staff

Cathy Sherwood, Interim Internal Audit Director

Vicky Yang, Staff Auditor (Intern)

Victoria Lei, Staff Auditor (Intern)

Table of Contents

Executive Summary

This report summarizes the scope, results, and recommendations from the work performed in conducting the Information Technology (IT) General Controls Assessment for NetPlus, the application used to bill Department of Information Resources (DIR) customers for telecommunications services.

The audit was performed as part of the Fiscal Year 2019 Internal Audit Annual Plan. The **audit objective** was to assess whether IT general controls were properly designed and working as intended. The **audit scope** included user access and configuration management controls from September 1, 2018 through April 1, 2019. See details about the **scope and methodology** for this audit in the Background section of this report.

Overall, improvements to IT general controls were identified and communicated to DIR management. Certain user access and configuration management controls could be strengthened to ensure that access is revoked for terminated account holders timely, privileged account access is restricted and monitored, password policies are consistent with agency policy, and more formalized configuration management processes are established to avoid the risk of one initiating and executing unauthorized changes that go undetected.

Based on the results of audit work performed, Internal Audit recommended that standard operating procedures be developed for IT general controls to support efforts to ensure integrity and reliability of the system and to secure underlying call data supporting telecom billing. Issues were reported in two main categories: user access controls and configuration management in the detailed report.

User Access Controls

- The account management process should ensure that all terminated user accounts are properly deactivated in the system timely and that appropriate access levels are assigned in NetPlus based on the employee's role in the organization.
- Procedures should be established to ensure that privileged user accounts are monitored, especially when one individual is tasked with managing the application.
- NetPlus password policy should align with the agency level password policy.

Configuration Management

- Standard operating procedures should be established to include a requirement for formal change requests for any changes classified as a system enhancement managed by a DIR change control board.

Background

Communications Technology Services (CTS) is a core program authorized by Texas Government Code (TGC) Chapter 2170, supporting statewide voice, video, and data services through the state's communications system, the Texas Agency Network (TEX-AN). Under Texas statute (TGC §2170.004), DIR is authorized to offer TEX-AN services to a broad range of government and other entities that voluntarily take advantage of TEX-AN's reduced pricing. These voluntary customers include institutions of higher education, public schools and assistance organizations, as well as city and county governments.

DIR customers can download their monthly invoice via NetPlus portal. Each agency customer is allowed access for multiple users, each with a unique ID and password. It is an important objective of NetPlus to ensure that DIR customers (state and local governments, public schools and higher education) can timely and securely access their monthly telecom invoices with accurate, protected information.

This audit project was performed as part of the Fiscal Year 2019 Internal Audit Annual Plan. The **audit objective** was to assess whether IT general controls were properly designed and working as intended. The **audit scope** included user access and configuration management control activities from September 1, 2018 through April 1, 2019.

The **audit methodology** included:

- Conducting interviews with the NetPlus System Administrator and selected users,
- Reviewing relevant system documentation, DIR standard operating procedures, relevant criteria, such as Federal Information Security Controls Audit Manual (FISCAM), Global Technology Audit Guide (GTAG), and NIST SP800-53,
- Comparing established controls with industry criteria
- Reviewed NetPlus password policy to compare with DIR password policy, and
- Reviewed NetPlus user accounts (active and deactivated user) to compare with current and terminated employees.

We conducted this performance audit in conformance with the International Standards for the Professional Practice of Internal Auditing and in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our issues and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

Detailed Results

Overall, improvements to IT general controls were identified and communicated to IT Services management. Certain user access and configuration (change) management controls could be strengthened to ensure that:

- Password policies are consistent with agency policy. We recommended that IT Services management update the NetPlus password policy and related settings in NetPlus to ensure consistency with DIR agency-wide password policies.
- User access is modified appropriately when account holders change jobs within the organization. We recommended that DIR Human Resources expand their onboarding and exit notification process to include employee job/role changes.
- More formalized change management processes are established to avoid the risk of one initiating and executing unauthorized changes that go undetected. We recommended that IT Services management document a standard operating procedure and require all NetPlus system changes be tracked as part of an agency-wide process.

System Deactivations Were Effectively Managed

Internal Audit requested and reviewed lists of active and inactive user accounts from the NetPlus system administrator as well as employee details from DIR Human Resources. We reviewed both employees with termination dates September 1, 2018 and March 4, 2019 and employees who changed jobs within the organization between September 1, 2018 and March 4, 2019.

From the list of all DIR employees from Human Resources, there were six (6) terminations reviewed. Internal Audit validated that each user account was deactivated in NetPlus, but there was no date and time stamp to validate whether the action was performed timely. To ensure that the system had not been accessed by these account holders after the employee termination date, the Last Login Date was reviewed. All six accounts were deactivated in NetPlus, and all Last Login Dates were before the Termination Date.

Terminated Employees	Was System Access Removed? (Y/N)	Last Login Date	Termination Date	Was the Last Login Date before the Termination Date? (Y/N)
Employee 1	Y	12/18/2018	1/1/2019	Y
Employee 2	Y	10/26/2018	11/01/2018	Y
Employee 3	Y	10/12/2018	10/15/2018	Y
Employee 4	Y	10/22/2018	11/01/2018	Y
Employee 5	Y	04/01/2015**	03/01/2019	Y
Employee 6	Y	04/25/2017**	01/24/2019	Y

For Employee 5 and 6, the Last Login Date was over two years before the employee's termination date. Internal Audit recommended that management consider revoking access for any accounts not accessed in over six (6) months and requiring a new request for access after that time.

Agency-wide IT General Controls

Several key recommendations were made to improve processes that will help strengthen IT general controls. Some of the high and priority recommendations that could also be applied to all DIR managed systems included:

- Establish a standardized user access authorization process to ensure timely modification of user accounts when DIR employees move from one role to another within the organization.
- Conduct and document periodic access reviews to:
    - Identify terminated and inactive users who may not be deactivated in the system, and
    - Ensure active account holders have a valid business purpose for accessing the system.

  As part of the periodic access review, identify and resolve potential segregation of duties issues that result from existing roles across the agency.
- Consider revoking access for accounts that have not been accessed for over six months, or some other term deemed appropriate by IT Services standard operating procedures.
- Establish agency level policy for the authorization to set up privileged user accounts, including those used to run routine periodic jobs.
- Determine appropriate monitoring responsibility of privileged user activity logs.
- Develop criteria to categorize system changes into a) standard changes which are low to zero risk, usually related to routine maintenance and b) system enhancements where new features or performance enhancements are added to the system. Set up requirements for the authorization, testing, approval, implementation and documentation for standard changes and system enhancements.

DIR management concurred with the results and recommendations reported by Internal Audit and provided action plans, estimated completion dates, and assigned responsibility to management staff for implementing the recommendations.

Risk ratings are described below.

Issue Rating	Description of Rating
Low	The audit identified strengths that support the agency's ability to administer the activity audited or the issue identified does not present a significant risk or effects that would negatively affect the agency's ability to effectively administer the activity audited.
Moderate	The issue identified presents risks or effects that if not addressed could moderately affect the agency's ability to effectively administer the activity audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.
High	The issue identified presents risks or effects that if not addressed could substantially affect the agency's ability to effectively administer the activity audited. Prompt action is essential to address the noted concern(s) and reduce risks to the agency.
Priority	Issues identified presents risks or effects that if not addressed could critically affect the agency's ability to effectively administer the activity audited. Immediate action is required to address the noted concern(s) and reduce risks to the agency.

Section 1: User Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure.

Issue 1: Periodically Review User Access Levels in NetPlus

Element of a Finding	Results
Condition	User access roles granted to DIR employees were not always aligned with their current role in the agency. NetPlus active user roles did not always reflect changes in an account holder's job (agency role and responsibilities). For example: • At least three (3) active users have current access levels that are not needed. • Out of the 73 NetPlus active users, 32 had a Last Login Date before September 1, 2018, indicating that they no longer had a need for user access. In addition, one NetPlus vendor account holder has the same user access level as the DIR system administrator.
Criteria	FISCAM[1] (Access Control Section AC-3.1.5) Resource owners periodically review access authorizations for continuing appropriateness. FISCAM (Access Control Section AC-3.1.6) Access is limited to individuals with a valid business purpose (least privilege). FISCAM (Access Control Section AC-3.1.7) Unnecessary accounts are removed, disabled, or otherwise secured.
Cause	Some users were granted a specific access level on a project basis. No formal policy is in place to inform the system administrator about changes to user access levels when account

[1] The Federal Information System Controls Audit Manual (FISCAM) presents a methodology for auditing information system controls in federal and other governmental entities. This methodology is in accordance with professional standards.

	holders change jobs/roles or when they no longer need a specific access level when they are finished with projects.
Effect	With inappropriate user access level, individuals can perform incompatible functions or functions beyond their responsibility in NetPlus. They can make unauthorized changes that are outside their job duty or gain access to information that should not have been viewed based on their job duty.
Audit Recommendations	Update the current user activation policy to ensure processes are in place for creating user accounts, assigning roles, monitoring usage and system activity, updating user account profiles, and revoking user access levels, as appropriate. Specifically, Internal Audit recommends that IT Services: A. Establish a process to conduct formalized periodic reviews that include documented input from the employee's manager of record about whether the active accountholders in NetPlus need the level of access granted. Procedures should include standardized procedures to a) request user access with a description of system role(s) that the account holder needs, b) change the level of access for an account holder who has changed jobs within the organization, and c) request user account deactivations for terminated employees or for those who no longer need access to the system. B. Deactivate all activate users who have last login date older than six months.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).
Action Plans	IT Services will: • Will use the Salesforce ticket system to remove internal user access when a user's role changes, or they separate from the agency.

	• Remove access for user accounts where last login dates are prior to September 1, 2018.
Planned Implementation Date	Implemented August 31, 2019
Responsible Leadership	DIR IT Services Director

Issue 2: Ensure Password Policy Aligns with Agency Password Policy

Elements of a Finding	**Results**
Condition	Currently, NetPlus password policy is not configured consistently with DIR password policy. The only active password policy in NetPlus is the password length requirement of minimum 6 characters, which is also not in accordance with DIR password policy.
Criteria	DIR password policy requires that at a minimum, a password must: • Be a minimum of 10 alpha/numeric/special characters • Be set to be changed after 180 days • Not be a word or words found in a dictionary • Not be in all or part a common name such as the User's last name or children's names, or the name of a favorite sports team or pet, etc. • Not be an acronym or term used by the state or DIR or be the User ID for any account • Not be reused for a minimum period of six cycles from its last use
Cause	All information in the system is subject to open records requests under the Public Information Act, and the NetPlus system

	administrator indicated that no proprietary information is stored and that a stronger password policy would lead to more time spending on resolving password resets for users who get locked out of the system.
Effect	NetPlus passwords might not be robust enough and might be guessed or disclosed easily, leading to unauthorized access to the system.
Audit Recommendations	The IT Services Director should update the NetPlus password policy and related settings in NetPlus to align requirements with agency level password policies.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).
Action Plans	IT Services will update current NetPlus password policy to align with DIR password policy for internal users.
Planned Implementation Date	December 31, 2019
Responsible Leadership	DIR IT Services Director

Issue 3: Monitor Administrator User Account Activity

Elements of a Finding	**Results**
Condition	The NetPlus administrator role is given to 18 users (13 active and 5 deactivated) who are not all system administrators. Of the 13 active administrator accounts, 8 are vendor default accounts, 3 are active DIR user (2 NetPlus administrator and 1 BMC Remedy administrator) 1 is the backend user who configurate the application and 1 is vendor account.

	Furthermore, there is currently no monitoring of the activity logs for these privileged accounts
Criteria	FISCAM (Access Control Section AC-4.1.1) Access to sensitive/ privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose. FISCAM (Access Control Section AC-4.1.3) Use of sensitive/ privileged accounts is adequately monitored.
Cause	All of the vendor accounts, with the exception of one, are obsolete and were in place when the application was Unix based. The one vendor account that is not obsolete is used by the NetPlus vendor when the DIR system administrator requests investigation of engineering issues. An administrator account is required for the operation of background jobs running independent of an operator input. NetPlus does not have separate logs for privileged accounts but only an overall log for the whole system.
Effect	Granting inappropriate privileged administrator roles to employees and lacking monitoring of the use of privileged accounts can cause failure to identify inappropriate or unusual behavior which may indicate unauthorized access or an individual who is improperly exploiting access privileges.
Audit Recommendations	DIR management from the Information Technology Services (ITS) should: A. Establish policies to approve the authorization for privileged accounts, B. Determine appropriate monitoring responsibility of privileged user activity logs, and C. Deactivate obsolete vendor default accounts.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).

Action Plans	IT Services will • Establish policies to ensure administrator access is assigned appropriately. • Deactivate obsolete administrator accounts.
Planned Implementation Date	Obsolete accounts were deactivated. Policies will be established by August 31, 2020.
Responsible Leadership	DIR IT Services Director

Section 2: Configuration Management

Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle.

Issue 4: Establish a Configuration Management Policy for NetPlus

Element of a Finding	**Results**
Condition	NetPlus lacks a clear policy that regulates the authorization, testing, approval, implementation and documentation of the configuration or other system changes. Some changes are documented while others are not. There is also no clear segregation of duties in change process.
Criteria	FISCAM (Configuration Management Section CM-3.1) All configuration changes are properly managed (authorized, tested, approved, and tracked). FISCAM (Configuration Management Section CM-3.1.1) An appropriate formal change management process is documented. FISCAM (Configuration Management Section CM-3.1.2) Configuration changes are authorized by management. Configuration management actions are recorded in sufficient

	detail so that the content and status of each configuration item is known, and previous versions can be recovered. GTAG[2] Change Management 5.3.3.3 suggest that proper change management processes should be enforced to ensure that changes to the IT environment, systems software, application systems, and data are applied in a manner that enforces appropriate segregation of duties; ensures that changes work and are implemented as required; and prevents changes from being exploited for fraudulent purposes.
Cause	System administrator indicates that small changes would not need formal authorization/testing/ documentation because they are just system enhancements.
Effect	Unauthorized changes could be introduced into the production environment without being detected.
Audit Recommendations	DIR management from the Information Technology Services (ITS) should: A. Develop criteria to categorize changes into a) standard changes which are low to zero risk, transparent to all users and are usually related to routine maintenance and b) system enhancement where new features or performance enhancements are added to the system. B. Set up requirements for the authorization, testing, approval, implementation and documentation for standard changes and system enhancement.
Management Response	
Statement of Agreement	Management agreed with internal audit recommendation(s).

[2] Global Technology Audit Guides (GTAGs) describe relevant risk and control frameworks so that governing bodies, executives, IT professionals, and internal auditors can address significant IT-related risk and control issues.

Action Plans	Management will develop criteria to categorize changes into a) standard changes which are low to zero risk, transparent to all users and are usually related to routine maintenance and b) system enhancement where new features or performance enhancements are added to the system. In addition, they will establish requirements for the authorization, testing, approval, implementation and documentation for standard changes and system enhancements.
Planned Implementation Date	December 31, 2019
Responsible Leadership	DIR IT Services Director

Report Distribution

Internal Report Distribution

Department of Information Resources (DIR) Board

DIR Executive Director

DIR Deputy Executive Director and Texas Chief Information Officer

DIR IT Services Director

External Report Distribution

Texas Office of the Governor

Texas Legislative Budget Board

Texas State Auditor's Office

Texas Sunset Advisory Commission