Internal Audit Report

Identity Access Management

Todd Wilkins, CISA, CRISC

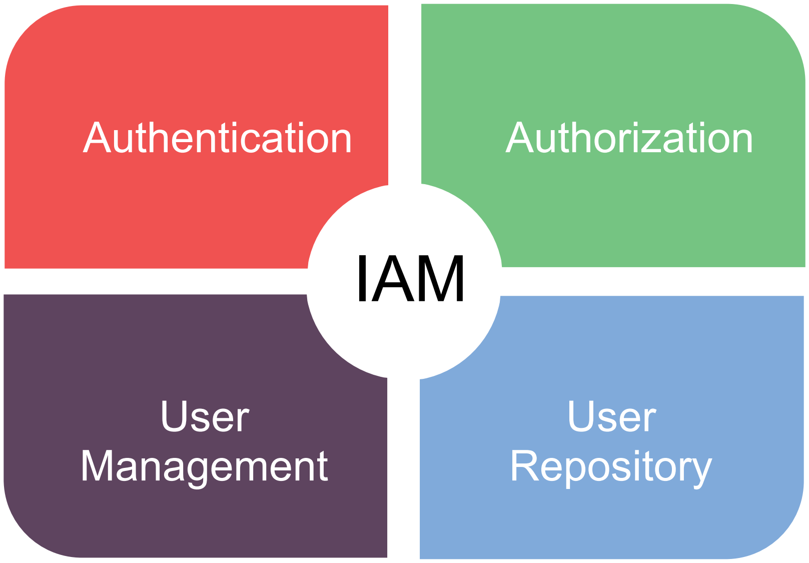
2022

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR

1. Executive Summary

Objective

Management's objectives with the Information Technology function are to ensure critical infrastructure is safeguarded from intrusion and inadvertent internal disruptions while also protecting the confidentiality, integrity, and availability, the CIA security triad, of the agency's information asset. At the heart of safeguarding the agency's information asset are the mechanisms (user names and passwords) used to provision access to the agency's information asset is properly provisioned, controlled, and managed. This is known as Identity Access Management (IAM). IAM is a framework of processes, policies, and technologies that facilitates the management of account identities and resource access.



Background

A consistent topic emerges during the 2019 IT Audit Plan which encompasses the management of identities (users) and access (resources) for both administrators and external users. A separate audit is originally anticipated for each unique type of user. However, we discover during initial planning and scoping brainstorming that similar controls and processes are used regardless of user type and we determine to group these audit projects into a single audit in hopes of lightening the load on IT staff and resources.

We consider administrators to be IT users with elevated privileges to manage a system by being able to perform actions and functions not awarded to common users. We consider external users as any user account that is provisioned for individuals who are not considered DOT employees by ordinary rights and privileges as an agency employee, namely their actions are not governed by the Human Resources employee manual.

Results

Observations, recommendations, and management action plans are developed and discussed with SCDOT Executive Leaders. This information is not included in this report due to the confidential nature of information security and is closed to public release by SC Code of Laws Section 30-4-20 (c).

Contents

2. Forward

Authorization

The South Carolina Office of the State Auditor established the Internal Audit Services division (IAS) pursuant to SC Code Section 57-1-360 as revised by Act 275 of the 2016 legislative session. IAS is an independent, objective assurance and consulting function designed to add value and improve the operations of the South Carolina Department of Transportation (SCDOT). IAS helps SCDOT to achieve its objectives by bringing a systematic, disciplined approach to evaluating the effectiveness of risk management, internal control, and governance processes and by advising on best practices.

Statement of Independence

To ensure independence, IAS reports administratively and functionally to the State Auditor while working collaboratively with SCDOT leadership in developing an audit plan that appropriately aligns with SCDOT's mission and business objectives and reflects business risks and other priorities.

Report Distribution

This report is intended for the information and use of the SCDOT Commission, SCDOT leadership, the Chairman of the Senate Transportation Committee, the Chairman of the Senate Finance Committee, the Chairman of the House of Representatives Education and Public Works Committee, and the Chairman of the House of Representatives Ways and Means Committee. However, this report is a matter of public record and its distribution is not limited.

Acknowledgement

We wish to thank members of management and staff in the Information Technology Services Division for their cooperation in assessing risks and developing actions to improve internal controls and enhance operating performance.

Lead Auditor

Todd Wilkins, CISA, CRISC
Senior Manager

Reviewer

Mark LaBruyere
Director of Internal Audit Services

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR
1401 Main Street, Suite 1200 • Columbia, SC 29201

3. Internal Auditor’s Report

June 24, 2022

Ms. Christy A. Hall, Secretary of Transportation
and
Members of the Commission
South Carolina Department of Transportation
Columbia, South Carolina

We have completed the review of the Agency’s Identity and Access Management (IAM) for External and Privileged Users. The overarching objective of this review was to assess the risk surrounding identity and access activity while also determining the completeness of controls for safeguarding Agency’s information. The results of our analysis are included in the Analysis Results section beginning on page 8.

We planned and performed the engagement with due professional care in order to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and recommendations. Our observations, recommendations, and management’s action plans were discussed with management.

George L. Kennedy, III

George L. Kennedy, III, CPA
State Auditor

4. Engagement Overview

Background

SCDOT is reliant upon technology solutions to help further the agency's mission in a more effective and efficient manner. The primary security controls for any of these technologies rely on effective Identity and Access Management (IAM) controls. These controls are designed to uniquely identify access accounts on any given system. The system should be designed in a manner to grant or deny access authorization based on authentication criteria and track actions through logging mechanisms. The strength of the Identity and Access controls will, in some manner, illustrate the security posture for IT Systems as these are foundational technology controls.

SCDOT does not utilize restricted data to perform its core objectives. While most of SCDOT's information is available for request by the public under the Freedom of Information Act; SCDOT possesses data that falls under the "Internal Only" and "Confidential" data classifications. This data is held as Public Trust, which means that SCDOT must protect this information to maintain agency reputation and taking due care responsibility.

PUBLIC	INTERNAL ONLY	CONFIDENTIAL	RESTRICTED
Data that may be freely disclosed to the public	**Internal data not meant for public disclosure**	**Sensitive data that if compromised could negatively affect operations**	**Highly sensitive corporate data that if compromised could put the organization financial or legal risk**
Marketing Materials Contact Information Price Lists etc	Battlecards Sales Playbooks Organizational Charts etc	Contracts with Vendors Employee Reviews etc	IP Credit Card Information Social Security Numbers PHI

Objective

Management's objectives with the Information Technology function are to ensure that critical infrastructure is safeguarded from intrusion and inadvertent internal disruptions while also protecting the confidentiality, integrity, and availability of the agency's information asset. At the heart of safeguarding the agency's information asset is to ensure the mechanisms (usernames and passwords) used to provision access to the agency's information asset is properly provisioned, controlled, and managed.

Our objectives in this engagement are as follows:

- Determine if the appropriate identification and access management controls are addressed through policy and its implementation.
- Determine if the appropriate risk management practices are employed to identify, track, and mitigate Identity and Access Management risks.
- Determine if the appropriate identification and account management methodologies are strategically and practically implemented.

Our engagement primarily focused on Identity and Access Management processes within Information Technology (IT) but also included overlapping processes within Human Resources (HR) and other business units. Internal Audit Services (IAS) collaborated with process owners to identify opportunities where processes and or controls were not implemented properly or effectively.

In short, the goal of the review was to assess whether the appropriate controls and processes were in place to provide the right people with the right access to the right information at the right time.

Scope

The triggers for initiating an IAM request such as a new account or account disablement occur outside of IT (i.e. new hire and termination). IT is responsible for processing the request and setting access permissions correctly. All approved requests come through as a help desk ticket and are assigned to a technician to create a new account or modify an existing account. A single access request could potentially require additional requests depending on services or access to permit/ deny. When this happens, multiple IT workgroups must work in concert to adequately set access permissions

The help desk, under End User Services is the hub for collecting IAM requests and is responsible for distributing the requests through the help system. Each spoke in the process ties into the help desk system for tracking ticket details of the request.

During planning, IAS and IT collaboratively dissected the IAM process into parts categorized on action and purpose. The following process parts were assessed for riskiness:

- Account creation
- Account modification
- Account removal
- Account re-certification
- Account resets
- Account maintenance

Based on the identified process and workflow, IAS evaluated a subset of controls based on the risk rankings from the following security control families:

- AC – Access Control
- AU – Audit and Accountability
- IA – Identity and Authentication
- PS – Personnel Security
- SI – System and Information Integrity

The review process involved interviews to gain a better understanding of the current control environment which included the extent controls were implemented. Based on risk, a walkthrough and control tests were performed to evaluate the effectiveness of high-risk controls.

Out of Scope

Specifically, this review evaluated the implementation of Identity and Access Management controls as they related to only administrative or external user accounts. Thus, service accounts and regular internal user account controls were not evaluated.

Although on-boarding and off-boarding processes were considered in scope, we only evaluated the process and controls which are intended for SCDOT. Any part of the process or control which is expected to be implemented externally was not considered within our scope

Approach

We have leveraged IAS' 2019 IT audit for DIS-200 compliance. This audit first evaluated current policies that cover identity and access control. Because the 2019 audit used NIST 800-53 r4 as a baseline, this audit will also use this document even though a more recent version is available. Furthermore, the Agency has not pursued using the more recent edition of the standard.

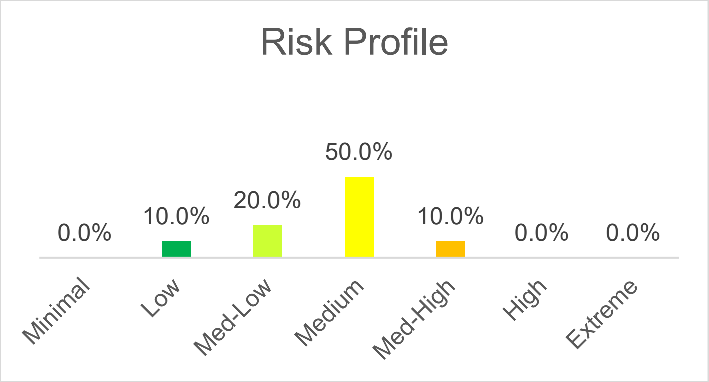
Now that IAS has ascertained an understanding of the policy environment, the audit pivots to review the current procedures in place for identity and access management. The processes under review spanned the identification and access management life cycle starting with requests and ending with removal or deletion of accounts. At this point, IAS has taken a second pivot to examine risks and controls in place to safeguard the information asset.

5. Analysis Results

Identity Access Management Controls

IAM Purpose: To safeguard the confidentiality, integrity, and availability of information by granting users an appropriate level of access to information resources at the appropriate time.

Inherent Risk: The Department of Administration Technology Division identified a list of nine risks associated with user access. We adopted this list of risks as our baseline for risk identification. We facilitated management's assessment of inherent risk for the IAM process. The Risk Profile chart shows the inherent risk for IAM which is "Medium". It should be noted that inherent risk doesn't take into consideration the implementation of a control – only the risk that is present for operating in the current environment. We utilized the inherent risk score to focus our testing on primary controls which covered the Medium or higher risks.



Observations and Recommendations

We collaborated with IT Services and Security Management to develop the observations and recommendations for remediating any discovered deficiency. IAS and SCDOT Executive Leaders discussed these observations and recommendations.

Development of Management Action Plans

IAS facilitated Management's development of action plans for any identified observation to improve control design with practical, cost-effective solutions. These improvements, if effectively implemented, are expected to reduce the overall risk exposure to an acceptable level (i.e. within the Agency's risk appetite).

We will follow up with Management on the implementation of the proposed actions on an ongoing basis and provide SCDOT leadership with periodic reports on the status of management action plans and whether those actions are effectively and timely implemented to reduce risk exposure to an acceptable level.

Reporting of Confidential Information

Due to the confidential nature of information security, the observations, recommendations, and management action plans are not included in this report. This information is not considered or deemed "public record" in accordance with the SC Freedom of Information Act pursuant to SC Code of Laws Section 30-4-20 (c) which states that information relating to security plans and devices proposed, adopted, installed, or utilized by a public body, other than amounts expended for adoption, implementation, or installation of these plans and devices, is required to be closed to the public and is not considered to be made open to the public under the provisions of this act.