# Facility Physical Security

Todd Wilkins, CISA, CRISC

**2024**

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR

# 1. Executive Summary

## Objective

Management's objectives for the Information Technology (IT) include safeguarding critical infrastructure from intrusion and internal disruptions, while protecting the confidentiality, integrity, and availability of agency information assets. The audit aims to ensure adequacy and effectiveness in governance, internal controls, and risk management practices related to physical security. It assesses:

- Governance roles and responsibilities for physical security.
- Physical security risk management processes.
- Adequacy of physical access controls to facilities, information, and technology assets.
- Employee awareness and compliance with physical security policies and directives.

## Background

The South Carolina Department of Transportation (SCDOT) employs approximately 3,800 individuals, making it the third-largest state agency in South Carolina as of March 2024. With 250 facilities spread across the state, SCDOT serves as key hubs for information storage and processing. Recognizing the importance of data-driven decisions, SCDOT has recently prioritized the establishment of a Data Governance function to enhance data management processes, viewing information as a valuable asset requiring protection.

Effective physical security programs within organizations yield several expected outcomes:

- Governance structures and resources are established to manage security across all agency facilities efficiently.
- Key departments, including Legal, Human Resources, Public Relations, Security, IT Security, and Facility Management, effectively coordinate security efforts and manage risks.
- Consistent security and identity management practices facilitate interoperability and information exchange.
- Continuity of operations and services is maintained during security incidents, disruptions, or emergencies.

To ensure effective physical security, SCDOT must adopt a collaborative, coordinated, and monitored approach. Implementing a framework such as the National Institute of Standards and Technology 800-53 or Controls Objectives for Information Technologies (COBIT) will streamline and enhance the physical security program.

## Conclusion

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 who collaborated with us. We visited the following facilities: Calhoun, Fairfield, Headquarters, Lexington, Newberry, Orangeburg, and Richland. Because of their efforts and cooperation, we were able to assess risks and develop actions to improve internal controls and enhance operating performance.

## Lead Auditor

Todd Wilkins, CISA, CRISC
Senior Manager

## Auditor

Pamela Johnson
Audit 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

July 22, 2024

Mr. Justin P. Powell, Secretary of Transportation
and
Members of the Commission
South Carolina Department of Transportation
Columbia, South Carolina

We have completed the review of the South Carolina Department of Transportation's (SCDOT's) Facility Physical Security Program. The overarching objective of this review was to assess the risk surrounding sensitive information, both physical and digital, while also determining the completeness of controls for safeguarding agency's information asset. The results of our analysis are included in the Conclusion section beginning on page 9.

- Facilitation of Management's assessment of risks associated with the Facility Physical Security activity.
- Independent assessment of the design and effectiveness of internal controls to determine whether those controls effectively manage the identified risks to an acceptable level.

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 collaboratively developed with management.

George L Kennedy, III

George L. Kennedy, III, CPA
State Auditor

# 4. Engagement Overview

## Background

Physical security is defined as the security measures designed to deny unauthorized access to facilities, equipment, and resources, with the goal of protecting personnel and property from damage or harm. This working definition combines elements from various sources to describe the key principles of physical security. When physical security is properly implemented and managed, these security measures will help to:

- Safeguard information, assets, and services.
- Protect employees and staff.
- Establish governance structures for effective security management.
- Manage security incidents.
- Facilitate interoperability and information exchange.
- Maintain continuity of agency operations in the face of security incidents, disruptions, or emergencies.

It is imperative that the agency adopts a collaborative, coordinated, and monitored approach to support the effectiveness of its physical security measures. As previously outlined in the executive summary, physical security encompasses the implementation of security measures designed to deny unauthorized access to facilities, equipment, and resources, thereby safeguarding personnel and property from harm or damage. To achieve this goal, the agency should rely on established frameworks such as NIST 800-53 or COBIT, which integrate various functions and elements of security into a cohesive strategy. By leveraging such frameworks, the agency can enhance the efficiency and effectiveness of its physical security program, ensuring the protection of information, assets, and personnel against security threats and risks.

While the working definition of physical security recognizes the protection of different categories of assets, it's important to note that this audit was specifically scoped to focus solely on the agency's digital and physical information assets. The agency is entrusted with the responsibility of safeguarding its valuable digital and physical information assets. To achieve this, it must carefully assess and determine the most cost-effective strategy for implementing a comprehensive physical security program tailored specifically to protect these information assets across all its facilities and buildings. We do suggest management take a holistic approach to physical security which includes all the different categories of assets and not to focus on a specific category or asset as this audit does.

In recognition of this priority of effectiveness and efficiency, the audit, at the request of agency management, was scoped to focus solely on digital and physical information assets. Therefore, while physical security encompasses a broader range of considerations, including personnel safety and protection of other assets, the audit's scope was limited to assessing the effectiveness of security measures related to information assets.

The federal government has provided guidelines and a security framework, such as NIST 800-53, which are mandatory for federal facilities and highly suggested for state agencies. While these resources can serve as valuable tools for our agency, management retains the discretion to tailor implementation to the agency's specific needs and priorities.

## Objective

Management’s objectives with the Facility Management function are to ensure that critical physical infrastructure is safeguarded from intrusion and disruptions while also protecting the agency's assets housed at each facility including personnel. However, this audit focused primarily on a single asset - information.

This is expressed through these three components:

- Determine if the appropriate physical security program management controls are addressed through policy and its implementation for protecting the agency’s information asset.
- Determine if the appropriate risk management practices are working to identify, track, and mitigate physical security program management risks for protecting the agency’s information asset.
- Determine if the appropriate physical security program management methodologies are strategically and practically implemented for protecting the agency’s information asset.

Our objective is to provide assurance that internal controls are adequately designed and operating effectively to manage risks that may hinder the achievement of Management’s objectives for the Facility Physical Security activity.

## Scope

The scope of the audit included SCDOT headquarters facility located at 955 Park St., Columbia, SC, two SCDOT district offices, five SCDOT County offices, and one lab. The scope included information and technology assets contained in these facilities. Specific physical and environmental controls were selected based on a minimum protection philosophy established by NIST. These controls, with the exception of one, are also included in the DIS-200 catalog of controls.

The review process mainly revolved around interviews and walkthroughs to gain a better understanding of the current control environment including the extent to which controls are implemented. Based on risk, a closer examination of controls helped determine the effectiveness of the implemented controls.

During planning, IAS and Facility Management collaboratively dissected the facility physical security program into parts categorized by activity and purpose. The following process parts were assessed for risks:

1. Planning Facility Physical Security Requirements
2. Assessing Facility Physical Security Risks
3. Implementing Facility Physical Security Requirements
4. Monitoring Facility Physical Security

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

- PE – Physical and Environmental

There are twenty-three (23) controls under the PE family; however, due to SCDOT's environment and risks, we evaluated nine (9) of these controls.

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 engagement only evaluated the implementation of physical security program management controls as they relate to protecting the agency's information asset, both electronic and physical which also included technology components physically installed at local sites. Buildings or facilities where data is not stored, transferred, or processed such as parking garages were excluded from scope.

## Approach

**Control Selection**

The South Carolina Department of Administration (Admin) established the Division of Information Security (DIS) in response to the 2012 data breach at the South Carolina Department of Revenue. DIS developed the State's security standard, DIS-200, based on NIST Special Publication 800-53 r4, released in January 2015. However, both DIS-200 and its underlying framework are nearly a decade old. Furthermore, no updates to DIS-200 have been made since its release in 2015.

Today there is a newer revision to the NIST 800-53. The most recent revision, NIST 800-53 r5, was finalized in December 2020. R5 reflects advancements in technology and addresses evolving risks which the previous revision doesn't. The updated standard provides a more current and robust framework for managing security.

Despite the absence of an official designation of NIST 800-53 as a standard by agency management, the agency's technology policies explicitly reference compliance with NIST standards. This acknowledgement suggests an implicit adoption of NIST as the agency's security standard. As such, it was logical for IAS to consider NIST 800-53 as the appropriate baseline for the evaluation of control standards. Keep in mind, the use and adoption of NIST 800-53 does not replace DIS-200 but rather enhances it.

In a previous audit conducted by Internal Audit Services (IAS) in 2019 addressing the agency's compliance with DIS-200, NIST controls were utilized in our evaluation, and communication with management was conducted using NIST control language. Notably, during this physical security audit, the physical security controls under scope were mapped from DIS-200 to both NIST 800-53 r4 and r5. The control language was unchanged between the two NIST 800-53 revisions for the controls under scope. Therefore, if the agency were in compliance with NIST 800-53 r4 for the controls in the scope of the audit, the agency would be also compliant with NIST 800-53 r5 for the same controls.

Internal Audit Services (IAS) will continue to advocate for the adoption of NIST 800-53 r5 as the baseline for control standards, leveraging the precedent set in past audits and emphasizing the benefits of aligning with the latest industry standards to mitigate evolving technology risks.

**Audit Standard**
Internal Audit Services (IAS) performed the audit in accordance with the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing, as outlined in the International Professional Practices Framework (IPPF), and conformed to the Internal Auditing Service (IAS) Standards.

**Audit Planning**
The planning phase of the audit included preliminary interviews and the collection and review of documentation in order to understand the current state of security management within the agency's facilities. The audit program was then designed and based on the information gathered during planning.

**Audit Fieldwork**
During the fieldwork phase of the audit, the audit team conducted interviews, observed the physical safeguards in different areas and locations listed above, and assessed current security practices against DIS-200 and NIST 800-53 r5.

## Methodology

For the processes included in the engagement scope, we performed the following procedures:

1. We facilitated Management’s completion of a process narrative that documents the steps in the process and the individuals responsible for those steps.
2. We facilitated Management’s completion of a risk and control matrix used to:
    a. Identify risks which threaten process objectives;
    b. Score the risks as to their consequence and likelihood of occurrence using the risk scoring matrix in Appendix B;
    c. Determine if controls are adequately designed to manage the risks to within the agency’s risk appetite; and
    d. Propose design improvements to controls when risks are not managed to within the agency’s risk appetite.
3. We evaluated Management’s assessment to determine if it was reasonable and comprehensive.
4. We tested key controls intended to manage risks with inherent risk scores of 9 and above [scale of 1 (low) to 25 (high)] to determine if controls are designed adequately and operating effectively. Our testing included inquiry, observation, inspection of documentation, and re-performance of process steps to determine if key controls are operating effectively.
5. We developed observations for controls determined to be inadequate in design and/or ineffective in operation.

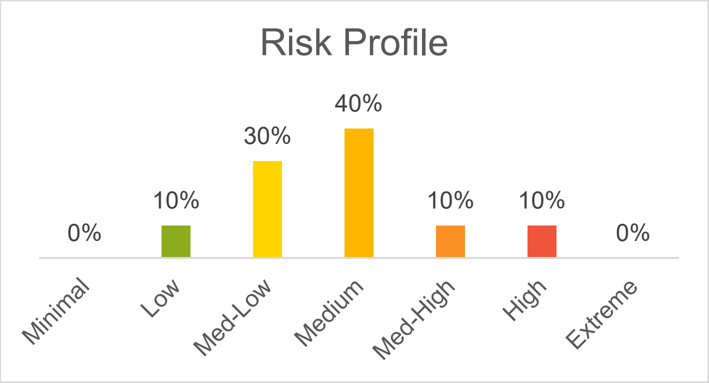
6. We collaborated with management to develop action plans to improve control design and/or operating effectiveness for the identified control deficiencies.
7. While our engagement primarily focused on risk management, we identified other matters that represent opportunities for process improvement.
8. We will collaborate with Management to develop action plans for the identified opportunities for process improvement.

# 5. Conclusion

## Facility Physical Security Controls

**Purpose:** To safeguard the confidentiality, integrity, and availability of information by focusing on the physical protection of information, buildings, personnel, and other resources. Physical access control represents one of three fundamental security controls which make up computer security; technical and procedural are the other fundamental control types which were not assessed during this audit.

**Inherent Risk:** We adopted a list of risks compiled by Information Systems Audit and Control Association (ISACA) as our baseline for risk identification. We collaboratively assessed the inherent risk for the facility physical security program. The Risk Profile chart shows the inherent risk for the program 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. Nine PE – Physical and Environmental controls were selected for evaluation.



## Observations and Recommendations

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

## Development of Management Action Plans

We 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.

## Appendix A - Process Descriptions

**Process 1 Assessing Facility Physical Security**
Each facility location has a primary facility manager who is responsible for determining/ recommending both capital improvements and security enhancements. Each site annually submits a list of three improvements/ enhancements and are reviewed by headquarter leadership who approves and makes budgetary allowances to implement approved projects.

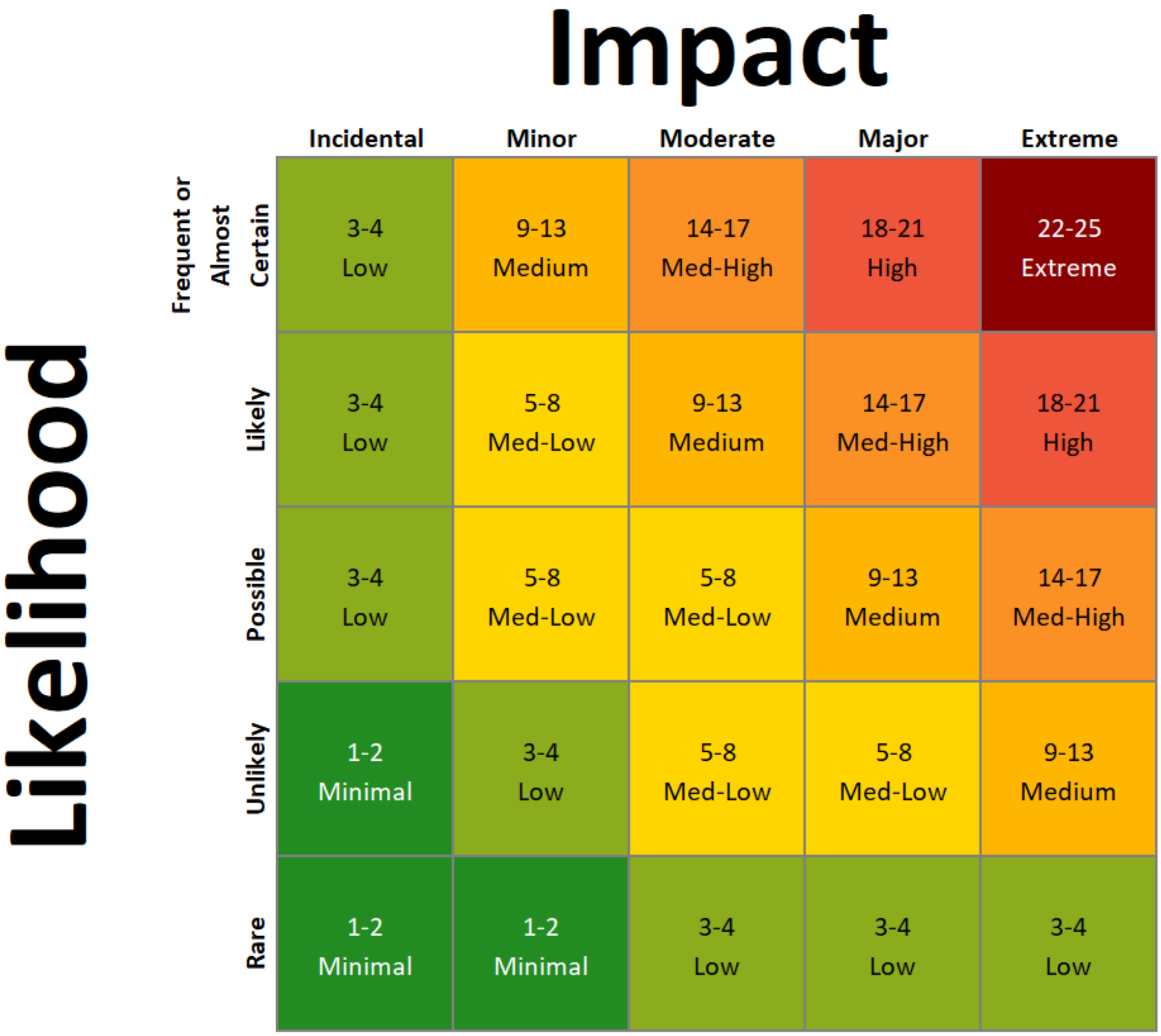
**Process 2 Planning Facility Physical Security Requirements**
Each local facility manager is to understand and determine security requirements within reason for their site based on environment and circumstances.

**Process 3 Implementing Facility Physical Security Requirements**
Once headquarters approves improvement/ enhancement projects, depending on scope and magnitude of the project, the site will coordinate and work to implement the project.

**Process 4 Monitoring Facility Physical Security**
Each facility management is to monitor their site for security purposes. The facility manager and often times the OSHA officer will routinely evaluate the site for safety and security concerns.

## Appendix B - Risk Scoring Matrix

Risk significance is rated on a scale of 1 (lowest) to 25 (highest) and is the product of the risk consequence score (1 to 5) multiplied by the risk likelihood score (1 to 5). The following matrix provides a color scale corresponding to risk significance scores.



Impact

Likelihood

| | Incidental | Minor | Moderate | Major | Extreme |
|---|---|---|---|---|---|
| Frequent or Almost Certain | 3-4<br>Low | 9-13<br>Medium | 14-17<br>Med-High | 18-21<br>High | 22-25<br>Extreme |
| Likely | 3-4<br>Low | 5-8<br>Med-Low | 9-13<br>Medium | 14-17<br>Med-High | 18-21<br>High |
| Possible | 3-4<br>Low | 5-8<br>Med-Low | 5-8<br>Med-Low | 9-13<br>Medium | 14-17<br>Med-High |
| Unlikely | 1-2<br>Minimal | 3-4<br>Low | 5-8<br>Med-Low | 5-8<br>Med-Low | 9-13<br>Medium |
| Rare | 1-2<br>Minimal | 1-2<br>Minimal | 3-4<br>Low | 3-4<br>Low | 3-4<br>Low |

## Appendix C - Risk Appetite

Risk appetite is defined as the amount of risk the agency is willing to accept in the pursuit of its objectives. Management's goal is to manage risks to within the appetite where mitigation is cost- beneficial and practical. Management has set the agency's risk appetite by risk type using scoring methodology consistent with the Risk Scoring Matrix shown in Appendix B. Risk appetites by risk type are as follows:

| Risk Type | Examples | RISK APPETITE SCORE<br>1 = Minimal Risk 25 = Extreme Risk<br>(See Scoring Matrix in Appendix B) |
|---|---|---|
| Safety | Employee and Public Well-Being | 2 |
| Ethical | Fraud, Abuse, Mismanagement, Conflict of Interest | 2 |
| Financial | Funding, Liquidity, Credit, Reporting | 4 |
| Strategic | Resources not Aligned, Unclear Objectives | 4 |
| Reputational | Unintentional Unwanted Headlines | 4 |
| Operational | Delays, Cost Overruns, Waste, Inefficiency | 6 |
| Regulatory | Non-Compliance | 6 |
| Legal | Lawsuits | 10 |