Internal Audit Report

Personal Identifiable Information - PII

Todd Wilkins, CISA, CRISC, CISM, CDPSE

2024

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR

1. Executive Summary

Objective

SCDOT's objective with the information lifecycle management is to ensure information collected or created is properly safeguarded during its lifecycle (from time of creation or receipt to disposal or destruction). IAS's objective is to provide assurance that internal controls are adequately designed and operating effectively to manage risks that may hinder the achievement of SCDOT's objectives.

The objective of the audit is to provide assurance that governance, internal controls and risk management practices related to information lifecycle management are adequate and effective. The audit will assess the effectiveness and adequacy of SCDOT's security measures and management controls. The audit includes an assessment of:

- Governance, roles and responsibilities of all parties involved with Personal Identifiable Information (PII),
- PII risk management processes and practices,
- Internal control effectiveness for safeguarding PII, and
- Employee awareness and compliance with policies and directives regarding PII.

Background

PII is a specific type of sensitive data and should be classified as Restricted according to the state's data classification schema. PII is a combination of data that distinguishes a specific individual, such as full legal name and social security number. One piece of PII alone is not significantly useful for distinguishing an individual unless it is linked to other PII data. It is the linking of PII data that makes it possible to trace an individual's identity. Laws and regulations are established to prevent the abuse, misuse, and fraud because of PII's sensitive nature. The requirements for protecting PII depend on the type of data and are included in both federal and state regulations. Examples include the U.S. Privacy Act, the U.S. Health Insurance Portability and Accountability Act, and the SC Code of Law.

Governmental entities such as SCDOT collect many types of PII data in order to provide services to the public, ranging widely in sensitivity and use. PII may be collected from staff or contractors for the purpose of employment while other PII data may be collected from the public for the purpose of providing a service or assistance. This data can be considered in one of two broad groups: publicly accessible information and private information. Publicly accessible information is not protected from access by the general public and not usually considered sensitive in nature. SCDOT is entrusted to correctly distinguish information because private PII is protected and should never be made publicly accessible. In the government context, private PII is collected from an individual usually through a form for the purpose of receiving some government-provided service or assistance.

Several government and privacy organizations have tracked data breaches to determine the risk and trends associated with PII. The nonprofit consumer information and advocacy organization Privacy Rights Clearinghouse (PrivacyRights.org | Privacy Rights Clearinghouse) started tracking PII incidents. In the state of SC, there are 73 reported breaches to-date, and this includes both public and private organizations. However, 27 of these reported breaches are from state and local governments. The total loss of records from SC's governmental breaches are over 7M records with an average record loss at 250K+ per incident.

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 for their cooperation in assessing risks and developing actions to improve internal controls and enhance operating performance.

Lead Auditor

Todd Wilkins, CISA, CRISC, CISM, CDPSE
Senior Manager

Pamela Johnson
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 30, 2024

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

IAS has completed the risk and control assessment of the South Carolina Department of Transportation's (SCDOT's) information lifecycle management, defined as the management of information from creation or receipt until disposal or distruction. The objective of this assessment was to contribute to the improvement of risk management by evaluating SCDOT's exposure to risks and the controls designed by SCDOT to manage those risks. Our engagement included two aspects:

- Facilitation of SCDOT's assessment of risks associated with PII, as defined under "personal information" at S.C. Code Section 30-2-30(1), and

- Independent assessment of the design and effectiveness of internal controls to determine whether those controls effectively manage the identified risks to an acceptable level.

IAS 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 proposed SCDOT's management action plans were discussed with SCDOT.

George L Kennedy, III

George L. Kennedy, III, CPA
State Auditor

4. Engagement Overview

Background

The purpose of the evaluation is to assist SCDOT in protecting the confidentiality of Personally Identifiable Information (PII) regardless of format such as digital or physical. The U.S., unlike the European Union, does not have an overarching privacy law such as the General Data Protection Regulation (GDPR). In addition to the state's requirements detailed below, this evaluation used as a general basis the Fair Information Privacy Practices (FIPPS – Federal Privacy Council), which are the principles underlying most privacy laws and privacy best practices recognized by the federal government and subsequently the U.S. Transportation Department. An organization, when utilizing these established principles along with information lifecycle management, which is a systematic approach to managing data from creation/ acquisition to disposal/destruction, can expect the following results:

- PII assets are safeguarded from misuse,
- Governance structures and mechanisms are in place to ensure effective and efficient management of PII across departmental operations and the agency as a whole.

According to National Institute of Standards and Technology, there is a surge of security breaches which involves PII and contributed to the loss of millions of records. This report stated that both individuals and organizations are threatened by data breaches that involves PII. These threats include identity theft, embarrassment, blackmail, loss of public trust, legal liability, and remediation costs.

SCDOT is responsible to the public and other stakeholders to determine and implement the best cost-effective strategy to provide Information lifecycle management for safeguarding SCDOT's PII as well as other sensitive information.

The South Carolina Department of Administration (SC Admin) developed the Information Security (InfoSec) program which consists of information security policies, procedures, and other guidance to establish a common information security framework across state agencies. Additionally, two provisos: 117.113 (2014) and 101.32 (2014) expressly make the adoption and adherence to the state's InfoSec policies and standards mandatory for state agencies. This assessment utilizes the SC Admin's governance, strategies, policies, procedures, standards, guidance & guidelines, and other resources as a baseline for helping SCDOT's management determine the best cost-effective strategy to provide Information lifecycle management for safeguarding the SCDOT's sensitive information specifically PII based on risk. This audit was performed in the spirit of the governance objectives developed by SC Admin.

Objective

SCDOT's objectives for the information lifecycle management are to ensure that sensitive information specifically PII is properly safeguarded.

- Determine if the appropriate Information lifecycle management controls are addressed through policy and its implementation for protecting the SCDOT's PII asset.

- Determine if the appropriate risk management practices are employed to identify, track, and mitigate information lifecycle management risks for protecting the SCDOT's PII asset.

- Determine if the appropriate information lifecycle management methodologies are strategically and practically implemented for protecting the SCDIOT's PII 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 SCDOT's objectives for the information lifecycle management.

Scope

The scope of the audit initially included all one hundred (100) confidential and restricted datasets. We narrowed the sample down to five (5) datasets based on sensitivity level, data volume, and data subject. We evaluated both digital and physical data formats. IAS evaluated controls based on risk and management rankings. The controls scoped were grouped by the Privacy Principles outlined in the Fair Information Practice Principles (FIPP) found at Federal Privacy Council (fpc.gov).

- Management
- Notice
- Choice and consent
- Collection
- Use, retention, and disposal
- Access
- Disclosure to third parities
- Security for privacy
- Quality
- Monitoring and enforcement

During planning, IAS and Legal Services collaboratively dissected the information lifecycle management into parts categorized by activity and purpose. The following process parts were assessed for riskiness:

- Data capture and collection
- Data storage
- Data Management
- Data transformation
- Data use and sharing
- Data archiving
- Data destruction

Controls under review came directly from State statutes, DIS-200, and other security documents put forth by SC Admin's Division of Information Security (DIS). Based on the identified process and workflow, IAS evaluated a subset of these controls based on the risk rankings.

There are forty-one (41) controls pulled from State statutes and DIS documents; however due to SCDOT's environment and risks we evaluated seventeen (17) of these 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 were implemented. Based on risk, a closer examination of controls helped determine the effectiveness of the implemented controls.

Out of Scope

Specifically, this engagement only evaluated the implementation of information lifecycle management controls as they related to protecting the SCDOT's PII, a specific type of sensitive information. Other periphery controls that were not associated with information lifecycle management of PII or sensitive information will be considered out of scope.

Methodology

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

1. IAS facilitated SCDOT's completion of a process narrative that documents the steps in the process and the individuals responsible for those steps.
2. IAS facilitated SCDOT'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 A;**
    c. Determine if controls are adequately designed to manage the risks to within the SCDOT's risk appetite; and
    d. Propose design improvements to controls when risks are not managed to within the SCDOT's risk appetite.
3. IAS evaluated SCDOT's assessment to determine if it was reasonable and comprehensive.
4. IAS 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. IAS's testing included inquiry, observation, inspection of documentation, and re-performance of process steps to determine if key controls were operating effectively.
5. IAS developed observations for controls determined to be inadequate in design and/or ineffective in operation.
6. IAS collaborated with SCDOT 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, IAS identified other matters that represent opportunities for process improvement.
8. IAS collaborated with SCDOT to develop action plans for the identified opportunities for process improvement.

5. Conclusion

Observations and Recommendations

IAS collaborated with SCDOT to develop the observations and recommendations for strengthening any areas of discovered weaknesses in information lifecycle management. IAS and SCDOT Executive Leaders discussed these observations and recommendations.

Development of Management Action Plans

IAS facilitated SCDOT's development of management action plans for each observation and/or performance opportunity to improve control design with practical, cost-effective solutions. These improvements are intended to reduce the overall risk exposure to an acceptable level (i.e. within SCDOT's risk appetite).

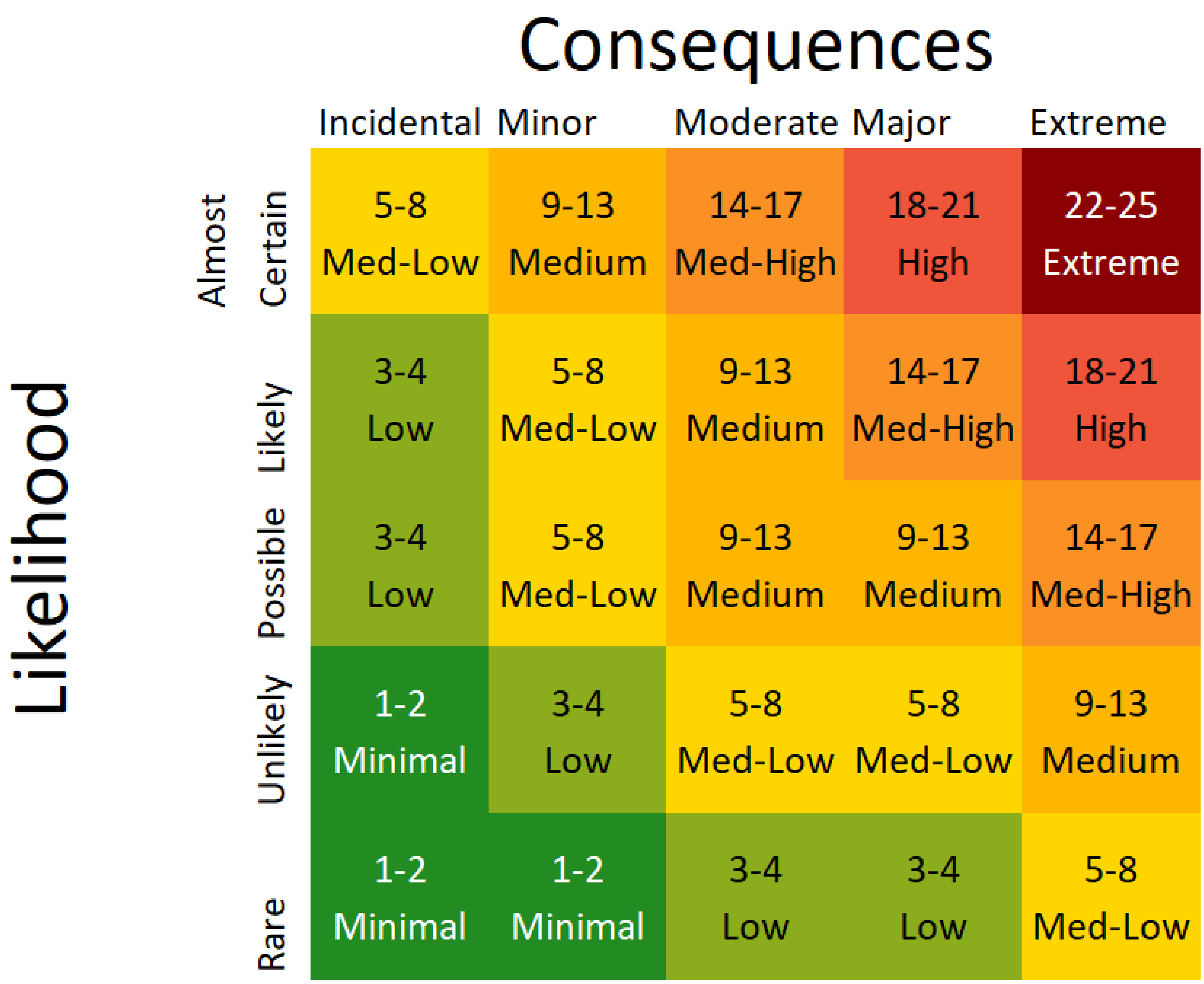
IAS intends to follow up with SCDOT on the implementation of the proposed actions on an ongoing basis and provide SCDOT leadership with periodic reports on the status of SCDOT's management action plans and whether those actions are effectively and timely implemented to reduce risk exposure to an acceptable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

Reporting of Confidential Information

Due to the confidential nature of information security, the observations, recommendations, and SCDOT's 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 - 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.

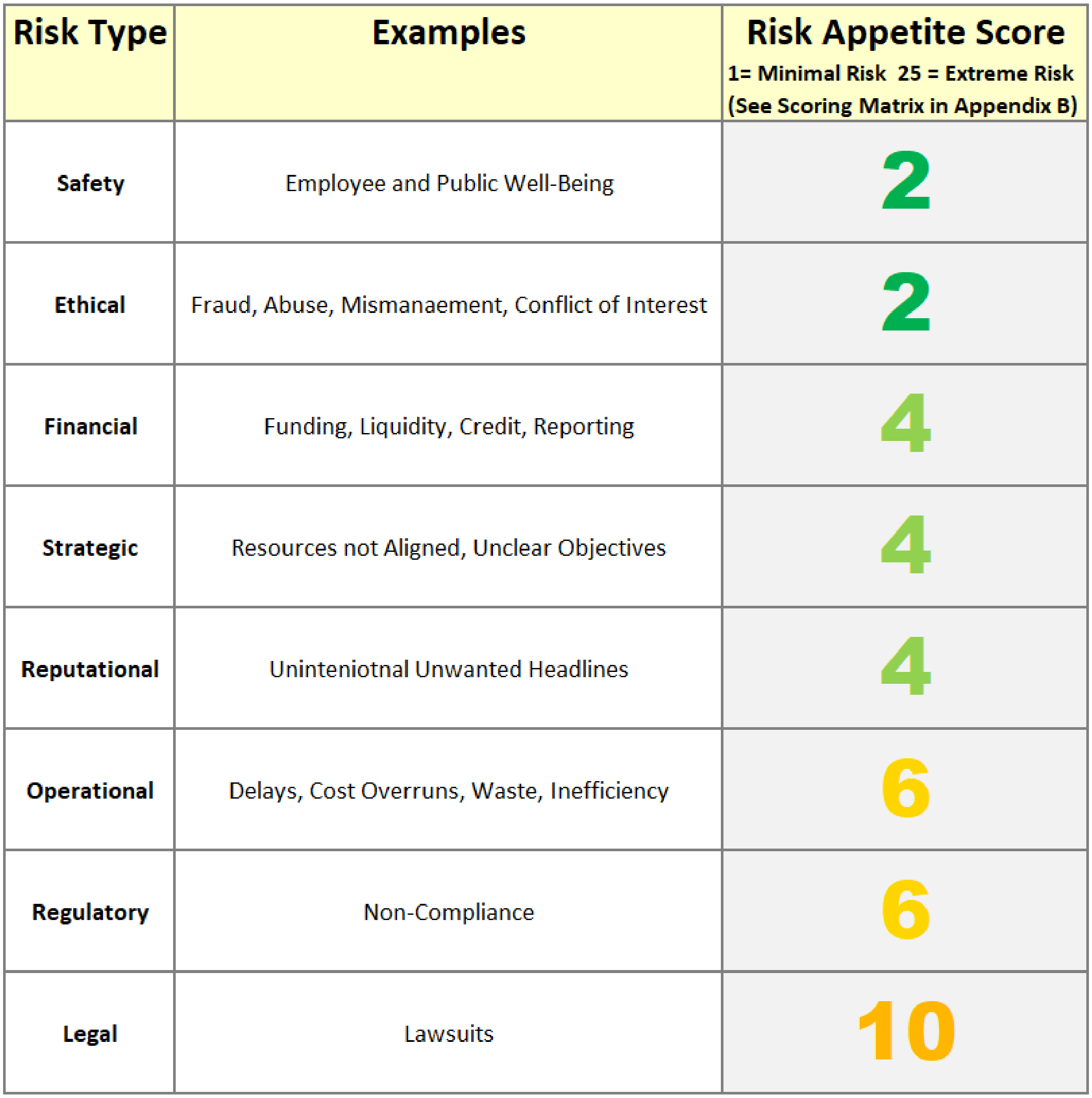


Consequences

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

Appendix B - Risk Appetite

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



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