INTERNAL AUDIT REPORT

2019

GAP ANALYSIS – SCDOT INCIDENT AND VULNERABILITY MANAGEMENT CONTROLS

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR

INTERNAL AUDIT SERVICES

May 28, 2019

1 EXECUTIVE SUMMARY

GAP ANALYSIS – INCIDENT AND VULNERABILITY MANAGEMENT CONTROLS

OBJECTIVE:
To facilitate with SCDOT Management the development of:

- A gap assessment of current conditions as compared with DIS-200 controls
- A listing of prioritized gaps using a risk-based approach
- Remediation actions for priority gaps meeting a defined threshold

BACKGROUND:

- State agencies are required to implement a set of 342 mandatory security controls commonly referred to as “DIS-200”.
- SCDOT has had a system of information security controls in place and has been incorporating the DIS-200 requirements since its release.
- Until DIS-200 controls are fully implemented, SCDOT will be exposed to unacceptable risks in maintaining data confidentiality, integrity, and availability.
- There are 342 DIS-200 controls which are categorized by 13 control families. We will perform the gap analysis and issue a report for each control family.
- This report focuses on the Incident and Vulnerability Management Control Family which has 28 controls.
- Of the 28 controls, 3 have priority gaps identified for remediation. These 3 controls are in a current low implementation state and represent unacceptable risk exposure to SCDOT.

RESULTS:

- Observations, recommendations, and management action plans have been 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 FOREWORD

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, CEH, ECIH,
CISA, CRISC, CISM, CPM
IT Audit Manager

REVIEWER

Wayne Sams, CPA
Director of Internal Audit Services

3 INTERNAL AUDITOR'S REPORT

May 28, 2019

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

We have completed a gap analysis of the South Carolina Department of Transportation's (SCDOT's) Incident and Vulnerability Management Controls promulgated by the State of South Carolina SCDIS-200 Security and Privacy Standards (DIS-200). Incident and Vulnerability Management is one of thirteen control families within DIS-200. We are issuing separate reports upon completion of fieldwork for each control family.

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 Management to manage those risks. Our analysis included the following aspects:

- Facilitating Management's assessment of gaps in the Agency's implementation of DIS-200
- Facilitating Management's prioritization of gaps using a risk-based approach
- Collaborating with Management on the development of priority gap remediation actions.

The results of our analysis are included in the *Gap 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 but are not included in this report pursuant to South Carolina Code of Laws Section 30-4-20 (c) which requires information security plans to be closed to the public.

George L. Kennedy, III

George L. Kennedy, III, CPA
State Auditor

4 ENGAGEMENT OVERVIEW

4.1 BACKGROUND

The South Carolina Department of Administration (Admin) created the Division of Information Security (DIS) in response to the South Carolina Department of Revenue's 2012 data breach. Subsequently, the State enacted legislation to help regulate State agencies' security posture. DIS promulgated a set of 342 mandatory security controls in its SCDIS-200 Security and Privacy Standards commonly referred to as "DIS-200". SCDOT has had a system of information security controls in place and has been incorporating the DIS-200 requirements since its release. In 2016, the Agency provided to Admin a plan of action for implementing DIS-200. The Agency continues to implement the full set of DIS-200. Until DIS-200 controls are fully implemented, SCDOT will be exposed to significant risks in maintaining data confidentiality, integrity, and availability.

4.2 OBJECTIVE

Our engagement objective is to facilitate with Management the development of:

- A gap assessment of current conditions as compared with DIS-200 controls
- A listing of prioritized gaps using a risk-based approach
- Remediation actions for priority gaps meeting a defined threshold

4.3 SCOPE

There are 342 DIS-200 controls which are categorized by 13 control families. We will perform the gap analysis and issue a report for each control family.

4.4 APPROACH

Ranking the 13 Control Families: We collaborated with Information Technology Services (IT) to rank the order of control families by which we would perform the gap analysis. We used two scoring factors: levels of importance and levels of urgency. For any score ties, we used a third factor: IT staff availability for the gap assessment since this would enable faster completion.

Ranking Controls within a Family: For each control family, collaborative review conferences were scheduled with IT staff to determine the significance of risks managed by each control and the stage of control implementation. The following scales were used:

Risk Exposure Range

Extreme
High
Medium-High
Medium
Medium-Low
Low
Minimal

Stage of Implementation

Fully
Nearly
Partially
Planning
Non-Existent
Compensating*

***Compensating means the Agency implemented a different control with a similar control objective due to lower complexity or cost. Compensating controls were not identified as gaps for the purpose of our analysis.

Gap Threshold for Mitigation: The volume and nature of DIS-200 controls make implementation time-consuming and resource-intensive. While it is the Agency's intent to address all gaps over time, this engagement is designed to drive resources to gaps that could have the greatest risk impact to the Agency. Accordingly, gaps that meet both of the following threshold criteria using the above scales were addressed in this engagement:

1. Risk scores of Medium-High, High, or Extreme, and
2. Implementation level of Compensating, Nonexistent, Planning or Partially

4.5 CONTROL FAMILIES

The 342 DIS-200 controls are grouped into thirteen families listed below in ranked order of urgency and importance:

1. **Access Management** – Includes activities for limiting/prevent unauthorized access by providing authorized means to grant and permit legitimate and approved access to Agency resources. Control count: 62.

2. **Incident and Vulnerability Management** – Includes activities for identifying, monitoring, resolving, and preventing disruptive events within the scope of technology services. Control count: 28.

3. **Information Security Management/ Administration** – Includes the roles, responsibilities, functions, policies, and procedures to support the security program. Control count: 33.

4. **Data Management** – Includes activities for identifying and safeguarding data in accordance with its value and sensitivity categorization. Control count: 26.

5. **Physical & Environmental Security Management** – Includes activities for establishing a safe and secure location and atmosphere for technical and data assets such as securing perimeters and uninterrupted power supply (UPS). Control count: 31.

6. **Risk Management** – Includes activities for identifying, documenting, and responding to potentially adverse or beneficial happenings. Control count: 9.

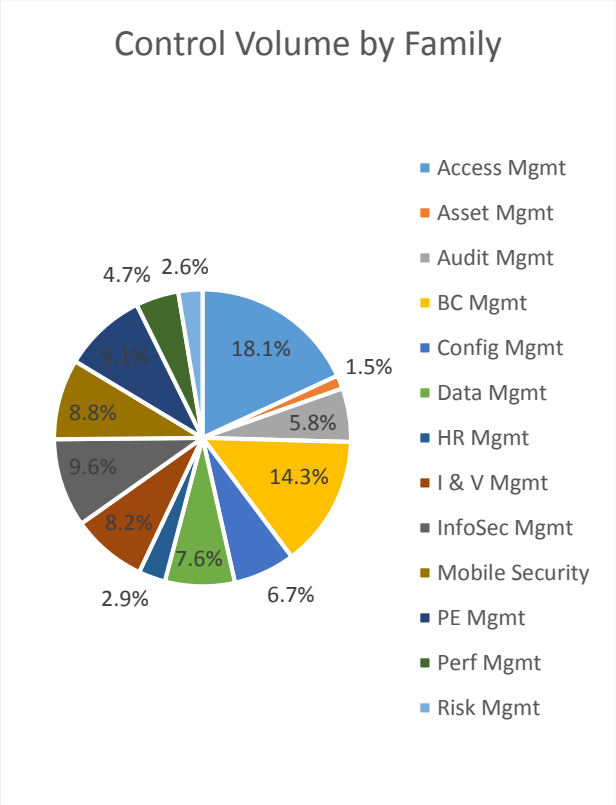
7. **Asset Management** – Includes activities for identifying, documenting, and reconciling inventories of IT assets such as data, documentation, services, software, and hardware. Control count: 5.

8. **Configuration Management** – Includes activities for establishing a well-defined security baseline and progressing the IT environment from one secure baseline to the next. Control count: 23.

9. **Business Continuity Management** – Includes activities for planning and testing for permanency should an adverse event occur which disrupts IT services. Control count: 49.

10. **Human Resource Management** – Includes activities for recruiting and retaining skilled security minded professionals. Control count: 10.

11. **Mobile Security Management** – Includes activities for defining and establishing a secured mobile environment such as procedures for handling lost or stolen devices. Control count: 30.



12. **Performance Management** – Includes activities for baselining performance and improving performance based on selected metrics. Control count: 16.

13. **Audit (Log) and Compliance Management –** Includes activities for documenting and reviewing events which occur within an information system. Control count: 20.

4.6 OVERALL ENGAGEMENT PROGRESS

Status: **On Schedule**

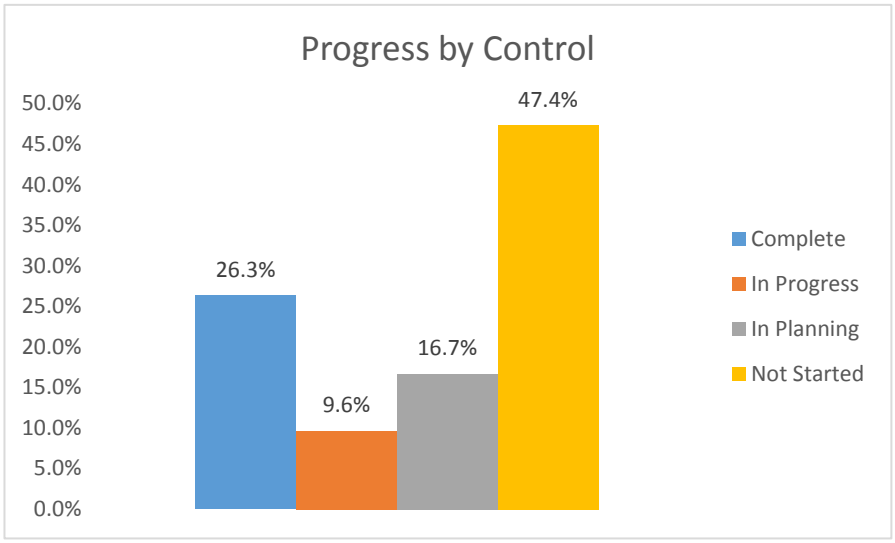
The overall engagement encompasses the 13 control families and each will be reviewed and reported on in the order shown in Section 4.5 above. The graph below shows which families have been through the evaluation process, currently under review, currently in planning, and those not yet started.

Overall Engagement Completeness: Gap Assessment of 13 Control Families

1	2	3	4	5	6	7	8	9	10	11	12	13

- Complete – 15.4%
- In Progress – 7.7%
- In Planning – 15.4%
- Not started – 61.5%

The control families have a wide control count range thus a more precise way to view project completeness is by control count. After evaluating the current control family, we have analyzed 26.3% of all DIS-200 controls.

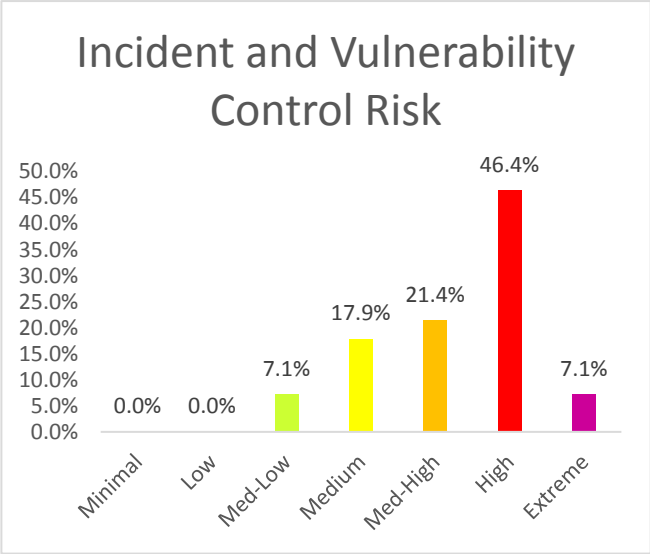


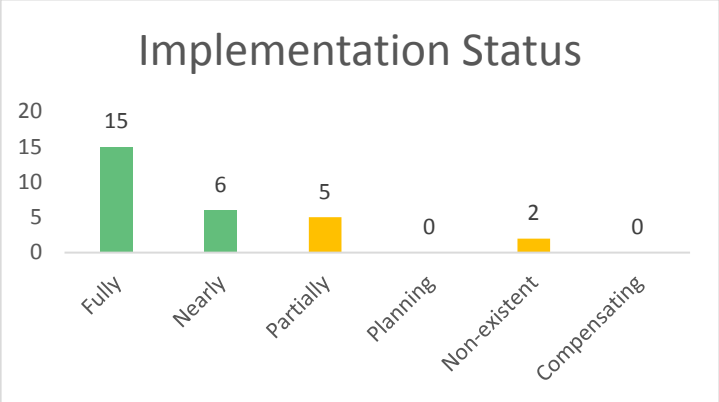
5 GAP ANALYSIS RESULTS

5.1 INCIDENT AND VULNERABILITY MANAGEMENT CONTROLS

Control Family Purpose: To identify, monitor, resolve, and prevent disruptive events which will have negative impact on agency resources.

Inherent Risk Assessment: The chart to the right describes the inherent risk addressed by the Incident and Vulnerability Management controls. This chart illustrates that nearly three-fourths of the inherent risk for this control family falls between med-high and extreme. 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. The Incident and Vulnerability control family accounts for less than 10% of all of the DIS-200 controls

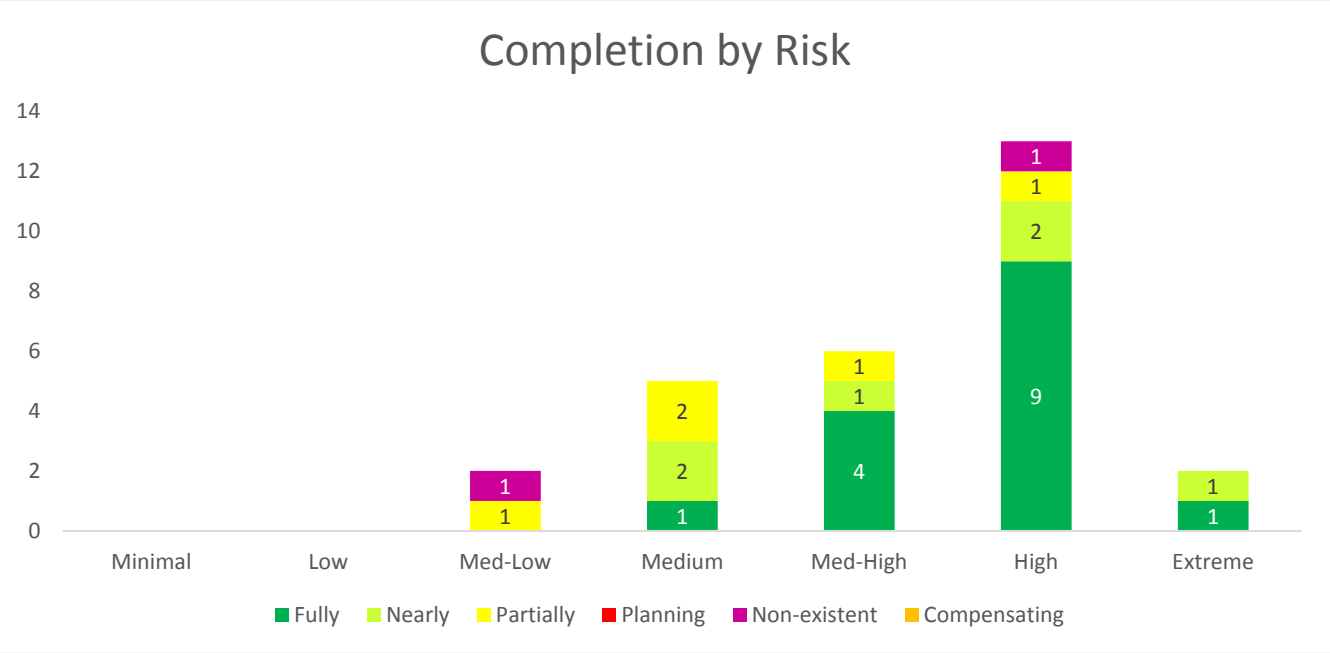




Implementation Status Assessment: As shown in the graph to the left, SCDOT has made significant progress implementing Incident and Vulnerability Management controls. Most controls (roughly 75%) are either fully or nearly implemented. Less than 10% of controls evaluated fell into the planning or non-existent completeness level.

The controls were also evaluated for inherent risk. Comparing the controls completeness score in relation to risk revels, we concluded that IT wisely prioritized its resources (time, budget, etc.) on implementing controls with the highest impact by risk.

Inherent Risk and Implementation Status Combined: The below graph shows the control risk by columns. Each column is banded by a color to show the implementation status within the band. The number is the control count for the level of completeness for each risk level column.



One control was identified in the non-existent (purple) stage at a med-low risk. Three other controls were partially implemented (yellow) with med-low or medium risk. These four controls had risk scores that fell below the threshold and were therefore excluded from priority gap remediation. Three controls were identified as partially implemented (yellow) or non-existent (purple) with substantial risk scores of med-high or higher which met the threshold for priority gap remediation.

5.2 PRIORITY GAP OBSERVATIONS AND RECOMMENDATIONS

We collaborated with IT Services and Security Management on the development of observations and recommendations for remediating each priority gap. Those observations and recommendations were discussed with SCDOT Executive Leaders.

5.3 DEVELOPMENT OF MANAGEMENT ACTION PLANS

We facilitated Management's development of action plans for each 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.

5.4 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.