Internal Audit Report

IT Asset Lifecycle Management

Todd Wilkins, CISA, CRISC, CISM, CDPSE

2025

SOUTH CAROLINA OFFICE OF THE STATE AUDITOR

1. Executive Summary

Objective

Management's objective with IT Asset Lifecycle Management is to ensure the effective and efficient management of all IT assets throughout their lifecycle, from acquisition to disposal, in order to maximize the asset's value, minimize risks, and support organizational goals and objectives. This includes maintaining accurate inventories, optimizing asset utilization, ensuring compliance with regulations and policies, mitigating security risks, and aligning asset management practices with agency needs and priorities. The goal of Asset Lifecycle Management is to enhance operational efficiency, reduce costs, and improve decision-making processes related to IT investments and resource allocation.

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 as it relates to IT assets throughout their lifecycle. This includes evaluating the accuracy of asset inventories, assessing compliance with policies and state regulations, identifying and mitigating risks related to asset management, and ensuring that IT assets are utilized efficiently and effectively to support agency objectives. The goal is to provide assurance to management and stakeholders that IT assets are properly managed, protected, and aligned with business needs, while also identifying areas for improvement and recommending enhancements to strengthen IT asset management practices.

The objectives of this audit are to:

- Provide assurance that the agency's ITAM governance, internal controls, and risk management practices are sufficient and effective.
- Evaluate the accuracy, completeness, consistency, timeliness, and reliability of the IT asset inventory.
- Assess whether the agency's ITAM processes support sound lifecycle management from acquisition to disposal.
- Identify compliance gaps and security risks associated with current asset management practices.
- Promote accountability, cost-effectiveness, and operational efficiency through better IT asset governance.

Background

As part of the Internal Audit Plan, the Internal Audit is initiating an evaluation of the agency's IT Asset Management (ITAM) practices, controls, and lifecycle governance. ITAM is a foundational IT governance function that ensures the agency has visibility into its IT infrastructure: hardware, software, digital systems, and related information assets.

This audit aligns with the State's Information Security (Infosec) Program, which requires agencies to coordinate efforts across technical, physical, and personnel domains to protect

state information systems. The Infosec Program establishes a policy framework through DIS-200 and related guidance, against which each agency must assess its own security posture.

Currently, SCDOT's ITAM program is acknowledged to be in early stages of maturity. Management aspires to reach Maturity Level 3 (Defined) in the process maturity model, which is characterized by consistent, documented, and enforced ITAM practices across the organization. While some lifecycle stages, such as procurement and retirement, are subject to state requirements, other phases such as asset tracking, deployment, and data flow monitoring are more ad hoc and decentralized.

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).

2. Contents

3. 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 Finance and Administration and Information Technology 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
Associate Director of Internal Audit Services

Reviewer

Mark LaBruyere
Director of Internal Audit Services

4. Internal Auditor's Report

November 20, 2025

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

We have completed risk and control assessment of the South Carolina Department of Transportation's (SCDOT's) IT Asset Lifecycle Management. 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 engagement included two aspects:

- Facilitation of Management's assessment of risks associated with IT Asset Inventory, 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.

We planned and performed the engagement with due professional care 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.

Mark LaBruyere

Mark A. LaBruyere
Director of Internal Audit Services

5. Engagement Overview

Background

The South Carolina Department of Transportation (SCDOT) recognizes the strategic importance of effective IT Asset Management (ITAM) in supporting operational efficiency, cybersecurity, and informed decision-making. From an audit perspective, an IT asset is defined as anything within the technology environment that provides value, and whose use or misuse may introduce risk, cost, or compliance obligations. This definition is consistent with the intent of the DIS-200 standard and reflects the agency's responsibility to manage IT resources holistically.

Traditionally, IT asset management (ITAM) has focused on tangible hardware and licensed software. However, as technology environments have grown more dynamic, IT assets now also include virtual servers, cloud-based applications, and other non-physical resources that play a vital role in agency operations. These virtual assets, though not physically tagged, still require tracking, updates, and protection to ensure security and performance.

Similarly, the agency's systems increasingly depend on data flows, integrations, and application interdependencies that must be maintained with the same level of oversight. A mature ITAM approach at SCDOT should aim to expand visibility and management to these components over time. This direction is consistent with the intent of the DIS-200 standard, which emphasizes risk-based protection of information systems. A healthy ITAM program enables the agency to ensure that all assets (whether physical, virtual, or logical) are effectively managed in alignment with strategic goals and risk posture.

As part of the IAS' Internal Audit Plan, the Internal Audit Division initiated an evaluation of the agency's ITAM practices, controls, and governance across the asset lifecycle. This review builds on prior audits related to access controls, personal information protection, and DIS-200 compliance, and represents a logical progression toward improving asset accountability and lifecycle management.

This audit aligns with the State's Information Security Program, which requires agencies to implement coordinated safeguards across personnel, physical, and technical domains. Anchored in DIS-200 and related guidance, the security program establishes minimum expectations for asset protection, lifecycle controls, and operational resiliency. Internal Audit used DIS-200 as a foundational reference point, applying its required controls creatively across ITAM lifecycle phases to assess process maturity rather than simple control compliance.

This audit does not report on control effectiveness in isolation. Instead, it evaluates how well ITAM principles are being met across the lifecycle, with the intention of encouraging IT leadership to focus on strengthening the underlying processes that support maturity. This approach avoids a punch-list mindset and instead promotes long-term sustainability, accountability, and strategic alignment. The principles evaluated for each phase of the ITAM lifecycle include:

Governance Principle: Effective asset management is built on intentional governance such as clear leadership, aligned policies, and strategic integration with risk management.

System and Information Principle: The tools and data used to manage IT assets must be accurate, accessible, and trustworthy. They must support the entire asset lifecycle with integrity and integration.

Plan Principle: Assets should be planned with the full lifecycle in mind and based on agency needs, risk, and budget.

Acquire Principle: Assets should be acquired through processes that ensure visibility, necessity, risk awareness, and alignment with lifecycle stewardship.

Deploy Principle: Asset deployment should maintain continuity of tracking, assignment of ownership, and reflect current usage and configuration.

Maintain and Monitor Principle: Asset should be maintained and monitored to ensure performance, security, and relevance with activities tied to risks.

Retire and Dispose: Retirement and disposal should be deliberate, documented, and secure, with both physical and logical controls to eliminate residual risks.

SCDOT leadership has identified the desire to improve its ITAM capabilities and has expressed the goal of reaching **Maturity Level 3 (Defined)**, where ITAM practices are documented, consistently applied, and enforced throughout the organization (*Maturity model can be found in Appendix B*). A strong ITAM program reduces the risk of data breaches, asset loss or misuse, noncompliance with state requirements, and inefficient resource utilization. Conversely, weak ITAM practices increase the likelihood of incomplete inventories, misaligned investments, unmanaged system interdependencies, and vulnerabilities due to unpatched or unmonitored assets.

This audit is intended to assess the maturity of the agency's ITAM processes and provide actionable insights that will support lifecycle accountability, improve interdepartmental coordination, and close the visibility gap between business units and IT. Planning and execution were carried out in close collaboration with IT leadership, with emphasis placed on evaluating maturity at each lifecycle phase through the lens of risk and shared ownership.

Objective

Management's objective for Asset Lifecycle Management is to ensure that IT Assets are properly safeguarded throughout their lifecycle. Assets are expected to be protected from loss, misuse, or compromise, and to be maintained to support business operations and managed in accordance with applicable policies and risk priorities. IAS in collaboration with IT Services was asked to:

1. Evaluate whether policies and practices support the effective implementation of asset lifecycle management principles, enabling protection, performance, and alignment with organizational objectives.
2. Assess whether risk-based processes are integrated throughout the asset lifecycle to identify, track, and mitigate threats to IT assets, including those affecting performance, security, and compliance.

3. Determine the extent to which asset lifecycle management activities are strategically aligned, operationally consistent, and practically implemented across IT services to support ITAM maturity.

Internal Audit's objective is to provide assurance on the extent to which internal controls and supporting processes are designed and functioning effectively to manage risks that may hinder the achievement of management's objectives for IT Asset Lifecycle Management. This includes evaluating how well asset-related activities align with strategic priorities, protect agency resources, and contribute to the agency's desired level of ITAM maturity.

Scope

The scope of this audit included a comprehensive evaluation of the agency's IT Asset Management (ITAM) lifecycle processes with a focus on how well they align with defined ITAM principles and contribute to the agency's goal of reaching Maturity Level 3. Rather than evaluating individual control effectiveness in isolation, the audit emphasized the processes, interdependencies, and governance structures that support the management and protection of IT assets throughout their lifecycle.

The audit covered the following ITAM lifecycle activities:

- **Inventory Management:** Assessed the tools, practices, and accountability mechanisms used for asset discovery, tracking, inventory accuracy, and documentation integrity.
- **Asset Lifecycle Management:** Evaluated how procedures for acquisition, deployment, maintenance, and retirement are implemented and governed across organizational units.
- **Security and Compliance:** Reviewed adherence to applicable state security requirements (DIS-200), including how ITAM activities incorporate risk-based safeguards.
- **Vendor and Contract Oversight**: Examined vendor-related processes and service level agreements (SLAs) related to the procurement, maintenance, and support of IT assets.
- **Risk Management:** Assessed whether the agency identifies, monitors, and responds to risks associated with unmanaged, obsolete, or underutilized IT assets.
- **Data Privacy and Protection**: Evaluated whether ITAM activities support the safeguarding of sensitive data stored on or flowing through IT assets, particularly during transfers or disposals.
- **User Training and Awareness:** Assessed whether staff and stakeholders receive sufficient guidance and training related to asset stewardship, data protection, and compliance expectations.

For the purposes of this audit, an IT asset is considered any component within the technology environment that provides value and whose use or misuse may introduce risk, cost, or

compliance obligations. This definition aligns with the intent of the DIS-200 standard and the agency's responsibility to manage IT resources effectively. The scope of assets included:

- Physical assets such as servers, desktops, laptops, VOIP phones, mobile devices, and other endpoint hardware;
- Logical assets including virtual servers and cloud-hosted environments;
- Software and applications, including licensing management and SaaS platforms such as O365;
- Data assets, data flows, and system interconnections considered critical to agency operations.

The audit approach began with planning discussions and interviews with key stakeholders to understand roles, responsibilities, and the current state of ITAM processes. The audit team evaluated relevant documentation, policies, and procedures; conducted process walkthroughs; and tested selected controls based on risk. Lifecycle activities were assessed both individually and collectively to determine the maturity and integration of the agency's asset management practices.

Out of Scope

This audit did not evaluate capital asset financial reporting or the physical inventory processes managed solely for accounting purposes. Additionally, this review focused exclusively on IT assets; non-IT assets were excluded.

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 C;
    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. In addition to control-level assessments, we evaluated the extent to which underlying processes aligned with key ITAM principles, in order to support the agency's progress toward ITAM maturity.
6. We evaluated the design and operating effectiveness of key controls through the lens of ITAM principles. We developed observations for controls determined to be inadequate in design and/or ineffective in operations. Where applicable, we identified systemic process gaps that may impact the agency's ability to meet ITAM objectives.
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.

6. Conclusion

Asset Lifecycle Management Controls

Purpose: The purpose of IT Asset Management (ITAM) is to ensure the effective governance, utilization, and protection of IT assets throughout their lifecycle; including planning, acquisition, deployment, maintenance, and disposal, in support of organizational objectives and information security requirements. A well governed ITAM program establishes clear processes and supporting controls to ensure that IT assets are accurately tracked, maintained, and aligned with business, operational, and risk considerations. Effective ITAM helps optimize resource allocation, mitigate risks, maintain regulatory compliance, and maximize the value of IT investments. It provides visibility into the agency's hardware, software, data, and digital infrastructure, helping safeguard the confidentiality, integrity, and availability of information systems. This audit focused on how well SCDOT's ITAM practices support these outcomes, using state's DIS-200 standard and ITAM lifecycle principles as a reference point. Our approach emphasized evaluating the underlying processes and the extent to which they enable the agency to mature its asset management practices.

Inherent Risk: For this engagement, we began with the State's DIS-200 control set and selected controls that were most relevant to IT Asset Management (ITAM) or its underlying processes. Using these controls as a starting point, we reverse-engineered risk statements by evaluating each control through the lens of ITAM principles and lifecycle objectives. These derived risks were then presented to IT Management, who were asked to identify the controls they believed mitigated each risk.

Following this, Management rated the inherent risk of each item based on likelihood and consequence, without consideration of existing controls. This risk-informed approach allowed us to focus our evaluation on the highest-risk areas and assess whether existing practices and controls are sufficient to manage ITAM related risks.

Fifty-three controls were ultimately selected for evaluation based on their relevance to ITAM and alignment with medium or higher inherent risk ratings. Although traditional control testing was conducted, the audit emphasized understanding the degree to which processes and control activities enable ITAM maturity, visibility, and alignment with organizational objectives.

Observations and Recommendations

We collaborated with Finance and Administration and Information Technology 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

We facilitated Management's development of action plans for each observation and/or performance opportunity 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

ITAM Process and Maturity Overview

SCDOT management has acknowledged that the agency's current IT Asset Management (ITAM) processes are still maturing, with the goal of achieving Maturity Level 3 and reflects a "defined" state, in which policies, procedures, and standards are documented, consistently applied, and enforced agency-wide to guide ITAM activities. Currently, SCDOT's ITAM processes reflect a combination of informal internal practices (particularly in planning, deployment, and maintenance) and formal external requirements (notably in acquisition and retirement, shaped by State Procurement Code and DIS-200 security standards). While these compliance-driven activities provide some structure, the overall program would benefit from stronger process integration, centralized coordination, and alignment with ITAM principles such as lifecycle visibility, risk-based decision making, and continuous improvement.

ITAM Lifecycle

Planning Phase:

- Define ITAM objectives and goals aligned with organizational needs.
- Establish policies, procedures, and governance frameworks for ITAM.
- Conduct asset discovery and inventory assessment to identify existing assets.
- Assess risks and prioritize mitigation strategies.
- Develop an ITAM roadmap and implementation plan.

Acquisition Phase:

- Procure IT assets based on predefined requirements and budget constraints.
- Validate purchase orders and contracts to ensure compliance with organizational policies.
- Receive and document newly acquired assets into the inventory management system.
- Perform initial asset tagging and labeling for identification purposes.

Deployment Phase:

- Configure and customize IT assets according to business requirements.
- Install necessary software and applications.
- Deploy assets to end-users or designated locations.
- Conduct user training and provide support for asset utilization.
- Monitor asset performance and address any deployment issues.

Monitor and Maintain Phase:

- Monitor asset usage, performance, and health status.
- Conduct regular maintenance activities, such as software updates, patches, and upgrades.
- Implement security controls and measures to protect assets from threats and vulnerabilities.

- Track asset utilization and conduct periodic audits to ensure compliance with policies and regulations.
- Address end-of-life considerations, such as asset retirement and disposal.

Retirement and Disposal Phase:

- Decommission obsolete or redundant assets.
- Ensure proper data sanitization and disposal procedures to protect sensitive information.
- Update inventory records to reflect asset status changes.
- Dispose of assets in compliance with environmental regulations and organizational policies.
- Conduct post-retirement assessments to identify lessons learned and improve future asset management practices.

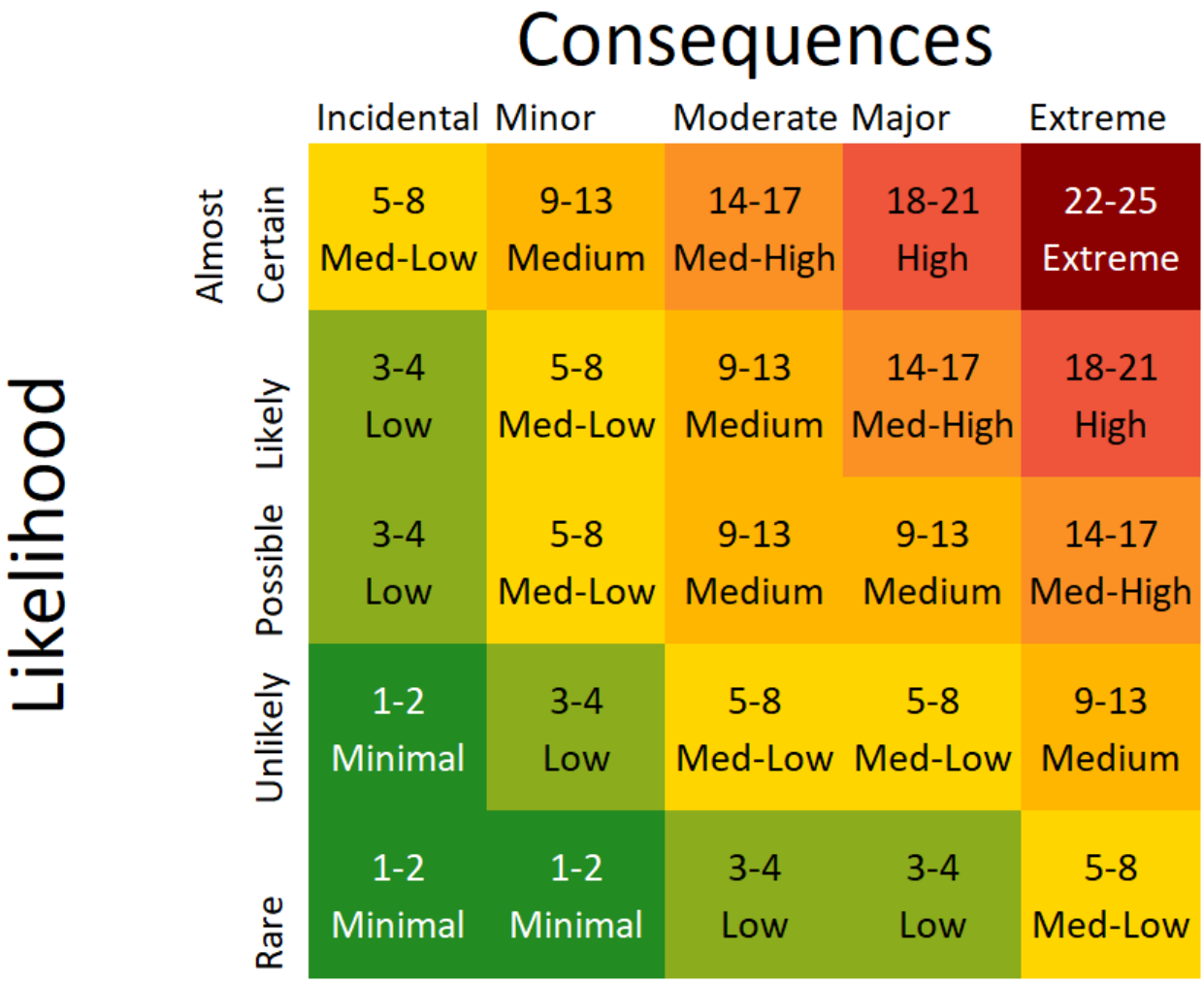
Appendix B – Generic Maturity Model

Maturity Level		Description
1	**Initial**	• Roles and responsibilities are not formally defined. • Processes are ad hoc, undocumented, and vary across teams. • **Success depends on individual efforts, not repeatable systems.** *Governance is informal or absent*.
2	**Managed**	• **Some policies and procedures are documented and implemented, but coverage is inconsistent across teams/ divisions/ organization**. • Processes are repeatable in limited areas and lack organization-wide coordination. • Processes typically reflect baseline requirements or team-level priorities but lack organization-wide governance. *Governance is reactive and localized*.
3	**Defined**	• Policies, procedures, and standards are documented and consistently applied across all applicable areas of the organization. • **Processes are designed to ensure consistency and effectiveness, not just meeting external requirements**. • Gaps and risks in the process begin to be recognized beyond compliance drivers. *Governance is structured and organization wide*.
4	**Quantitatively Managed**	• Processes are consistently implemented and measured across the organization. • **Performance measures are used to evaluate process effectiveness, identify risks, and drive decisions**. • Risk-based process adjustments are regularly made to improve outcomes. *Governance is proactive and data-informed**.
5	**Optimizing**	• **A culture of continuous improvement is embedded throughout the organization**. • Feedback loops, innovation practices, and lessons learned are actively used to refine the process. • Metrics and improvement goals are routinely reviewed and adjusted to reflect changes in risk, performance, and strategic direction. *Governance is strategic and embedding in the culture*.

Data-informed – Using data as a key input to guide decisions, while also considering human judgement, experience, and strategic priorities.

Appendix C - 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.



Appendix D - 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 C. 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	Uninteniotnal Unwanted Headlines	**4**
Operational	Delays, Cost Overruns, Waste, Inefficiency	**6**
Regulatory	Non-Compliance	**6**
Legal	Lawsuits	**10**