admin
SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Checking our Cyber Vital Signs

How Statewide Cyber Risk Management Enables Cyber Health in South Carolina

STATE:	**South Carolina**
AGENCY:	**Department of Administration**
CATEGORY:	**Cybersecurity**
PROJECT TITLE:	**SC Cyber Health**
PROJECT DATES:	**FYs 2024-25 and 2025-26**
CONTACT:	**Ben Willis | State Chief Information Security Officer** ***ben.willis@admin.sc.gov***

LEAD. COLLABORATE. INNOVATE.

EXECUTIVE SUMMARY

South Carolina's integrated, statewide cyber risk management program (SC Cyber Health) drives continuous, measurable improvement to cyber health across state government.

Until recently, South Carolina monitored cyber risk through a combination of robust security and privacy standards, agency security support services and real-time monitoring of agency assets through the state Security Operations Center (SOC). Those capabilities were strong, but largely agency centric. While agencies could monitor their own activity, review reports and access security support services, they lacked a standardized way to benchmark their total exposure, remediation progress or agency cyber program maturity compared to the rest of the state. A program enhancement was desired to bring enterprise visibility, alignment and maturity to statewide cyber health.

To enable this statewide view, the South Carolina Department of Administration's (Admin) Division of Information Security (DIS) has spent the last two years building a new enterprise cyber risk management program that provides a real-time view of cyber risk across more than 80 state agencies and continually updates how the state calculates and visualizes cyber risk as the threat landscape continually evolves.

To build this multipart program, DIS established or revitalized critical components, including governance standards, risk data sources, risk management processes, reporting tools and a dedicated agency-engagement team. It then integrated them into a unified statewide program with common goals and measures.

Key accomplishments during the two-year buildout of SC Cyber Health include revising the state's security control framework, completing the first statewide cybersecurity audit, centralizing findings and remediation workflows in a single system of record, providing agency personnel with access and training on how to use the system, developing common statewide metrics and reporting on agency adoption of statewide security tools and creating a real-time cyber risk dashboard based on standardized cyber vital signs and risk scores with both agency-level and statewide views.

With this program, state and agency leaders have achieved a new level of coordination in managing cyber risk, extending established oversight and support activities into a shared-responsibility operating model in which agencies manage remediation and the state provides governance, visibility and support.

The impact is measurable: achieved **100% participation** across state agencies and a **25% reduction** in identified cyber risk findings statewide. Active risk management through structured remediation surged **over 10x**, driving a **sustained downward trend** in agency cyber risk scores.

SC Cyber Health Program

Statewide Visibility

Shared Responsibility

Targeted Investment

Measurable Cyber Health

IDEA

What problem or opportunity does the project address?

South Carolina has long had strong cybersecurity activity across state government, supported by common information security standards, information security program support and technical security operations. The opportunity was to build on that foundation by giving agencies and state leaders a more current, consistent and enterprise-level view of cyber health at both the agency level and across the state.

SC Cyber Health connects more than 80 agency risk management relationships into one statewide program that gives all agency and state leaders a common view of where cyber risk exists, how it is changing and where attention or investment would have the greatest effect.

Why does it matter?

South Carolina's cyber health affects a **$42.6 billion state budget**, a workforce of roughly **395,000 public employees** and services for **5.57 million residents**. The state's **80+ state agencies** are a critical part of that cyber health. When Admin saw the opportunity to enhance statewide visibility and coordination, the value was not merely theoretical. A real-time, standardized, enterprise-level view accelerates remediation, clarifies shared risks and helps target resources where they would have the largest shared impact, bolstering cyber health for the whole state.

What makes it different?

South Carolina's differentiator is integration. SC Cyber Health connects pieces of cyber risk management that are often separate (standards, assessments, remediation status, technical adoption metrics and data-driven risk calculations) into one unified program.

It also integrates the state enterprise itself. All state agencies now use the same standards, workflows, scoring model, tools and dashboard to understand risk, track progress and focus remediation support.

What makes it universal?

Every state faces the same operating reality: cyber risk is distributed across many agencies and remediation responsibilities are spread across those agencies. Yet effective statewide strategy, accountability and investment require coordination and an enterprise view.

South Carolina's model is repeatable because it is built around common public-sector needs and existing cybersecurity and compliance capabilities. The result is transformative, but the path is practical. Any state can build a similar program by bolstering and enhancing its existing capabilities through investment, partnership and consistent execution.

IMPLEMENTATION

What was the road map?

DIS used a two-phase approach to develop and implement SC Cyber Health. Each phase was structured as a fiscal-year strategic project within Admin, giving executive leadership clear visibility and the Admin Program Management Office (PMO) full oversight of deliverables, milestones and success metrics.

Phase One: Build the foundation. DIS hired key cyber risk and relationship management staff, gathered and structured existing agency risk data, updated statewide security standards and developed a consistent risk framework with direct comparison across agency cyber risk profiles.

Phase Two: Scale statewide. DIS rolled agency-level views into an enterprise view, refreshed the statewide governance, risk and compliance (GRC) platform with streamlined processes, and launched the statewide risk dashboard and updated risk management processes for state agencies.

Who was involved?

SC Cyber Health was envisioned by Admin executive leadership in cooperation with the state chief information security officer (CISO). Together they defined the two-phased approach, project milestones and expected outcomes. Execution was led by the state CISO and the DIS team, including cyber risk, audit and assessment, security engineering and agency security engagement staff.

Agency participation was critical. Admin's legislative mandate to develop and implement the statewide information security program provided the foundation for accountability. DIS built on that foundation through existing agency partnerships, regular communication, training, feedback cycles and direct support to help agencies understand findings, use the GRC platform and act on their risk profiles.

SC Cyber Health's 10 Cyber Vital Signs

MFA | Identity & Access | Vulnerability Management | Logging & Monitoring | Endpoint Protection | Network Protection | Encryption | Backups | Training & Awareness | Incident Readiness

How was it done?

Hiring new DIS staff was the critical first step for building SC Cyber Health. Existing technical and compliance teams were supplemented with two new capabilities: a cyber risk management team and an agency engagement team. Early in the project, DIS hired leaders and key staff for Phase One; most of the agency engagement team was onboarded in Phase Two as rollout began.

SC Cyber Health did not replace South Carolina's existing governance toolset; it extended and unified it. New leadership and staff organized existing standards, audit data, the GRC platform, agency relationships and security operations data into one statewide risk management model. The only major new tool was Power BI, used to present risk data in clear agency and statewide views.

The technical approach was deliberately practical: DIS defined standards, assessments generated findings, the GRC platform tracked remediation, cyber vital signs and technical adoption metrics created the shared language, and Power BI made the results visible. The real work was connecting people, processes and data so Admin and agencies could manage cyber risk from the same set of facts.

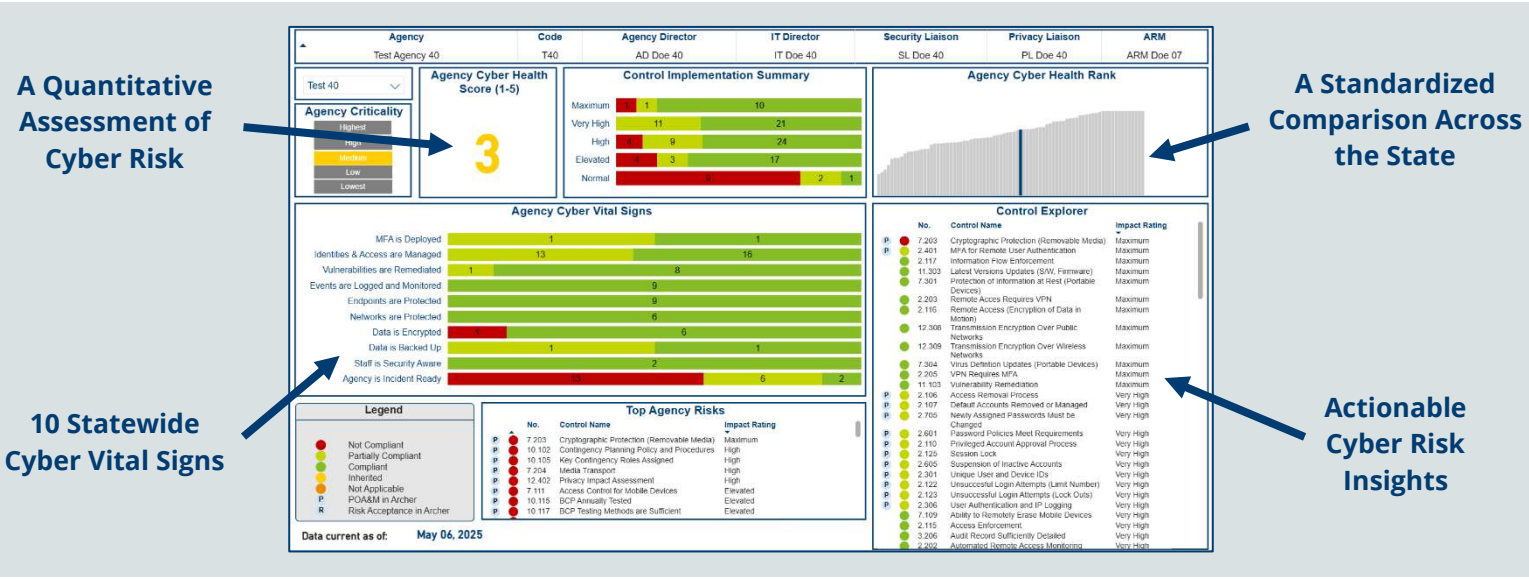
IMPACT

What did the project make better and how do we know?

SC Cyber Health improved statewide cyber risk management in three practical ways: it made risk **visible**, strengthened **coordination** between Admin and agencies and turned risk data into **action**.

VISIBILITY: One Statewide View of Cyber Health

SC Cyber Health enhanced established security operations, remediation updates and agency-by-agency conversations with a shared statewide view of cyber health. After implementation, the statewide SC Cyber Health dashboard gave Admin and agencies a shared view of cyber risk, remediation status, cyber vital signs and agency risk profiles across 80+ state agencies.



This visibility matters because leaders now compare risk using the same facts, identify high-priority control areas, see whether remediation is reflected accurately and apply resources where they will reduce the most risk.

For the first time, **100% of state agencies** are participating in a common statewide cyber risk baseline. Agencies are not limited to traditional audit reports that show their posture alone; they use continuously updated data to manage their own progress and see where they fall relative to their peers.

COORDINATION: From Compliance to Collaboration

Better visibility is only one part of the positive impact of SC Cyber Health. Improved agency relationships driven by the expanded DIS agency engagement capability have been a major contributor as well. DIS virtual CISOs, cyber risk analysts and security subject matter experts have used the increased visibility provided by the SC Cyber Health dashboard as a springboard for dialog, leading to stronger relationships and sustained remediation momentum. Agencies now have a clearer picture of their own security posture and a more direct channel to DIS for support.

There is strong qualitative evidence of SC Cyber Health's positive impact on agency relationships and coordination. One agency, after seeing its cyber health score on the SC Cyber Health dashboard, used the data as a catalyst for deeper self-review. As a result, they proactively performed a fresh self-assessment against the statewide control set and voluntarily reported the results to DIS.

The evidence is not merely programmatic. It is human as well. A long-time DIS employee described the

new agency engagement team as having a **"significantly positive impact"** on agency relationships. Agency decision makers are experiencing the difference in their ability to target and drive change.

"In a resource-constrained environment where threats are ever-increasing, the easy access to timely, accurate information provided by SC Cyber Health has made security-related budget requests much easier to defend."

– SC Cabinet Agency CIO

ACTION: Measurably Improved Cyber Health

SC Cyber Health makes cyber risk actionable. Agencies can see which findings, controls and cyber vital signs are driving their cyber health score and what actions will improve their cyber health most.

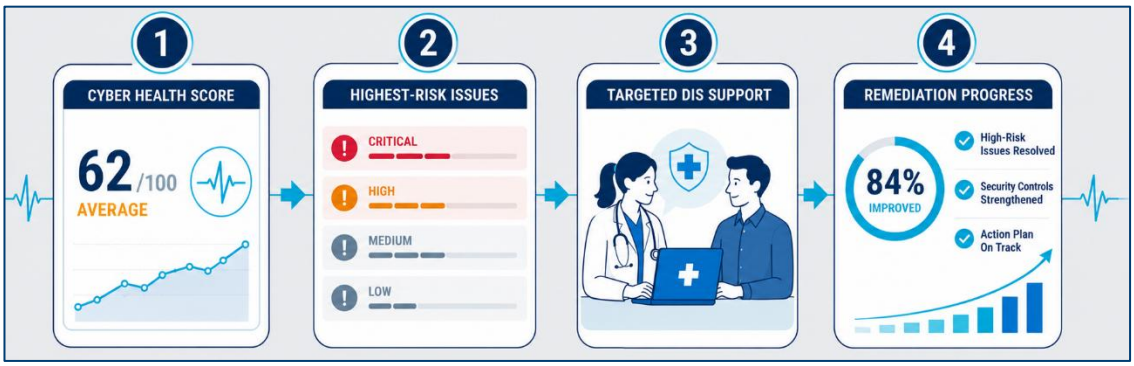
This actionable intelligence has changed the conversation from "Where are we?" to "What do we do next?" Agencies are using the dashboard to prioritize remediation and track whether completed work is reflected in their health score. When they need help, they proactively come to DIS with specific needs and receive targeted support, including tools, templates and subject matter expert assistance.

The metrics show how much is possible in just a short time:

- **100% participation** across state agencies.
- **More than 10x increase** in findings actively managed through plan of action and milestones (POA&Ms).
- **25% reduction** in identified cyber risk findings statewide.
- **Sustained downward trend** in enterprise risk scores.
- **80+ agencies** using the same standards, workflows, scoring model and dashboard.

SC Cyber Health has provided South Carolina with a practical, unified enterprise risk management model: Agencies know where they stand and have a clear path forward to improved cyber health.

SC Cyber Health: An Enterprise Approach with Measurable Results



WHAT NOW?

SC Cyber Health is an ongoing operating model, not a static dashboard or one-time reporting effort. It is the mechanism South Carolina uses to monitor cyber health, empower agency remediation and adapt statewide cyber risk management strategy as technology and threats change.

The next phase focuses on four priorities:

1. Add real-time vulnerability reporting.

DIS will integrate reporting on aged critical vulnerabilities from the vulnerability management program into the cyber health score. This will make the score more responsive to current technical risk, while continuing to incorporate assessment findings, remediation status and security toolset adoption.

2. Complete the next statewide audit cycle.

Beginning in FY 2026-27, DIS will conduct the next two-year statewide audit cycle using newly updated statewide security standards created as part of the SC Cyber Health program. This will refresh the statewide baseline and provide a new, consistent view of agency cyber health.

3. Align the dashboard to updated standards.

As findings against the newly updated statewide standards are identified, DIS will revise the SC Cyber Health dashboard so agency scores, control views and risk summaries continue to reflect the current security baseline.

4. Keep the risk model current.

DIS will continue refining risk calculations as the threat landscape changes, especially as AI-driven threats increase the speed, scale and sophistication of cyber risk.

The initial investment was worthwhile because it created more than a one-time report; it created an evergreen statewide capability. South Carolina now has the people, processes, data and dashboard foundation to view risk, focus support and measure progress across all state agencies. Ongoing investment is justified because cyber health is never static. The same model that helped South Carolina establish visibility and coordination will equip the state to keep pace with new vulnerabilities, new standards and new threats.