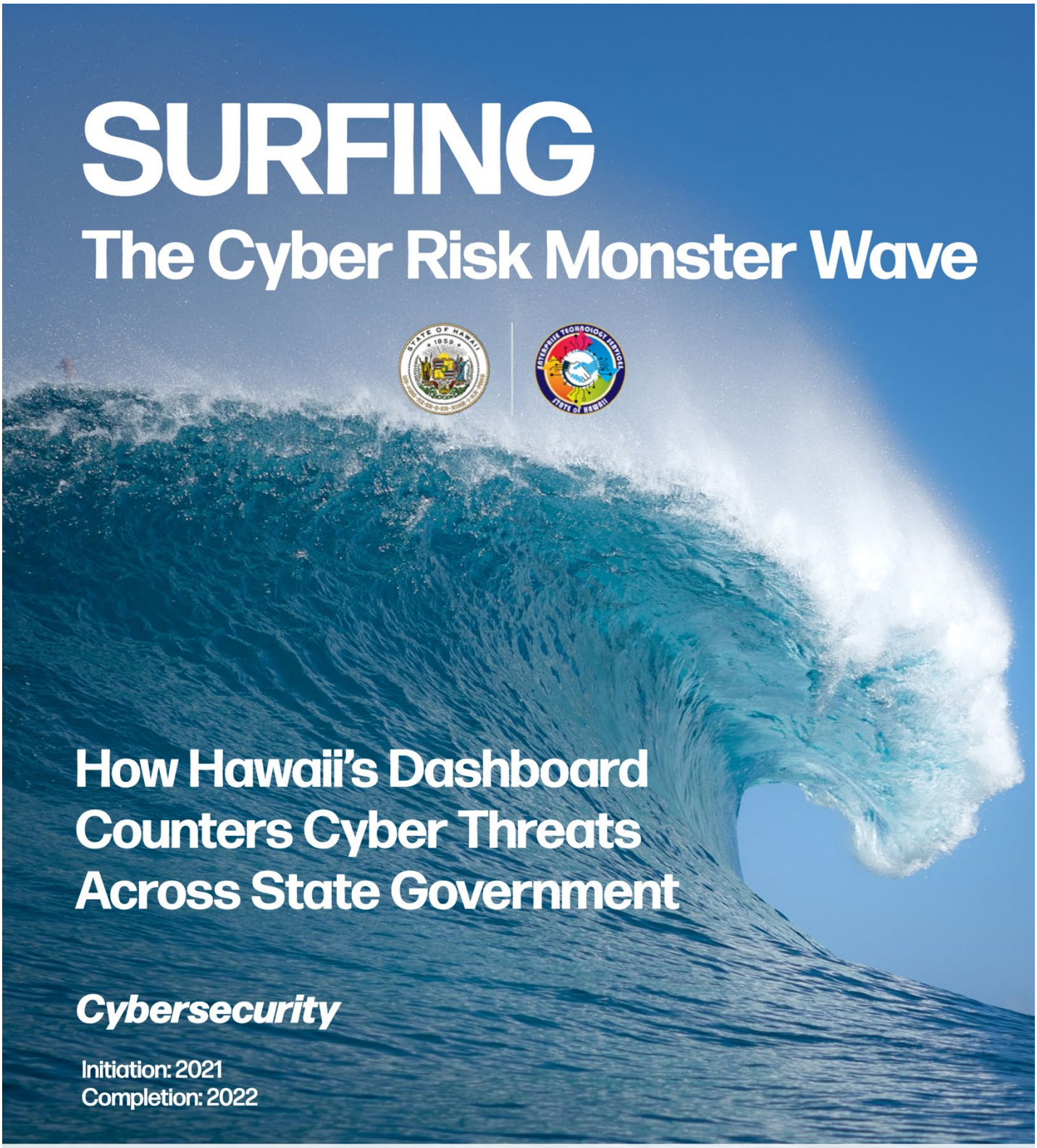
SURFING

The Cyber Risk Monster Wave



How Hawaii's Dashboard Counters Cyber Threats Across State Government

Cybersecurity

Initiation: 2021
Completion: 2022

Doug Murdock

Chief Information Officer
Office of Enterprise Technology Services
State of Hawaii
douglas.murdock@hawaii.gov

NASCIO STATE IT RECOGNITION AWARDS

Executive Summary

Big wave surfing in Hawaii is a sport that holds significant respect around the world. Surfing requires not only physical prowess but qualities such as courage, respect, and humility. However, riding big waves comes with big risks, and surfers must manage their risks carefully to avoid catastrophic wipeouts.

Similarly, state governments face an ever-increasing "wave" of cyber threats that, if unmanaged, can lead to devastating consequences. In both surfing and cybersecurity preparation, real-time awareness and the use of the right tools and strategies are all essential to staying safe.

To ensure those protections, we developed the State of Hawaii Cyber Risk Scoring System (CRSS) to deliver real-time visibility around cybersecurity controls and risk posture across all state departments in the executive branch. Operated by the State of Hawaii Office of Enterprise Technology Services (ETS), this tool aggregates risk data from every endpoint in the executive branch into an easily digestible risk score that is updated for state leadership, including the Office of the Governor, State CIO, and State CISO as frequently as every two minutes.

Figure 1: All Dashboards displayed reflect ETS' implementation using mock data from a test environment.

This project is amongst the first in the nation to show a standardized, comprehensive risk score across multiple distinct departments in real-time with an easy to digest view. (Note: A lower score indicates a lower risk.)

We are excited to share this project with NASCIO, and hope that it may serve as an inspiration to other states for real-time cybersecurity reporting.

Idea

A Universal Challenge

Cybersecurity and risk management has been the #1 NASCIO Top-Ten Priority every year for a decade. States are tasked with securing high-value assets and information systems that are taxpayer funded with limited resources. Many of these information systems manage our critical infrastructure such as dams, harbors, airports and highways (which is why protecting critical infrastructure is also the top priority of The White House Cybersecurity Strategy); as well as protecting sensitive constituent data, ensuring continuity of operations from crippling ransomware, and are essential to upholding the public's trust.

Despite emphasis from the National Institute of Standards and Technology's Cybersecurity Framework and numerous other guidance materials on the importance of starting with visibility to identify areas for improvement, many state CISOs struggle to achieve it. Accessing security metrics and measuring risk posture across state departments at a time when threats are becoming more sophisticated, and the cyber workforce gap continues to increase is truly challenging. To address these challenges, overlapping tools are pieced together which increase IT complexity, risk and cost. Outdated processes present a drain on resources and can be at odds with achieving a more secure government.

Impact to Hawaii

ETS provides governance for executive branch IT projects across all state agencies and seeks to identify, prioritize, and advance innovative initiatives such that state program objectives may be achieved.

ETS faced specific challenges when it came to managing and reducing their cybersecurity risk across all departments, including:

- **Manual, time-consuming way of estimating risk**: The only way to get a view of IT risk was to rely on reviewing self-reported manual assessments from each department that became quickly outdated;
- **No inventorying of critical systems**: The inability to prioritize risk remediation based on criticality;
- **Addressing the workforce gap**: Operating with limited resources and tedious processes;
- **Leveraging existing investments**: Getting more value out of the cybersecurity tools already in use;
- **Addressing top-down concerns**: Communicating the need for cybersecurity investments to non-technical leadership across departments;
- **Benchmarking risk posture**: No way of tracking the relative risk between departments, or understanding of how well Hawaii is doing compared against other public sector entities.

The State of Hawaii IT leadership, State Chief Information Officer Doug Murdock and Chief Information Security Officer Vince Hoang, implemented a solution that increased the availability of limited cybersecurity resources and enhanced the visibility and control of their interconnected systems across all executive branch departments.

A Scalable Solution: The Cyber Risk Scoring System

The Cyber Risk Scoring System (CRSS), built on top of the Tanium Platform, addresses major business challenges with visibility, accuracy, and certainty across all endpoints within the executive branch. The tool allows departments to have full control over their IT risk – all in a real-time, easy-to-understand view that delivers valuable insight for the security analysts as well as the governor's office and everyone in-between.

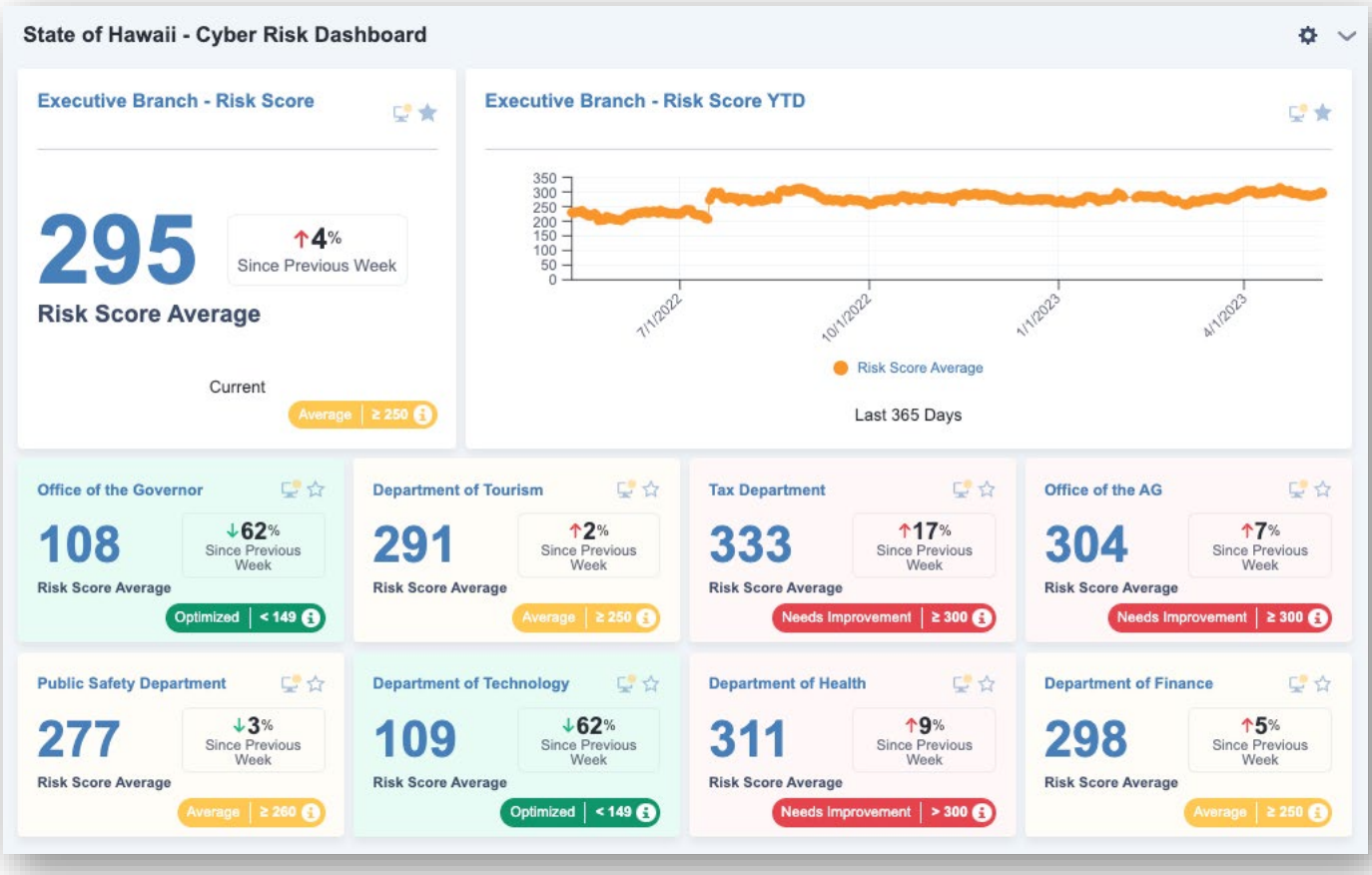


Figure 2: Notional CRSS Dashboard recreated with mock data

A Novel Approach to Statewide Risk Dashboarding

The Cyber Risk Scoring System uniquely solves these needs by leveraging **real-time data** and **simultaneous cross-department collaboration**.

> *"This system allows the State of Hawaii and our department to identify and prioritize risks intelligently, and in lockstep with one another. With the CRSS we are able to be more effective, make better informed decisions, and advise state entities by building a roadmap to improve cyber security readiness." – Steve Sakamoto, Chief of the Health Information Systems Office, Hawaii Department of Health.*

The major attributes of the dashboard that contribute to its success include:

- **Simultaneous cross-department collaboration:** The dashboard automatically aggregates real-time risk data from the executive branch departments into a single view, allowing for continuous improvement and collaborative remediation between departments and ETS;
- **Data is updated in real-time**: The system pulls real-time data, updating results from Windows, Mac and Linux endpoints **every two minutes** regardless of if they are on-premises, telework, or cloud-hosted;
- **Comprehensive, universally weighted risk scoring:** The risk score is based on mathematical equations that cannot be altered and includes multiple areas of risk, unlike other dashboards which often focus only on one area of risk or can be manipulated;

- **Easy to understand and benchmark against peers:** The system allows the State and its departments to understand the efficacy of their security program against their peers, and see areas where they lead or lag, helping communicate funding and policy needs to lawmakers, agency directors and the governors' office;
- **Pivot to remediation with actionable insights:** The system provides ETS actionable tasks to effectively reduce attack surface and enables the team to complete those remediation actions within the same tool. This means that ETS can both deliver remediation as a service to under-resourced departments and allows ETS to provide the authority to departments to manage their own risk.

Implementation

Using Current Resources, Getting Buy-In, Prioritizing the Platform, Accuracy of the Risk Score

The key components that contributed to a successful implementation include:

Making the Most of Our Resources

The CRSS was an idea that resulted from a brainstorm between Hawaii CISO, Vince Hoang, Tanium Technical Account Manager Zachary Nandapurkar, and members of the ETS staff. It was an idea that leveraged technology already in use by the State for asset management and patching. This meant that implementing the CRSS would only be a matter of deploying a few extra components on endpoints to calculate the scores and organizing the data by department.

Hoang also had a unique solution to the cyber workforce gap. With a budget for only seven staff members total (three for this project), he fostered relationships with local universities to source and develop cybersecurity talent and prioritized internship candidates with an open mind and willingness to learn. From the onset, the project team included recent college graduates who brought optimism and fresh ideas to the table. With this outlook, Hoang hopes to create new pathways to public service and harness the technology expertise within the State.

Getting Buy-In

Gaining buy-in for the project was shaped by ETS' ability to lead with empathy. Rather than forcing mandates, they brokered partnerships with the departments by understanding their pain points and offered to problem-solve together. ETS strives for a culture that resembled a start-up within state government, channeling the art of the possible.

The Roadmap

Because ETS had existing technical infrastructure to support the CRSS idea, it meant they could leverage the technology to implement the idea faster. In 2021, Tanium released a new risk scoring feature – an idea that Hoang expanded on to include a multi-department view. ETS tested the functionality and in 2022, created a dashboard to consolidate and break down risk both by department and criticality, calling it the Cyber Risk Scoring System. The entire implementation took just one year with its agile framework.

How the Risk Score is Calculated

The CRSS is anchored by a weighted risk score, which is a numerical score built on weighted vectors that represent the overall risk of the State and each department based on data from every managed system in the executive branch. The possible range for a risk score is between 1-1000. A lower score indicates a lower risk for the enterprise or endpoint and scores are categorized into low, medium, high, or critical. Target goals can be customized by ETS to match their risk-tolerance and existing processes.

Endpoint risk scores are weighted both by how critical the endpoint is to business operations and the following risk vectors:

System Vulnerability 40%	System Compliance 20%	Administrative Access 20%	Password Identification 10%	Expired Certificates 5%	Insecure TLS/SSL 5%

Several compensating controls (security best practices or configurations of hardware, operating systems, and storage derived from NIST frameworks) such as whether anti-virus is enabled, and disk encryption status are also considered when calculating risk scores.

The following, automated mathematical equations are used to calculate risk for Endpoints, Departments, and the State Total respectively:

- Endpoint Score = (Vector Score x Endpoint Criticality) x (100% - Compensating Control)
- Department Score = AVG($\sum_{i=1}^{i}$ Endpoint Score$_i$)
- State Total Score = AVG($\sum_{n=1}^{n}$ Endpoint Score$_n$)

Department scores are averages of all endpoint scores within the department, and the state score is an average of all department scores.

Impact

Far-Reaching Impacts That Will Grow Over Time

The business outcomes of this project include:

- **Measuring and communicating IT and security risks:** Allows ETS staff to easily view and communicate cyber risk on a statewide and departmental level to legislators, the governor's office and other key stakeholders;
- **Industry comparison:** Benchmark risk against industry peers;

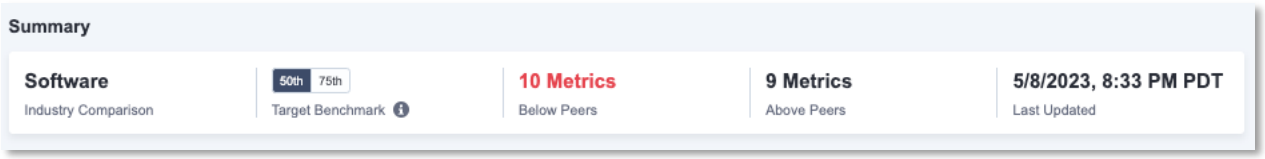
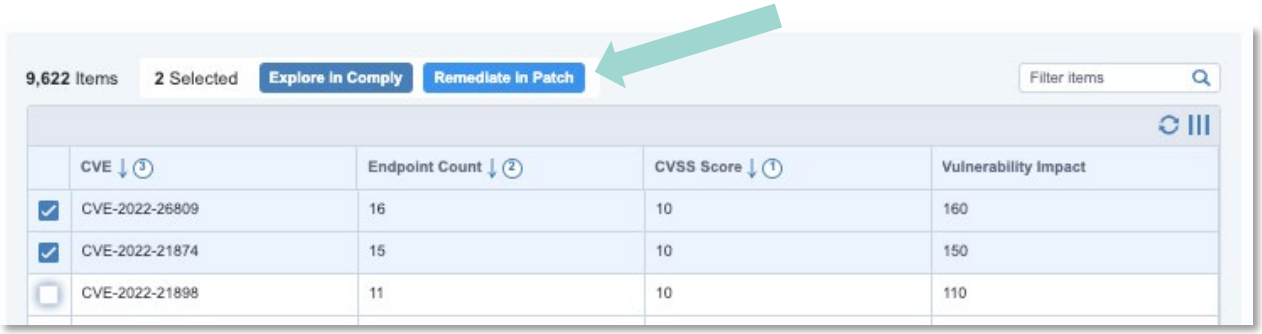


Figure 3: Mock Data of Benchmark Comparison Metrics

- **Reducing IT and security risk with one tool**: Allows ETS to provide patching-as-a-service or conditional access to remediate vulnerabilities across departments from a digestible risk score that translates to the tactical steps needed to remediate issues found – all within the same tool;



- **Ensuring ROI:** With a real-time view of security controls, and how they contribute to statewide risk posture department by department, executive level leadership can validate the return on investment of security programs and expenditures, avoid unnecessary expenses on external cyber risk audits, and reduce risk exposure thereby avoiding future expenses;
- **Leveraging automation and aligning teams:** The single roll-up of view of real-time accurate asset data allows IT Staff across all state departments to collaborate and reduces time spent on tedious, manual work like combining disparate and outdated datasets.

Measuring Success

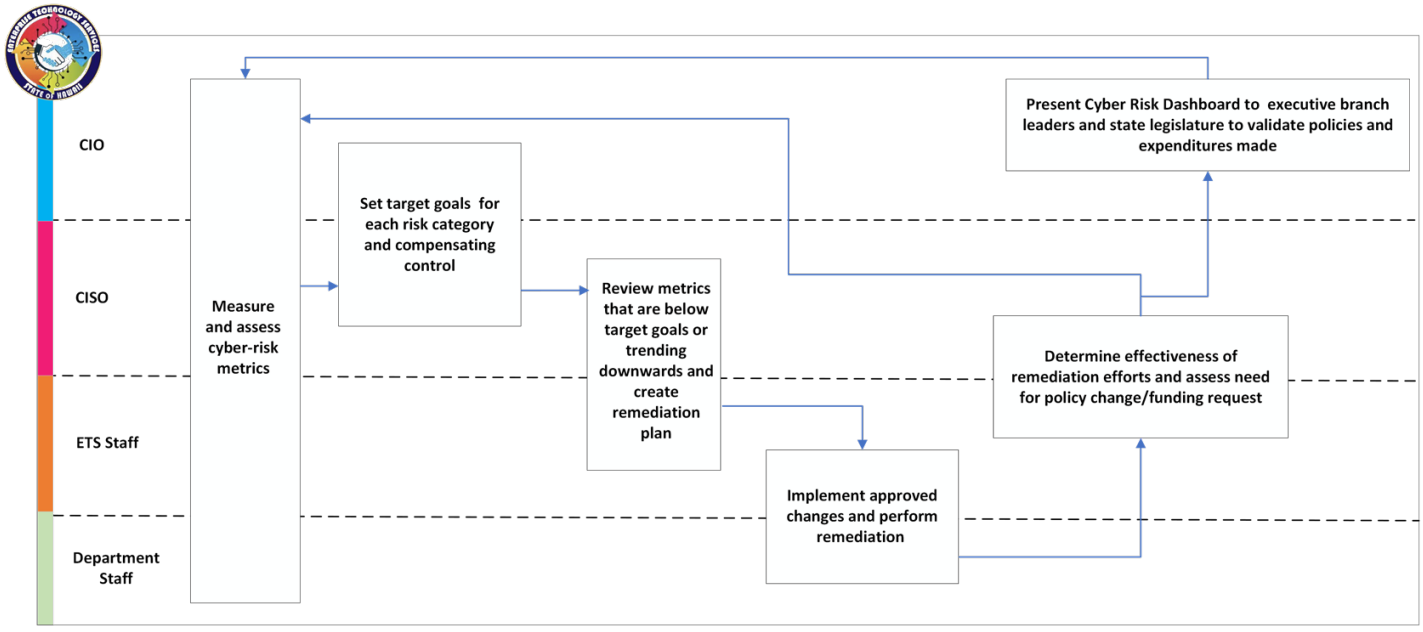
In three months since the project was made accessible to departments:

17 of 18	**14.8%**	**45%**
Executive Branch departments realized a reduction in risk score	Overall reduction in risk score for the **Executive Branch** as a whole	**Reduction in risk score** by one department

Maturing the Process

This process of proactive risk reduction never ends, but the CRSS allows ETS to continually raise the bar. While the dashboarding system is complete, ETS is now looking into all the ways we can operationalize the data.

The chart below illustrates the process to identify problems, set priorities, create solutions, implement changes, measure effectiveness, plan future investment decisions, and inform all decision makers including the state legislature, governor's office, as well as ETS and departmental IT staff.



Seeing Beyond the Monster Waves

Though the cyber threats will continue to come in waves, big and small, the State of Hawaii ETS team is better able to stay on top of them with this innovative Cyber Risk Scoring System and we look forward to being a resource for other states faced with their own sets of incoming waves.