



Salt Lake County is the largest county in Utah, home to over 1 million residents. Like many municipalities, it serves its constituents across a variety of social services and is responsible for a host of personal data of its citizens. The security team of Salt Lake County supports teams across a wide range of stakeholders within the local government and must be able to effectively report upwards, to both county leaders and to governing bodies at the state and federal levels.

Due to the layers of government and stakeholders that the county is held accountable to, they are responsible for achieving and maintaining compliance with a wide range of security standards and frameworks including the NIST Cybersecurity Framework and the CIS Top 20 controls among many others, while also managing cybersecurity risk.

BUSINESS CHALLENGE

Increasingly Complex Compliance Standards | Need for Better Reporting | Process Inefficiencies

Mark Evans leads cybersecurity at Salt Lake County, being a part of the team for twelve years and bringing 20+ years of experience with him. Over the years, as more regulations and standards have emerged, Mark made the decision to base his security strategy on the NIST Cybersecurity Framework and the CIS Top 20. Yet, for many state and local government security teams like Mark's, managing the array of security standards and requirements becomes a matter of prioritizing what the team can get to in the allotted amount of time. Thankfully, the NIST CSF and CIS 20 cover a majority of objectives for Mark and his team but even so, the team was left scrambling to achieve compliance. Especially in the past couple of years, as the standards increased in complexity and reporting requirements became more complicated, Mark realized that spreadsheets, email chains, and hours of manual efforts preparing presentations would no longer suffice.

With a host of stakeholders within the county delivering assessment information as well as superiors that needed to report up the chain of command, Mark needed to implement a solution that would support his team's efforts to keep Salt Lake County secure.

Because his superiors understood program efficacy in dollars and cents, not the traditional information security metrics that he was used to delivering, Mark realized it was time to standardize on a centralized solution that would enable his team and streamline program workflows while adding clear measurement. Mark also needed to balance the cost as well as the simplification that he was after for his program. To this end, he looked at a few more traditional, modular GRC tools and consistently found them too complex, costly, and legacy for his needs.

“ My tools always lacked robust risk rating systems to report on the impact of cybersecurity investments. I needed a solution that was advanced in its capabilities but that would also simplify program management.”

CHALLENGE

Managing a plethora of dynamic regulatory standards and reporting to both technical and non-technical stakeholders.

SOLUTION

CyberStrong's agile and scalable compliance and risk management program supported by real-time dashboards, automated reporting, and flexible framework support.

SOLUTION: CYBERSTRONG IRM

Agile and Flexible Framework Support | Ease of Use for Team Members | Clear Reporting and Dashboards

“ As an organization that faces a wide range of risk across multiple departments, CyberStrong has helped us track and manage new and unprecedented risks as they emerge in a standardized way that was previously impossible, helping us achieve a truly integrated approach to cybersecurity program management.”

Mark and his team selected CyberStrong for its unprecedented ease of use, automated reporting and real-time dashboards, and integrated risk and compliance workflows. Mark’s team is now able to leverage a unified language for risk and compliance management - unifying the language and deepening understanding around Salt Lake County’s cybersecurity program.

“ Because of the CyberStrong platform, I’ve been able to handle my normal workload while also getting to many of the tasks I was forced to put on the back burner when we were using spreadsheets.”

Since implementing CyberStrong, Mark has transformed Salt Lake’s cybersecurity program. By streamlining and centralizing the assessment process, all stakeholders have a clear understanding of their role in data collection and analysis. The reports and dashboards have also enabled Mark to facilitate more informed discussions with municipal leaders and effectively and efficiently report out to upper levels of government on the County’s cybersecurity posture.

“ I’ve coupled the annual National Cybersecurity Review score with the CyberStrong score and the results from CyberStrong are aligned and have real integrity - the CyberStrong score is a great way to track progress throughout the year and make sure we’re tracking for the National Review annually.”

Aligned

- ▲ Compliance efforts across multiple frameworks and requirements.

Standardized

- ▲ Salt Lake’s program strategy on the NIST CSF and CIS Top 20.

Enhanced

- ▲ Stakeholder reporting with real-time dashboards and automated reporting.

Unified

- ▲ Risk and compliance efforts across the county in a single-pane-of-glass solution.