Division *of* Technology Services

State of Utah

Division of Technology Services

Cross-Boundary Collaboration

Strengthening Utah's Security Posture

July 1, 2025

Alan Fuller - alanfuller@utah.gov
Stephanie Weteling - stephanie@utah.gov

EXECUTIVE SUMMARY

The implementation of GovRAMP for cloud contracts in Utah is a monumental achievement in cross-boundary collaboration that has fundamentally transformed vendor risk management. Pioneering a verify once, use for many framework, GovRAMP establishes a unified, federal-grade security standard that solves the critical problem of inefficient, disparate security checks. This innovative model replaces point-in-time checks with rigorous, continuous monitoring based on NIST 800-53 Rev. 5 standards, significantly enhancing the state's risk posture and protecting sensitive data like PII and health records. The measurable impacts are transformative:

- **Accelerated Security:** The review process for pre-certified vendors is reduced from weeks or months to mere days, achieving up to a 50% reduction in the authorization timeline.
- **Substantial Cost Avoidance:** The project implemented a risk-transfer mechanism, leveraging centralized Third-Party Assessment Organization (3PAO) assessments and transferring the financial burden of security compliance—potentially millions of dollars in custom audit costs—directly to vendors.
- **Enhanced Public Trust:** By requiring 24/7 continuous monitoring for all cloud vendors, especially those managing sensitive data like PII and health records, the state has significantly reduced the likelihood of a catastrophic security incident.

GovRAMP is not just a success for Utah; it directly addresses the NASCIO Top Ten Priority: Cybersecurity and Risk Management. Utah's centralized, GovRAMP-based authorization model provides a crucial blueprint for other states facing the security-versus-speed dilemma. This project is an essential investment in state resilience, safeguarding data, accelerating secure cloud adoption, and protecting the public's trust in digital government.

IDEA

Problem or opportunity addressed

We have partnered with GovRAMP to enhance cybersecurity measures and ensure compliance with national security standards. This helps us protect sensitive government data, mitigate cyber risks, and streamline procurement for cloud service providers. By adopting GovRAMP's standardized approach, Utah is improving efficiency, fostering innovation, and ensuring that cloud vendors meet rigorous security requirements before engaging with state agencies.

Before implementing GovRAMP, the internal DTS security team verified vendor adherence to security requirements for contracts with cloud solutions. By implementing GovRAMP, Utah has established a unified, widely accepted government security standard. It solves the critical business problem of vendor risk management by providing a *verify once, use for many* framework, ensuring that any cloud product used by the state meets a rigorous, baseline security threshold without needing to be reinvented by every single agency.

Why it matters

Business Rationale: As the state moves toward cloud-first and digital government initiatives, the attack surface grows. GovRAMP enables a rapid, secure transition to the cloud.

Supporting Data: Traditional vetting could take months; GovRAMP reduces the authorization timeline by up to 50% for pre-certified vendors.

Affected Population: This affects every individual interacting with state digital services, ensuring their data (PII, tax info, health records, etc.) is protected by federal-grade security standards.

Consequences of Not Acting: Without this, the state faces increased risk of data breaches, high administrative overhead for security teams, and vendor lock-in due to the difficulty of switching to newly vetted providers.

Risk Posture Improvement: By standardizing the cloud security under GovRAMP, the state is shifting from disparate, point-in-time agency security checks to a unified, continuous monitoring framework based on the rigorous NIST 800-53 Rev. 5 standards. This fundamentally improves our risk posture by conducting regular third-party penetration testing, continuous vulnerability management, and formal incident response protocols for all cloud vendors hosting state data. Implementing the GovRAMP Fast Track and Progressing Snapshot programs ensures that we eliminate critical blind spots across the supply chain, ultimately safeguarding resident data from modern cyber threats.

What makes it different

Utah's implementation is innovative because it bridges the gap between federal FedRAMP standards and state-level agility. Unlike generic security questionnaires, GovRAMP provides a continuous vendor monitoring framework. It is distinct because it doesn't just check a box at procurement; it establishes a lifecycle of security accountability for vendors that is shared across the entire state executive branch.

What makes it universal

This project aligns directly with the NASCIO Top Ten Priority: Cybersecurity and Risk Management. It is universal because all 50 states face the same security vs. speed dilemma. Utah's model of adopting a centralized, GovRAMP-based authorization process serves as a blueprint for other states to achieve economies of scale in cybersecurity. Currently, there are approximately 71 states and government entities in various stages of implementing GovRAMP; the more that implement this, the better the standard becomes for all vendors who do business with government entities.

IMPLEMENTATION

Roadmap

Enterprise View: GovRAMP is the cornerstone of the state's **Zero Trust Architecture**. It fits into the enterprise view by serving as the gatekeeper for the state's SaaS, PaaS, and IaaS ecosystem.

Management Approach: We utilized a gradual implementation approach to give vendors time to become familiar with GovRAMP and work towards getting certified. On July 1, 2025, we started with the Information Technology Contract Terms and Conditions containing standard verbiage around the requirement for all new solicitations/contracts. Within these new solicitations/contracts, we provide standard language in the scopes of work based on the level of data the solution contains, with a ramp-up requirement of verified Core Authorized status no later than 12 months after the date of contract execution, and those with sensitive data achieving GovRAMP Moderate Authorized no later than 24 months after the date of contract execution. Effective July 1, 2027, all solicitations with a requirement of GovRAMP or FedRAMP will require that the product already hold an appropriate verified status (Core, Ready, Authorized/Provisionally Authorized). DTS is coordinating with executive branch agencies during this ramp-up period to have existing contracts amended to include GovRAMP requirements where applicable. There will also be annual reviews and audits of vendor compliance with the GovRamp standards.

Success Metrics: Success is defined by 100% of new cloud contracts being GovRAMP-compliant, a reduction in the average number of days to complete a System Security Plan (SSP) review, and assurance that the vendor is operating securely and meeting compliance requirements, thus reducing security risks to the state.

Vendor Compliance Timeline showing the 2-month, 12-month, and 24-month milestones.

Existing Contract Review Scope: Utah has identified a massive portfolio of 393 existing IT contracts and purchase orders spanning multiple departments (including Technology Services,

Health and Human Services, Natural Resources, and Public Safety). These existing contracts will undergo a strategic review and amendment phase to seamlessly transition our legacy cloud portfolio into alignment with the new GovRAMP minimum mandatory security requirements, without disrupting critical services.

Training and Adoption: To guarantee a smooth rollout, Utah conducted a series of targeted training and awareness campaigns.

- We successfully trained over 430 state employees—including agency IT Directors, purchasing agents, and Information Security Officers—on the new process and the GovRAMP contract execution lifecycle.
- We have also successfully introduced GovRamp requirements into all Enterprise Architecture reviews, thereby increasing the state's overall security level and ensuring only compliant vendors and their technologies are added into our technology stack.
- We hosted comprehensive webinars for the vendor community, with over 100 vendors attending to learn about the GovRAMP Progressing Snapshot program, the Fast Track option for FedRAMP-authorized products, and the mandatory 12-to-24-month compliance milestones.

Who was involved

Key Groups: The Division of Technology Services (DTS) including the DTS Security team, Office of the Chief Technology Officer, Enterprise Architecture, DTS Business Operations, DTS Public Information Officer; Division of State Purchasing; and external partners from GovRAMP.

Buy-in & Adoption: Buy-in was secured through a series of webinars for agency directors and personnel. We communicated the value proposition not as "more red tape," but as a **risk-transfer mechanism** that relieves the state of the burden of deep technical security auditing. Many webinars have also been held for the vendor community to make them aware of the program, timeline of implementation, and the state's requirements.

How we did it

Resources: We leveraged existing DTS, Division of State Purchasing, and GovRAMP personnel time. A financial investment will be on the vendors as they obtain GovRAMP membership.

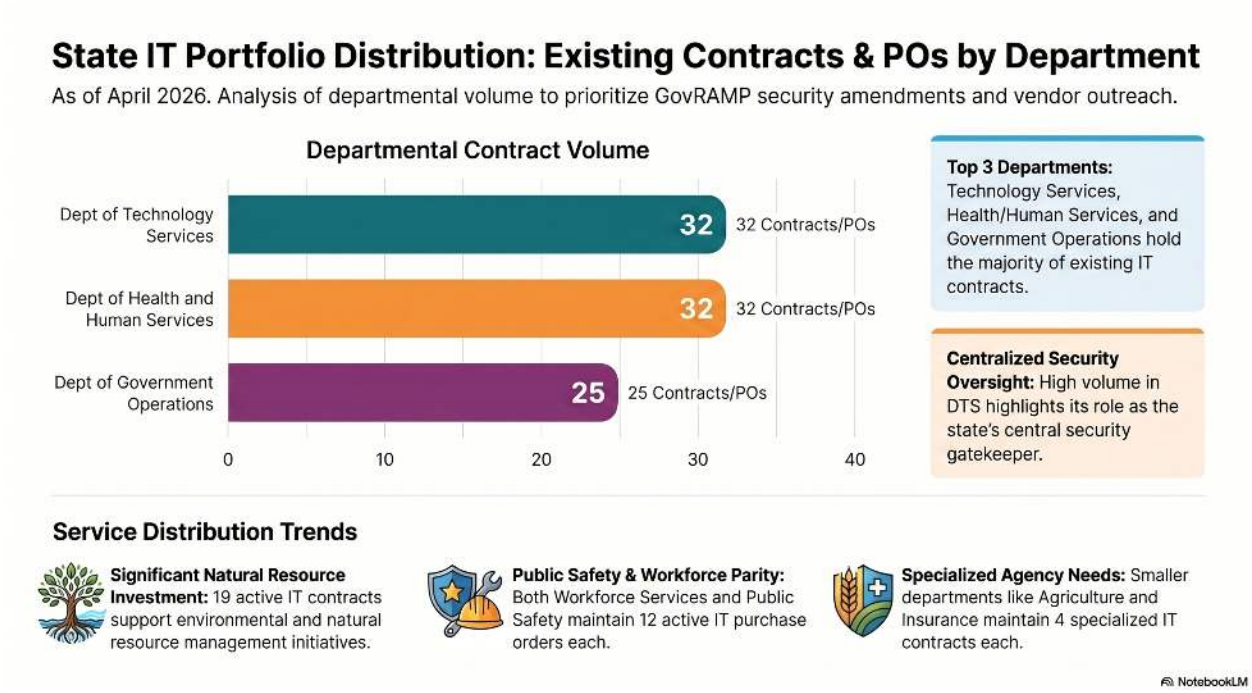
Technical Architecture: The framework relies on a **centralized repository of authorized vendors** held and maintained by GovRAMP, which focuses on *standardized controls* (NIST 800-53). This allows for automated compliance checking and ensures that, regardless of the vendor, the security language remains consistent across the state's network.

IMPACT

What the project made better

The implementation of GovRAMP fundamentally transformed vendor risk management in Utah. It replaced the "wild west" of cloud procurement with a disciplined and secure ecosystem. Before GovRAMP, security was an afterthought in procurement; now, it is a prerequisite for engaging with state agencies.

- **Elevated Security Posture:** The state shifted from disparate, point-in-time agency security checks to a unified, continuous monitoring framework based on the rigorous NIST 800-53 Rev. 5 standards. This fundamentally improves the state's risk posture by mandating regular third-party penetration testing, continuous vulnerability management, and formal incident response protocols for all cloud vendors hosting state data.
- **Process Efficiency:** The project established a *verify once, use for many* framework, which accelerates the risk mitigation of innovative cloud tools because the security heavy lifting is already completed.
- **Risk Transfer:** GovRAMP introduced a risk-transfer mechanism that relieves the state of the burden of deep technical security auditing. This ensures the state is protected by federal-grade security standards while transferring the financial burden of security



How we know

- **Quantitative:** We have seen a measurable decrease in the time required for security sign-offs. For vendors already in the GovRAMP pool, the review process is reduced from weeks to days.

- **Qualitative:** Feedback from agency IT leads indicates they feel more confident in their security posture, knowing that their vendors are subject to 24/7 continuous monitoring rather than a one-time or once-a-year audit.
- **Testimony:** *"For the Utah Department of Health & Human Services, the implementation of GovRAMP means faster deployment of critical health technologies, robust protection of sensitive PHI (Protected Health Information), and a reduction in the administrative burden on IT and security teams. GovRamp ensures that the digital tools serving our most vulnerable populations are not only innovative but meet the highest tier of national security standards."* — Rachael Stewart, DHHS IT Director.

Cost Avoidance & Efficiency ROI: The financial impact of implementing GovRAMP is substantial in terms of cost avoidance and resource optimization.

- **Audit Cost Avoidance:** By leveraging GovRAMP's centralized Third-Party Assessment Organization (3PAO) security assessments, the state avoids the prohibitive costs of conducting individual, custom technical audits for every cloud procurement. Vendors directly absorb the GovRAMP authorization review fees—which range from $1,500 to $7,500 depending on vendor revenue—effectively transferring the financial burden of security compliance away from the state's budget.
- **Accelerated Review Time:** The introduction of the Fast Track option for vendors with existing FedRAMP authorizations allows us to rely on pre-vetted GovRAMP statuses. This *verify once, use many* approach reduces internal DTS security review times from weeks or months down to mere days.
- **Breach Mitigation:** Most importantly, transitioning our nearly 400 legacy IT contracts to NIST 800-53 Rev. 5 standards with 24/7 continuous monitoring significantly reduces the likelihood of a catastrophic data breach, avoiding millions of dollars in potential recovery costs, legal liabilities, and the loss of public trust.

What now

Long-term Plan & Maintenance: The project will be maintained through a newly assigned DTS Project Manager, DTS Security, and DTS Business Operations teams.

Why It's Worth It: The implementation of GovRAMP is an investment in **state resilience.** While vendors carry the burden of the cost for this program and may pass it on to state agencies, the cost of a single major data breach far outweighs the potential cost of this program. By standardizing our defenses, we are not just protecting data; we are protecting the public's trust in digital government.