GovRAMP Learning Series: Preparing for the Cyber Summit

A Guide to Shared Responsibility, Procurement, and Partnerships in Cloud Security

GovRAMP

Published 2025

Foreword

At GovRAMP, we believe secure cloud adoption depends on collaboration. That's why we created the inaugural Learning Series: Preparing for the Cyber Summit.

This three-day virtual series brought together government leaders, providers, and partners to revisit the fundamentals — the shared responsibility model, procurement and contracting strategies, and building true partnerships across the ecosystem.

This e-book compiles highlights from each day, along with practical takeaways for both governments and providers. Think of it as your on-ramp to the conversations we'll continue in person at the GovRAMP Cyber Summit with presenting sponsor Carahsoft, October 2–3, 2025 in Chicago.

Why Focus on Shared Responsibility?

Because sometimes we all need to get back to basics.

Navigating shared responsibility is one of the most foundational challenges in pursuing security but can also offer some of the best opportunity for partnership between the public and private sectors.

Today's complex and nuanced digital supply chain requires that both 'sides' take a fresh look at shared responsibility and begin incorporating it as a fundamental part of the contracting and operationalization process.

CONTENTS

Day 1: Private Sector Focus — Cloud Security & Collaboration

Keynote: The Future of Cloud Responsibility

Joe Bielawski, President, Knowledge Services & GovRAMP Co-Founder

Joe reminded us that the shared responsibility model is more than a technical framework — it's a partnership model. State and local governments depend on providers not just for products, but for trust.

Key Takeaways

- Treat public–private partnerships as shared responsibility in action — not just contracts.
- Don't wait for perfect conditions; start wherever you are in your security journey.
- Reputation and transparency are stronger differentiators than price in public procurement.

> *"Procurement runs on terms and conditions; security runs on controls. When those worlds don't mix, we default to self-attestation and check-the-box risk."*
>
> Joe Bielawski, Knowledge Services

🎯 **GovRAMP Resource**

Download the **Customer Responsibility Matrix (CRM)** template to map your responsibilities.

> *"Reputation—not revenue—is what carries you through hard moments. Have a servant's heart."*
>
> Joe Bielawski, Knowledge Services

Day 1: Private Sector Focus — Cloud Security & Collaboration

Drawing the Line: What You Own vs. What the Cloud Secures

Tory Crass (Tanium), Josh Daymont (Securisea), Tim Davis (Fortreum)

“The biggest security gap isn’t a control — it’s a misunderstanding of who owns what,” saif panelist Tory Crass from Tanium. Panelists explored how providers and governments can better align roles in IaaS, PaaS, and SaaS. They discussed how misaligned expectations often create vulnerabilities and highlighted that tools like Customer Responsibility Matrices and Center for Internet Security (Control Implementation Summary (CIS)) Critical Security Control worksheets should be treated as living documents that evolve with the partnership.

Key Takeaways

- Ask for and share the CRM early — it sets the foundation for trust.
- Document what’s promised during sales to avoid painful surprises at audit.
- SaaS requires the closest scrutiny; responsibilities blur more than with IaaS or PaaS.
- Misunderstandings spread fastest when assumptions are left undocumented.

What This Means for You

- **Providers**: Go beyond generic documentation — deliver CRMs early, update them often, and make sure your sales commitments match what’s written in your security package.
- **Governments**: Don’t just request a CRM; insist on walking through it with providers and use it as a living tool to confirm who owns what in SaaS, PaaS, and IaaS environments.
- **Both**: Treat misunderstandings as risks equal to technical gaps — resolve them quickly through transparent conversations.

> *“CRMs should be living documents; assumptions are where risk hides.”*
>
> Tim Davis, Fortreum

> *“Shared responsibility is one of the most complex parts of this endeavor...CRM is the baseline, but you still need real conversations.”*
>
> Josh Daymont, Securisea

Watch the entire Day 1 session recording. ▶

Day 2: Public Sector Focus — Procurement & Risk Evaluation

Keynote: Building Shared Responsibility into Cloud Contracts

Jessica Van Eerde (GovRAMP) & Travis Abatemarco (Okta)

Jessica and Travis emphasized that contracts are where risk expectations should be crystal clear. Service Level Agreement (SLA)s, accountability clauses, and shared responsibility provisions ensure security isn't just assumed — it's enforced by both parties.

Key Takeaways

- Use **RACI (Responsible, Accountable, Consulted, Informed) charts** to translate shared responsibility into concrete roles and actions.
- Frame contracts as **partnership tools, not adversarial checklists** — the goal is collaboration that strengthens security on both sides.
- Build in accountability clauses and SLAs that encourage transparency and problem-solving, not finger-pointing.

> *"Don't leave shared responsibility until later—build it into the contract."*
>
> Jessica Van Eerde, GovRAMP

> *"CRM and configuration guides turn 'who owns what' into 'how it's actually done."*
>
> Travis Abatemarco, Okta

Day 2: Public Sector Focus — Procurement & Risk Evaluation

How to Vet Cloud Providers — The Smart Government Playbook

Trace Ridpath (Optiv), David Resler (GovRAMP PMO)

Panelists highlighted how governments can make smarter procurement decisions by blending audits and frameworks like System and Organization Controls 2 (SOC 2), Federal Risk and Authorization Management Program (FedRAMP), and GovRAMP. With GovRAMP Snapshot, Core, Ready, and Authorized, agencies now have scalable ways to align security with risk. But the panelists agreed: procurement isn't just about frameworks — it's about building trust.

Key Takeaways

- Frameworks signal different levels of assurance — know the difference between audits like SOC 2, and frameworks like FedRAMP and GovRAMP.
- Transparency is now a market differentiator; lack of it should be treated as a risk signal.
- Governments and providers both strengthen security when they approach procurement as a partnership, not a transaction.

What This Means for You

- **Governments**: Don't just collect acronyms — demand clarity. Ask providers how their controls actually map to your operations, and treat unwillingness to share as a warning sign.
- **Providers**: Be proactive in showing how your GovRAMP package supports state and local requirements. Demonstrate transparency early — it builds trust and speeds procurement.
- **Both**: Use GovRAMP as a common language for responsibility, and frame contracts as tools to collaborate, not as adversarial checklists.

> *"The difference between frameworks isn't just acronyms — it's about the level of assurance you can provide."*
>
> David Resler, GovRAMP PMO

> *"Trust is built when providers are transparent, not when they hide behind acronyms."*
>
> Trace Ridpath, Optiv

Watch the entire Day 2 session recording. ▶

Day 3: Combined Focus — Oversight & Partnerships

Keynote: Staying Ahead of Evolving Requirements

Pete Dudek (A-LIGN), Alex Whitworth (Carahsoft)

Pete and Alex explored how automation, AI, and framework harmonization are reshaping oversight. The shift isn't about more paperwork — it's about real-time validation. Agencies must ensure providers "walk the talk," and providers must be ready for faster, more automated assurance.

Key Takeaways

- Compliance is moving from static reports to continuous, automated monitoring.
- Agencies need to anticipate new requirements that demand near real-time visibility.
- Providers should embed security deeply into operations and prepare systems for automated reporting.

> *"AI-native GRC will fast-track compliance validation and harmonization."*
>
> Alex Whitworth, Carahsoft

🎯 Looking Ahead

1. Expect oversight to rely more on automation and AI-native GRC tools.
2. Prepare for expanded state & federal harmonization requirements in 2–3 years.

> *"Automation is powerful, but agencies still need judgment to know what matters."*
>
> Pete Dudek, A-LIGN

Day 3: Combined Focus — Oversight & Partnerships

From Siloed to Shared — Building Real Partnerships

Emily Larimer (Indiana), Matt Connor (Second Front Systems), Dan Frei (Utah)

This panel emphasized the human side of cloud security: partnerships flourish when governments and providers commit to regular, transparent dialogue. Procurement, IT, and legal teams must align internally before they can collaborate externally.

Key Takeaways

- Frequent, transparent conversations — even when inefficient — create resilient partnerships.
- Local governments strengthen statewide security when included in oversight conversations.
- Oversight frameworks like GovRAMP reduce duplication and accelerate due diligence.

What This Means for You

- **Governments:** Train procurement, IT, and legal teams to use a common risk language. Require providers to demonstrate transparency through continuous monitoring and framework harmonization.
- **Providers:** Reduce silos by offering integrated solutions and invest in clear, ongoing communication. Proactively share how your GovRAMP status meets state-specific needs (e.g., CJIS).
- **Both:** Treat conversations as security investments, not inefficiencies. Trust grows from clarity, consistency, and partnership.

> *"Procurement should be careful on how much we keep providers at arms' length. We need to invite them to the table as partners, not adversaries."*
>
> Dan Frei, State of Utah

> *"The 'inefficient but highly effective' conversations are how we move to a more secure future."*
>
> Emily Larimer, State of Indiana

Watch the entire Day 3 session recording. ▶

> *“The Summit is where ideas turn into action. This series was just the beginning.”*
>
> — Leah McGrath, GovRAMP Executive Director

Building Toward the Cyber Summit

Over three days, we moved from provider-focused security, to government-focused procurement, to shared partnerships and oversight.

This Learning Series was designed to give everyone a common foundation before October.

Next stop: the GovRAMP Cyber Summit, October 2–3, 2025 in Chicago — where these conversations continue, face-to-face.

Register for the 2025 GovRAMP Cyber Summit

Learn more about GovRAMP’s mission

Have questions? Reach us at info@govramp.org

GovRAMP