The Advantages of Compliance-as-a-Service for Defense Contractors

SecurScale

One Fixed Price. Complete Confidence.
Affordable. Scalable. Audit-Ready.

Riverstone Solutions Inc

641 Wynn Drive
Huntsville, AL 35816
info@riverstonesolutions.com
256-716-8379

Executive Summary

Defense contractors face unprecedented demands for cybersecurity compliance. Requirements such as DFARS 252.204-7012, NIST SP 800-171, and the Cybersecurity Maturity Model Certification (CMMC) are now prerequisites for winning and retaining contracts.

For many small and mid-sized contractors, the challenge is not a lack of commitment, but a lack of resources, expertise, and time. Traditional approaches to compliance — building in-house teams, buying multiple tools, and managing manual documentation — are costly and inefficient.

Compliance is mandatory but expensive and unpredictable. SecurScale™ solves this with one fixed price, scalable tiers, and built-in expertise that keep the DIB audit-ready and trusted by primes.

Most importantly, SecurScale™ Compliance as a Service (CaaS) offers a fixed monthly payment - eliminating hidden costs and ensuring predictable budgeting for risk-averse contractors. Small businesses avoid large, up-front costs for services.

The Compliance Challenge for Defense Contractors

Cybersecurity compliance requirements have grown in both scope and enforcement:

- DFARS 252.204-7012 mandates safeguarding of Covered Defense Information, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
- NIST SP 800-171 establishes 110 controls for protecting CUI.
- CMMC 2.0 introduces a maturity model requiring independent third-party certification for many contractors.

The implications are significant:

- Contractors who fail to comply risk being ineligible to bid on contracts.
- Prime contractors increasingly require subcontractors to prove compliance before partnering.
- Non-compliance creates exposure to cyber incidents, reputational damage, and legal consequences.

For small and mid-sized GovCons, hiring staff, managing tools, and staying audit-ready is costly and complex.

Traditional In-House Compliance vs. SecurScale™

Many contractors attempt to handle compliance in-house, only to encounter high costs, skill shortages, and slow progress. Table 1 below shows some of the challenges of Do It Yourself (DIY) Compliance and how **SecurScale™ CaaS can help**.

Requirement	Do it Yourself Compliance	SecurScale™ CaaS
Staffing	Hire cybersecurity & compliance staff (analysts, engineers, vCISO).	Expert team included, no hiring needed.
Cost	High overhead: salaries, benefits, tools, training.	One fixed monthly price — predictable and lower than hiring in-house.
Tools	Must purchase, integrate, and maintain SIEM, scanners, ticketing. Different renewal periods for licenses, tokens or certificates is time consuming to maintain.	Integrated platform included and managed so you can focus on your business and your customer's mission.
Expertise	Limited by internal skills.	Certified specialists across frameworks (CMMC, NIST, ISO, HIPAA).
Time to Compliance	Slower; staff must learn and implement controls.	Faster; pre-built templates and automation.
Audit Readiness	Manual evidence gathering.	Automated evidence capture; auditor liaison.
Scalability	Difficult to grow as requirements increase.	Tiered model scales affordably with business.
Risk Management	Reactive, siloed.	Proactive risk registers, SCRM, oversight.
Outcome	*High cost, high risk, slower adoption.*	*Affordable, predictable, audit-ready confidence.*

Table 1: Benefits of SecurScale™ CaaS over DIY Compliance

Advantages of SecurScale™

Predictable Pricing

One fixed monthly fee provides affordability and budget confidence for risk-averse contractors. One of the greatest challenges for small and mid-sized defense contractors is financial uncertainty. Hiring cybersecurity staff, purchasing multiple tools, and managing ongoing compliance often leads to **unpredictable and escalating costs**. Unexpected audit preparation, tool integration, or consultant fees can quickly overwhelm a budget.

SecurScale™ CaaS eliminates this uncertainty through **one fixed monthly fee**. Contractors know exactly what they will pay each month, making it easier to forecast budgets, control expenses, and avoid surprising costs.

Predictable pricing means compliance is no longer a fluctuating burden — it becomes a

controlled, affordable investment that enables long-term planning, stability, and peace of mind. It also gives a contractor a strong competitive edge over other businesses!

Expertise on Demand

Certified experts across frameworks deliver confidence without costly hires. Defense contractors are expected to navigate complex regulations and frameworks like FAR 52.204.21, **DFARS 252.204-7012, NIST SP 800-171, CMMC 2.0, ISO 27001, ISO 9001, HIPAA, and CMMI** — each with its own requirements, documentation standards, and audit expectations. Building an in-house team with this breadth of knowledge is **cost-prohibitive** for most small and mid-sized GovCons. Salaries for cybersecurity specialists, compliance analysts, and vCISOs can easily exceed hundreds of thousands of dollars annually.

SecurScale™ CaaS solves this by providing **immediate access to certified experts** across all relevant frameworks. Instead of carrying overhead of full-time hires, contractors gain the benefit of seasoned professionals who understand how to interpret requirements, implement controls, and prepare audit-ready evidence.

This **on-demand expertise** reduces the learning curve, accelerates compliance readiness, and instills confidence that every control has been addressed correctly. With SecurScale™, GovCons don't have to gamble with limited internal knowledge — they have a trusted partner ensuring compliance is handled accurately, efficiently, and in alignment with DoD and prime contractor expectations.

Scalable

A tiered model lets organizations progress from foundational to multi-framework maturity. Compliance is not a one-time project — it's a journey. Small businesses may begin with only the minimum requirements to safeguard Federal Contract Information (FCI), but as they grow, they often face new obligations such as handling Controlled Unclassified Information (CUI), preparing for CMMC Level 2, or meeting multiple frameworks like ISO, HIPAA, or CMMI.

Building this maturity in-house usually means starting over with new tools, staff, or consultants every time requirements evolve — a costly and disruptive process.

SecurScale™ eliminates that disruption through a **tiered model** that scales with your business. Contractors can start with the **Essentials tier** to establish a baseline, then move to **Growth** and **Equipped** tiers as they pursue higher-value contracts. Eventually, organizations can adopt **Governance** and **Comprehensive** tiers to manage risk at an enterprise level and demonstrate multi-framework compliance.

This scalable approach ensures you only pay for the level of support you need today while maintaining the ability to seamlessly expand as your compliance obligations and business opportunities grow. With SecurScale™, scalability is built in — keeping you audit-ready at every stage of maturity without unnecessary overhead or complexity.

Faster Compliance

Pre-built policies, SSP/POA&M, and automation accelerate readiness. For most defense contractors, achieving compliance is a **time-consuming and resource-heavy process**. Drafting policies from scratch, building a System Security Plan (SSP), creating and managing a Plan of Actions and Milestones (POA&M), and gathering evidence can take months — even years — when handled internally. Delays often mean lost contract opportunities, higher consulting costs, and greater exposure to compliance risk.

SecurScale™ CaaS dramatically shortens this timeline by providing **pre-built, proven policy templates** aligned with DFARS, NIST, and CMMC requirements. These policies are tailored to your organization's environment, ensuring accuracy without the wasted effort of starting from zero. In addition, SecurScale™ accelerates documentation with **ready-to-deploy SSP and POA&M structures**, making it faster to identify gaps, track remediation, and demonstrate compliance progress.

Automation further speeds the process. Continuous monitoring, vulnerability scanning, and evidence capture reduce manual effort and ensure that compliance isn't a reactive, paper-heavy burden. Instead of scrambling to prepare for an audit, organizations can demonstrate readiness at any time.

With SecurScale™, GovCons move from **months of reactive preparation to weeks of proactive readiness**, giving them a competitive edge in bidding, smoother audits, and greater confidence in their security posture.

Audit Ready

Evidence capture, periodic reviews, and access to an auditor liaison keep you prepared at all times. For defense contractors, one of the greatest risks is being caught unprepared when an audit or assessment is announced. Too often, organizations scramble to collect evidence, update documentation, and justify controls at the last minute. This reactive approach not only consumes valuable time but also increases the likelihood of gaps, errors, and failed audits — putting contracts and reputation at risk.

SecurScale™ CaaS eliminates this uncertainty by making audit readiness a continuous state, not a one-time event. The service automates evidence capture for key security and compliance activities, ensuring that documentation is always current and easily accessible. Regular periodic reviews keep compliance artifacts aligned with the latest requirements and frameworks, reducing the risk of drift or oversight.

When it comes time for an audit, SecurScale™ provides direct auditor liaison support, guiding contractors through the process with confidence. Instead of piecing together controls or scrambling for proof, GovCons can demonstrate a clear, well-documented compliance posture — instilling confidence in primes, the DoD, and certification bodies.

With SecurScale™, being **audit-ready at any moment** becomes the norm, not the exception — delivering peace of mind, lowering risk, and protecting valuable contract opportunities.

Risk Reduction

SIEM monitoring, vulnerability scanning, and SCRM reduce exposure. In today's defense contracting environment, compliance alone is not enough — organizations must also be able to **actively reduce cybersecurity risk**. Threats are evolving daily, and without continuous visibility, small gaps can quickly turn into major vulnerabilities. For many GovCons, limited staff and reactive processes mean risks often go undetected until it's too late, leading to costly incidents or failed audits.

SecurScale™ addresses this challenge with **integrated security operations** that go beyond paperwork. Continuous **SIEM monitoring** delivers real-time visibility into potential threats with 24x7 alerts and dashboards that simplify decision-making. Automated **vulnerability scanning** identifies weaknesses before adversaries can exploit them, ensuring timely remediation and stronger defenses. Additionally, SecurScale™ extends protection through **Supply Chain Risk Management (SCRM)**, providing policy guidance and oversight to reduce exposure from third-party vendors and partners.

Together, these capabilities transform compliance from a static checkbox exercise into a **proactive defense strategy**. Contractors gain the assurance that risks are being actively managed and minimized, which not only strengthens security but also builds trust with primes and the DoD.

With SecurScale™, **risk reduction is built into the service**, giving contractors peace of mind that their compliance program is also a resilience program.

Trusted by Primes

Audit-ready posture and governance oversight make you a low-risk partner. For small and mid-sized defense contractors, winning subcontract opportunities often comes down to **trust**. Large prime contractors seek partners who can handle sensitive information responsibly, demonstrate consistent compliance, and reduce overall program risk. Unfortunately, many subcontractors lose opportunities not because of lack of capability, but because their compliance posture is **perceived as uncertain or immature**.

By maintaining a **continuous audit-ready posture**, contractors can demonstrate that they are fully prepared for assessments at any time. This assurance signals to primes that they are a **low-risk, dependable partner** who can be relied upon to safeguard data and meet contractual obligations without adding compliance headaches or risk to the supply chain.

In addition, SecurScale™ provides **governance oversight and executive-level reporting**, helping contractors present their security and compliance maturity in terms that resonate with leadership and decision-makers. This transparency not only builds trust but also strengthens credibility during teaming discussions, proposal evaluations, and contract negotiations.

With SecurScale™, GovCons gain more than compliance — they gain the **confidence of primes and the DoD**, positioning themselves as reliable, competitive partners in an increasingly security-conscious industry.

The SecurScale™ Journey: A Tiered Path to Maturity

Essentials – "Build your base."

Who is it for? Small businesses seeking a strong compliance foundation. Provides baseline self-assessments, starter policies, and annual security training.

Growth – "Advance your compliance maturity."

Who is it for? Government contractors pursuing CUI work. Includes gap analysis against NIST 800-171, SSP/POA&M preparation, role-based training, and compliance advisory support.

Equipped – "Enhance your security with integrated tools."

Who is it for? Organizations ready to operationalize enterprise security with the right tools. Integrates Oxbow Security Platform®, SIEM monitoring, vulnerability scanning, and a FedRAMP authorized change management system.

Governance – "Reduce risk as a trusted partner."

Who is it for? Mature companies requiring enterprise risk and governance oversight. Adds supply chain risk management, organizational risk registers, vCISO support, and continuous monitoring.

Comprehensive – "Achieve Enterprise-level compliance maturity."

Who is it for? Enterprises managing multiple compliance frameworks. Achieves maturity across ISO, HIPAA, and CMMI, delivering resilience and competitive advantage.

A full comparison chart for the SecurScale™ Tiers is available in Appendix A.

Oxbow Security Platform ® - Simplified Cybersecurity Management

At the heart of SecurScale's *Equipped*, *Governance*, and *Comprehensive* tiers is the **Oxbow Security Platform®** —a modular, compliance-driven cybersecurity management solution. Oxbow provides a **single secure login, single platform, and streamlined view** into an organization's security posture, simplifying what is often a fragmented and costly compliance effort.

Core capabilities of Oxbow include:

- **Managed SIEM & Threat Intelligence** – 24x7 monitoring, tailored alert correlation, and real-time dashboards ensure threats are detected and acted upon quickly.
- **Continuous Vulnerability Scanning** – Automated scans identify and prioritize weaknesses, reducing the risk of exploitation and creating a defensible evidence trail for audits.
- **Compliance & Audit Support** – Oxbow directly aligns audit and accountability with NIST SP 800-171 control requirements, with built-in evidence capture and artifact management.
- **Customizable Dashboards** – Executives and technical teams gain role-based visibility, with compliance and security status available at a glance.

By integrating these capabilities, Oxbow transforms compliance from a static checklist into a **continuous, proactive, and measurable process**. Contractors not only gain stronger protection against threats but also **build a continuous audit-ready posture** that primes and DoD agencies trust.

Conclusion

For defense contractors, compliance is not just a requirement — it is a competitive differentiator. The traditional in-house model is expensive, slow, and difficult to sustain.

SecurScale™ CaaS offers a better path. It provides the expertise, tools, and oversight contractors need to stay audit-ready, reduce risk, and win the trust of primes and the DoD. With SecurScale™, there may be many paths to compliance, but only one way to keep it affordable and predictable. Through one fixed monthly price, organizations gain scalable support, budget confidence, and continuous audit readiness.

Ready to simplify compliance and stay contract-ready? Contact us to start your journey today.

Why choose Riverstone Solutions and SecurScale™ CaaS?

- **Defense Contractor Expertise** – We understand DoD requirements and contracting realities.
- **Scalable Model** – Flat-rate packages that grow with you.
- **Peace of Mind** – Onboarding, oversight, and ongoing support — without surprises.

Schedule an Discovery Call to Learn More:

☎ +1 (256) 716-8379

✉ info@riverstonesolutions.com

🌐 www.riverstonesolutions.com

📍 **Locations**

Huntsville Downtown Office:
109 Jefferson Street Suite 11
Huntsville, AL 35801

Huntsville Principal Office:
641 Wynn Drive Suite 102B
Huntsville, AL 35816