// MISSION-CRITICAL MACHINING

Security Tools Are Not a Compliance Program

A shop with internal IT, real security tooling and a vendor quote labelled “your CMMC solution” — and no way to tell how much of the framework any of it actually covered. From that starting point to 110 out of 110 on SPRS.

TUSA-CASE-001 · V1.0 · 11 SEPTEMBER 2026 · PUBLIC · TRANUSA, LLC

Client profile. A mission-critical precision machining shop supporting aerospace, defense, space and adjacent technology programs, already performing on Department of Defense contracts.

Client name and identifying details have been withheld or generalized to protect confidentiality, consistent with TRANUSA’s practice across all client engagements.

110/110	~50%	2×	Audit-Ready
SPRS self-assessment score	Cut in Microsoft licensing cost	Revenue growth during engagement	Compliant, awaiting C3PAO

01 The Problem

The shop was doing what a responsible subcontractor is supposed to do. They had internal IT. They had security tooling in place. They were actively engaged with their obligations under NIST SP 800-171 and treating them as a priority. What they did not have was a reliable way to tell how much of the framework any of it actually covered.

That is a harder question than it looks, and the market does not make it easier. Internal IT was leading the search and evaluating point solutions, and vendors were happy to supply them. One quote paired an EDR product with a SIEM and presented the bundle as “your CMMC solution.” Those are real controls doing real work. They also answer a fraction of the assessment objectives, and leave policy, documented and repeatable process, evidence collection, the System Security Plan and POA&M untouched. A shop can buy in good faith, act on the best information it has been given, and still be a long way from a complete program — with nothing visible to signal the difference.

The rest of the gap was operational rather than technical. Their IT function was built for uptime, which is what a manufacturer needs it to do: keep the machines running and the people working. Access to mission-critical systems was not being logged or reviewed — not because anyone had decided it did not matter, but because operations teams are not measured that way, and there was no system in place to make it routine.

02 What TRANUSA Did

TRANUSA came in first as an advisor rather than as an MSSP — engaged to review what the client was already doing on their CMMC journey and map it against the framework, control by control. That review is what made the picture legible: which objectives the tooling on the table genuinely satisfied, and which parts of the program no product was going to answer. It moved the conversation from which solution to buy to what a compliant operation has to look like.

By the client's own account, that is what decided the engagement. The alternative in front of them was another point solution and an assurance that it would be enough.

TRANUSA arrived with a plan instead of an assortment of products: a tiered, sequenced approach setting out what had to be true at each stage to reach compliance and, ultimately, certification. Behind the plan was a partner prepared to manage the whole of security compliance as an ongoing responsibility — scoping, remediation, evidence, and the day-to-day operations underneath it. Compliance ownership stays with the client, as it always does; what changes is who is accountable for running the program.

Scoping the enclave

Because the client was already on Microsoft 365 GCC High, TRANUSA scoped the CUI enclave enterprise-wide from the outset: every user inside the boundary rather than a subset of them.

A narrower enclave looks cheaper until you ask who maintains it. Keeping controlled data inside a partition, keeping everyone else out of it, and being able to prove both is the client's responsibility — physical and logical access segregation is a business function, not something a security compliance MSSP performs on their behalf. Scoping wide removed that standing job rather than creating it, and removed the scoping rework that otherwise arrives every time the business changes shape.

The licensing review nobody quoted

About a month in, with the environment understood well enough to be worth examining, TRANUSA reviewed the client's GCC High licensing. Microsoft had by then released GCC High Business Premium tiers carrying the feature set a CMMC Level 2 program needs, at close to half the per-seat cost of what the client was paying. Those tiers did not exist when the engagement was signed. Moving the client onto the appropriate SKUs cut their Microsoft licensing spend by roughly half, and those savings went on to cover most of the cost of the compliance program.

No one had promised that going in, and no one could have: it was not a discount available to quote. It came from continuing to watch the licensing landscape on the client's behalf after the engagement was already underway, and acting on it when it moved.

The program itself

From there the engagement ran end to end: scoping, a gap assessment against NIST SP 800-171, a full POA&M, and remediation of every item on it, alongside deployment of TRANUSA's security tool stack. Several tools the client was already paying for were retired where ours covered the same ground, streamlining their spend further. We built the compliance-driven operations they did not have — auditing and logging across mission-critical and privileged access, and a formal service desk in place of the informal one.

The division of labor is deliberate. TRANUSA sits behind the client's own IT as escalation rather than in front of it. We are their security compliance MSSP, not their operational IT department, and the engagement was structured that way on purpose.

Application control was introduced the way it has to be in a production environment. The Zero Trust platform spends roughly thirty days learning what normal operation looks like before enforcement begins, so day-to-day work is part of the baseline rather than blocked by it. System-level changes go through whitelisting after that. The friction is real, and it is a requirement of the framework rather than a preference of ours — the job is to sequence it so it never lands on the floor unannounced.

The ticketing system mattered more than anyone expected. The client had none. TRANUSA stood ours up for the compliance work and then extended it across IT operations, so user onboarding and offboarding, change management, incident response and security events all run through a single system of record. Security awareness and phishing training moved onto our platform in the same pass.

03 The Outcome

The client reached a Supplier Performance Risk System score of **110 out of 110** — a full NIST SP 800-171 implementation with no open deductions — and continues to win Department of Defense work on the strength of that self-attestation. Defense contracts account for roughly a quarter of their business today, and that share is growing.

Over the year of the engagement the shop doubled its revenue while headcount grew by only about a fifth — output scaled well ahead of hiring. In the client's view, a settled compliance posture is part of what made that possible. A shop unsure of where it stands bids carefully, because winning work it cannot support in a compliant way is how a prime relationship gets damaged. A shop that knows exactly where it stands can go after the work in front of it.

Growth of that kind is also the harder test of a compliance program. Doubling output means more jobs, more people touching controlled data, and more change moving through the environment every week. A program that only holds at low volume is not a program — it is a snapshot that survives until the business gets busy. Because the enclave was scoped enterprise-wide from the outset and the operational work already ran through a single system of record, the program absorbed that growth without the boundary moving and without the process reverting to a fire drill.

The clearest signal of how the engagement has gone is that the client has referred TRANUSA to a number of the contractors and vendors in their own supply chain.

04 Where Things Stand Today

The client is fully compliant and audit-ready at 110 out of 110 on SPRS, and has not yet been certified by a C3PAO. **These are different claims:** the compliance work is done and evidenced; the formal certification has not been issued.

Approaching a year into the engagement, TRANUSA remains the client's MSSP and maintains their evidence locker on an ongoing basis, so the SPRS score reflects a live program rather than a point-in-time push. The remaining step is the assessment itself, not further remediation.

> THE DECISION THAT CARRIED IT
>
> What used to be a fire drill — chase down the accounts, hope nothing was missed, reconstruct after the fact if anyone asked — is now a workflow that captures its own evidence as it goes. Come assessment time the evidence is already there, because it is a by-product of how the work gets done rather than a project that starts when the assessor calls.

05 What We Learned

- **A tool is not a program, and the market is full of quotes that blur the two.** EDR and SIEM are real controls and they do real work, but they answer a fraction of the assessment objectives in NIST SP 800-171. No product satisfies the policy, process, evidence, SSP and POA&M obligations that make up the rest of it. When a prospect says they already have a CMMC solution, the useful next question is which controls and objectives it actually covers — and the answer is usually a short list.
- **Having on-site IT is not the same as having security operations.** The difference stays invisible until someone asks for evidence. An operations team is measured on uptime; NIST SP 800-171 is measured on records — who accessed what, when, and whether anyone reviewed it. Shops with IT staff are often the most confident that they are covered, and the most surprised by the gap.
- **Licensing is not a one-time decision, and the savings that matter most may not exist yet.** The tiers that halved this client's Microsoft spend were released after the engagement was already running. Nobody could have quoted that discount at signing, and nobody would have found it by checking once and moving on. Compliance is almost always sold as fixed cost stacked on top of what a shop already pays — it is worth more when it occasionally hands budget back.

06 The Stack Behind It

Every engagement is backed by the same tool stack and operating model, regardless of client size. TRANUSA does not operate a staffed watch floor and does not describe itself as one.

- Continuous SIEM alerting with 24/7 escalation to TRANUSA on-call engineering
- Threat intelligence and log aggregation hosted on U.S. private cloud infrastructure
- Zero Trust endpoint defense with default-deny application control
- Continuous vulnerability management, prioritized by risk and CUI proximity

- SLA-driven patch management, with critical patches deployed to defined, reportable targets
- Enterprise GRC practice, including System Security Plan and POA&M management
- 100% U.S. Persons — no offshore personnel or subcontractors inside the compliance boundary

See what audit-ready looks like for a shop your size

Thirty-minute readiness call. calendly.com/tony-tranusa/cmmc-readiness-call · CMMC@tranusa.com

---

About this document. TRANUSA Case Study TUSA-CASE-001, version 1.0, issued 11 September 2026 by TRANUSA, LLC, Buford, Georgia. Public; may be forwarded freely.

Basis. TRANUSA engagement records and the client's own account of the engagement, reviewed with the client before publication. Client identity, location and exact figures are withheld under the engagement agreement.

Limitations. This describes one engagement and is not a prediction of results for any other organization. TRANUSA is not a C3PAO and cannot issue a CMMC certification. "Compliant and audit-ready" and "certified by a C3PAO" are different claims and are distinguished in the text above. Current as of the issue date.