

Advanced Computing Risk Management

Why a New Risk Paradigm Is Emerging

Part 2 of AGMA Global's Advanced Computing Risk Management Series

Executive framing

Advanced computing governance is increasingly about understanding the full transaction: who is buying, who will use the technology, where it will be deployed, and whether the commercial facts are coherent.

The New Reality of Advanced Computing

The global technology ecosystem is entering a period unlike any it has experienced before.

Advanced computing technologies—including artificial intelligence infrastructure, graphics processing units (GPUs), high-performance servers, accelerators, and advanced semiconductor systems—have become foundational to economic growth, scientific advancement, and digital transformation. At the same time, governments worldwide are paying unprecedented attention to where these technologies are deployed, who ultimately use them, and what capabilities they may enable.

For manufacturers, distributors, integrators, and technology providers, this creates a new set of challenges that extend beyond traditional compliance concerns. Organizations must now navigate evolving export regulations, increasingly sophisticated procurement ecosystems, complex supply chains, and heightened reputational expectations.

While the technologies themselves may be new, the underlying challenge is familiar. For decades, AGMA members have worked collaboratively to mitigate risks associated with diversion, gray marketing, counterfeiting, warranty abuse, and intellectual property theft. Throughout those efforts, one lesson has remained consistent: effective risk management starts with a fundamental understanding of where products go, who uses them, and whether the transaction makes commercial sense.

Today, those principles are more relevant than ever.

Why Advanced Computing Is Different

Not all technology products present the same level of risk.

Historically, organizations could often focus their compliance efforts on a relatively limited set of products, embargoed destinations, or risky/restricted entities. Advanced computing has changed that equation.

Modern GPUs and AI systems possess extraordinary computational capabilities. They support legitimate business functions ranging from medical research and weather forecasting to manufacturing optimization



Advancing Intellectual Property Protection

and digital services. Yet many of the same technologies have strategic significance because they can potentially support advanced military, intelligence, surveillance, or cyber capabilities.

As a result, regulatory frameworks have become increasingly sophisticated. Organizations today must consider export control classifications, restricted party lists, military end-user restrictions, ownership-related concerns, and a rapidly changing regulatory environment.

For many businesses, this means traditional compliance approaches are no longer sufficient.

The Shift from Transaction Compliance to Transaction Understanding

One of the most important developments in advanced computing governance is a shift away from purely transactional compliance.

Historically, organizations often focused on answering questions such as:

- Is the customer on a denied-party list?
- Is the destination restricted?
- Is an export license required?

Those questions remain important. However, advanced computing risk programs increasingly require broader analysis:

- Who is ultimately using the technology?
- Does the customer's business profile align with the proposed purchase?
- Where will the products be delivered, integrated, and ultimately deployed?
- Are there intermediaries whose roles are not fully explained?
- Does the proposed use case make commercial and technical sense?

These are not purely legal questions. They are fundamental business questions.

Understanding the transaction often provides greater risk visibility than screening the transaction alone.

This principle closely aligns with long-standing AGMA best practices around end-user validation, authorized channels, auditability, and transaction transparency. Organizations that successfully combat gray market diversion have long understood the value of verifying commercial realities rather than relying solely on paperwork.

Case Study: The “Perfectly Compliant” Opportunity

A reseller submits a request for a substantial quantity of advanced computing servers. Initial review reveals no obvious screening issues, and the documentation appears complete.

- No party appears on a sanctions list.
- The destination country is not restricted.
- Pricing appears reasonable.
- Contractual documentation is complete.

Best-practice insight: A deeper review, however, raises questions. The end customer is a recently established company with limited public presence. While the opportunity involves infrastructure

capable of supporting large-scale AI workloads, public records indicate only a small number of employees. When asked about deployment plans, explanations remain vague and inconsistent. No single factor proves wrongdoing. Yet several indicators collectively suggest additional diligence may be appropriate. The key lesson: Context matters, and transaction understanding frequently provides insights that automated screening cannot.

Case Study: When Everything Makes Sense

A large research institution requests advanced computing infrastructure to support climate modeling and scientific simulations.

- The organization maintains a long operating history.
- Its mission aligns closely with the requested technology.
- The deployment location is known.
- Key personnel are readily identifiable.
- Technical requirements match the proposed solution.
- Independent information sources corroborate the institution's activities.

Best-practice insight: In this case, the transaction demonstrates consistency across the customer profile, technical requirement, intended use, deployment environment, and organizational capability. Effective governance should enable legitimate business activity while appropriately managing risk. The deeper one looks, the more sense the transaction should make. If the picture becomes increasingly convoluted as more answers are provided, AGMA recommends the examiner stop and takes a very careful look at the legitimacy of the transaction.

The Value of a Prevention-First Mindset

Many organizations still concentrate significant portions of their compliance effort at or near the shipment.

Yet by the time a transaction reaches the fulfillment stage, commercial commitments have often already been made.

Advanced computing risk management increasingly favors preventive controls that begin earlier in the sales cycle. A prevention-first approach allows organizations to identify concerns before resources are committed, contracts are finalized, and expectations are established.

This philosophy mirrors broader AGMA principles that emphasize governance, strong channels, transparency, documentation, and early intervention. Successful programs generally focus not only on detecting problems but also on preventing them from occurring in the first place.

Organizations adopting this approach often seek to:

- Understand opportunities earlier.
- Validate assumptions sooner.



- Escalate unusual circumstances promptly.
- Apply consistent documentation standards.
- Maintain clear decision records.

These practices create stronger outcomes regardless of whether the underlying concern is regulatory, operational, financial, or reputational.

Looking Ahead

Advanced computing technologies will continue to transform industries and create extraordinary opportunities for innovation.

At the same time, governments, customers, investors, and the broader public increasingly expect organizations to demonstrate responsible stewardship of powerful technologies.

The most successful risk programs will not be those that simply identify prohibited transactions.

Rather, they will be those that consistently ask the right questions, understand the underlying facts, and apply sound judgment supported by documented processes.

In many respects, this is not an entirely new challenge. It is the evolution of principles AGMA members have championed for years: transparency, diligence, verification, and prevention.

As advanced computing continues to reshape the technology landscape, those principles may prove to be more valuable than ever.

AGMA Best Practice Takeaways

Focus on understanding the transaction, not just screening it. Validate that the customer profile aligns with the proposed technology and use case. Begin risk assessment as early as practical. Document decisions and supporting rationale. Treat advanced computing governance as both a regulatory compliance process and business risk management discipline.

Next in this series: Building a Prevention-First Control Framework for Advanced Computing Transactions.