

# Rethinking Risk in Aerospace & Defense

## From Checklist to Strategy



**Erika Trujillo**  
Managing Director,  
Trade Compliance  
SEIA GmbH



**Shahab Wahdatehagh**  
Vice President, Global  
Trade Intelligence  
EMEA/AP  
Descartes Systems Group



# Speakers



## Erika D. Trujillo

Erika Trujillo is the Co-founder & Director at SEIA GmbH, a compliance technologies company delivering world class risk management solutions based on advanced data analytics. Prior to launching SEIA, Erika held a senior position with a Big Four Consulting and Law Firm, where she served as a trusted advisor for clients in the field of Foreign Trade Law, with a focus on multijurisdictional export controls and sanctions, and led initiatives in trade compliance tech. Erika was also previously the EMEA leader for Trade Controls for a global automotive supplier and worked as an international trade specialist at the U.S. Department of Commerce.



## Shahab Wahdatehagh

Shahab is a senior sales & business leader with over 30 years of experience in manufacturing, consulting and B2B SaaS. His focus is on supply chain management, freight/logistics and global trade compliance and he has led teams in different roles in the Far & Middle East, Europe and the Americas. At Descartes, Shahab leads the Global Trade Intelligence business in EMEA/AP. His team's focus is supporting organizations in establishing trade and export compliance practices, which are best practices enabled by the right solutions approach. Shahab is passionate about business value delivery as well as good practices that drive social & environmental responsibility in an interconnected world.

# Agenda

- 1 Introductions
- 2 Current Aerospace & Defense Landscape
- 3 Digitalization Challenges & Impact
- 4 Best Practices for A&D Risk Management
- 5 Closing Remarks + Interactive Q&A Session



# Current Defense Landscape

Global rearmament cycle driven by geopolitical instability, aging fleets, and reshoring of critical defense manufacturing.

## Regional dynamics:

- **U.S.:** Focus on modernization, power projection, and new domains (hypersonics, space).
- **Europe:** Rapid defense buildup post-Ukraine
- **Indo-Pacific:** Japan, Australia, India increasing defense allocations to ensure supply-chain sovereignty.

**\$2,718 billion**

In 2024 global military spending reached, a **9.4% increase** from 2023, marking the steepest year-on-year rise since at least 1988.

**60% of global military spend:**

United States  
China  
Russia  
Germany  
India

**\$23.53 billion**

Expected growth in global defense IT spending market between 2024 and 2028.

# Current Defense Landscape

The growth of investment and activity in the aerospace and defense space requires investment in trade compliance capabilities to keep pace.

## Protect Technological Superiority:

Strategic Advantage protected through trade controls of critical technology.

## Generate Value:

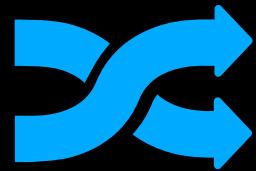
To keep up with the pace of change, trade compliance needs to have clear visibility and efficient processes.

## Maintain Regulatory Compliance:

Defense Companies are in the spotlight, and with so much investment, there is a lot of enforcement in this space.

# Technology & Adaptive Solutions

- Growth means higher complexity & volume
- Technology and adaptive solutions as extended capabilities
- Reduction of “noise in the system” is critical to manage scope



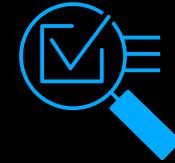
No Disruption



Contained Cost



Improved Speed



Highly Compliant

# A&D Supply Chain risks go beyond the shipped product



**Multi-tier, multinational suppliers & customers**



**Dual-use technologies and blurred boundaries**



**Digital exports and data sharing across borders**



**Thousands of components from vendors in sensitive jurisdictions**



**Exposure across procurement, joint ventures, and MRO partnerships**

# Digitalization Challenges & Impact



# A&D Digitalization Challenges



## Fragmented Master Data and Systems:

Disconnected ERPs and compliance tools prevent a single source of truth. Data quality built upon year of M&A activity and technical changes presents challenges.

## Security Architecture:

Strict controls around CUI, IL5/IL6 data environments, and NIST/CMMC mandates limit system flexibility.

## Cyber Uplift vs. Legacy Infrastructure:

Long program lifecycles and decades-old, highly customized systems hinder integration and modernization.

## Organizational Resistance:

Risk-averse culture and skill gaps slow adoption of new digital practices.

## Fast-Changing Regulations:

Trade controls change rapidly meaning that the needs of the organization evolve faster than technology update cycles. A&D also have many requirements beyond usual commercial needs.

# Traditional compliance frameworks not suitable for today's volatility



**Documentation over decision-making**



**Fragmented ownership across departments**



**Reactive rather than proactive risk management**

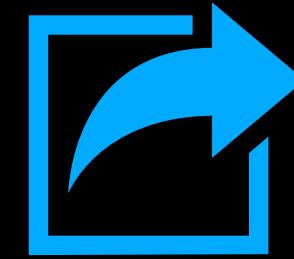
# The Cost of Reactive Compliance



**Program delays and  
reputational damage**



**Investigations  
exceeding deal values**



**Case examples: export  
control lapses**

# Demands on Trade Compliance

Regulatory obligations also tightened:

- EU's Dual-Use Regulation 2021/821 modernized the regime; the control list was updated again on Sept. 8, 2025.
- NIST SP 800-171 Rev.3 (May 2024) raised cybersecurity expectations for CUI across defense suppliers.
- CMMC final rule is rolling out in phases starting Nov. 10, 2025, adding assessed cyber controls into contracts.

Company	Penalty	Year	Violation Type
Aerospace and Defense Technology Corporation	\$29.74 million	2025	FCPA
Major Integrated Defense Contractor	\$950+ million	2024	FCPA, ITAR, Defective Pricing
Global Aerospace Manufacturer	\$51 million	2024	ITAR (199 violations)
Global Connectivity Solutions Provider	\$5.8 million	2024	EAR violations to Chinese military
Electronic Test and Measurement Equipment Manufacturer	\$6.6 million	2021	ITAR (24 violations)
Global Aerospace and industrial automation Conglomerate	\$13 million	2021	ITAR (34 violations)

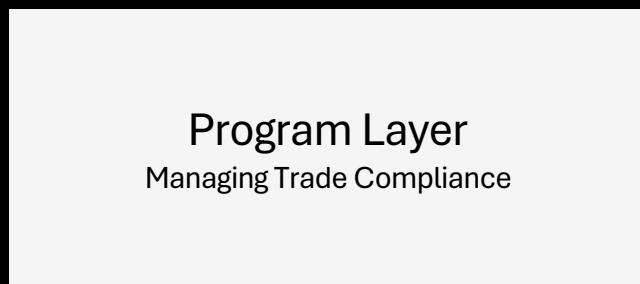
# Best Practices for Risk Management



# Modern Trade Compliance Program



Digital but designed for people.



Usually manual processes.



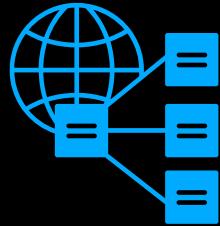
Combination of automation  
and manual processes.

# Operational Layer

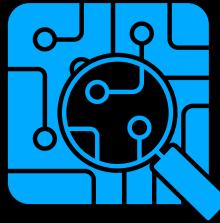
# Compliance Foundations in Aerospace & Defense



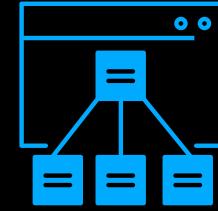
**Denied Party  
Screening**



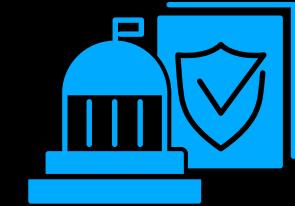
**Export  
Classification  
& License  
Determination**



**Controlled  
Technology  
Management**



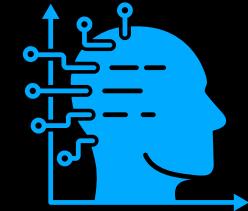
**Customs Duties  
& Trade Data**



**Regulatory  
Filing**

# Technology helps where Volume becomes a Challenge

Domain	Problem	Technology	Value	
DPS		High False Positives	AI supported Entity resolution & contextual matching	Better Precision Fewer manual reviews
Export Classification		Long manual turnaround	AI/NLP supported feature extraction & classification hinting	Improved speed Higher reliability
License Determination		Repetitive checks, consumption management, Routing	AI/ML rules & learning	Decision consistency
Deemed (Technology) Export		Embedded controls across	Contextual access control	Auditability

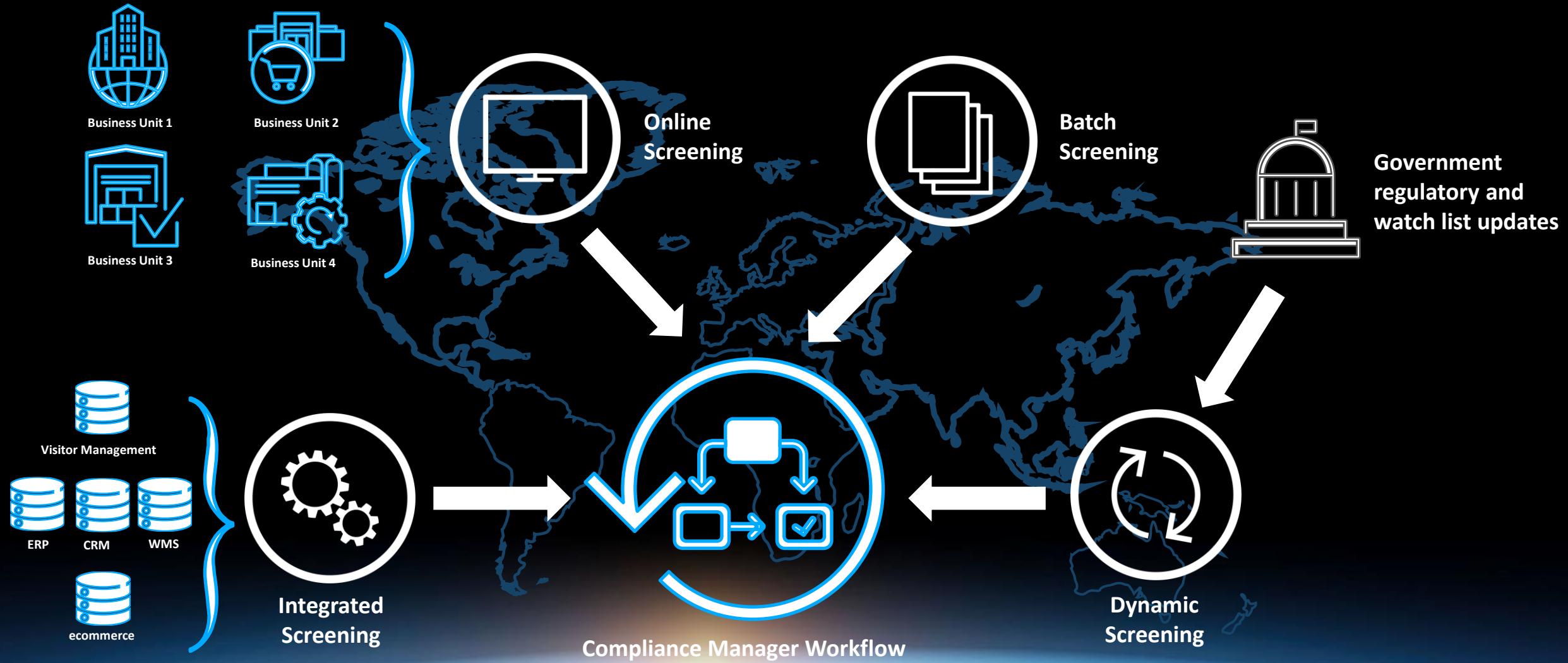


**Technology as additional capacity**



**Human oversight as ultimate authority**

# Example: Holistic DPS – Covering the Entire Enterprise



# Assurance Layer

# Understanding the Assurance Layer

The **Assurance Layer** sits on top of the trade compliance program and is designed to support the user in answering core questions like:

1. How can I prioritize my actions in a risk-based way?
2. Where is my risk exposure and why is it happening?
3. Does my trade compliance program work as intended?
4. How can I optimize my processes?
5. Have I overlooked any red flags?
6. What locations need training or support and in what areas?
7. Where can I get information for cost savings?



**Transparency**



**Continuous Monitoring**



**Program Assurance**



**Data-driven Risk Assessment**



**Review Audit Trail**

# Shifting from Checklist to Strategy



# Assurance Layer Best Practices

## Data Quality As a Measurable Risk-

Think about bad data as a risk to be measured- Bad data cannot be an excuse to avoid taking action, we rely on it to make significant decisions and we have liability for the company's collective knowledge

## Holistic Data Oversight

Do not be afraid of your data- get as much oversight as you can, maybe you also find good things like Cost Savings

## Trade Compliance Context for Data

Beyond pure analytics and reporting- Contextualize the data for trade compliance - Pure data needs SME interpretation

## Flexible Assurance Framework

Build approaches that can flexibly expand to incorporate new risks areas, policy & process changes, or business expansions (M&A)

# Art of the Possible

An advanced data analytics on-premise solution for transparency, continuous internal risk monitoring, and clear actionable insights into program assurance.

## SEIA's PERCEIVE



**Become aware of what you know.**  
Collection of Holistic Business Data  
leveraging the existing IT  
Infrastructure of the company

**SEIA connects the dots.**  
SEIA applies its unique Risk Indicators across  
the business data for regulatory and  
operational risk identification

**PERCEIVE more with SEIA.**  
Transparency, Data-Adjusted Risk  
Assessments, and Continuous Internal  
Monitoring

# Top 3 Risk Areas identified by SEIA in A&D

Infrastructure Recommendations for A&D businesses in building a strong assurance layer

1.

## U.S. Re-export issues

Especially for European companies with dual-use items, we regularly see items with indication of U.S. origin or jurisdiction without appropriate ECCNs causing re-export license determination overishgt.

2.

## License Term non-compliance

Shipping after license expiry, values not properly stored for license compliance

3.

## Sanctions Circumvention

In the defense industry especially component circumvention is a massive risk area.

# Cooperative Trade Compliance



# Closing Remarks

## Q&A



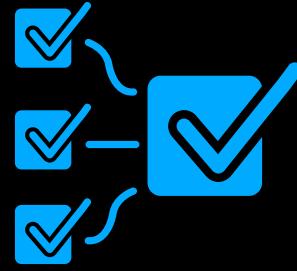
# Risks move as fast as policy does



**Geopolitical shifts and  
evolving regulations**



**Increased regulatory  
and partner scrutiny**



**Strategic consequences  
of compliance failures**



## CONTACT US:

 +49 162 7487487

 Arcostr. 3, 80333, Munich, DE

 [www.seiatech.com](http://www.seiatech.com)

 [contact@seiatech.com](mailto:contact@seiatech.com)



## CONTACT US:

 +49 89 961 60 61 60

 Martin-Luther-Ring 13, 04109, Leipzig, DE

 [www.descartes.com](http://www.descartes.com)

 [info@descartes.com](mailto:info@descartes.com)

- This communication contains general information only and is not suitable for addressing the particular circumstances of any individual company and is not intended to be used as a basis for commercial decisions or decisions of any other kind. Neither SEIA GmbH nor Descartes Systems inc. are, by means of this communication, rendering professional advice or services. No entity in the Descartes Systems inc. or SEIA GmbH network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.
- SEIA GmbH and Descartes Systems inc. provide SaaS solutions, IT related products and services to public and private clients spanning multiple industries. SEIA GmbH and Descartes Systems inc. do not provide legal advisory services.