Cyber Tech Proving Grounds

Team IT-AAC, through its agile partnership model, facilitates organizations in implementing their Zero Trust strategy. Our team provides a flexible tech assessment process, we enable organizations to assess and validate their technology components effectively. This approach leverages a diverse pool of SMEs and a virtual network of testing facilities, ensuring rigorous evaluation and decision-making. By tapping into Silicon Valley and Fortune 500 standards and innovations, we further enhance organization's' capabilities to align with and implement robust Zero Trust practices, crucial for navigating today's evolving cybersecurity landscape.

- Dr. Chase Cunningham, Dr Zero Trust (CTRC (SW) USN Ret.) PM for DOD CIO ZTA
- John Weiler, Exec Director, Interop. Clearinghouse & Chairman, IT-AAC
- VADM (ret) Kevin Green, Vice Chairman IT-AAC, former Navy DCNO
- Tom Suder, CEO ATARC.org
- Gary Wang, Research Fellow, former Army DCIO, OUSD (I) CIO
- Gregg Smith, CEO Technology Advancement Center
- Ted Manakas, Strategic Partnerships Director
- Dennis Nadler, Sr. Fellow
- Dr. Georgia Shea, Chief Technologist, Foundation for Defense of Democracies, IT-AAC Fellow

Who We Are… a public/private partnership;

Testing Labs, Do Tanks, Honest Brokers, SDOs

Our Cyber Proving Grounds Partners Include:

CISQ
Consortium for IT Software Quality

tac

Carnegie Mellon University
CyLab
Security and Privacy Institute

OMG
WE SET THE STANDARD

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

CSA cloud security alliance℠

ATARC

TIA
ADVANCING GLOBAL COMMUNICATIONS
TIAONLINE.ORG

Space Dynamics
LABORATORY
Utah State University Research Foundation

digital twin™
CONSORTIUM

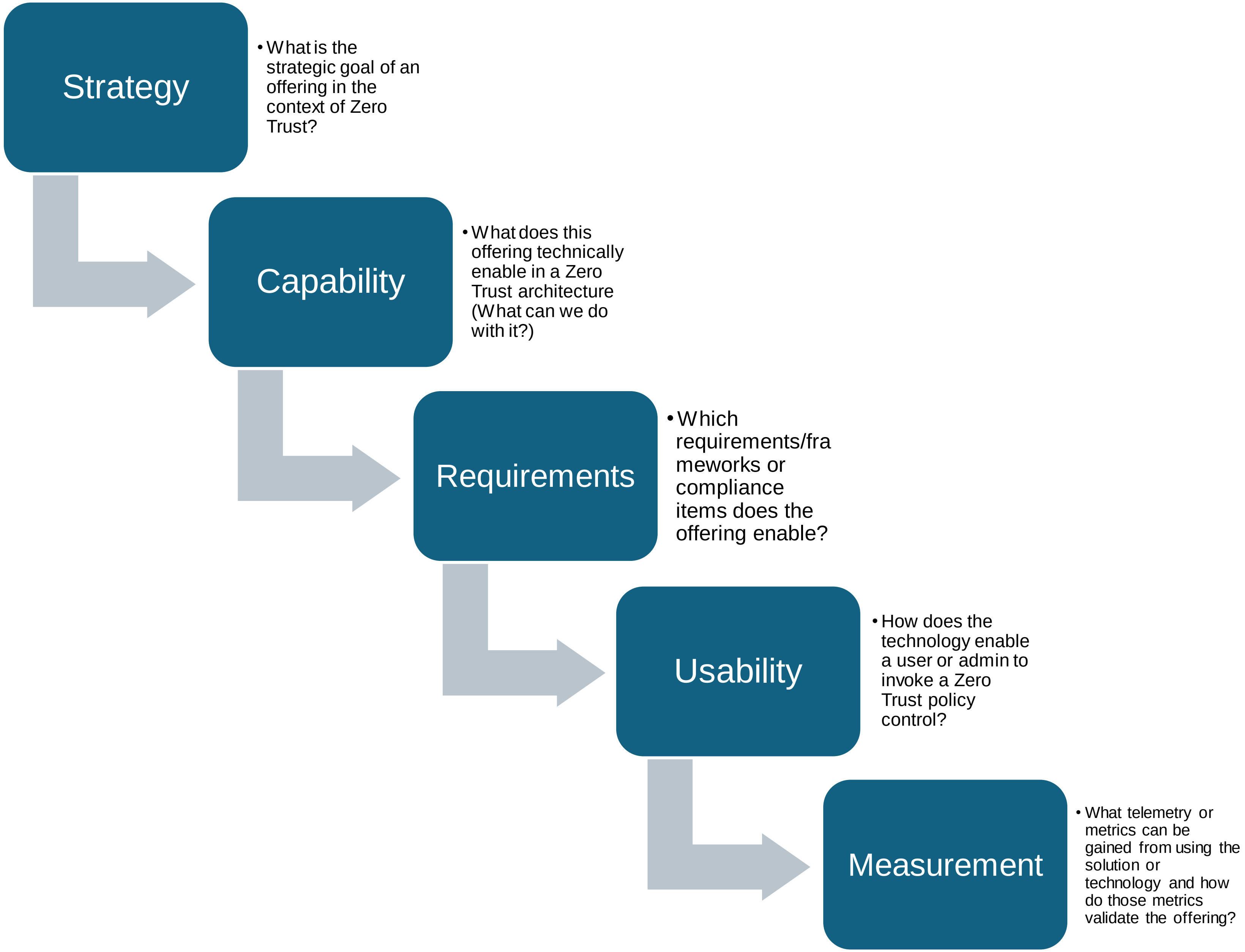
Our Combined Capabilities…

IT-AAC is an unbiased evaluator and innovator focused on the implementation of Zero Trust architectures. Our strategic capabilities center on the fundamental principle of "never trust, always verify," ensuring that access to resources and systems is continuously authenticated and authorized, regardless of user or location. By adopting Zero Trust principles and evaluating Zero Trust solutions, we fortify our clients cyber defenses against evolving threats, mitigating risks associated with unauthorized access and lateral movement within networks while aligning the overall strategy and technology portfolio to Zero Trust tenants. Through meticulous planning and cutting-edge technology integration, our team empowers our clients to achieve resilience in the face of increasingly sophisticated cyber adversaries, safeguarding critical assets and mission-critical operations.

. Key enablers include -

- Extensive ZT Expertise. Co-authored: "Zero Trust Security: An Enterprise Guide, Cyberwarfare: Truth, Tactics, and Strategies.”
- Virtual ZT Testing Lab- a virtual innovation lab composed of Universities, Standards Bodies, Communities of Practice, Innovators and SMEs that are not vested in the status quo, reaching deep into a $4Trillion global IT market.
- Our team housed and deployed Zero Trust architecture instantiations for the NSA in FY2023 via our partnership with the Technology Advancement Center in Columbia MD.
- We worked with the USAF Sabre Zero Trust program team to evaluate vendor solutions and measure their alignment and effectiveness for implementation in their operational environment.
- Collaborated with the White House National Security Telecommunications Council to aid in the Executive Order on Zero Trust.
- Created the Zero Trust eXtended Ecosystem Framework that has been foundational to the growth of Zero Trust across the globe.
- Our team has extensive OT/IOT experience related to cybersecurity architectures and implementation across various enterprise and government related efforts.

Dr.ZeroTrust SCRUM Method for Zero Trust Success.



Strategy

- What is the strategic goal of an offering in the context of Zero Trust?

Capability

- What does this offering technically enable in a Zero Trust architecture (What can we do with it?)

Requirements

- Which requirements/frameworks or compliance items does the offering enable?

Usability

- How does the technology enable a user or admin to invoke a Zero Trust policy control?

Measurement

- What telemetry or metrics can be gained from using the solution or technology and how do those metrics validate the offering?

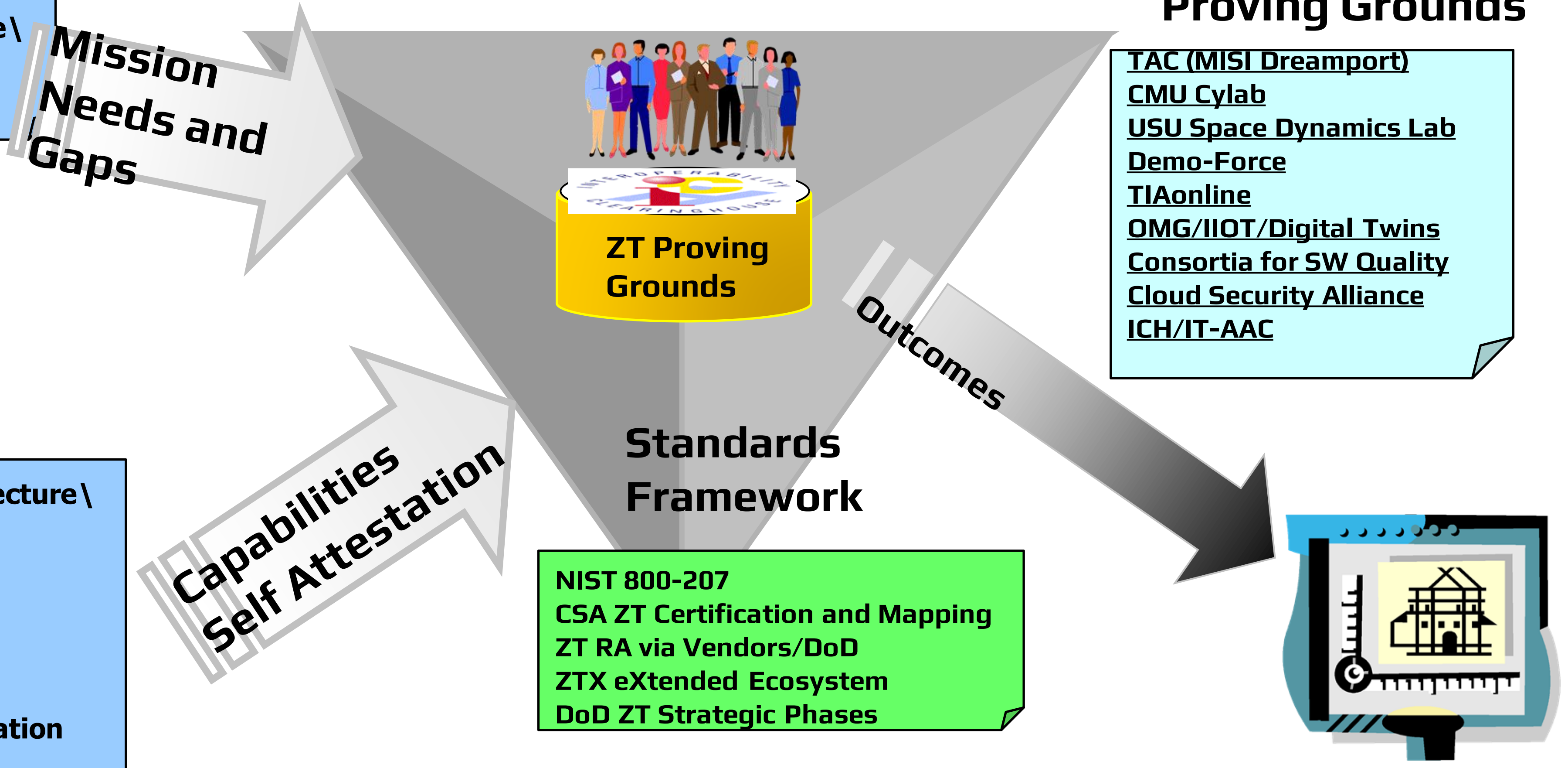
Rapid Evaluation of Emerging Tech Capabilities via Virtual Proving Grounds at the Speed of Need

Govt CxOs

- **Zero Trust Architecture**
- **Portfolio Inventory**
- **ZT Requirements**

Virtual ZTA Solution Proving Grounds

- [TAC (MISI Dreamport)]
- [CMU Cylab]
- [USU Space Dynamics Lab]
- [Demo-Force]
- [TIAonline]
- [OMG/IIOT/Digital Twins]
- [Consortia for SW Quality]
- [Cloud Security Alliance]
- [ICH/IT-AAC]



Vendor ZT Solutions

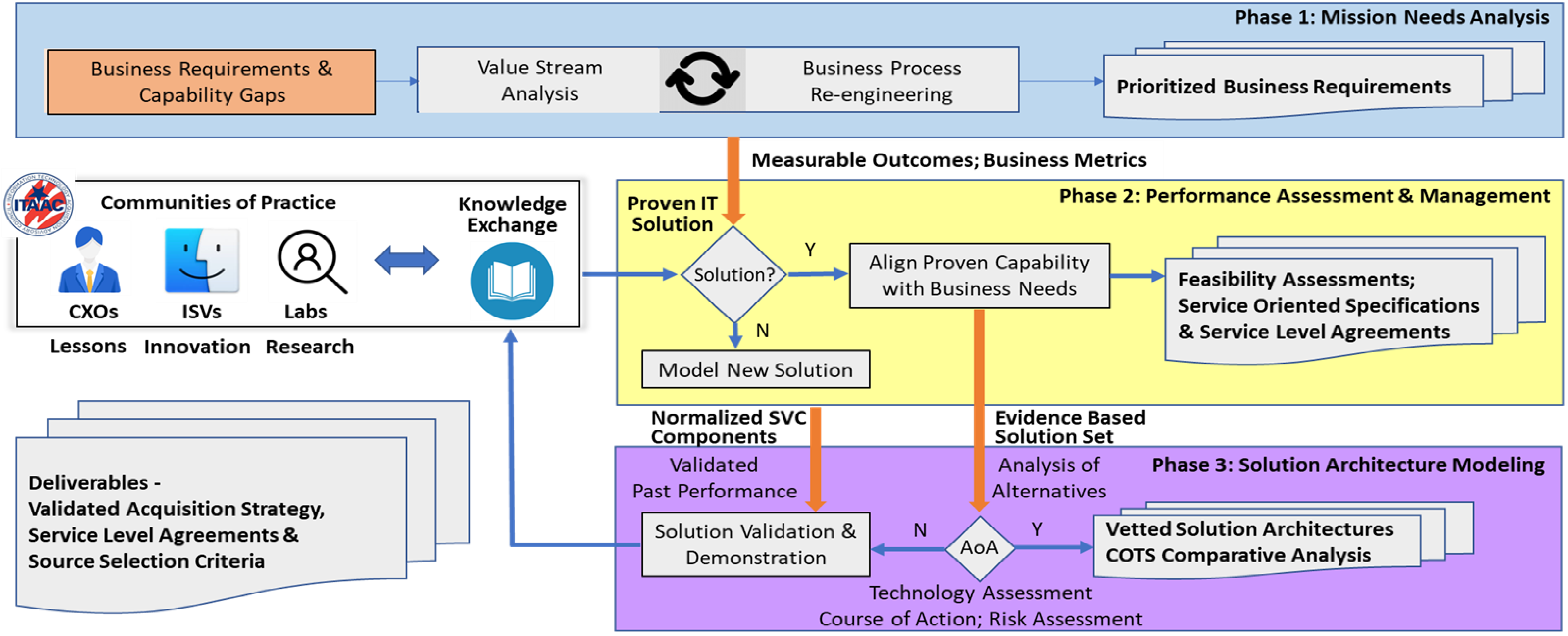
- **Zero Trust Architecture**
- **Aligned Offerings**
- **ZTNA**
- **NGFW**
- **ZTA**
- **Biometrics**
- **ZT Data Security**
- **ZT Microsegmentation**
- **ZT Policy Engine**
- **Etc.**

Standards Framework

NIST 800-207
CSA ZT Certification and Mapping
ZT RA via Vendors/DoD
ZTX eXtended Ecosystem
DoD ZT Strategic Phases

Design Patterns
Performance Metrics
ZT AOA
Acquisition Ready

IT-AAC Proving Grounds facilitates every phase of migration to Model and Map ZT capabilities to measurable outcomes…



Phase 1: Mission Needs Analysis

Business Requirements & Capability Gaps

Value Stream Analysis

Business Process Re-engineering

Prioritized Business Requirements

Measurable Outcomes; Business Metrics

Communities of Practice

Knowledge Exchange

Lessons Innovation Research

Phase 2: Performance Assessment & Management

Proven IT Solution

Align Proven Capability with Business Needs

Feasibility Assessments; Service Oriented Specifications & Service Level Agreements

Model New Solution

Normalized SVC Components

Evidence Based Solution Set

Deliverables - Validated Acquisition Strategy, Service Level Agreements & Source Selection Criteria

Phase 3: Solution Architecture Modeling

Validated Past Performance

Analysis of Alternatives

Solution Validation & Demonstration

Vetted Solution Architectures COTS Comparative Analysis

Technology Assessment Course of Action; Risk Assessment

AAM Tools	Problem Statement	Capability Analysis	Solution Determination	Capability Prioritization	Feasibility Assessment	Economic Analysis	Roadmap Planning	Risk Assessment

IT-AAC Zero Trust Tech Assessment Model

Zero Trust Metrics and Mapping

- ✓ Measure what matters; risk, cost, outcomes.
- ✓ You can only manage what you measure,   build controls into contracts that measure risk/value/cost of all delivered and managed systems
- ✓ Leverage industry accepted ZT frameworks and technology alignment

Service Level and Risk Management

- ✓ SLAs that treat software enhancements and maintenance as a service; track levels, penalties, credits
- ✓ Align SLAs with Mission Outcomes and Incentives
- ✓ Cyber Resilience must be architecturally driven
- ✓ Zero Trust enablement and outcome mapping specific to DoD ZT Phases

Zero Trust Efficacy and Technology Measurement Matrices

- ✓ Start with Capability Based, Mission specific requirements currently published via the ZT PMO
- ✓ Align requirements with commercial standards and market capabilities (MOSA)
- ✓ Remove “make bias”, leverage 80% COTS solution that are service oriented and open
- ✓ Test and vet vendor solutions in a virtual open platform to produce metrics and measurements that feed the DoD ZT selection process

Systematic Alignment of Vendor Technologies with DoD's Zero Trust Strategy & NIST 800-207

Defining Zero Trust Components

To validate these offerings, IT-AAC would meticulously define Zero Trust architecture components according to the guidelines outlined in NIST 800-207, tailoring them to meet the specific needs and constraints of the agency's current and future architecture state. This involves a thorough understanding of DoD's Zero Trust requirements, mapping them systematically to the identified components to ensure alignment and effectiveness. Furthermore, prioritization of these components would be conducted based on DoD's operational needs, utilizing methodologies such as SCRUM to ensure agile and iterative implementation while aligning with the foundational pillars of Zero Trust for comprehensive security coverage.

- Define the Zero Trust architecture components as outlined in NIST 800-207 specific to agency needs and current and future architecture state.
- Map DoD’s Zero Trust requirements to these components.
- Prioritize components based on CIO/CISO operational needs and align them to the SCRUM method and ZT Pillars.

Establishing Assessment Criteria

To validate these offerings, IT-AAC would establish rigorous criteria for technology assessment, drawing upon NIST principles to ensure robustness and adherence to industry best practices. This process would include the incorporation of DoD-specific security protocols and compliance requirements, guaranteeing that selected technologies meet the highest standards of security and regulatory compliance. Furthermore, IT-AAC would develop a comprehensive matrix to systematically evaluate vendor technology against these criteria, enabling transparent and objective decision-making in the procurement process.

- Establish criteria based on NIST principles for technology assessment.
- Incorporate DoD-specific security protocols and compliance requirements.
- Develop a matrix to evaluate vendor technology against these criteria.

Zero Trust Market Research and Technology Assessment

The IT Acquisition Advisory Council (IT-AAC) would conduct comprehensive market research by leveraging its extensive network of industry experts, engaging in dialogue with technology vendors, and analyzing market trends and emerging technologies. Through rigorous evaluation and assessment, IT-AAC would identify innovative solutions and best practices tailored to the specific needs of the Department of Defense (DoD), ensuring informed decision-making and optimal utilization of resources.

Key aspects of IT-AAC's market research process:

- Engage with industry stakeholders: Establish communication channels with technology vendors, industry associations, and subject matter experts to gather insights on cutting-edge solutions and market trends.
- Analyze market intelligence: Conduct thorough analysis of market reports, industry publications, and technological advancements to identify emerging trends, potential disruptors, and innovative solutions relevant to the DoD's requirements.
- Evaluate vendor capabilities: Assess the capabilities, track record, and reputation of technology vendors through in-depth evaluations, product demonstrations, and reference checks to ensure alignment with DoD's needs and standards.
- Consider regulatory and compliance requirements: Stay abreast of regulatory changes, standards, and compliance requirements impacting the procurement of IT solutions within the government sector, ensuring adherence to legal and security frameworks.
- Facilitate collaboration and knowledge sharing: Foster collaboration and knowledge sharing among government agencies, industry partners, and academia to exchange insights, lessons learned, and best practices in IT acquisition and implementation.

Quantitative Scoring System

To further validate these offerings, IT-AAC would implement a quantitative scoring system for technology evaluation, facilitating a systematic and data-driven approach to assessing vendor solutions. This scoring system would factor in compliance with both NIST and DoD-specific requirements, ensuring alignment with industry standards and government regulations. Additionally, IT-AAC would highlight areas where vendor technology excels or may fall short, providing clear insights to inform decision-makers about the strengths and weaknesses of each solution under consideration.

- Implement a quantitative scoring system for technology evaluation.
- Factor in compliance with NIST and DoD-specific requirements.
- Highlight areas where vendor technology exceeds or falls short.

Longitudinal Analysis and Procurement Strategy

To further validate these offerings, IT-AAC would conduct ongoing analysis to assess the alignment of vendor technology with Zero Trust principles over time. This includes leveraging historical data and trends to predict future compliance and alignment, enabling proactive adjustments to procurement strategies. By employing results-based analysis, IT-AAC ensures that the procurement process remains dynamic and responsive to evolving security requirements and technological advancements within the Zero Trust framework.

- Analyze the alignment of vendor technology with Zero Trust principles over time.
- Use historical data and trends to predict future compliance and alignment.
- Adjust procurement strategies based on results based analysis.

Adaptive Evaluation and Continuous Improvement

To validate these offerings comprehensively, IT-AAC will incorporate feedback loops for continuous vendor evaluation, fostering iterative improvements and maintaining a high standard of performance. This process includes updating criteria and testing methodologies in response to evolving security landscapes, guaranteeing relevance and effectiveness in addressing emerging threats. Furthermore, IT-AAC will ensure alignment with DoD and NIST updates and amendments, staying current with the latest regulations and best practices to uphold the highest standards of security and compliance.

- Incorporate feedback loops for continuous vendor evaluation.
- Update criteria and testing methodologies based on evolving security landscapes.
- Ensure alignment with DoD and NIST updates and amendments.

Penetration and Scenario-Based Testing

To further validate these offerings, IT-AAC will conduct penetration tests simulating advanced persistent threats (APTs), providing realistic scenarios to assess the robustness of vendor solutions under adversarial conditions. Additionally, scenario-based testing will be employed to evaluate the vendor's response capabilities, ensuring they can effectively mitigate and contain potential threats. The outcomes of these tests will be meticulously mapped to Zero Trust architecture components, offering concrete insights into the effectiveness of the security measures in place. Moreover, IT-AAC will validate the Zero Trust architecture against red team operations, simulating DoD instantiation of tools, techniques, and procedures to ensure resilience against real-world threats and adversaries.

- Conduct penetration tests simulating advanced persistent threats (APTs).
- Use scenario-based testing to evaluate vendor's response capabilities.
- Map test outcomes to Zero Trust architecture components.
- Validate ZT architecture against red team operations for DoD instantiation of tools, techniques and procedures.

Phases

- 2023: Initial mapping of vendor technologies to Zero Trust components as outlined in NIST 800-207. (Completed)
- 2024: Development of specific assessment criteria for vendor technologies based on DoD and NIST requirements. Implementation of comprehensive penetration and scenario-based testing protocols.
- 2025: Integration of quantitative scoring systems for detailed technology evaluation. Analysis of vendor technology alignment with Zero Trust principles over time, using historical data.
- 2025-2026: Adaptation of procurement strategies and continuous improvement mechanisms based on evolving security landscapes.

Past Performance…

Navy: Assessment of AFLOAT Program – CANES SOA & Security Strategy Eliminated hi-risk Requirements by 23%, $100Ms in potential savings	USAF: Streamlined COTS Acquisition Process. Applied to Server Virtualization. Established optimal arch with ROI of 450% & $458 million savings	AFISRA: Applied AAM to conduct ISR Portfolio Risk Assessment (PRA) Guiding reorganization and restructure of ISR Portfolio
DISA CAE: DISN GSM-O Re-compete Restructured performance metrics, acquisition strategy and SLAs to enable 30% savings on existing DISN Mgt. Greatly Exceeded Forecasted Saving in both analysis and acquisition	GSA CFO: Financial Mgt. System consolidation using AAM. Moved GSA FMS from OMB "red" to "green". Eliminated duplicative investments that saved $200M	BTA DBSAE: Transformed DOD's Requirements and Agile process, with 2 successful pilots $300 million in potential savings with minimal investment
Discovery Channel: Apply AAM to complete AoA and BCA for Enterprise Web Services/Tactical Cloud Provided actionable roadmap for world wide multi-media web services	GPO: Developed Acquisition Strategy for Future Digital System FDSys Led to successful acquisition and implementation on time, on budget and 80% cheaper than NARA RMS	DHS CIO: Agile Acquisition Roadmap Applying AAM to comply with NDAA/FITARA IT Reform Directives Partnered with DHS FFRDC to shift DHS away from failed weapon systems approach to IT acquisition

Office of the Secretary of Defense, DCIO (2001) *"Since the value of the ICH to our programs increases rapidly through results sharing, we encourage the defense community and IT industry to participate directly in the public service initiative in terms of sponsorship and lessons learned"*