Acquisition
Research Program
Naval Postgraduate School

Acquisition Cybersecurity Management Framework

Randy William Maule, Ph.D.

Research Associate Professor

Graduate School of Operational and Information Sciences

Information Sciences Department
Naval Postgraduate School

Monterey, CA 93943

rwmaule@nps.edu
831-915-2430

16TH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

Problem: Current organizational structures insufficient for cyber security.

Solution: Expand acquisition role to support information assurance throughout the supply chain and across the lifecycle of the equipment.

Objective: Methodology and workflows to support cyber security information assurance to inform acquisition decisions and ensure systems security and data validity.

Question: Will a centralized information assurance process lessen the inter- and intra-organizational boundaries that have limited cybersecurity initiatives?

Method: Model-based system engineering techniques for systems test and measurement integrated into acquisition audit workflows.

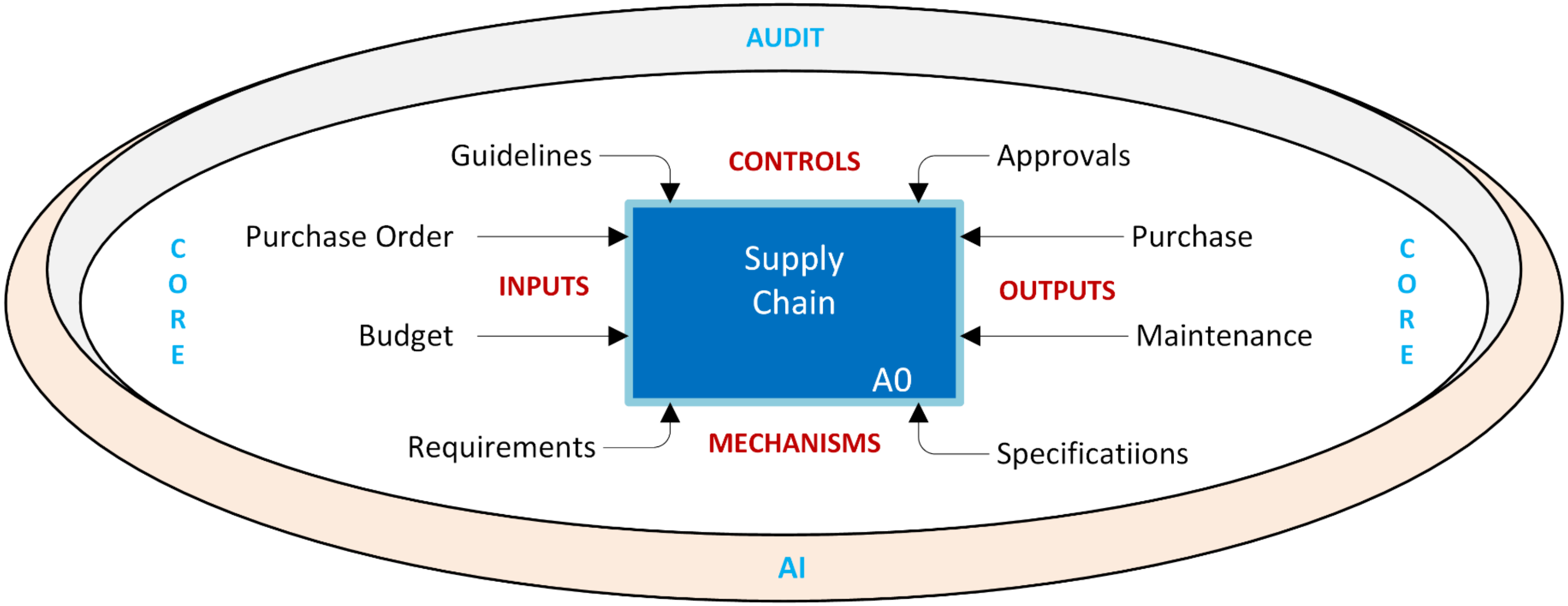
Procedure: Develop supply chain audit from purchase order, through vendor selection, maintenance and lifecycle compliance assessment, to obsolescence and destruction.

Supply Chain Problem and Solution

Report Says US Navy “Under Cyber Siege”

(March 13, 2019)

An internal US Navy review obtained by the Wall Street Journal says that the Navy and Navy contractors are “under cyber siege” by numerous foreign adversaries, including hackers working on behalf of China. The attackers are stealing national security secrets such as plans for a supersonic antiship missile. The report says that the Navy and the Defense Department “have only a limited understanding of the actual totality of losses that are occurring” because of the complexity of tracking contractor and subcontractor cyber incidents.



AUDIT

CONTROLS

Guidelines

Approvals

INPUTS

Purchase Order

Budget

Supply Chain

A0

OUTPUTS

Purchase

Maintenance

MECHANISMS

Requirements

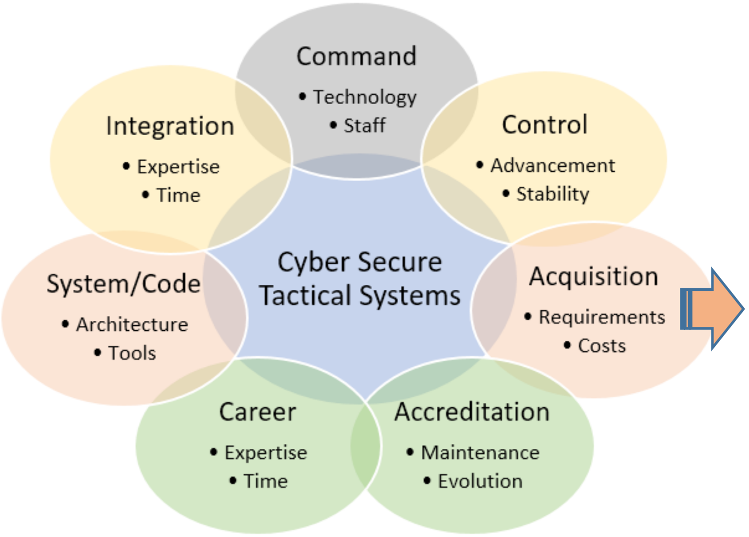
Specificatiions

CORE

CORE

AI

Supply Chain Cyber Assurance



Command
- Technology
- Staff

Integration
- Expertise
- Time

Control
- Advancement
- Stability

System/Code
- Architecture
- Tools

Cyber Secure Tactical Systems

Acquisition
- Requirements
- Costs

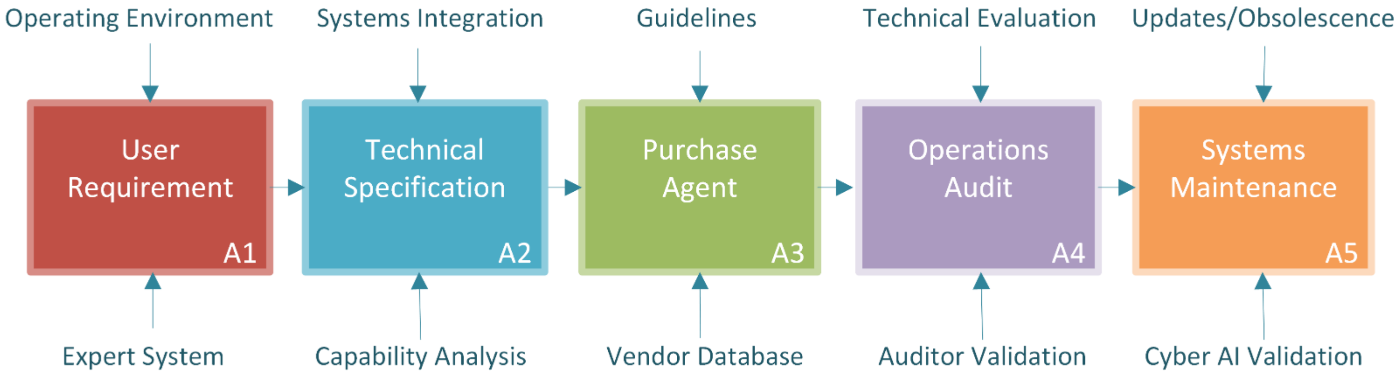
Career
- Expertise
- Time

Accreditation
- Maintenance
- Evolution

Supply Chain Standards

- ISO 9000: Quality management systems
- ISO/TS 10303-1307: Industrial automation systems
- ISO 16678: Counterfeiting and illicit trade
- ISO/TR 17370: Data carrier supply chain management
- ISO/IEC 20243: Mitigating maliciously tainted products
- ISO/TS 22375: Security and resilience guidelines
- ISO/IEC 27036: Security for supplier relationships
- ISO 28000: Supply chain security – Specifications
- ISO 28001: Supply chain security – Assessments
- ISO 28002: Supply chain security – Resilience
- ISO 28003: Supply chain security – Audits

Adopt industry security audit standards
Implement industry supply chain verification procedures



Operating Environment

User Requirement A1

Expert System

Systems Integration

Technical Specification A2

Capability Analysis

Guidelines

Purchase Agent A3

Vendor Database

Technical Evaluation

Operations Audit A4

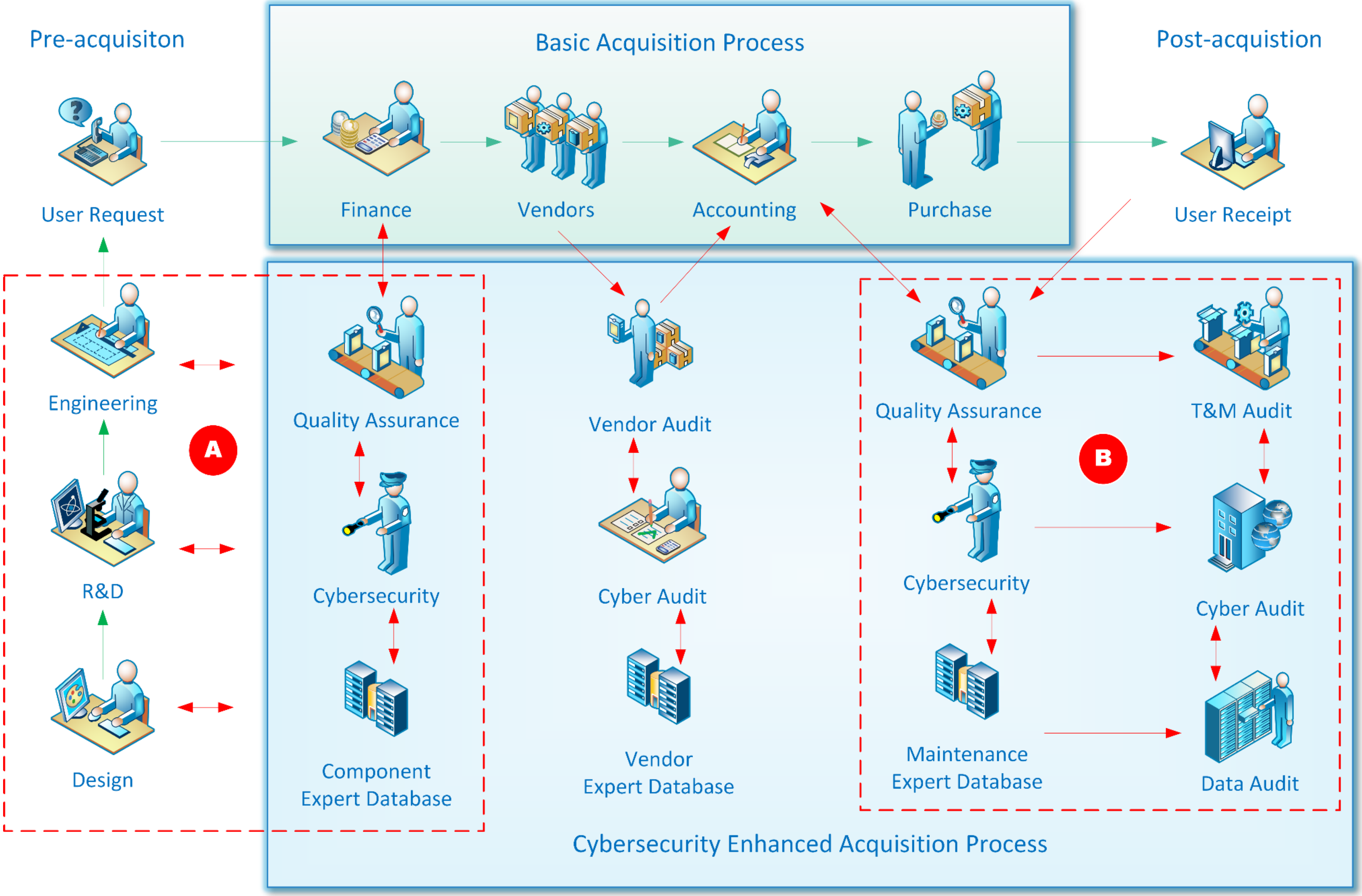
Auditor Validation

Updates/Obsolescence

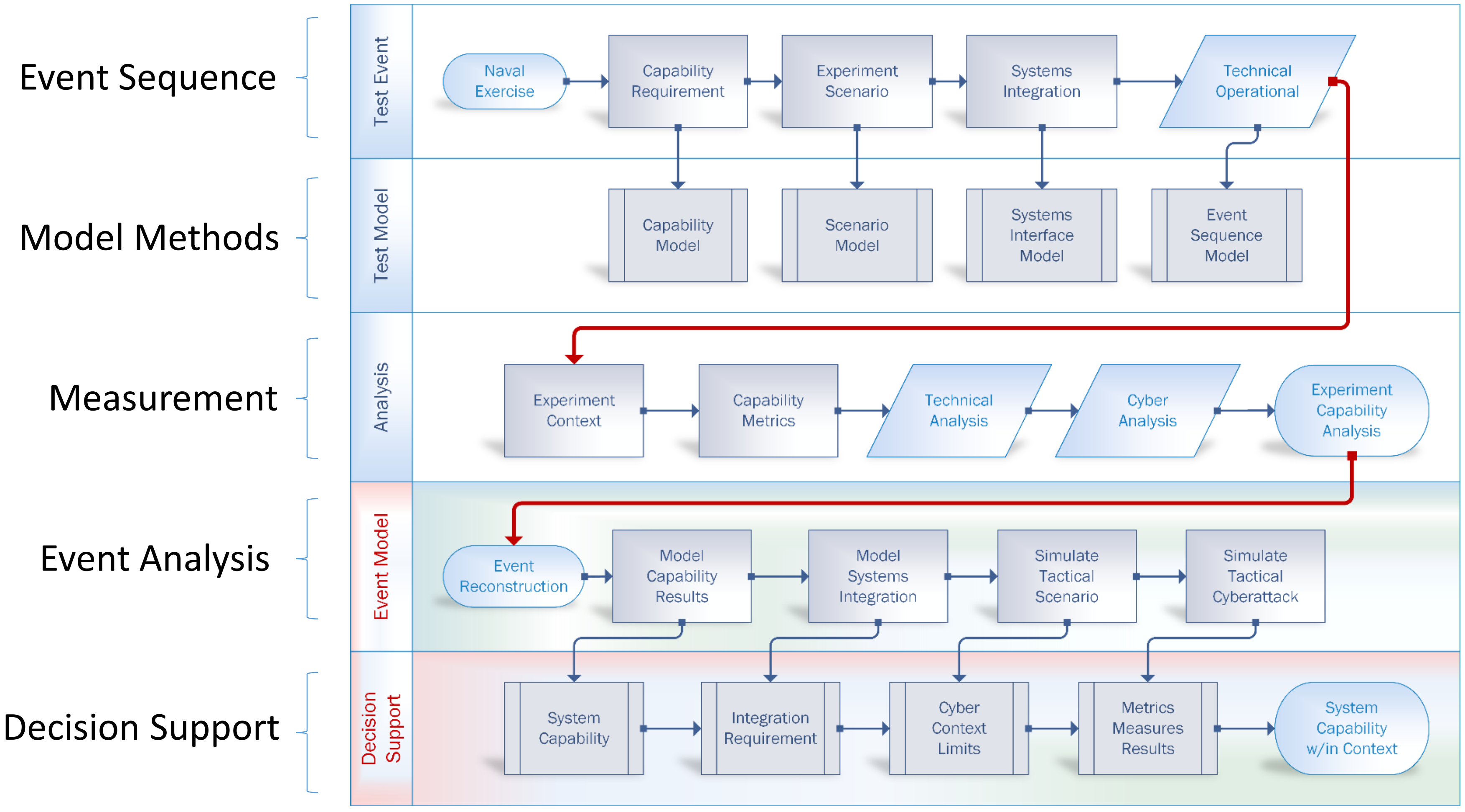
Systems Maintenance A5

Cyber AI Validation

Supply Chain Cyber Assurance Workflow



Supply Chain Cyber Figure of Merit

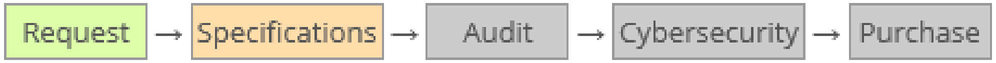


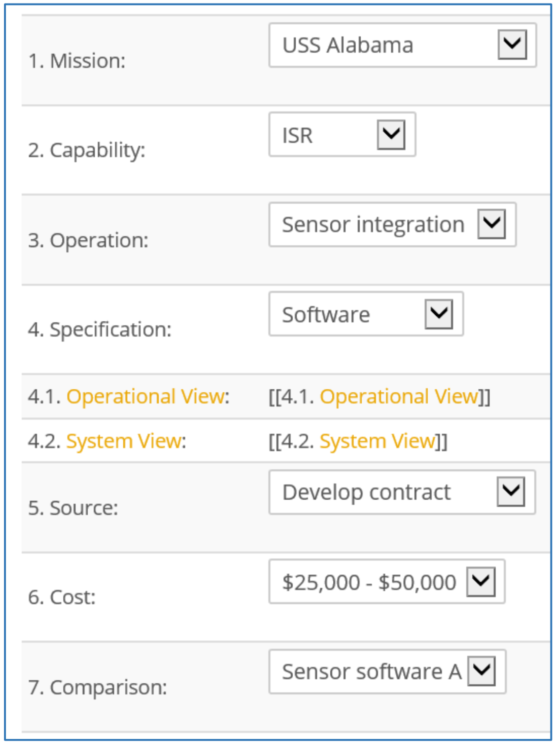
Readiness Assessment Coefficient = (Lifecycle Area Measures) / (Completeness of Measured Areas)

Readiness Confidence = (Lifecycle Area Measures) / (Measured Areas) * (Independent Context Evaluations)

Proof-of-Concept: AWS GovCloud/JEDI

Pre-Acquisition Cyber Assessment Workflow System

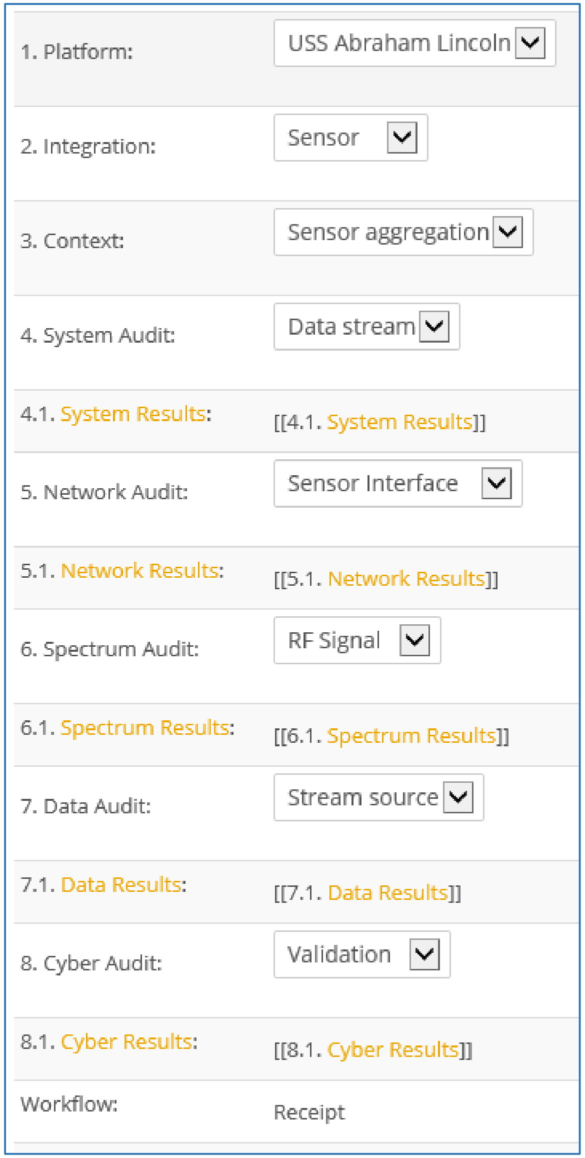

Request → Specifications → Audit → Cybersecurity → Purchase



1. Mission:	USS Alabama
2. Capability:	ISR
3. Operation:	Sensor integration
4. Specification:	Software
4.1. Operational View:	[[4.1. Operational View]]
4.2. System View:	[[4.2. System View]]
5. Source:	Develop contract
6. Cost:	$25,000 - $50,000
7. Comparison:	Sensor software A

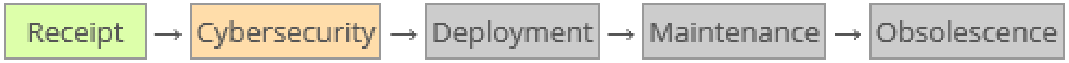
Pre-Acquisition Cybersecurity Evaluation Form

Post-Acquisition Cybersecurity Audit Form



1. Platform:	USS Abraham Lincoln
2. Integration:	Sensor
3. Context:	Sensor aggregation
4. System Audit:	Data stream
4.1. System Results:	[[4.1. System Results]]
5. Network Audit:	Sensor Interface
5.1. Network Results:	[[5.1. Network Results]]
6. Spectrum Audit:	RF Signal
6.1. Spectrum Results:	[[6.1. Spectrum Results]]
7. Data Audit:	Stream source
7.1. Data Results:	[[7.1. Data Results]]
8. Cyber Audit:	Validation
8.1. Cyber Results:	[[8.1. Cyber Results]]
Workflow:	Receipt

Post-Acquisition Cyber Audit Workflow System


Receipt → Cybersecurity → Deployment → Maintenance → Obsolescence

Results and Recommendations

Results

- Established acquisition department IA role
- Applied industry standards for IA assessment
- Research methods for supply chain cyber assessment
- Designed workflow for supply chain audit implementation
- Implemented cyber figure-of-merit to quantify readiness

Recommendations

- Expand proof-of-concept to prototype
- Implement autonomous systems for acquisition analytics
- Implement machine learning for assessment automation
- Expand AI to acquisition decision support