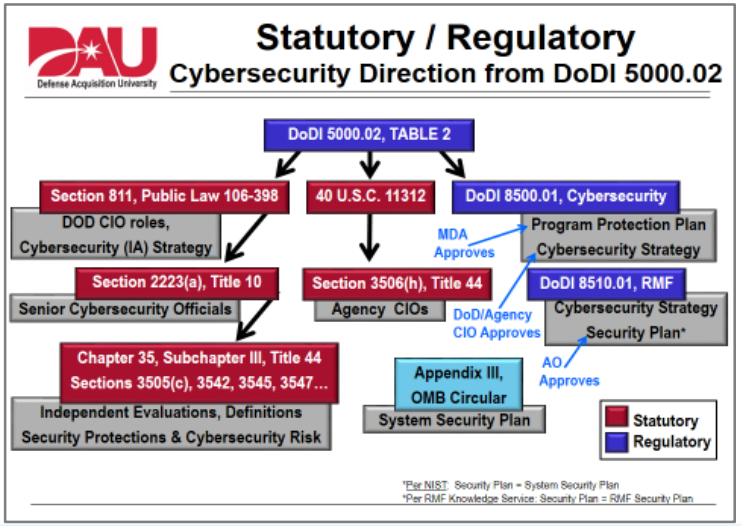
Defense Acquisition University (DAU)
Cybersecurity Black Card
June 2016

Cybersecurity - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its **availability, integrity, authentication, confidentiality,** and **nonrepudiation**. – DoDI 8500.01, 14 Mar 14

Confidentiality	Integrity	Availability	Non-Repudiation	Authentication
Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.	The property whereby an entity has not been modified in an unauthorized manner.	Being accessible and useable upon demand by an authorized entity.	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity.	Verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.

Legislation, Policy and Guidance:

See DoD Cybersecurity Policy Chart: http://iac.dtic.mil/csiac/download/ia_policychart.pdf



Operational Resilience - requires three conditions to be met:

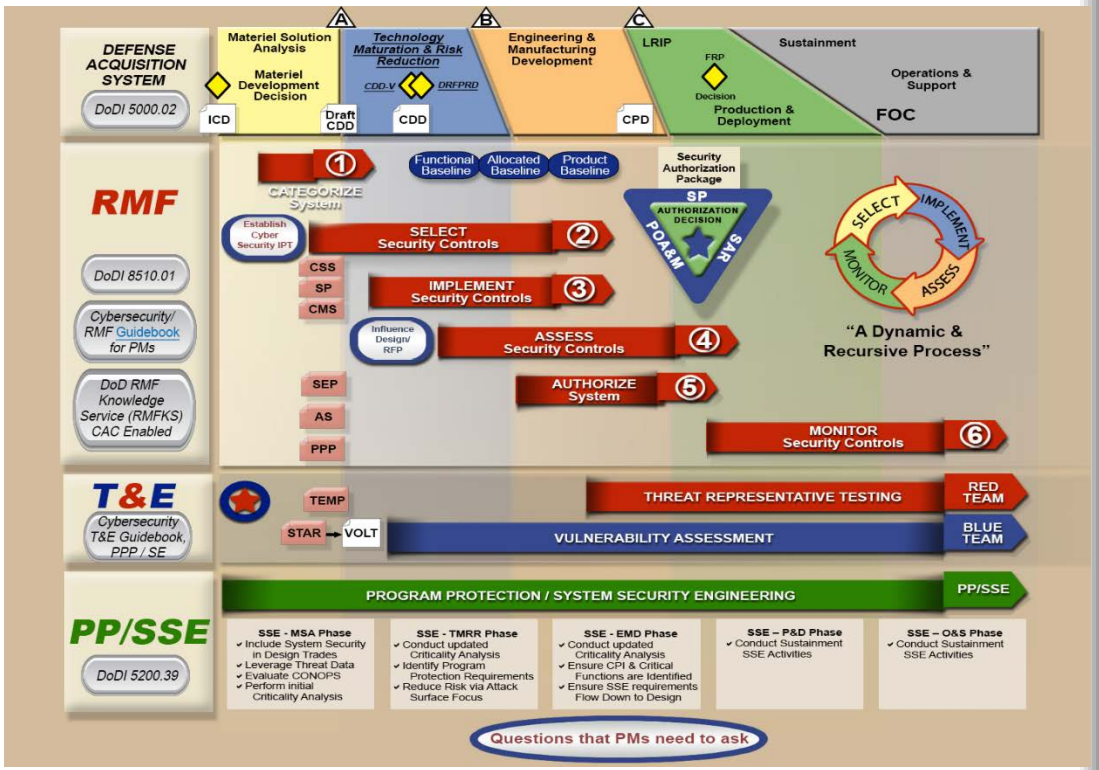
1. information resources are trustworthy
2. missions are ready for information resources degradation or loss
3. network operations have the means to prevail in the face of adverse events

– DoDI 8500.01, 14 Mar 14

Integrating Cybersecurity across the Acquisition Lifecycle

Effective integration of cybersecurity into the DoD acquisition lifecycle encompasses several different processes:

- DoDI 5000.02 – DoD Acquisition Lifecycle
- Risk Management Framework (RMF) for DoD Information Technology (IT)
- Cybersecurity Test and Evaluation
- Program Protection
- System Security Engineering (SSE)



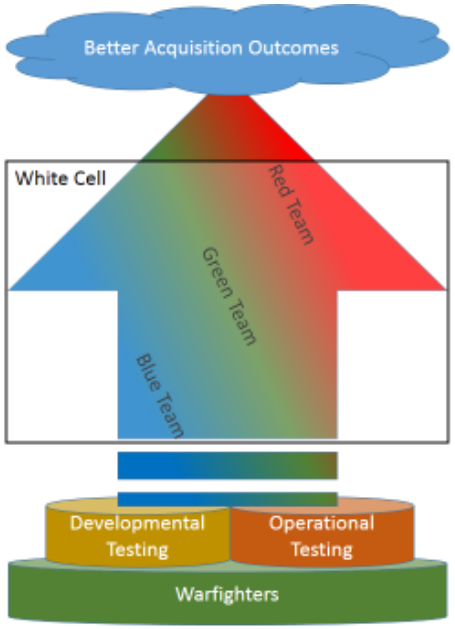
The **Cybersecurity & Acquisition Lifecycle Integration Tool (CALIT)** provides the user the ability to:

- Visualize how these processes work together
- Identify Cybersecurity risks and opportunities across the acquisition lifecycle

Access CALIT here: https://acc.dau.mil/CommunityBrowser.aspx?id=740975&lang=en-US

Defense Acquisition University (DAU)
Cybersecurity Black Card
January 2016

Blue Team is a security posture assessment and evaluation team. They determine the vulnerabilities and exposures of an asset.



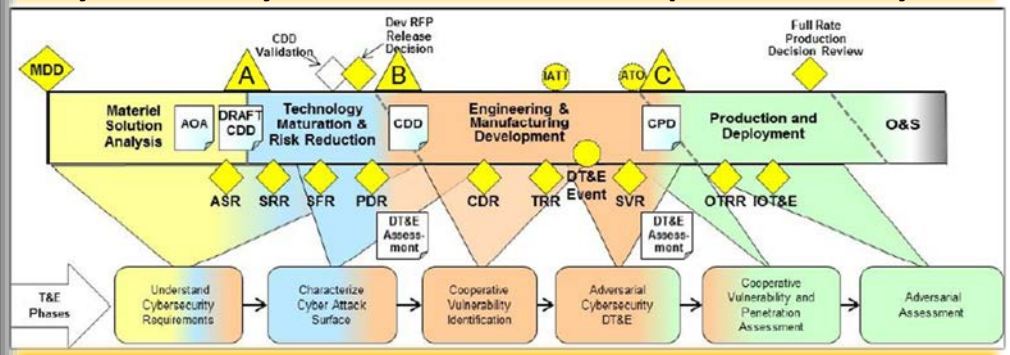
Red Team is a simulated adversary. They attack an asset using validated threat Tactics, Techniques and Procedures in order to help measure mission risk.

Green Team is a training group. They assist the asset owners with targeted vulnerability and exposure remediation that has been identified by the Blue Team.

White Cell controls the environment during an exercise. They provide the framework in which the Red Team attacks friendly forces.

Reference: DOT&E TEMP Guide v2.1, 12 July 13

Cybersecurity T&E Phases and the Acquisition Life Cycle

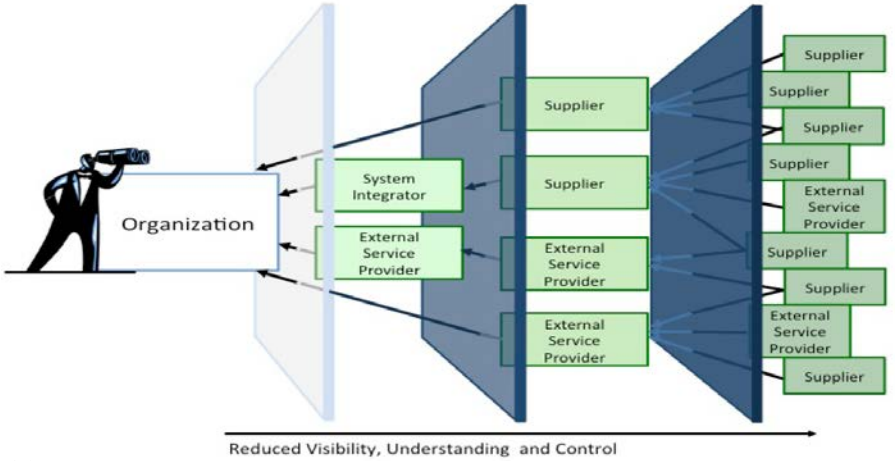


DoDI 5000.02 clearly provides direction to integrate cybersecurity test and evaluation (T&E) early and continuously in the acquisition life cycle.

Software Assurance (SwA) – the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner.

- CNSS Instruction 4009, National Information Assurance Glossary, 26 Apr 10

Supply Chain Risk Management (SCRM)

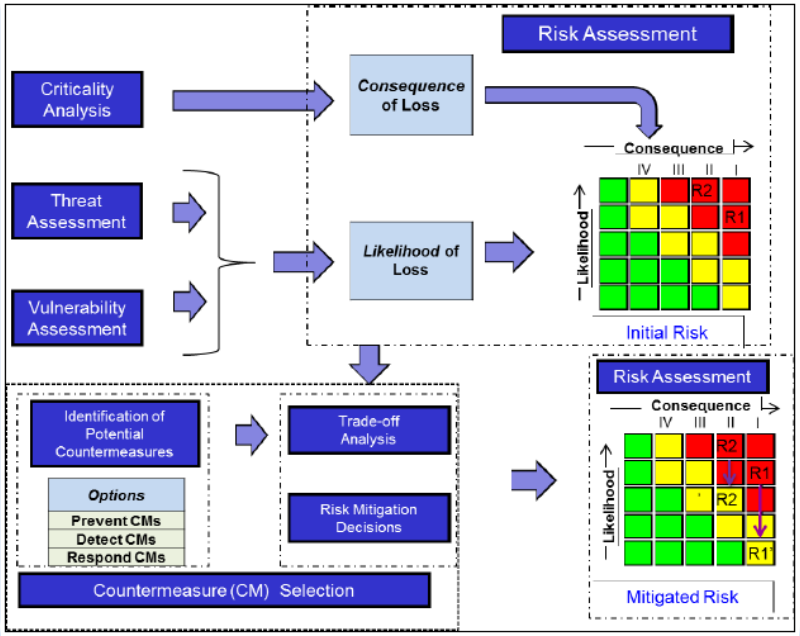


NIST Special Publication 800-161, Apr 15

SCRM - A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

- DoDI 5200.44, 5 Nov 12

Trusted Systems and Network Analysis Methodology



Trusted Systems and Network (TSN) Analysis, Jun 14

The TSN analysis consists of several activities: a criticality analysis to determine the most critical functions of the system, a threat assessment to understand the likely attacks, a vulnerability assessment to recognize vulnerabilities in the design and the commercial off-the-shelf products, a risk assessment, and selection of security countermeasures (risk mitigations) based on a cost-benefit trade-off analysis. When the selected security countermeasures are planned for implementation into the system, the system's supply chain, and the system's development environments, the risk is reassessed.