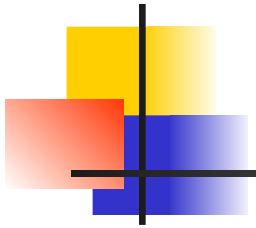


CSE 543
Information Assurance and Security

Mission Assurance

Professor Stephen S. Yau

Fall 2022

Mission Assurance

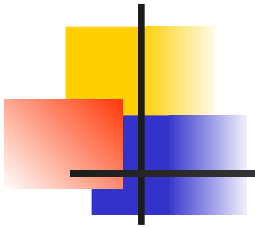
- ***Mission Assurance***
  - A ***life-cycle engineering process*** to ***identify and mitigate*** the ***deficiencies of mission requirements, design, production, test, and field support for mission success***

Mission Assurance

- ***Goal*** of Mission Assurance
  - To create a ***state of resilience*** that supports the ***continuation*** of an entity's ***critical business processes and protects its employees, assets, services, and functions.***

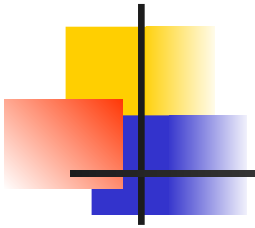
Mission Assurance (cont.)

- Includes ***disciplined application*** of ***system engineering, risk management, quality and management principles*** to achieve ***success*** of the following,
  - ***Requirement analysis***
  - ***Design***
  - ***Development***
  - ***Testing***
  - ***Deployment***
  - ***Operations process***



Mission Assurance (cont.)

- Also covers the ***enterprise, supply base, business partners, and customer base*** to enable ***mission success***.

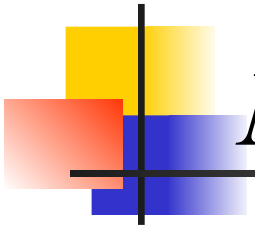


Mission Assurance (cont.)

- In practice, information assurance (IA) focuses on protection of data and systems, often conflicts with the "get the job done" attitude of mission assurance.

Mission Assurance (cont.)

- This conflict is largely eliminated when the focus of information assurance is bifurcated into
  - ***protecting the infrastructure and data***, and
  - ***securely sharing information with authorized recipients.***



Mission Assurance Use Cases

- The US DoD 8500-series of policies has defined three ***mission assurance categories (MACs)*** that form the basis for ***availability and integrity requirements***

Mission Assurance Use Cases

- ***MAC I*** systems handle information ***vital*** to the ***operational readiness or effectiveness of deployed or contingency forces***.
  - Loss of MAC I data would cause ***severe damage*** to the successful completion of a DoD mission.
  - MAC I systems must maintain the ***highest*** *levels* of both ***integrity and availability*** and ***use the most rigorous measure of protection.***

Mission Assurance Use Cases (cont.)

- ***MAC II*** systems handle information ***important*** to ***the support*** of ***deployed and contingency forces***.
  - Loss of MAC II systems could have a ***significant negative impact on the success of the mission or operational readiness***.
  - MAC II systems must maintain the ***highest*** level of ***Integrity***.
  - The loss of availability of MAC II data can be ***tolerated only for a short period of time***, so MAC II systems must maintain a ***medium level of availability***.
  - MAC II systems require ***protective measures above industry best practices*** to ensure ***adequate integrity and availability of data.***

Mission Assurance Use Cases (cont.)

- ***MAC III*** systems handle information that is ***necessary*** for ***day-to-day operations***, but not directly related to the support of deployed or contingency forces.
  - Loss of MAC III data would ***not have a significant immediate impact*** on mission effectiveness or operational readiness in short term
  - MAC III systems are required to maintain ***basic levels of integrity and availability.*** MAC III systems must be protected by measures considered as ***industry best practices***.

References

- J. G. Boyce, D. W. Jennings, *Information Assurance*: *Managing Organizational IT Security Risks*. Butterworth Heineman, 2002, ISBN 0-7506-7327-3
- M. E. Whitman and H. J. Mattord , Principles of Information Security, 6th edition, Thomson Course Technology, November 2018
- Rahul Gupta, "The Need for Mission Assurance". *PRTM Magazine*, 2006.