Information Assurance Mission Assurance Category and Confidentiality Level

Mission Assurance Category (MAC).

The mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

MAC 1	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.
MAC II	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.
MAC III	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

Confidentiality Level.

The other major component in forming the baseline set of IA controls for every information system is determined by selecting the appropriate confidentiality level based on the sensitivity of the information associated with the information system. DoD has defined three levels of confidentiality:

Classified	Systems processing classified information.
Sensitive	Systems processing sensitive information as defined in DoDD 8500.1, to include any unclassified information not cleared for public release.
Public	Systems processing publicly releasable information as defined in DoDD 8500.1 (i.e., information that has undergone a security review and been cleared for public release).