High-Level Security Requirements in FIPS 200

(Adapted from the federal information processing standards 200 [1])

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training I (AT–I): Organizations must ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems.

Awareness and Training II (AT–II): Organizations must ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability I(AU–I): Organizations must create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

Audit and Accountability II (AU–II): Organizations must ensure that the actions of individual information system users can be uniquely traced to those users, so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments I (CA–I): Organizations must periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

Certification, Accreditation, and Security Assessments II (CA–II): Organizations must develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

Certification, Accreditation, and Security Assessments III (CA–III): Organizations must authorize the operation of organizational information systems and any associated information system connections.

Certification, Accreditation, and Security Assessments IV (CA–IV): Organizations must monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management I (CM–I): Organizations must establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Configuration Management II (CM–II): Organizations must establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response I (IR–I): Organizations must establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recover, and user response activities.

Incident Response II (IR–II): Organizations must track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance I (MA–I): Organizations must perform periodic and timely maintenance on organizational information systems.

Maintenance II (MA–II): Organizations must provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection I (MP–I): Organizations must protect information system media, both paper and digital.
Media Protection II (MP–II): Organizations must limit access to information on information system media to authorized users.

Media Protection III (MP–III): Organizations must sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection I (PE–I): Organizations must limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.

Physical and Environmental Protection II (PE–II): Organizations must protect the physical plant and support infrastructure for information systems.

Physical and Environmental Protection III (PE–III): Organizations must provide supporting utilities for information systems.
Physical and Environmental Protection IV (PE–IV): Organizations must protect information systems against environmental hazards.

Physical and Environmental Protection V (PE–V): Organizations must provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security I (PS–I): Organizations must ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions.

Personnel Security II (PS–II): Organizations must ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.

Personnel Security III (PS–III): Organizations must employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition I (SA–I): Organizations must allocate sufficient resources to adequately protect organizational information systems.

System and Services Acquisition II (SA–II): Organizations must employ system development life cycle processes that incorporate information security considerations.

System and Services Acquisition III (SA–III): Organizations must employ software usage and installation restrictions.

System and Services Acquisition IV (SA–IV): Organizations must ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communication Protection I (SC–I): Organizations must monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

System and Communication Protection II (SC–ii): Organizations must employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity I (SI–I): Organizations must identify, report, and correct information and information system flaws in a timely manner.

System and Information Integrity II (SI–II): Organizations must provide protection from malicious code at appropriate locations within organizational information systems.

System and Information Integrity III (SI–III): Organizations must monitor information system security alerts and advisories and take appropriate actions in response.

[1] National Institute of Standards and Technology, “Minimum Security Requirements for Federal Information and Information Systems,” Std. FIPS 200, 2006.

High-level security requirements dependencies in FIPS 200

	AC	AT-I	AT-II	AU-I	AU-II	CA-I	CA-II	CA-III	CA-IV	CM-I	CM-II	CP	IA	IR-I	IR-II	MA-I	MA-II	MP-I	MP-II	MP-III	PE-I	PE-II	PE-III	PE-IV	PE-V	PL	PS-I	PS-II	PS-III	RA	SA-I	SA-II	SA-III	SA-IV	SC-I	SC-II	SI-I	SI-II	SI-III
AC																	→		→	→	→																		
AT-I																																							
AT-II																																							
AU-I					→	→			→			→			→															→					→		→	→	
AU-II																																							
CA-I																														→									
CA-II	→					→				→						→															→	→	→						
CA-III	→			→																																			
CA-IV						→																																	
CM-I											→																												
CM-II	→																		→														→						
CP					→										→				→																				
IA	→																		→																				
IR-I		→			→																																		
IR-II					→																																		
MA-I																																							
MA-II			→																																				
MP-I																			→	→																			
MP-II																																							
MP-III																																							
PE-I																																							
PE-II																																							
PE-III																																							
PE-IV																																							
PE-V																																							
PL	→																																						
PS-I						→																																	
PS-II	→													→																→									
PS-III																																							
RA		→																																					
SA-I																																							
SA-II																																							
SA-III																																							
SA-IV	→																																						
SC-I	→	→																												→									
SC-II																																→							
SI-I														→																									
SI-II																																							
SI-III																														→									

How to read this table?

If there is an arrow in row AC and column MA-II, that means AC depends on MA-II (AC→MA-II).