Risk Management Framework (RMF) – GLOSSARY

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A	
Agency	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency
Allocation	The process an organization employs to assign security or privacy requirements to an information system or its environment of operation; or to assign controls to specific system elements responsible for providing a security or privacy capability (e.g., router, server, remote sensor).
Application	A software program hosted by an information system.
Assessment and Authorization (A&A)	The standard DOD approach for identifying information systems security requirements, providing security solutions, and managing the security of DOD Information Systems.
Authorization Boundary	Historically, NIST has used the terms authorization boundary and system boundary interchangeably. The term authorization boundary is now used exclusively to refer to the set of system elements comprising the system to be authorized for operation or authorized for use by an authorizing official. Authorization boundary can also refer to the set of common controls to be authorized for inheritance purposes.
AO	Authorizing Official is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and national security.
AODR	Authorizing Official Designated Representative, an organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with the authorization process.
Assessor	The individual, group, or organization responsible for conducting a security or privacy assessment.

Back to Top

B	
Baseline Configuration	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

Back to Top

C	
CIO	Chief Information Officer is a senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
CNSSI	Committee on National Security Systems Instruction
COI	Community of Interest
Common Control	A security or privacy control that is inherited by multiple information systems or programs.
Common Control Provider	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., controls inheritable by organizational systems).
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions.
Control Assessor	The individual, group, or organization responsible for conducting a control assessment.
Control Baseline	The set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk.
Control Effectiveness	A measure of whether a given control is contributing to the reduction of information security or privacy risk.
Cybersecurity Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.
Cybersecurity Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Control Inheritance	A situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

Back to Top

D	
DATO	Denial of Authorization to Operate
DISA	Defense Information Systems Agency
Department of Defense (DOD)	The DOD is an executive branch department of the federal government of the U. S. charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces. The major elements of these forces are the Army, Navy, Marine Corps, and Air Force.

DODD	Department of Defense Directive
DODI	Department of Defense Instruction

Back to Top

E	
Enterprise Architecture	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
Environment Of Operation	The physical surroundings in which an information system processes, stores, and transmits information.
Event	Any observable occurrence in a network or information system.

Back to Top

F	
Federal Information System	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
FISMA	Federal Information Security Modernization Act

Back to Top

G	

Back to Top

H	
HVA	High Value Assets
Hybrid Control	A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control. See common control and system-specific control.

Back to Top

I	
Impact	With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.
Impact Level/Value	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.

Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information Life Cycle	The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (ISO)	An individual responsible for identifying all information types. An information type is considered any specific category of information defined by an organization or, in some instances, by a public law, executive order, directive, policy, or regulation.
Information System Security Manager (ISSM)	An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.
Information System Security Officer (ISSO)	An individual assigned by the ISSM when the facility has multiple authorized ISs in multiple facility organizations in which the ISSM has oversight responsibility for the multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment.
Information Technology (IT)	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
Information type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.

Back to Top

J

Back to Top

K	
Key Management Personnel (KMP)	Key management personnel are Senior Management Officials (SMO) who have the authority to directly or indirectly plan and control business operations. KMPs require an eligibility determination before a facility is granted an FCL.

Back to Top

L	

Back to Top

M	
MA	Mission Area.

Back to Top

N	
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
NIST	National Institute of Standards and Technology

Back to Top

O	
OMB	Office of Management and Budget
Operations Technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements).
Organizationally tailored Control Baseline	A control baseline tailored for a defined notional (type of) information system using overlays and/or system-specific control tailoring and intended for use in selecting controls for multiple systems within one or more organizations.

Back to Top

P	
Personally Identifiable Information (PII)	PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Plan of Action and Milestones (POA&M)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Privacy Architect	Individual, group, or organization responsible for ensuring that the system privacy requirements necessary to protect individuals' privacy are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and information systems processing PII.
Privacy Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's privacy protection processes, technical measures, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
Privacy Plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
Privacy Posture	The privacy posture represents the status of the information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes.
Privacy Program Plan	A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
Privacy Requirement	A requirement that applies to an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, regulations, procedures, and/or mission/business needs with respect to privacy. Note: The term privacy requirement can be used in a variety of contexts from high-level policy activities to low-level implementation activities in system development and engineering disciplines.
Privacy Information	Information that describes the privacy posture of an information system or organization.

Back to Top

Q

Back to Top

R	
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
Risk Management Framework (RMF)	Establishes a common set of guidelines for the assessment and authorization of information systems (ISs) and provide a holistic and strategic process for the risk management of ISs.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Back to Top

S	
SAISO	Senior Agency Information Security Officer
Security	A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization’s risk management approach.
Security Architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization’s core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans.
Security Categorization	The process of determining the security category for information or a system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems.

Security Controls	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
Security Requirement	A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.
Software	Computer programs and associated data that may be dynamically written or modified during execution.
Specification	A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component and often the procedures for determining whether these provisions have been satisfied. See specification requirement.
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Supply Chain Risk Management (SCRM)	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.
System Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
System User	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
System Privacy Engineering	Process that captures and refines privacy requirements and ensures their integration into information technology component products and information systems through purposeful privacy design or configuration.

Back to Top

T	
Tailoring	The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls.
Tailored Control Baseline	A set of controls resulting from the application of tailoring guidance to a control baseline.

Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

Back to Top

U

Back to Top

V

Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks.

Back to Top

W

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top