Security Phase	Security Task Focus	Level of Effort	Task #	Secure Engineering Activity	Activity Description	Reasonable Task Deliverable(s)	Applicable Privacy Management Task #	Applicable NIST 800-160 Control #	Applicable NIST 800-53 Control #	Applicable ISO 27002 Control #	Status	Notes / Findings / Recommendations	Security Architecture	Security Engineering	Governance, Compliance & Risk	Security Operations	Project Owner	Project Manager	Project Team	Technology Architecture	Infrastructure Team	Application Team
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Prepare for the security aspects of business or mission analysis.	Basic	1-1	Identify preliminary stakeholders who will contribute to the identification and assessment of any mission, business, or operational problems or opportunities.	These stakeholders encompass all individuals, organizations, representatives, and delegates with concerns across the life cycle of the system.	- Project stakeholder list (strategic personnel, business units and third parties)	Task 5: Identify Actors	BA-1.1	PL-1 PL-8 PM-11 SA-8	5.1.1 5.1.2 6.1.1 12.1.1 14.1.1 14.2.5 18.1.1 18.2.2			C	I	C	I	A/R	C	C	C	C	C
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Prepare for the security aspects of business or mission analysis.	Basic	1-2	Review problems and opportunities with respect to desired security objectives.	This review examines organizational problems or opportunities and the security objectives that must be considered to address those problems or opportunities from the business or mission perspective. The review also includes any gaps in the existing systems or services related to protection or security capability that would preclude the organization from achieving the identified security objectives.	- Business requirements. - Use case description.	Task 1: Use Case Description	BA-1.2	PL-8 PL-9 PM-11 SA-8	14.1.1 14.2.5			R	I	I	I	A	C	C	I	I	I
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Prepare for the security aspects of business or mission analysis.	Basic	1-3	Define the security aspects of the business strategy analysis.	Security aspects of the business or mission strategy analysis are used to inform the definition of the problem space, characterization of the solution space, and selection of a solution class.	- Listing of applicable statutory, regulatory and contractual requirements.		BA-1.3	PL-8 [illegible]	14.1.1 14.2.5			R	I	I	I	A	C	C	I	I	I
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Prepare for the security aspects of business or mission analysis.	Basic	1-4	Identify, plan for, and obtain access to the systems and services that support the security aspects of the proposed solution.	Specific enabling systems and services may be required to support the security aspects of the business or mission analysis process. These enabling systems and services are relied upon to provide the capability to realize and support the system-of-interest, and therefore impact the trustworthiness of the system. The business or mission analysis-oriented security concerns for enabling systems and services used to support the business or mission analysis process must be determined and captured as security requirements and as security-driven constraints for the interfaces and interactions with the system-of-interest. The Validation process is used to confirm that enabling systems and services achieve their intended use and do so with an appropriate level of trustworthiness.	- Listing of expected systems and services that will be required to support the proposed solution.		BA-1[illegible]	PL-8 SA-8	14.[illegible] 14.2.5			R	I	I	I	A	C	C	I	I	I
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Define the security aspects of the problem or opportunity.	Basic	1-5	Analyze the problems and opportunities in the context of the security objectives and measures of success to be achieved.	The security objectives that are part of any solution determine what it means to be adequately secure. These objectives also address the scope of security for the system including the assets requiring protection and the consequences or impacts against which security is assessed. Measures of success establish the trustworthiness of the system in terms of the specific and measurable criteria relative to the operational performance measures and the stated security objectives. These measures include both strength of protection and the level of assurance, or confidence, in the protection capability. The results of the analyses inform decisions on the suitability and feasibility of alternative options to be pursued.	- Risk Assessment - Risk Register (RR)	Task 17: Conduct R[illegible]ssment Task 18: Iterate The A[illegible]nd Refine	BA-2.1	PL-8 PM-11 SA-8	14.1.1 14.2.5			R	I	C	I	A	C	C	C	C	C
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Define the security aspects of the problem or opportunity.	Basic	1-6	Define the security aspects and considerations of the project / initiative.	Information is elicited from stakeholders to acquire an understanding of the mission, business, or operational problem or opportunity from a system security perspective.	- Data classification is i[illegible]fied. - System criticality is id[illegible]ed.	Task 3: [illegible]olicy Conformance [illegible]a	BA-2.2	PL-8 PM-11 SA-8	14.1.1 14.2.5			R	I	C	I	A	C	C	C	C	C
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Characterize the security aspects of the solution.	Basic	1-7	Define the security aspects of the preliminary operational concepts throughout all life cycle stages for the project / initiative.	Security considerations are defined relative to all preliminary life cycle concepts including, for example: acquisition, development, engineering, manufacturing, production; deployment and operation; sustainment and support (training, maintenance, logistics, supply, and distribution); disposal and retirement; and any other life cycle concept for which security aspects are necessarily a part of or inform secure execution and achievement of security objectives. Speci[illegible] operational concepts include, for example: modes of secure operat[illegible]urity-related operational scenarios and use cases; or secure usage wi[illegible]mission area or line of business. Security considerations are integrated into [illegible]entified life cycle concepts and used to support feasibility analysis and ev[illegible]ion of candidate alternative solution classes.	- Te[illegible]ve life cycle is i[illegible]fied.	Task 3: Privacy Policy [illegible]nance Criteria	[illegible]	PL-8 PM-11 SA-8	14.1.1 14.2.5			R	[illegible]	C	C	A	C	R	C	C	C
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Characterize the security aspects of the solution.	Enhanced	1-8	Identify alternative solutions that can achieve the security objectives within limitations, constraints, and other considerations.	Relevant security issues or concerns relate[illegible] candidate a[illegible]ve solution classes are identified and recorded. In a[illegible], any security-rela[illegible]tions or constraints on life cycle concepts o[illegible]gineering of each alterna[illegible]ion class are examined.			[illegible]3.2	[illegible]	14.1.1 14.2.5			A/R	C	C	C	C	C	C	C	C	C
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Evaluate and select solution classes.	Enhanced	1-9	Assess each alternative solution, taking into account the security objectives, limitations, constraints, and other relevant security considerations.	Security aspects are one o[illegible] decision criteria used [illegible]ss each alternative solution class. Security [illegible]ents may be accom[illegible] in combination with or as a separate informing as[illegible]t of the non-[illegible] decision criteria. The System Analysis process is us[illegible]form t[illegible]rity analyses required t[illegible] inform the al[illegible]ative solution a[illegible]			BA-4.1	PL-8 SA-8	14.1.1 14.2.5			[illegible]	C	C	C	C	C	C	C	C	C
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Evaluate and select solution classes.	Enhanced	1-10	Select the preferred alternative solution based on the identified security objectives and other criteria defined by the organization.	Stakeholder as[illegible]s of each solu[illegible] are carried out in[illegible]eration of all relevant criteria [illegible] inform the se[illegible]ecision-ma[illegible]cess is provided by the Risk M[illegible]ent and System [illegible] is pr[illegible], and the Validation process ensu[illegible]eferred alterna[illegible]lass(es) fit in the context of the prop[illegible] mission strateg[illegible] Decision Management process is emplo[illegible]valuate [illegible]ives and to select the preferred alternative so[illegible]ass or classes.			BA-4.2	PL-8 SA-8	14.1.1 14.2.5			C	I	I	I	A/R	C	C	I	I	I
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Manage the security aspects of business or mission analysis.	Basic	1-11	Document findings to main[illegible]e security aspects of the p[illegible]s / initiative's business strategy analysis.	B[illegible] traceability is maintained between all identified security aspects and supp[illegible]curity data associated with the business or mission problems and opportu[illegible]e proposed solution class or classes; the organizational strategy; stakeholder [illegible]ion needs and security requirements; and system analysis results.	- Pr[illegible] solution is documented [illegible] t[illegible]ptures security-relevant criteria [illegible] tentative requiremen[illegible] System Security Pla[illegible]	[illegible]k 3: Privacy Policy C[illegible]nance Criteria	BA-5.1	PL-[illegible] PL-9 SA-5 SA-8	14.1.[illegible] 14.2.5			C	C	C	C	A	R	I	I	I	I
1 - CATEGORIZE	**Business or Mission Analysis Process (BA)** - Manage the security aspects of business or mission analysis.	Basic	1-12	Generate relevant d[illegible]ntation / artifacts to enable the appropriat[illegible]f analysis by cybersecurity staff for t[illegible]n the project / initiative life cycle.	S[illegible] aspects are [illegible]tured in various artifacts that are maintained in an ide[illegible] baseline for the life cycle of the system. The security-relevant con[illegible]tion items from this process are identified and incorporated into eng[illegible]ng baselines so that they may be produced and [illegible] re[illegible] throughout the system life cycle. The Config[illegible]anagem[illegible]t process [illegible]es the baseline and the artifacts identified b[illegible]rocess. The Information [illegible]agement process determines the appropriat[illegible]s of information and protections for the information that is provided [illegible]keholders.	[illegible]y Perform[illegible]ndicators (KPIs)		BA-5[illegible]	PM-[illegible] SA-[illegible]	12.1.1 [illegible]			R	R	R	R	A	I	I	I	I	I
1 - CATEGORIZE	**Stakeholder Needs and Requirements Definition Process (SN)** - Prepare for stakeholder protection needs an security requirements definition.	Basic	1-13	Identify the stakeholders who have a security interest in the project / initiative throughout its life cycle.	Stakeholders include persons, groups, and organiz[illegible]ed delegate thereof) that impact the system or are impacted by th[illegible]ncluding the protection aspects of the system. Stakeholders are identified, including their security interest and specific roles and responsibilities relative to the systems engineering effort. Key stakeholders are those stakeholders that h[illegible] decision-making responsibility associated with life cycle concepts; progra[illegible] control, and execution; acquisition and life cycle milestones; engineering [illegible]; risk management; system acceptance; and trustworthiness. Key stakeholders and their associated decision-making authority are correlated to each of the engineering activities performed in each life cycle stage.	- Secu[illegible]takeholder list (key security perso[illegible]and teams)	Task 5: Identify Actors	SN-1.1	PL-8 SA-8	14.1.1 14.2.5			C	I	C	I	A	R	C	I	I	I
1 - CATEGORIZE	**Stakeholder Needs and Requirements Definition Process (SN)** - Prepare for stakeholder protection needs an security requirements definition.	Basic	1-14	Define the stakeholders' protection needs and security requirements.	This strategy addresses the elicitation activities, methods, and techniques used to acquire information from stakeholders and the security analyses conducted to help identify, disambiguate, and otherwise enable an accurate and complete transformation of protection needs into verifiable security requirements. The strategy strives to achieve stakeholder consensus on a common set of security requirements and system assurance objectives.	- Risk Assessment - Risk Register (RR)	Task 17[illegible]uct Risk Assessment Tas[illegible]erate The Analysis and [illegible]fine	SN-1.2	PL-8 SA-8	14.1.1 14.2.5			R	C	C	C	A	R	R	C	C	C
1 - CATEGORIZE	**Stakeholder Needs and Requirements Definition Process (SN)** - Prepare for stakeholder protection needs an security requirements definition.	Basic	1-15	Identify, plan for, and obtain access to the systems and services that support the security aspects of the stakeholder needs and requirements definition process.	Specific enabling systems and services may be required to support the security aspects of the stakeholder needs and requirements definition process. These enabling systems and services are relied upon to provide the capability to realize and support the system-of-interest, and therefore impact the trustworthiness of the system. The stakeholder needs and requirements definition-oriented security concerns for enabling systems and services used to support the stakeholder needs and requirements definition process must be determined and captured as security requirements and as security-driven constraints for the interfaces and interactions with the system-of-interest. The Validation process is used to confirm that enabling systems and services achieve their intended use and do so with an appropriate level of trustworthiness.	- Privacy Impact Assessment (PIA)	Task 4[illegible]eparation	SN-1.3	AR-2 PL-8 SA-8	5.1.1 14.1.1 14.2.5			R	I	I	I	A	C	C	I	I	I

Vendor Management Phase	Vendor Management Task Focus	Task #	Secure Engineering Activity	Activity Description	Reasonable Task Deliverable(s)	Applicable NIST 800-160 Control #	Applicable NIST 800-53 Control #	Applicable ISO 27002 Control #	Status	Notes / Findings / Recommendations	Security Architecture	Security Engineering	Governance, Compliance & Risk	Security Operations	Project Owner	Project Manager	Project Team	Technology Architecture	Infrastructure Team	Application Team
Vendor Management	**Acquisition Process (AQ) -** Prepare for security aspects of the acquisition.	VM-1	Define the security aspects for how the acquisition will be conducted.	The security aspects include how security objectives, protection needs, and security concerns are achieved by the acquisition strategy. Security concerns and considerations impact and are impacted by the objectives and scope of the engineering effort; the life cycle models to be used; the acquisition activities, milestones, gates, and associated review and approval criteria; the protection of data, information, and material assets; risk and issues mitigation; the selection of suppliers; and acceptance conditions to include demonstrations of compliance or conformance to laws, directives, regulations, policies, or other criteria. The acquisition strategy may describe life cycle models; liabilities; methods or processes; levels of criticality; levels of trustworthiness and assurance; and priority of relevant trade factors.	- Defined security controls that are based on data classification and system criticality (e.g., basic or enhanced requirements).	*AQ-1.1*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	C	I	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Prepare for security aspects of the acquisition.	VM-2	Prepare a request for a product or service that includes the security requirements.	The security requirements are integrated with and provided as part of the stakeholder requirements or system requirements depending on the type of acquisition approach and specifics of the product or service required. The security requirements are developed by application of the requirements engineering approach described in the acquisition strategy. This approach achieves the outcomes of the Stakeholder Needs and Requirements Definition and System Requirements Definition processes. The request includes security criteria for the business practices to which the supplier is to comply, a list of bidders with adequate security qualifications, and the security criteria that will be used to select the supplier.	- Defined statutory, regulatory and contractual compliance obligations.	*AQ-1.2*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	R	I	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Advertise the acquisition and select the supplier to conform with the security aspects of the acquisition.	VM-3	Communicate the request for a product or service to potential suppliers consistent with security requirements.	All forms of communications and interactions associated with the advertisement of acquisition requests (i.e., the solicitation) are to be conducted with adequate protection of data, information, material, technology, and human assets. This includes protection concerns of data and information sensitivity and privacy; knowledge of stakeholder organizations and personnel; the nature, timing, schedule, performance, and other characteristics of the acquisition; and intellectual property and technologies. Communication with potential suppliers includes subcontractors and other supporting organizations to those suppliers.	- Vendor Compliance Program (VCP) documentation.	*AQ-2.1*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	I	I	I	A	R	R	I	I	I
Vendor Management	**Acquisition Process (AQ) -** Advertise the acquisition and select the supplier to conform with the security aspects of the acquisition.	VM-4	Select one or more suppliers that meet the security criteria.	Subject-matter experts with relevant security expertise participate in the supplier selection process. The subject-matter experts make selection recommendations and rankings based on the strengths and weaknesses of the candidate supplier's ability to deliver the requested product or service in satisfaction of the stated security requirements and secure business practice criteria. The subject-matter experts also provide justification to support the recommendations provided. Supplier selection includes subcontractors and other supporting organizations to the supplier.	- Risk Assessment - Privacy Impact Assessment (PIA)	*AQ-2.2*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	C	I	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Establish and maintain the security aspects of agreements.	VM-5	Develop an agreement with the supplier to satisfy the security aspects of acquiring the product or service and supplier acceptance criteria.	The security aspects of the agreement address business practice security expectations and constraints including, for example: configuration management, risk reporting, reporting of security measures, and security measure analysis; security requirements; secure development; security verification; security validation; security acceptance procedures and criteria to include regulatory body acceptance, authorization, and approval; procedures for transport, handling, delivery, and storage; security and privacy protections and restrictions on the use, dissemination, and destruction of data, information and intellectual property; security-relevant exception handling procedures and criteria; agreement change management procedures; and agreement termination procedures. The security aspects of the agreement also include application of all of the above to subcontractors and other supporting organizations to the supplier.	- Non-Disclosure Agreement (NDA) - Contractual obligation to comply with applicable statutory, regulatory and contractual obligations. - Contractual obligation to adhere to "security by design" and "privacy by design" principles.	*AQ-3.1*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	R	I	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Establish and maintain the security aspects of agreements.	VM-6	Identify and evaluate the security impact of necessary changes to the agreement.	Necessary changes to agreements may be identified by the acquirer or the supplier. The basis for the agreement change may or may not be security-driven. However, there may be security-related impact regardless of the basis for the change. A security-related evaluation of the needed change identifies any security relevance and determines impact in terms of schedule, cost, plans, technical capability, quality, assurance, and trustworthiness.	- Business Impact Analysis (BIA)	*AQ-3.2*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	R	C	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Establish and maintain the security aspects of agreements.	VM-7	Negotiate and institute changes to the agreement with the supplier to address identified security impacts.	Changes to security aspects are captured in relevant agreements. The security aspects of the initial agreement and of all agreement revisions are negotiated in the context of the identified security impacts and the needs of the acquirer, with consideration of the feasibility of delivering an acceptable product or service within associated constraints. The security-relevant results are captured in project plans and communicated to all affected parties and stakeholders.		*AQ-3.3*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	R	C	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Monitor the security aspects of agreements.	VM-8	Assess the execution of the security aspects of the agreement.	Adherence to the security aspects of agreements is to be confirmed on a continuing basis to ensure that all parties are meeting their security responsibilities. Necessary corrective actions and adjustments are made to address any non-conformances or deficiencies identified. The Project Assessment and Control process is used to evaluate projected cost, schedule, performance, and the impact of undesirable security-related outcomes that are identified. The Risk Management process identifies associated risks and provides recommendations for risk treatment.	- Defined Key Performance Indicators (KPI) pertaining to vendor management.	*AQ-4.1*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	R	I	I	A	R	R	C	C	C
Vendor Management	**Acquisition Process (AQ) -** Monitor the security aspects of agreements.	VM-9	Provide data needed by the supplier in a secure manner in order to achieve timely resolution of issues.	Agreement execution issues may require specific data for timely and effective response action by the supplier. The issue to be resolved may or may not be security-relevant. However, the data provided to the supplier must be appropriately protected throughout all forms and manner of its communications to the supplier. The nature of the acquisition, stakeholders involved, sensitivity and proprietary aspects of data, to include privacy concerns all factor into the method of secure provision of data to the supplier.		*AQ-4.2*	*SA-1* *SA-4* *SA-8* *SA-12*	*5.1.1* *5.1.2* *6.1.1* *12.1.1* *14.1.1* *14.2.5* *14.2.7* *14.2.9* *15.1.1* *15.1.2* *15.1.3* *18.1.1* *18.2.2*			I	R	I	I	A	R	R	C	C	C

Security Culture Phase	Security Culture Task Focus	Task #	Secure Engineering Activity	Activity Description	Reasonable Task Deliverable(s)	Applicable NIST 800-160 Control #	Applicable NIST 800-53 Control #	Applicable ISO 27002 Control #	Status	Notes / Findings / Recommendations	Security Architecture	Security Engineering	Governance, Compliance & Risk	Security Operations	CEO	CISO	CIO	Legal	Human Resources	PMO	Enterprise Architecture	Infrastructure Management	Application Development
Security Culture	**Life Cycle Model Management (LM)** - Establish the security aspects of the process.	SC-1	Establish policies and procedures for process management and deployment that are consistent with the security aspects of organizational strategies.	The policies and procedures may be explicit to security or may have security-informing aspects. Organizational strategies are to include security objectives and considerations that aid in determining the most effective means to ensure that policies and procedures are consistent.	- Security Concept of Operations (CONOPS).	*LM-1.1*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	C	C	C	A	R	R	C	I	C	C	C	C
Security Culture	**Life Cycle Model Management (LM)** - Establish the security aspects of the process.	SC-2	Define the security roles, responsibilities, and authorities to facilitate implementation of the security aspects of processes and the strategic management of life cycles.	Appendix E of NIST 800-160 provides information on roles and responsibilities.	- Roles and responsibilities.	*LM-1.2*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	C	C	C	[illegible]	[illegible]	R	C	I	C	I	I	I
Security Culture	**Life Cycle Model Management (LM)** - Establish the security aspects of the process.	SC-3	Define the security aspects of the business criteria that control progression through the life cycle.	Security criteria must inform gates, checkpoints, and entry and exit criteria for key milestones and decision points used to control the progression of the engineering project through the stages in the system life cycle. This ensures that the security objectives, success measures, concerns, and considerations are explicitly part of all life cycle decision making.	- Published SDLC phases.	*LM-1.3*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	C	C	R	A	R	R	I	I	R	C	C	C
Security Culture	**Life Cycle Model Management (LM)** - Establish the security aspects of the process.	SC-4	Establish the security criteria of standard life cycle models for the organization.	Security criteria is identified for a standard life cycle model and for each of its constituent stage models. The security criteria are used to reflect the security purpose, outcomes, and level of assurance of each stage. The security criteria also address tailoring needs to optimize the standard model to suit the specific needs of the engineering project for delivering a specific system of interest to meet assurance, trustworthiness objectives, and identified constraints.	- Defined milestones / gateways for each SDLC phase.	*LM-1.4*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	C	I	C	A/R	R	I	I	C	I	I	I
Security Culture	**Life Cycle Model Management (LM)** - Assess the security aspects of the process.	SC-5	Monitor and analyze the security aspects of process execution across the organization.	Monitoring and analysis identifies security-relevant trends regarding the efficiency and effectiveness of the process in achieving the intent of the engineering organization policies and complying with relevant laws, regulations, directives, or policies. The scope of monitoring includes the security-specific process execution methods and the process execution of methods that are not producing any specific security outcome but must operate effectively within security-oriented constraints. The security aspects monitored include those aspects associated with levels of assurance.	- Defined Key Performance Indicators (KPIs) pertaining to SDLC phases.	*LM-2.1*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	R	I	I	A/R	C	C	I	C	I	I	I
Security Culture	**Infrastructure Management (IM)** - Establish the secure infrastructure.	SC-10	Define the infrastructure security requirements.	The infrastructure includes facilities, tools, hardware, software, firmware, services, personnel, and standards used to engineer the system-of-interest. The enabling systems of the system-of-interest may be part of the infrastructure and may also be produced by the same infrastructure. Therefore, they are subject to the same level of trustworthiness and risk thresholds as the system-of-interest. Infrastructure protection needs, associated constraints, and assurance and trustworthiness objectives for the infrastructure are defined and driven by the project assets and the associated asset loss consequences in consideration of disruptions, hazards, and threats. The protection needs are transformed into security requirements for the infrastructure and associated security constraints that inform all infrastructure requirements. The technical processes are used to provide a secure infrastructure in accordance with engineering organizational and project strategic plans and policies. In addition, the infrastructure security requirements and security constraints informed by the protection needs for project data and information include stakeholder data and information used by the project. The results of the Information Management process along with the results of the other technical processes are leveraged by this task.	- Defined security controls that are b data classification and system cr ty (e.g., basic or enhanced requireme	*IF-1.1*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	R	I	I	A/R	C	C	I	C	I	I	I
Security Culture	**Infrastructure Management (IM)** - Maintain the secure infrastructure.	SC-12	Evaluate the degree to which delivered infrastructure resources satisfy project protection needs.	The method of evaluation and evaluation criteria are identified as part of defining the infrastructure security requirements. Evaluation may be based on methods used for verification and validation, to include methods for delivery, acceptance, assembly, and checkout. The scope of evaluation includes facilities, personnel, procedures, and processes. The Transition, Verification and Validation processes may be used to conduct evaluation of the degree of effectiveness.	- Report on Information Assurance (IA) testing.	*IF-2.1*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	R	I	I	A/R	C	C	I	C	I	I	I
Security Culture	**Portfolio Management (PM)** - Define and authorize the security aspects of projects.	SC-14	Identify potential new or modified security capabilities or security aspects of missions or business opportunities.	There are two aspects of security that are to be considered. First, there is a basic need for across-the-board consideration of security in all project matters. Second, the primary project objective may be to address the need for a new or modified security capability, product, or security service. The Business or Mission Analysis and Stakeholder Needs and Requirements Definition are leveraged in determining security-oriented needs and opportunities of the portfolio of projects, which are then managed through this process.	- Business Impact Analysis (BIA)	*PM-1.1*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	R	I	I	A/R	C	C	I	C	I	I	I
Security Culture	**Portfolio Management (PM)** - Define and authorize the security aspects of projects.	SC-17	Identify the security aspects of goals, objectives, and outcomes of each project.	Security aspects include those that define, constrain, and inform goals, objectives, and outcomes of each project. Specific security-driven objectives and constraints include level of assurance and risk thresholds.	- Key Performance Indicators (KPIs).	*PM-1.4*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	R	I	I	A/R	C	C	I	C	I	I	I
Security Culture	**Portfolio Management (PM)** - Define and authorize the security aspects of projects.	SC-21	Authorize each project to commence execution with consideration of the security aspects of project plans.	Execution of projects should be dependent on a determination that security considerations have been adequately addressed and properly captured by the security aspects in project plans.	- "Go Live" authorization decision.	*PM-1.8*	*CA-1 CA-6 PL-1 PL-2 PM-13 SA-8 SA-15*	*5.1.1 5.1.2 6.1.1 6.1.5 7.2.2 12.1.1 14.1.1 14.2.1 14.2.5 18.1.1 18.2.2*			C	I	R	I	I	A/R	C	C	I	C	I	I	I

Privacy Domain	Privacy Task Focus	Privacy Management Task	Task #	Privacy Task Objective	Context	Privacy Status	Notes / Findings / Recommendations	Applicable NIST 800-160 Control #	Security Architecture	Security Engineering	Governance, Compliance & Risk	Security Operations	Legal / Privacy	Project Owner	Project Manager	Project Team	Technology Architecture	Infrastructure Team	Application Team
High Level Privacy Analysis & Use Case Description	Application & Business Process Descriptions	Use Case Description	1	Provide a general description of the use case.	The first step in applying the **OASIS Privacy Management Reference Model and Methodology (PMRM)** requires the scoping of the application(s) or business service(s) in which Personal Information (PI) is associated. The intent is to identify the complete environment where privacy and data protection requirements are applicable.			*BA-1.2* *SN-2.1* *SN-3.1*	C	C	C	I	C	A/R	R	R	I	I	C
		Use Case Inventory	2	Provide an inventory of the capabilities, applications and policy environment under review at the level of granularity appropriate for the analysis covered by the PMRM and define a high-level use case which will guide subsequent analysis.	The inventory can include applications and business processes; products; policy environment; legal and regulatory jurisdictions; systems supporting the capabilities and applications; data; time; and other factors Impacting the collection, communication, processing, storage and disposition of PI. The inventory should also include the types of data subjects covered by the use case together with individual user privacy options (such as policy preferences, privacy settings, etc. if these are formally expressed). In order to facilitate the analysis described in the Detailed Privacy use case Analysis, the components of the use case Inventory should align as closely as possible with the components that will be analyzed in the corresponding detailed use case analysis.			[illegible] *SN-3*[illegible]	C	C	C	I	C	A/R	R	R	I	I	R
	Application Privacy Policies	Privacy Policy Conformance Criteria	3	Define and describe the criteria for conformance of a system or business process (identified in the use case and inventory) with an applicable privacy policy.	Where task #2 itemizes the environmental elements relevant to the use case, task #3 focuses on the privacy requirements specifically. As with the use case Inventory described in task # 2 above, the conformance criteria should align with the equivalent elements in the Detailed Privacy use case Analysis. Wherever possible, they should be grouped by the relevant **Fair Information Practices/Principles (FIP/Ps)** and expressed as privacy constraints.			*BA-2.2* *BA-3.1* *BA-5.1* *SN-4.2* *SN-4.3*	C	I	C	I	R	A	C	C	I	I	C
	Initial Privacy Impact (or other) Assessment(s)	Assessment Preparation	4	Prepare an initial **Privacy Impact Assessment (PIA)**, or as appropriate, a risk assessment, privacy maturity assessment, compliance review, or accountability model assessment applicable within the scope of analysis carried out in previous steps.	Such an assessment can be deferred until a later iteration step or inherited from a previous exercise.			*SN-1.3*	C	I	C	I	R	A	C	C	I	I	C