Control Validation Testing (CVT)
Mapping To Leading Cybersecurity and Privacy Practices

Phase	Task #	Name	Task	Outcomes	ISO 27002	NIST CSF	NIST 800-53	NIST 800-160	NIST 800-171	Secure Controls Framework
Prepare (organization)	P-1	Risk Management Roles	Identify and assign individuals to specific roles associated with security and privacy risk management.	• Individuals are identified and assigned key roles for executing the Risk Management Framework.		ID.AM-6 ID.GV-2	PL-9 PM-2 PM-6			GOV-04
Prepare (organization)	P-2	Risk Management Strategy	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.	11.1.4	ID.RM ID.SC	PM-9 RA-	3.3.4	NFO	RSK-01
Prepare (organization)	P-3	Risk Assessment (organization)	Assess organization-wide security and privacy risk and update the results on an ongoing basis.	• An organization-wide risk assessment is completed or an existing risk assessment is updated.	11.1.4	ID.RA ID.SC-2	RA-2 RA-3		3.11.1	RSK-03 RSK-04
Prepare (organization)	P-4	Organization-Wide Tailored Control Baselines & Profiles	Establish, document, and publish organization-wide tailored control baselines and/or profiles.	• Tailored control baselines for organization-wide use are established and made available.						CFG-02.9
Prepare (organization)	P-5	Common Control Identification	Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.	• Common controls that are available for inheritance by organizational systems are identified, documented, and published.						GOV-02
Prepare (organization)	P-6	Impact-Level Prioritization	Prioritize organizational systems with the same impact level.	• A prioritization of organizational systems with the same impact level is conducted.		ID.AM-5				CFG-02.5
Prepare (organization)	P-7	Continuous Monitoring Strategy (organization)	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.	• An organization-wide strategy for monitoring control effectiveness is developed and implemented.	12.4.1	DE.CM ID.SC-4	AU-1 SI-4		NFO	MON-01
Prepare (system-level)	P-8	Business Focus	Identify the missions, business functions, and mission/business processes that the system is intended to support.	• Missions, business functions, and mission/business processes that the system is intended to support are identified.		ID.BE	CP-2(8)			BCD-02
Prepare (system-level)	P-9	Stakeholder Identification	Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	• The stakeholders having an interest in the system are identified.		ID.AM ID.BE	PL-2(3)		NFO	IAO-03.1
Prepare (system-level)	P-10	Asset Identification	Identify assets that require protection.	• Stakeholder assets are identified and prioritized.	8.1.1	ID.AM	CM-8 PM-5		3.4.1 3.4.2	AST-02
Prepare (system-level)	P-11	Define Scope	Determine the authorization boundary of the system.	• The authorization boundary (i.e., system) is determined			PL-2 SA-5(1) SA-5(2) SA-5(3) SA-5(4)			AST-04
Prepare (system-level)	P-12	Information Types	Identify the types of information to be processed, stored, and transmitted by the system.	• The types of information processed, stored, and transmitted by the system are identified.	8.2.1	ID.AM-5				DCH-02
Prepare (system-level)	P-13	Information Life Cycle	Identify and understand all stages of the information life cycle.	• Identify and understand all stages of the information life cycle.	14.2.2		SA-3	3.2.1	NFO	PRM-07
Prepare (system-level)	P-14	Risk Assessment (system)	Conduct a system-level risk assessment and update the risk assessment on an ongoing basis.	• A system-level risk assessment is completed or an existing risk assessment is updated.	11.1.4	ID.RA ID.SC-2	RA-2 RA-3		3.11.1	RSK-03 RSK-04
Prepare (system-level)	P-15	Security & Privacy Requirements	Define the security and privacy requirements for the system and the environment of operation.	• Security and privacy requirements are defined and prioritized.	14.2.5	ID.GV PR.IP	AR-7 SA-8 SA-13 SC-7(18) SI-1	2.1 2.2 2.3 2.4	3.13.1 3.13.2 NFO	SEA-01
Prepare (system-level)	P-16	Enterprise Architecture	Determine the placement of the system within the enterprise architecture.	• The placement of the system within the enterprise architecture is determined.	14.1.1		PL-8 PM-7	3.4 3.4.1 3.4.2 3.4.3 3.4.4 3.4.5 3.4.6	NFO	SEA-02
Prepare (system-level)	P-17	System Registration	Register the system with organizational program or management offices.	• The system is registered for purposes of management, accountability, coordination, and oversight.		ID.GV	PM-5			AST-01
Categorize	C-1	Security Categorization	Categorize the system and document the security categorization results.	• A security categorization of the system, including the information processed by the system represented by the organizationidentified information types, is completed. • Security categorization results are documented in the security and privacy plans. • Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes. • Security categorization results reflect the organization's risk management strategy.		ID.AM-5	CA-1 PM-10		NFO	IAO-01
Categorize	C-2	Security Categorization Review & Approval	Review and approve the security categorization results and decision.	• The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.			CA-1 PM-10		NFO	IAO-01
Categorize	C-3	System Description	Document the characteristics of the system.	• The characteristics of the system are described and documented.			PL-2		3.12.1 3.12.2 3.12.3 3.12.4 NFO	IAO-03
Select	S-1	Requirements Allocation	Allocate security and privacy requirements to the information system and to the environment of operation.	• Security and privacy requirements are allocated to the system and to the environment in which the system operates.		ID.GV				IAO-03.2
Select	S-2	Control Selection	Select the controls for the system and the environment of operation.	• Control baselines necessary to protect the system commensurate with risk are selected. • Controls are assigned as system-specific, hybrid, or common controls.		PR.IP	CA-1 PM-10		NFO	IAO-01
Select	S-3	Control Tailoring	Tailor the controls selected for the system and the environment of operation.	• Controls are tailored producing tailored control baselines			CA-1 PM-10		NFO	IAO-01
Select	S-4	Plan Development	Document the controls for the system and environment of operation in security and privacy plans.	• Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.			PL-2		3.12.1 3.12.2 3.12.3 3.12.4 NFO	IAO-03
Select	S-5	Continuous Monitoring Strategy (system)	Develop and implement a system-level strategy for monitoring control effectiveness to supplement the organizational continuous monitoring strategy.	• A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.	12.4.1	ID.GV DE.CM	AU-1 CA-7 CA-7(1) PM-14 SI-4	3.3.8	3.12.1 3.12.2 3.12.3 3.12.4 NFO	CPL-02 MON-01
Select	S-6	Plan Review & Approval	Review and approve the security and privacy plans for the system and the environment of operation.	• Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.			CA-1 PM-10		NFO	IAO-01
Implement	I-1	Control Implementation	Implement the controls in the security and privacy plans.	• Controls specified in the security and privacy plans are implemented. • Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans.		PR.IP-1 PR.IP-2	CA-1 PM-10		NFO	IAO-01
Implement	I-2	Baseline Configuration	Establish the initial configuration baseline for the system by documenting changes to planned control implementation.	• The configuration baseline is established. • The security and privacy plans are updated based on information obtained during the implementation of the controls.	14.1.1	PR.IP-1	CM-2 CM-6 SA-8	3.4.7 3.4.8	3.4.1 3.4.2	CFG-02
Assess	A-1	Assessor Selection	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.	14.2.8		CA-2 CA-2(1) CA-2(2) CA-2(3)		3.12.1 3.12.2 3.12.3 3.12.4 NFO	IAO-02 IAO-02.1 IAO-02.2
Assess	A-2	Assessment Plan	Develop, review, and approve plans to assess implemented controls.	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security and privacy assessment plans are developed and documented. • Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.			CA-1 CA-2(2) PM-10			IAO-01 IAO-02.2
Assess	A-3	Control Assessments	Assess the controls in accordance with the assessment procedures described in assessment plans.	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. • Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.	18.2.2 18.2.3		CA-2 CM-4(2)	3.4.9		CPL-03 CPL-03.2 IAO-06
Assess	A-4	Assessment Reports	Prepare the assessment reports documenting the findings and recommendations from the control assessments.	• Security and privacy assessment reports that provide findings and recommendations are completed.	18.2.2 18.2.3		CA-2	3.4.9		CPL-03 CPL-03.2
Assess	A-5	Remediation Actions	Conduct initial remediation actions on the controls and reassess remediated controls.	• Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. • Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions.		ID.RA-6	SA-11(2)			RSK-06 TDA-15
Assess	A-6	Plan of Action & Milestones (POA&M)	Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.	• A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed.		ID.RA-6	CA-5 PM-4		3.12.1 3.12.2 3.12.3 3.12.4	IAO-05
Authorize	R-1	Authorization Package	Assemble the authorization package and submit the package to the authorizing official for an authorization decision.	• An authorization package is developed for submission to the authorizing official.			CA-1 PM-10		NFO	IAO-01
Authorize	R-2	Risk Analysis & Determination	Analyze and determine the risk from the operation or use of the system or the provision of common controls.	• A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.	11.1.4	ID.RA ID.SC-2	RA-2 RA-3		3.11.1	RSK-03 RSK-04 RSK-05
Authorize	R-3	Risk Response	Identify and implement a preferred course of action in response to the risk determined.	• Risk responses for determined risks are provided.	8.3	ID.RA-6	CA-5 PM-4 RA-7		3.12.1 3.12.2 3.12.3 3.12.4	IAO-05 RSK-06.1
Authorize	R-4	Authorization Decision	Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	• The authorization for the system or the common controls is approved or denied.			CA-1 PM-10		NFO	IAO-01
Authorize	R-5	Authorization Reporting	Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.	• Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.			CA-1 PM-10		NFO	IAO-01
Monitor	M-1	System & Environment Changes	Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.	• The information system and environment of operation are monitored in accordance with the continuous monitoring strategy.		DE.CM ID.GV	CA-1 PM-10		NFO	IAO-01
Monitor	M-2	Ongoing Assessments	Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy.	• Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.		ID.SC-4	RA-4			RSK-07
Monitor	M-3	Ongoing Risk Response	Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.	• The output of continuous monitoring activities is analyzed and responded to appropriately.		ID.RA-6 RS.AN				RSK-06.1
Monitor	M-4	Authorization Updates	Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.	• Risk management documents are updated based on continuous monitoring activities.		RS.IM	CA-1 PM-10		NFO	IAO-01
Monitor	M-5	Security & Privacy Reporting	Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.	• A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.		PR.IP-8	AR-6 PM-6		3.3.7 3.3.8	GOV-05 PRI-14
Monitor	M-6	Ongoing Authorization	Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.	• Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.			CA-1 PM-10		NFO	IAO-01
Monitor	M-7	System Disposal	Implement a system disposal strategy and execute required actions when a system is removed from operation.	• A system disposal strategy is developed and implemented, as needed.	8.3.2 11.2.7	PR.IP-6	MP-6	3.4.14		AST-09