Operational Risk Management Regulation: technical evidence

Neither Mamluk LLC-FZ nor its products are affiliated with or endorsed by the Central Bank of the United Arab Emirates.

Regime	Operational Risk Management Regulation, Central Bank of the UAE, United Arab Emirates
Organisation	Example Bank
Cluster	example-production
Collected	2026-11-19T10:53:03Z
Collector	Bahriya Tersane Compliance and Assurance Convoy, collector 1.x.y

This report records technical evidence from one Kubernetes cluster. It maps the requirements of the regime named above to what the cluster shows, through the controls of NIST SP 800-53 Rev. 5. It does not state that the organisation complies with the regime.

The Central Bank publishes no mapping of this regulation to NIST SP 800-53. The mapping in this report is Mamluk's own.

The report covers Articles 8 (ICT and cybersecurity), 9 (incident management) and 12 (change management) in full, and clauses 3.4, 7.4.5, 7.13, 7.14 and 15.2 to 15.3. The regulation's other clauses, including those on the Board's and senior management's duties for ICT risk, are outside it.

Clause 8.10 requires compliance with the ICT, cyber and information security regulations of the relevant UAE authorities. The UAE Information Assurance Standard, one of them, is assessed in its own report, which this report does not repeat.

The regulation is published in Arabic and English and does not state which text prevails. The paraphrases in this report were made from the English text.

Organisational requirements are the organisation's to evidence, and the report marks them so. Where a requirement is only partly technical, the cluster evidences its part and the organisation the rest. Whether the organisation complies is determined by its assessor.

Requirement identifiers are the regulator's; each summary is Mamluk's own paraphrase, not the regulator's text. The files of this run are listed with their SHA-256 digests in manifest.sha256.

This report is the evidence. The ClusterComplianceReport tersane-compliance-nist that the cluster also holds is an indicative summary of trivy-operator's checks by NIST control, in which a check that has not run is shown as passed; it is not evidence for any regime.

Exempt namespaces: kube-system, kube-node-lease, kube-public, tigera-operator, calico-system, calico-apiserver, longhorn-system, cert-manager, kong, kuma-system, logging, netdata, bahriya-system, kyverno, trivy-system, local-path-storage, compliance, compliance-node. No policy this chart installs applies in these namespaces, and their failures are listed under each check without being counted: they hold the platform's own components (on a Bahriya Kubernetes Engine cluster, its system namespaces), the policy engine, the scanner and this Convoy, which need what the policies forbid. The namespace default is judged only while it holds a workload.

Summary

63 requirements: 0 enforced by a policy, 5 checked, 0 provided by the platform, 58 organisational (3 technical, outside the cluster; 47 non-technical; 8 technical and non-technical).

Outcome	Requirements	Meaning
Fail	1	The cluster was checked and something does not meet the requirement. The findings say what and where.
Not provided	0	A control the requirement needs is switched off on this cluster.
Incomplete	1	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	0	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	1 of which with exception: 0	Every check behind the requirement passed on this run's date. Where coverage is partial, the pass covers the cluster's part only.
Recorded	2	Facts collected for the organisation's reviewer, such as an inventory or a list of access; no verdict.
Nothing to check	0	The cluster has nothing of this kind yet, for example no Ingress to check for TLS. Neither a pass nor a failure.
Organisational evidence	58	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

2 object(s) fail at least one check: 2 cluster-wide and 0 in 0 namespace(s). They are listed under Fix first, the most severe first.

Fix first

Each object that fails a check, with the requirements it fails, what is wrong, how to fix it and the command that shows the full result. Objects are grouped by namespace; objects that belong to no namespace are cluster-wide. A group's place is set by its most severe finding, and within a group the most severe come first. Fixing an object clears its failure in every requirement listed against it. Failures in exempt namespaces are not listed here; they are listed, not counted, under each check.

Cluster-wide

2 object(s), most severe Critical.

ClusterRole **tigera-operator** Fails 7.4.5	
CRITICAL	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator' shouldn't have access to manage resource 'secrets' Check trivy.rbac-privilege, trivy-operator AVD-KSV-0041. **How to fix** Manage secrets are not allowed. Remove resource 'secrets' from cluster role (trivy-operator)
CRITICAL	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'tigera-operator' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"] Check trivy.rbac-privilege, trivy-operator AVD-KSV-0114. **How to fix** Remove webhook configuration resources/verbs, acceptable values for verbs ['get', 'list', 'watch'] (trivy-operator)
Full result	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator -o yaml`

ClusterRole **tigera-operator-secrets** Fails 7.4.5	
CRITICAL	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator-secrets' shouldn't have access to manage resource 'secrets' Check trivy.rbac-privilege, trivy-operator AVD-KSV-0041. **How to fix** Manage secrets are not allowed. Remove resource 'secrets' from cluster role (trivy-operator)
Full result	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator-secrets -o yaml`

Requirements

3 Operational resilience

3.4 Critical Operations identified, and each mapped to the assets it depends on (people, technology, processes, data, facilities and service providers, intragroup ones included) and to their interdependencies, with the mapping kept current through change management. **Recorded**

Checked, coverage partial. NIST SP 800-53: CM-8 System Component Inventory, CP-2(8) Identify Critical Assets.

Scope of this evidence The evidence is the cluster's workload inventory, recorded each day. The mapping of each Critical Operation to its assets, and every asset outside the cluster, are the institution's to evidence.

cluster.workload-inventory	**Recorded**	13 namespaces, 21 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.

7 Internal control

7.4 Control measures the regulation gives as examples

7.4.5 Among the control measures the regulation lists: access to and use of the institution's assets, and those entrusted to it, data included, safeguarded, with unauthorised access or misuse detected and reported early. **Fail**

Checked, coverage partial. NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege, AU-2 Event Logging, AU-12 Audit Record Generation, SI-4 System Monitoring.

Scope of this evidence The verdict covers access through the cluster's API: which roles and bindings grant broad rights, anonymous and kubelet access, service account tokens, and that the API server writes its audit log. Access to data through the applications, SSH and other access to the nodes, network access between workloads, access to data and assets outside the cluster, and the detection and reporting of misuse from the log, are the institution's to evidence.

Fails in ClusterRole tigera-operator, ClusterRole tigera-operator-secrets.

node.kubelet-authz	**Pass**	The kubelet authorises requests through the API server: so on all 1 node(s). Establishes: The kubelet authorises requests through the API server (Webhook mode).
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.
policy.no-default-token	**Pass**	Every object the policy judged passes it. Establishes: Pods say whether they mount a service account token, so that none receives one by default.
trivy.rbac-exec	**Pass**	Every object outside the exempt namespaces passes. Establishes: Roles that allow executing into Pods or impersonating privileged groups.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.
trivy.token-automount	**Pass**	Every object outside the exempt namespaces passes. Establishes: Pods that mount a service account token.

7.13 Operational risk stress tests run periodically, challenging the control environment across ICT systems, physical controls, people and other risk vectors, for example by penetration testing. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CA-8 Penetration Testing, CA-2 Control Assessments.

7.14	For Critical Functions at least, the periodic testing includes penetration testing by an independent third party, with the results presented to the Board. Organisational, technical, outside the cluster. NIST SP 800-53: CA-8(1) Independent Penetration Testing Agent or Team, CA-2(1) Independent Assessors.	**Organisational evidence**

8 ICT and cybersecurity

8.1 ICT and cybersecurity risk framework

8.1.1	An ICT and cybersecurity risk framework within operational risk management, with policies, processes and systems to identify and assess ICT risk. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-9 Risk Management Strategy.	**Organisational evidence**
8.1.2	ICT risk mitigated in proportion to its assessed level, for example through policies, processes and systems for cybersecurity, for response and recovery, and for handling changes and incidents. Organisational, technical and non-technical. NIST SP 800-53: RA-7 Risk Response, PM-9 Risk Management Strategy.	**Organisational evidence**
8.1.3	The mitigating measures monitored and tested regularly. Organisational, technical and non-technical. NIST SP 800-53: CA-7 Continuous Monitoring, CA-2 Control Assessments. **Scope of this evidence** The daily report records the cluster's own measures being checked. The institution's monitoring and testing of its measures is its own to evidence.	**Organisational evidence**
8.1.4	ICT and cybersecurity risks managed proactively and continuously. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-31 Continuous Monitoring Strategy.	**Organisational evidence**
8.2	The risk appetite and tolerance cover ICT and cybersecurity risk and resilience, with clear expectations for performance, resilience and tolerance for disruption. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
8.3	ICT and cybersecurity infrastructure adequate for current and projected business needs, in normal times and under stress, that preserves the confidentiality, integrity and availability of data and systems and supports integrated, comprehensive risk management. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2(2) Capacity Planning, SI-7 Software, Firmware, and Information Integrity, SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection, SC-28 Protection of Information at Rest. **Scope of this evidence** The cluster's encryption in transit and Secrets encrypted at rest are part of confidentiality only; the adequacy, capacity and availability of the infrastructure are the institution's to evidence.	**Organisational evidence**
8.4	The Board and senior management informed regularly of ICT and cybersecurity risk exposures, incidents, and weaknesses found by assessment and testing. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, IR-6 Incident Reporting.	**Organisational evidence**

8.5	Resilient ICT and cybersecurity, with protection, detection, response and recovery programmes that are tested regularly, draw on situational awareness and inform decisions that support Critical Operations. Organisational, technical and non-technical. NIST SP 800-53: IR-3 Incident Response Testing, CP-4 Contingency Plan Testing, PM-16 Threat Awareness Program.	**Organisational evidence**

8.6 Content of the ICT and cybersecurity policy, in support of the business objectives

8.6.1	The policy covers governance and oversight. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PL-1 Policy and Procedures.	**Organisational evidence**
8.6.2	The policy covers risk ownership, accountability and compliance. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PM-9 Risk Management Strategy.	**Organisational evidence**
8.6.3	The policy covers ICT security measures: access control, identity management, protection of critical information assets, network and supplier security, physical and environmental protection, vulnerability tests and classifying information. Organisational, non-technical. NIST SP 800-53: AC-1 Policy and Procedures, IA-1 Policy and Procedures, SC-1 Policy and Procedures, PE-1 Policy and Procedures, RA-1 Policy and Procedures, SR-1 Policy and Procedures. **Scope of this evidence** This requirement is what the policy covers. The cluster's evidence for access control and vulnerability testing is under 7.4.5 and 8.7.3.	**Organisational evidence**
8.6.4	The policy covers how ICT controls, and the thresholds and limits of the policy and of the risk appetite and tolerance, are evaluated and monitored regularly. Organisational, non-technical. NIST SP 800-53: CA-1 Policy and Procedures, CA-7 Continuous Monitoring.	**Organisational evidence**
8.6.5	The policy covers data management. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PM-23 Data Governance Body.	**Organisational evidence**
8.6.6	The policy covers ICT operations and service management, change and patch management included. Organisational, non-technical. NIST SP 800-53: CM-1 Policy and Procedures, SI-1 Policy and Procedures. **Scope of this evidence** This requirement is what the policy covers. The platform's versions are recorded under 8.8, and the workload inventory, from which changes can be seen, under 12.4.	**Organisational evidence**
8.6.7	The policy covers the plans for responding to and recovering from incidents, for keeping the business running, and for recovering from disaster. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures, CP-1 Policy and Procedures.	**Organisational evidence**
8.6.8	The policy covers ICT project management. Organisational, non-technical. NIST SP 800-53: SA-1 Policy and Procedures, PL-1 Policy and Procedures.	**Organisational evidence**

8.6.9	The policy covers systems development and acquisition. Organisational, non-technical. NIST SP 800-53: SA-1 Policy and Procedures.	**Organisational evidence**

8.7 Review and testing of ICT and cybersecurity risk management

8.7.1	ICT and cybersecurity risk management reviewed regularly to remain compliant with industry standards and good practice, and to address new technologies and threats. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, RA-3 Risk Assessment.	**Organisational evidence**
8.7.2	ICT and cybersecurity risk management tested regularly, to find gaps against the risk tolerance and to improve identification, protection, detection and event management. Organisational, technical and non-technical. NIST SP 800-53: CA-2 Control Assessments, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
8.7.3	Actionable intelligence used to improve the cybersecurity posture continuously, to keep aware of vulnerabilities in applications, networks and ICT systems, and to inform risk and change decisions. Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SI-5 Security Alerts, Advisories, and Directives, PM-16 Threat Awareness Program. **Scope of this evidence** The verdict concerns the vulnerability scans of the images of workloads outside the exempt namespaces: that they are current, and that no critical or high vulnerability is open; the age of each is recorded. The platform's own components, the nodes' operating systems, threat intelligence, and systems and networks outside the cluster are the institution's to evidence.	**Pass**

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.
cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

8.8 ICT and cybersecurity systems, those of third-party providers included, managed proactively, with a strategy and timeline to renew or retire obsolete and unsupported hardware and software. **Incomplete**

Checked, coverage partial. NIST SP 800-53: SA-22 Unsupported System Components.

Scope of this evidence The verdict covers the cluster's Kubernetes release, judged against the end-of-life dates the Kubernetes project publishes; its Bahriya Kubernetes Engine release, judged against Mamluk's published support policy; and the operating systems of the images outside the exempt namespaces, judged against trivy's end-of-life data. A release or an image out of support fails, and the versions are recorded. The nodes' operating systems, hardware, systems outside the cluster, and the strategy and timeline for renewal are the institution's to evidence.

platform.version-support	**Pass**	Kubernetes 1.36 is supported until 2027-06-28, as https://kubernetes.io/releases/ states. Bahriya Kubernetes Engine 2.6 is one of the 5 most recent minor releases, and supported under https://bke.bahriya.cloud/faq/#release-support. Establishes: The cluster's Kubernetes minor release is within its end-of-life date as the Kubernetes project states it, and its BKE minor release within Mamluk's published BKE support policy (one of the five most recent minor releases, or six months from its release, whichever is longer); a release past either fails, as end of support. Each table is dated, and a table not reviewed in time gives no verdict.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.
trivy.image-os-support	**Not evaluated**	No image outside the exempt namespaces runs on an operating system trivy recognises, so none was judged. Establishes: Every workload's images are scanned for the operating system they are built on; an image whose operating system trivy holds past its end of service life fails, as end of support. An image with no operating system that trivy recognises is listed by name and not judged.

8.9 The Master System of Record maintained continuously and kept in the UAE, outsourced arrangements included; a branch of a foreign institution may instead keep a current copy in the UAE, with the Central Bank's approval. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: SA-9(5) Processing, Storage, and Service Location.

8.10	Compliance with the ICT, cyber and information security regulations of the relevant UAE authorities. Organisational, non-technical. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures.	**Organisational evidence**

9 Incident management

9.1	Incident response and recovery plans developed and implemented, in line with the risk appetite and tolerance for disruption, for incidents that could disrupt Critical Operations, ICT and cyber incidents included. Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, IR-1 Policy and Procedures.	**Organisational evidence**
9.2	The plans reviewed, tested and updated regularly from lessons learned; the root cause of every material incident addressed to prevent recurrence or reduce its likelihood, and the effectiveness of this measured and reviewed. Organisational, technical and non-technical. NIST SP 800-53: IR-3 Incident Response Testing, IR-4 Incident Handling.	**Organisational evidence**
9.3	An inventory of the internal and third-party resources needed for response and recovery. Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, CP-2 Contingency Plan.	**Organisational evidence**

9.4 The incident life cycle

9.4.1	Incidents classified by severity against predefined criteria, such as impact and expected time to recover, to prioritise the response and its resources. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-8 Incident Response Plan.	**Organisational evidence**
9.4.2	Procedures to respond to and recover from incidents, and their link to the continuity plan and other contingency arrangements. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, CP-2 Contingency Plan.	**Organisational evidence**
9.4.3	The roles of staff and external parties in recording, analysing, escalating, deciding on, resolving and monitoring incidents. Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, IR-7 Incident Response Assistance.	**Organisational evidence**
9.4.4	Plans for reporting incidents to internal and external stakeholders, the Central Bank and other authorities included, with performance metrics during an incident and lessons learned after it. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting, IR-8 Incident Response Plan.	**Organisational evidence**

9.4.5	Every incident documented in a register, with its nature, the actions taken and the outcome. Organisational, non-technical. NIST SP 800-53: IR-5 Incident Monitoring, IR-6 Incident Reporting.	**Organisational evidence**
9.5	Incident management covers every Critical Operation and the resources its resilience and continuity need, as mapped under 3.4. Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, CP-2 Contingency Plan.	**Organisational evidence**

12 Change management

12.1	A well-resourced change management process that plans proactively for operational changes, and manages and approves them: new, changed or discontinued products, activities, processes and systems. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control, CM-1 Policy and Procedures.	**Organisational evidence**
12.2	The operational risk function involved throughout change management, so that controls are put in place and the control functions take part. Organisational, non-technical. NIST SP 800-53: CM-3(4) Security and Privacy Representatives.	**Organisational evidence**

12.3 Change management policies and procedures, and what they consider

12.3.1	The inherent risks of a change, legal, financial, compliance, model and ICT risks among them. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses, RA-3 Risk Assessment.	**Organisational evidence**
12.3.2	The change's effect on the risk profile, through the change itself and its effect on related activities, and on compliance with the risk appetite and tolerance. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses, PM-9 Risk Management Strategy.	**Organisational evidence**
12.3.3	The controls, risk management processes and mitigation the change needs. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses, RA-7 Risk Response.	**Organisational evidence**
12.3.4	The residual risk of the change. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses, RA-7 Risk Response.	**Organisational evidence**
12.3.5	New or changed risk limits or thresholds. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
12.3.6	How the risk of the change is measured, monitored and managed, with procedures and metrics. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control, PM-6 Measures of Performance.	**Organisational evidence**
12.3.7	The resources available and needed for the change, technology infrastructure, staff and expertise included, at every level from the Board to the three lines of defence. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources, CM-3 Configuration Change Control.	**Organisational evidence**
12.3.8	The part each line of defence plays in change management. Organisational, non-technical. NIST SP 800-53: CM-3(4) Security and Privacy Representatives.	**Organisational evidence**

12.3.9	The change's effect on the mapping of Critical Operations' interdependencies, on the continuity and disaster recovery plans, and on the rest of the operational risk framework. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses, CP-2 Contingency Plan.	**Organisational evidence**
12.3.10	The change's effect on risk data and systems, and on the data that must be captured. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses.	**Organisational evidence**
12.3.11	Proactive communication about the change with internal and external stakeholders, third-party providers included. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
12.3.12	How each of these applies to urgent and emergency changes. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
12.4	Changes monitored after they go live, to find and manage material differences from the expected operational risk profile. Checked, coverage partial. NIST SP 800-53: CM-2 Baseline Configuration, CM-3 Configuration Change Control, CM-4(2) Verification of Controls. Evidence counted: cluster.workload-inventory; the rest of the regime's mapping is not evidenced by the cluster. **Scope of this evidence** The evidence is the cluster's workload inventory, recorded each day; comparing successive reports shows what changed. The comparison with the expected risk profile is the institution's to evidence. cluster.workload-inventory — **Recorded** — 13 namespaces, 21 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.	**Recorded**

12.5 Changes material to Critical Operations or to customers

12.5.1	Such changes closely overseen and controlled, and tested thoroughly before they go live, with the results reviewed and approved by the relevant stakeholders. Organisational, technical and non-technical. NIST SP 800-53: CM-3(2) Testing, Validation, and Documentation of Changes, CM-4 Impact Analyses.	**Organisational evidence**
12.5.2	Plans to recover from a failed implementation: a way to roll back and, where a new ICT system replaces an old one, a parallel run long enough to show the new one works and is resilient. Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control, CP-2 Contingency Plan.	**Organisational evidence**
12.5.3	An external expert gives independent assurance at key steps, including a report on the proposed change and its controls. Organisational, non-technical. NIST SP 800-53: CA-2(1) Independent Assessors, CM-4 Impact Analyses.	**Organisational evidence**
12.5.4	Senior management reviews, endorses and responds to the expert's report before it goes to the Central Bank. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**

12.5.5	The Central Bank notified, with the expert's report, at least 30 calendar days before implementation. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
12.5.6	The Central Bank's written no-objection obtained before implementation. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
12.6	Customers not harmed by changes: where a change gives them materially wrong information, they are told clearly what the error did to their accounts or transactions, as part of correcting it, and the institution is liable for the resulting damage under the Central Bank's consumer protection rules. Organisational, non-technical. NIST SP 800-53: CM-4 Impact Analyses.	**Organisational evidence**

15 Notification and reporting

15.2 Notifying events that affect Critical Operations

15.2.1	The Central Bank notified within 4 hours of an event that significantly affects, or may affect, the continuity or integrity of any Critical Operation, naming the operations affected. Such events include any that sets off, or may set off, the continuity or disaster recovery plans, and any with a material actual or likely impact on customers, operations, profitability or capital. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
15.2.2	A summary report to the Central Bank within 24 hours: the event's nature, the actions under way, the likely impact and the expected time to return to normal. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
15.2.3	The Central Bank notified on the return to normal operations. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
15.2.4	Any further notification or information the Central Bank requires case by case, within the time it sets. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
15.3	The Central Bank notified of any high-risk incident within 72 hours, with the criteria for high risk set in Board-approved policy. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting, IR-8 Incident Response Plan.	**Organisational evidence**

Checks

cluster.scan-freshness **Pass**

When each workload was last scanned and how current the vulnerability database was.

Every workload outside the exempt namespaces was scanned within 48 hours.

- scans older than 48 hours fail
- 7 workload(s) outside the exempt namespaces

cluster.vulnerability-age Recorded

How long each open critical and high vulnerability has been reported.

No critical or high vulnerability is open outside the exempt namespaces.

- ages are counted from the first run of this collector that reported each one

cluster.workload-inventory Recorded

An inventory of the cluster's namespaces, workloads and the images they run.

13 namespaces, 21 workloads, 16 distinct images.

Namespace	Workload	Images
compliance	CronJob compliance-collect-nca-ecc	registry.example.com/tersane/convoy/compliance/core/collector:1.x.y@sha256:c6258
compliance	Deployment compliance-web-view	registry.example.com/tersane/core/nginxinc/nginx-unprivileged:1.x.y@sha256:f5116e
compliance	Pod reader	registry.example.com/tersane/core/nginxinc/nginx-unprivileged@sha256:f5116ed460
compliance-node	Job node-facts-gtn4z	registry.example.com/tersane/convoy/compliance/core/collector:1.x.y@sha256:c6258
kube-system	DaemonSet kube-proxy	registry.k8s.io/kube-proxy:v1.36.4
kube-system	Deployment coredns	registry.k8s.io/coredns/coredns:v1.14.2
kyverno	Deployment engine-admission-controller	registry.example.com/tersane/core/kyverno/kyvernopre:1.x.y@sha256:27f3cc52e628 registry.example.com/tersane/core/kyverno/kyverno:1.x.y@sha256:c8c4dd09e720d2
kyverno	Deployment engine-background-controller	registry.example.com/tersane/core/kyverno/background-controller:1.x.y@sha256:c46e124f21ef8a6bb4b48de57106808b1007edcd5ddd4ff7df5
kyverno	Deployment engine-cleanup-controller	registry.example.com/tersane/core/kyverno/cleanup-controller:1.x.y@sha256:d7340a
kyverno	Deployment engine-reports-controller	registry.example.com/tersane/core/kyverno/reports-controller:1.x.y@sha256:5fb6d3e
local-path-storage	Deployment local-path-provisioner	registry.example.com/storage/local-path-provisioner:1.x.y

payments	CronJob nightly	registry.example.com/payments/legacy-batch:1.0.0
payments	CronJob weekly	registry.example.com/payments/checkout:3.10.1
payments	Deployment ledger	registry.example.com/payments/checkout:3.10.1
payments	Deployment legacy-batch	registry.example.com/payments/checkout:3.10.1
payments	Deployment unsigned-app	registry.example.com/payments/legacy-batch:1.0.0
payments	Job migrate-once	registry.example.com/payments/checkout:3.10.1
payments	Pod one-off	registry.example.com/payments/checkout:3.10.1
tigera-operator	Deployment tigera-operator	quay.io/tigera/operator:v1.44.0
trivy-system	Deployment trivy-operator-engine	registry.example.com/tersane/core/aquasecurity/trivy-operator:1.x.y@sha256:05191a
trivy-system	StatefulSet trivy-server	registry.example.com/tersane/core/aquasecurity/trivy:1.x.y@sha256:790fd66d16973

node.kubelet-authz Pass

The kubelet authorises requests through the API server (Webhook mode).

The kubelet authorises requests through the API server: so on all 1 node(s).

- Read from the kubelet's configuration and flag files: a change made after the kubelet last started is not yet in effect, and is not visible to the node collector.

platform.anonymous Not evaluated

Anonymous requests to the API server are limited to the health endpoints.

Anonymous requests restricted to the health endpoints: the platform could not observe it.

- compliance.anonymous.configured: unknown
- compliance.anonymous.observed: unknown

platform.audit Pass

The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

API audit logging: in effect on every control-plane node.

- compliance.audit.configured: yes
- compliance.audit.observed: yes
- audit.policy: bke

platform.version-support Pass

The cluster's Kubernetes minor release is within its end-of-life date as the Kubernetes project states it, and its BKE minor release within Mamluk's published BKE support policy (one of the five most recent minor releases, or six months from its release, whichever is longer); a release past either fails, as end of support. Each table is dated, and a table not reviewed in time gives no verdict.

Kubernetes 1.36 is supported until 2027-06-28, as https://kubernetes.io/releases/ states. Bahriya Kubernetes Engine 2.6 is one of the 5 most recent minor releases, and supported under https://bke.bahriya.cloud/faq/#release-support.

- kubernetes-version: v1.36.4
- Kubernetes support table: https://kubernetes.io/releases/, published, as of 2026-11-10, to be reviewed by 2027-02-08
- bke-version: 2.6.1
- Bahriya Kubernetes Engine support table: https://bke.bahriya.cloud/faq/#release-support, published, as of 2026-11-18, to be reviewed by 2027-02-16

platform.versions Recorded

The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.

Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z.

- bke-version: 2.6.1
- kubernetes-version: v1.36.4
- observed-at: 2026-11-19T10:47:57Z

policy.no-default-token Pass

Pods say whether they mount a service account token, so that none receives one by default.

Every object the policy judged passes it.

- tersane-compliance-no-default-token: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

trivy.image-os-support Not evaluated

Every workload's images are scanned for the operating system they are built on; an image whose operating system trivy holds past its end of service life fails, as end of support. An image with no operating system that trivy recognises is listed by name and not judged.

No image outside the exempt namespaces runs on an operating system trivy recognises, so none was judged.

- 29 container image(s) scanned
- 0 outside the exempt namespaces on an operating system trivy recognises, 7 on none it recognises
- Images with no operating system trivy recognises (scratch, static or unrecognised), not judged by this check: registry.example.com/payments/checkout:3.10.1, registry.example.com/payments/legacy-batch:1.0.0

trivy.rbac-exec Pass

Roles that allow executing into Pods or impersonating privileged groups.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0053, AVD-KSV-0043

- 188 object(s) with a passing result, 0 failing, 3 failing in exempt namespaces

Fails in exempt namespaces, not counted (3)

Object	What is wrong	Full result
ClusterRole admin	Kubernetes default role; AVD-KSV-0053: Exec into Pods. ClusterRole 'admin' should not have access to resource '["pods/exec"]' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-admin -o yaml`
ClusterRole edit	Kubernetes default role; AVD-KSV-0053: Exec into Pods. ClusterRole 'edit' should not have access to resource '["pods/exec"]' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-edit -o yaml`
ClusterRole system:aggregate-to-edit	Kubernetes default role; AVD-KSV-0053: Exec into Pods. ClusterRole 'system:aggregate-to-edit' should not have access to resource '["pods/exec"]' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-7b884bc5d8 -o yaml`

trivy.rbac-privilege Fail

Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

2 object(s) fail.

- trivy checks: AVD-KSV-0041, AVD-KSV-0044, AVD-KSV-0045, AVD-KSV-0047, AVD-KSV-0051, AVD-KSV-0052, AVD-KSV-0111, AVD-KSV-0112, AVD-KSV-0113, AVD-KSV-0114, AVD-KSV-0122, AVD-KSV-0123
- 188 object(s) with a passing result, 2 failing, 17 failing in exempt namespaces

How to fix AVD-KSV-0041 Manage secrets are not allowed. Remove resource 'secrets' from cluster role (trivy-operator)

How to fix AVD-KSV-0114 Remove webhook configuration resources/verbs, acceptable values for verbs ['get', 'list', 'watch'] (trivy-operator)

Fails (3)

Object	What is wrong	Full result
ClusterRole tigera-operator	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator -o yaml`
ClusterRole tigera-operator	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'tigera-operator' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator -o yaml`
ClusterRole tigera-operator-secrets	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator-secrets' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator-secrets -o yaml`

Fails in exempt namespaces, not counted (18)

Object	What is wrong	Full result
ClusterRole admin	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'admin' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-admin -o yaml`
ClusterRole cluster-admin	Kubernetes default role; AVD-KSV-0044: No wildcard verb and resource roles. Role permits wildcard verb on wildcard resource	`kubectl get clusterrbacassessmentreport clusterrole-cluster-admin -o yaml`
ClusterRole edit	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'edit' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-edit -o yaml`
ClusterRole kyverno:admission-controller	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:admission-controller' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-78fb9f7b45 -o yaml`
ClusterRole kyverno:admission-controller:core	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:admission-controller:core' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-66dd849fcd -o yaml`
ClusterRole kyverno:cleanup-controller	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:cleanup-controller' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-5fc98dd666 -o yaml`
ClusterRole kyverno:cleanup-controller:core	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:cleanup-controller:core' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-757c5df67 -o yaml`

ClusterRole system:aggregate-to-edit	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:aggregate-to-edit' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-7b884bc5d8 -o yaml`
ClusterRole system:controller:legacy-service-account-token-cleaner	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:controller:legacy-service-account-token-cleaner' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-864fd65956 -o yaml`
ClusterRole system:kube-controller-manager	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:kube-controller-manager' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-b754c4cc6 -o yaml`
ClusterRole system:node	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:node' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-54cdc9b678 -o yaml`
ClusterRole trivy-operator	AVD-KSV-0041: Manage secrets. ClusterRole 'trivy-operator' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-trivy-operator -o yaml`
ClusterRole trivy-operator	AVD-KSV-0047: Do not allow privilege escalation from node proxy. Role permits privilege escalation from node proxy	`kubectl get clusterrbacassessmentreport clusterrole-trivy-operator -o yaml`
Role kyverno/kyverno:admission-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:admission-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-78fb9f7b45 -n kyverno -o yaml`
Role kyverno/kyverno:background-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:background-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-586b8c778d -n kyverno -o yaml`
Role kyverno/kyverno:cleanup-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:cleanup-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-5fc98dd666 -n kyverno -o yaml`
Role kyverno/kyverno:reports-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:reports-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-899885f55 -n kyverno -o yaml`
Role trivy-system/trivy-operator-engine	AVD-KSV-0113: Manage namespace secrets. Role 'trivy-operator-engine' shouldn't have access to manage secrets in namespace 'trivy-system'	`kubectl get rbacassessmentreport role-trivy-operator-engine -n trivy-system -o yaml`

trivy.token-automount Pass

Pods that mount a service account token.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0036
- 188 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

trivy.vulnerabilities Pass

Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

No container outside the exempt namespaces runs an image with a critical or high vulnerability.

- 29 container image(s) scanned
- oldest scan of a workload outside the exempt namespaces: 2026-11-19T10:52:08Z

Fails in exempt namespaces, not counted (8)

Object	What is wrong	Full result
Deployment compliance/compliance-web-view (nginx)	container nginx: 1 critical, 3 high	`kubectl get vulnerabilityreport replicaset-compliance-web-view-79cb6dfddf-nginx -n compliance -o yaml`
Deployment kyverno/engine-background-controller (controller)	container controller: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-background-controller-849b6675fd-controller -n kyverno -o yaml`
Deployment kyverno/engine-cleanup-controller (controller)	container controller: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-cleanup-controller-6f84876bfc-controller -n kyverno -o yaml`
Deployment kyverno/engine-reports-controller (controller)	container controller: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-reports-controller-86d87f4465-controller -n kyverno -o yaml`
Installation calico-system/default (calico-node)	container calico-node: 1 critical, 8 high	`kubectl get vulnerabilityreport daemonset-calico-node-calico-node -n calico-system -o yaml`
Installation calico-system/default (ebpf-bootstrap)	container ebpf-bootstrap: 1 critical, 8 high	`kubectl get vulnerabilityreport daemonset-calico-node-ebpf-bootstrap -n calico-system -o yaml`
Pod compliance/reader (reader)	container reader: 1 critical, 3 high	`kubectl get vulnerabilityreport pod-reader-reader -n compliance -o yaml`
StatefulSet trivy-system/trivy-server (trivy-server)	container trivy-server: 1 critical, 4 high	`kubectl get vulnerabilityreport statefulset-trivy-server-trivy-server -n trivy-system -o yaml`

NIST SP 800-53 controls

Each control of NIST SP 800-53 Rev. 5 that a requirement in this report names, with its statement as NIST publishes it. Text in square brackets is for the organisation to define. Each link opens the control in NIST's Cybersecurity and Privacy Reference Tool.

Control	Statement

AC-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AC-3 Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-6 Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
AT-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c. Review and update the current awareness and training: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AU-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c. Review and update the current audit and accountability: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

AU-2 Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined organization-defined event types (subset of the event types defined in [AU-2a.](#au-2_smt.a)) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
AU-12 Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in [AU-2a](#au-2_smt.a) on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in [AU-2c](#au-2_smt.c) that include the audit record content defined in [AU-3](#au-3).
CA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and c. Review and update the current assessment, authorization, and monitoring: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CA-2 Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined assessment frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
CA-2(1) Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.

CA-7 Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to [Assignment: organization-defined organization-defined personnel or roles] [Assignment: organization-defined organization-defined frequency].
CA-8 Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined system(s) or system components].
CA-8(1) Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.
CM-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c. Review and update the current configuration management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CM-2 Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances] ; and 3. When system components are installed or upgraded.
CM-3 Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency] ; when [Assignment: organization-defined configuration change conditions]].
CM-3(2) Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-3(4) Security and Privacy Representatives	Require [Assignment: organization-defined organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].
CM-4 Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(2) Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.
CM-8 System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information] ; and b. Review and update the system component inventory [Assignment: organization-defined frequency].
CP-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c. Review and update the current contingency planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-2 Contingency Plan	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by [Assignment: organization-defined organization-defined personnel or roles]; b. Distribute copies of the contingency plan to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system [Assignment: organization-defined frequency]; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.

CP-2(2) Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
CP-2(8) Identify Critical Assets	Identify critical system assets supporting [Selection: all; essential] mission and business functions.
CP-4 Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
IA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and c. Review and update the current identification and authentication: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-3 Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].
IR-4 Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
IR-5 Incident Monitoring	Track and document incidents.

IR-6 Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period] ; and b. Report incident information to [Assignment: organization-defined authorities].
IR-7 Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
IR-8 Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency] ; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined organization-defined incident response personnel (identified by name and/or by role) and organizational elements] ; and e. Protect the incident response plan from unauthorized disclosure and modification.
MA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
MP-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and c. Review and update the current media protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

PE-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c. Review and update the current physical and environmental protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PL-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and c. Review and update the current planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PM-1 Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and c. Protect the information security program plan from unauthorized disclosure and modification.
PM-3 Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.
PM-6 Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.

PM-9 Risk Management Strategy	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.
PM-14 Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-16 Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PM-23 Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-31 Continuous Monitoring Strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined monitoring frequencies] and [Assignment: organization-defined assessment frequencies] for control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined organization-defined personnel or roles] [Assignment: organization-defined organization-defined frequency].
PS-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c. Review and update the current personnel security: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

PT-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] personally identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and c. Review and update the current personally identifiable information processing and transparency: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
RA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
RA-3 Risk Assessment	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles] ; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-5 Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-7 Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
SA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SA-9(5) Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements].
SA-22 Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].

SC-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business-process-level; system-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and c. Review and update the current system and communications protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SC-8 Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-13 Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses] ; and b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography].
SC-28 Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SI-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and c. Review and update the current system and information integrity: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

SI-4 System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives] ; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
SI-5 Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles] ; [Assignment: organization-defined elements] ; [Assignment: organization-defined external organizations]] ; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
SI-7 Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined organization-defined software, firmware, and information] ; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined organization-defined actions].
SR-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].