Cyber Security Framework, version 1.0 (May 2017), as published in the SAMA Rulebook: technical evidence

Neither Mamluk LLC-FZ nor its products are affiliated with or endorsed by the Saudi Central Bank.

Regime	Cyber Security Framework, version 1.0 (May 2017), as published in the SAMA Rulebook, Saudi Central Bank (SAMA), Kingdom of Saudi Arabia
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.

SAMA publishes no mapping of the framework's considerations to NIST SP 800-53. The mapping in this report is Mamluk's own. SAMA assesses each sub-domain on a maturity scale. This report gives no maturity level: it records what the cluster shows for each consideration, and the maturity level remains the Member Organization's own assessment.

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

409 requirements: 5 enforced by a policy, 17 checked, 6 provided by the platform, 381 organisational (104 technical, outside the cluster; 229 non-technical; 48 technical and non-technical).

Outcome	Requirements	Meaning

Fail	7	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	4	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	1	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	11 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	5	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	381	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

15 object(s) fail at least one check: 3 cluster-wide and 12 in 1 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

3 object(s), most severe Critical.

ClusterRole **`tigera-operator`** Fails 3.3.5.4.a	
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 3.3.5.4.a

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
```

Cluster **backups** Fails 3.3.8.6.i

HIGH neither Longhorn nor Velero is installed

Check cluster.backups.

How to fix On a Bahriya Kubernetes Engine cluster, set components.longhorn.settings.backup.target and credentialSecret in config.yaml, and backup.daily.enabled to true, then run apply.sh --commit, which creates the recurring job bke-daily-backup. A target that is configured but not available gives its reason in the longhorn-manager log: kubectl -n longhorn-system logs -l app=longhorn-manager --tail=200 | grep -i backup. With Velero, create a backup storage location that Velero reports Available and a Schedule that is not paused, as Velero's documentation describes; kubectl get backupstoragelocations.velero.io -A gives each location's phase. (Bahriya Tersane)

Full result

```
kubectl api-resources | grep -E 'longhorn.io|velero.io'
```

Namespace payments

12 object(s), most severe High.

CronJob **nightly** Fails 3.3.8.6.a, 3.3.8.6.d, 3.3.8.6.f

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of CronJob 'nightly' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of cronjob "nightly" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

CronJob **weekly** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport f95320a9-ae62-47ac-8865-9ff294efe291 -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Deployment **ledger** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport dd716344-57f2-43ff-8850-cec7fbc7281f -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Deployment **legacy-batch** Fails 3.3.8.6.a, 3.3.8.6.d, 3.3.8.6.f

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "legacy-batch-5bdd998d78" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
	`kubectl get policyreport cc1c8507-d6bb-4e77-8205-1a214c884777 -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Deployment **unsigned-app** Fails 3.3.8.6.a, 3.3.8.6.d, 3.3.8.6.f

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "unsigned-app-b5567644f" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

Job **migrate-once** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport cdf45f25-40a7-4023-bc92-880235dc0c91 -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Job **nightly-now** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 6a73d7cc-01f5-42d8-9d6c-462a360b517b -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Pod **nightly-now-k7cbf** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 4074d46b-fb0f-4ce3-8312-15270922068d -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Pod **one-off** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 157881f3-9f3d-472c-9134-201b7cf0220e -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Pod **unsigned-app-b5567644f-vpkpp** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 3f291cbb-5fdd-4171-9ead-42230533be9f -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

ReplicaSet **unsigned-app-b5567644f** Fails 3.3.8.6.d, 3.3.8.6.f

HIGH images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0

Check policy.images-signed.

How to fix Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)

Full result

```
kubectl get policyreport 9f9f8242-9449-4023-a60b-aa60653c0b24 -n payments -o yaml
```

Kyverno names each policy report after the UID of the object it covers.

Namespace **payments** Fails 3.3.7.4.g, 3.3.8.6.e

MEDIUM namespace payments holds no NetworkPolicy

Check policy.namespace-network-policy.

How to fix Add NetworkPolicies to the namespace that allow only the traffic its workloads need. To start every new namespace closed, set generate.defaultDenyNetworkPolicy.enabled to true in the Convoy's values. (Bahriya Tersane)

Full result

```
kubectl get clusterpolicyreport 1bef7dc4-e354-4b6d-bc32-e548e1af4393 -o yaml
```

Kyverno names each policy report after the UID of the object it covers.

Requirements

3.1 Cyber security leadership and governance

3.1.1 Cyber security governance

3.1.1.1	A cyber security committee, mandated by the board.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-29 Risk Management Program Leadership Roles.	
3.1.1.2	The committee led by a senior manager from a control function who is independent.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	

3.1.1.3 Who sits on the committee

3.1.1.3.a	Senior managers of all relevant departments, the CIO, COO and compliance among them.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	
3.1.1.3.b	The CISO.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	
3.1.1.3.c	Internal audit, as an observer if it attends.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	

3.1.1.4 The committee's charter

3.1.1.4.a	A charter, developed and approved, that states the committee's objectives.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	
3.1.1.4.b	The charter states roles and responsibilities.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	

3.1.1.4.c	The charter states a quorum. Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**
3.1.1.4.d	The charter sets how often it meets, at least quarterly. Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**
3.1.1.5	A cyber security function. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.1.6	The cyber security function independent of IT, with separate reporting lines, budgets and staff evaluations. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.1.7	The cyber security function reports directly to the chief executive or the head of a control function. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.1.8	A full-time CISO appointed at senior management level. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**

3.1.1.9 The CISO's appointment

3.1.1.9.a	The CISO is a Saudi national. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.1.9.b	The CISO is adequately qualified. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-13 Security and Privacy Workforce.	**Organisational evidence**
3.1.1.9.c	SAMA's no-objection obtained before the CISO is appointed. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.1.10	The board allocates enough budget for cyber security. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources.	**Organisational evidence**

3.1.2 Cyber security strategy

3.1.2.1	A cyber security strategy, defined, approved, maintained and carried out. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-1 Information Security Program Plan.	**Organisational evidence**

3.1.2.2 What the strategy is aligned with

3.1.2.2.a	The strategy aligned with the organisation's objectives. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.2.2.b	The strategy aligned with its legal and regulatory obligations. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing.	**Organisational evidence**
3.1.2.2.c	The strategy consistent with the banking sector's own strategy for cyber security. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

3.1.2.3 What the strategy covers

3.1.2.3.a	The strategy states why cyber security matters to the organisation. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.2.3.b	The strategy describes the target state for resilience to current and emerging threats. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-16 Threat Awareness Program.	**Organisational evidence**
3.1.2.3.c	The strategy says which initiatives run when to reach the target state. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-3 Information Security and Privacy Resources.	**Organisational evidence**

3.1.3 Cyber security policy

3.1.3.1	A cyber security policy, defined, approved and communicated. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.3.2	The policy reviewed periodically under a defined review process. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**

3.1.3.3 The policy's place

3.1.3.3.a	The policy informs the organisation's other policies, such as HR, finance and IT. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.3.3.b	The policy supported by detailed standards and procedures. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.3.3.c	The policy based on good practice and national and international standards. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.3.3.d	The policy communicated to those it concerns. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PL-4 Rules of Behavior.	**Organisational evidence**

3.1.3.4 What the policy contains

3.1.3.4.a	The policy defines cyber security. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.3.4.b	The policy states the organisation's cyber security objectives and scope. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.3.4.c	The policy states the board's support for those objectives. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**

3.1.3.4.d	The policy assigns general and specific responsibilities. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.3.4.e	The policy refers to its supporting standards and procedures. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures.	**Organisational evidence**

3.1.3.4.f Requirements the policy sets

3.1.3.4.f.1	Information classified by its importance to the organisation. Organisational, non-technical. NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
3.1.3.4.f.2	Information protected to the security requirements, within the risk appetite. Organisational, technical and non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.3.4.f.3	An owner for every information asset. Organisational, non-technical. NIST SP 800-53: CM-8 System Component Inventory, PM-5 System Inventory.	**Organisational evidence**
3.1.3.4.f.4	Risk assessments of information assets. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.1.3.4.f.5	An awareness programme, so that stakeholders know what is expected of them. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.3.4.f.6	Regulatory and contractual obligations met. Organisational, non-technical. NIST SP 800-53: PM-28 Risk Framing, CA-2 Control Assessments.	**Organisational evidence**
3.1.3.4.f.7	Breaches and suspected weaknesses reported. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.1.3.4.f.8	Cyber security reflected in business continuity management. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**

3.1.4 Cyber security roles and responsibilities

3.1.4.1 The board's responsibilities

3.1.4.1.a	The board ensures enough budget for cyber security. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources.	**Organisational evidence**
3.1.4.1.b	The board approves the committee's charter. Organisational, non-technical. NIST SP 800-53: PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**

3.1.4.1.c What the board endorses after the committee

3.1.4.1.c.1	The board endorses cyber security governance. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.4.1.c.2	The board endorses the strategy. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.4.1.c.3	The board endorses the policy. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**

3.1.4.2 The committee's responsibilities

3.1.4.2.a	The committee monitors, reviews and communicates the risk appetite, periodically and on a material change. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.4.2.b	The committee reviews the strategy against the organisation's objectives. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

3.1.4.2.c What the committee approves, communicates, supports and monitors

3.1.4.2.c.1	The committee approves and monitors governance. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.4.2.c.2	The committee approves and monitors the strategy. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.4.2.c.3	The committee approves and monitors the policy. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.4.2.c.4	The committee approves and monitors programmes such as awareness, data classification, privacy and data leakage prevention. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.4.2.c.5	The committee approves and monitors the risk management process. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, RA-1 Policy and Procedures.	**Organisational evidence**
3.1.4.2.c.6	The committee approves and monitors key risk and performance indicators. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**

3.1.4.3 Senior management's responsibilities

3.1.4.3.a	Senior management sees that the organisation's standards, processes and procedures carry its security requirements, where they apply. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.4.3.b	Senior management ensures staff accept and follow the policy, standards and procedures as they change. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
3.1.4.3.c	Cyber security responsibilities written into the job descriptions of key and security staff. Organisational, non-technical. NIST SP 800-53: PS-9 Position Descriptions.	**Organisational evidence**

3.1.4.4 The CISO's responsibilities

3.1.4.4.a What the CISO develops and maintains

3.1.4.4.a.1	The CISO develops and maintains the strategy. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

3.1.4.4.a.2	The CISO develops and maintains the policy. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.4.4.a.3	The CISO develops and maintains the security architecture. Organisational, technical and non-technical. NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**
3.1.4.4.a.4	The CISO develops and maintains the risk management process. Organisational, non-technical. NIST SP 800-53: RA-1 Policy and Procedures, PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.4.4.b	The CISO ensures detailed standards and procedures are set, approved and applied. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures.	**Organisational evidence**
3.1.4.4.c	The CISO delivers risk-based solutions across people, process and technology. Organisational, technical and non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.4.4.d	The CISO develops the security staff to work in a business context. Organisational, non-technical. NIST SP 800-53: PM-13 Security and Privacy Workforce.	**Organisational evidence**

3.1.4.4.e Activities the CISO leads

3.1.4.4.e.1	Security monitoring, through a SOC. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.4.4.e.2	Monitoring of compliance with regulation, policy, standards and procedures. Organisational, non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**
3.1.4.4.e.3	Oversight of incident investigations. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
3.1.4.4.e.4	Threat intelligence gathered and analysed from inside and outside. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program.	**Organisational evidence**
3.1.4.4.e.5	Cyber security reviews. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
3.1.4.4.f	The CISO conducts risk assessments of information assets. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

3.1.4.4.g Support the CISO gives other functions

3.1.4.4.g.1	The CISO supports information and system classification. Organisational, non-technical. NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
3.1.4.4.g.2	The CISO sets security requirements for important projects. Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle, SA-4 Acquisition Process.	**Organisational evidence**
3.1.4.4.g.3	The CISO supports other functions with security reviews. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

3.1.4.4.h	The CISO defines and runs the awareness programmes. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

3.1.4.4.i What the CISO measures and reports

3.1.4.4.i.1	Indicators on the strategy. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**
3.1.4.4.i.2	Indicators on compliance with the policy. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance, CA-7 Continuous Monitoring.	**Organisational evidence**
3.1.4.4.i.3	Indicators on the standards and procedures. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**
3.1.4.4.i.4	Indicators on the programmes, such as awareness and data classification. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**

3.1.4.5 Internal audit's responsibilities

3.1.4.5.a	Internal audit performs cyber security audits. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

3.1.4.6 Every member of staff's responsibilities

3.1.4.6.a	All staff follow the policy, standards and procedures. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**

3.1.5 Cyber security in project management

3.1.5.1	Cyber security built into the project methodology, so a project identifies and treats its risks. Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle, PM-9 Risk Management Strategy.	**Organisational evidence**

3.1.5.2 What the project methodology ensures

3.1.5.2.a	Security objectives among a project's objectives. Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle.	**Organisational evidence**
3.1.5.2.b	The security function involved in every phase. Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle.	**Organisational evidence**
3.1.5.2.c	A risk assessment at the start, with requirements met by existing controls or new ones. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SA-4 Acquisition Process.	**Organisational evidence**
3.1.5.2.d	Security risks recorded and tracked in the project risk register. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, RA-3 Risk Assessment.	**Organisational evidence**
3.1.5.2.e	Security responsibilities in the project defined and assigned. Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle.	**Organisational evidence**

3.1.5.2.f	The project's security reviewed independently, from inside or outside the organisation. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, SA-11 Developer Testing and Evaluation.	**Organisational evidence**

3.1.6 Cyber security awareness

3.1.6.1	Awareness programmes, defined, approved and run, to build a security culture. Organisational, non-technical. NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.	**Organisational evidence**

3.1.6.2 Who the awareness programme reaches

3.1.6.2.a	Awareness for staff. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.6.2.b	Awareness for third parties. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, PS-7 External Personnel Security.	**Organisational evidence**
3.1.6.2.c	Awareness for customers. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.6.3	The programme tailored to each audience and delivered through several channels. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.6.4	Awareness activities through the year, periodically. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

3.1.6.5 What the awareness programme covers at least

3.1.6.5.a	The security measures in place, explained. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.6.5.b	Security roles and responsibilities. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.6.5.c	Emerging events and threats, such as spear-phishing. Organisational, non-technical. NIST SP 800-53: AT-2(1) Practical Exercises, AT-2 Literacy Training and Awareness.	**Organisational evidence**

3.1.6.6 How the awareness programme is evaluated

3.1.6.6.a	The effectiveness of awareness activities measured. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, PM-6 Measures of Performance.	**Organisational evidence**
3.1.6.6.b	Recommendations made to improve the programme. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.6.7	Awareness for retail and corporate customers lists measures they can take against their own risks. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

3.1.7 Cyber security training

3.1.7.1 Who receives specialist training

3.1.7.1.a	Specialist training for key roles. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
3.1.7.1.b	Specialist training for the cyber security function. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
3.1.7.1.c	Specialist training for those who develop and maintain information assets. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
3.1.7.1.d	Specialist training for those who perform risk assessments. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
3.1.7.2	Education so that staff can operate information assets securely. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, AT-3 Role-based Training.	**Organisational evidence**

3.2 Cyber security risk management and compliance

3.2.1 Cyber security risk management

3.2.1-1	A cyber security risk management process, defined, approved and applied. Organisational, non-technical. NIST SP 800-53: RA-1 Policy and Procedures, PM-9 Risk Management Strategy.	**Organisational evidence**
3.2.1-2	The process aims to protect information assets' confidentiality, integrity and availability. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.2.1-3	The process aligned with enterprise risk management. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

3.2.1-4 Stages the documented process covers

3.2.1-4.a	The process covers risk identification. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-4.b	The process covers risk analysis. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-4.c	The process covers risk response. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, RA-7 Risk Response.	**Organisational evidence**
3.2.1-4.d	The process covers monitoring and review. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, CA-7 Continuous Monitoring.	**Organisational evidence**

3.2.1-5 Assets the process covers

3.2.1-5.a	The process covers business processes. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-5.b	The process covers business applications. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

3.2.1-5.c	The process covers infrastructure components. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

3.2.1-6 When the process starts

3.2.1-6.a	A risk assessment early in a project. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SA-3 System Development Life Cycle.	**Organisational evidence**
3.2.1-6.b	A risk assessment before a critical change. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, CM-4 Impact Analyses.	**Organisational evidence**
3.2.1-6.c	A risk assessment when outsourcing is considered. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
3.2.1-6.d	A risk assessment before a new product or technology is launched. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-7	Existing assets reassessed periodically, by classification or risk profile. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

3.2.1-8 Who takes part

3.2.1-8.a	Business owners take part in risk management. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-8.b	IT specialists take part. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-8.c	Cyber security specialists take part. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-8.d	Key user representatives take part. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-9	Assessment results reported to the risk owner. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1-10	The risk owner accepts and endorses the results. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-9 Risk Management Strategy.	**Organisational evidence**
3.2.1-11	Risk appetite and tolerance defined and formally approved. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

3.2.1.1 Risk identification

3.2.1.1.1	Risks identified. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1.1.2	Identified risks recorded in a central register. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-9 Risk Management Strategy.	**Organisational evidence**

3.2.1.1.3	Identification looks at the relevant assets, the threats and weaknesses they face, and the main controls already in place. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

3.2.1.2 Risk analysis

3.2.1.2.1	Risks analysed. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
3.2.1.2.2	Analysis covers business impact and likelihood. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

3.2.1.3 Risk response

3.2.1.3.1	Risks treated according to risk appetite and security requirements. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, RA-7 Risk Response.	**Organisational evidence**
3.2.1.3.2	Treatment options documented: accept, avoid, transfer or mitigate. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**

3.2.1.3.3 Accepting a risk

3.2.1.3.3.a	Acceptance considers predefined limits on risk levels. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

3.2.1.3.3.b The business owner's sign-off

3.2.1.3.3.b.1	An accepted risk is within appetite and reported to the committee. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.2.1.3.3.b.2	An accepted risk does not conflict with SAMA's regulations. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing.	**Organisational evidence**
3.2.1.3.4	Avoiding a risk means the owner cancels or postpones the activity that brings it. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**

3.2.1.3.5 Transferring or sharing a risk

3.2.1.3.5.a	The risk shared with an internal or external provider. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
3.2.1.3.5.b	The receiving provider accepts it. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response, SA-9 External System Services.	**Organisational evidence**
3.2.1.3.5.c	The transfer actually takes place. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**

3.2.1.3.6 Mitigating a risk with controls

3.2.1.3.6.a	Suitable controls identified, and their strengths and weaknesses evaluated. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response, PL-2 System Security and Privacy Plans.	**Organisational evidence**

3.2.1.3.6.b Evaluating the controls' strengths and weaknesses

3.2.1.3.6.b.1	The cost of the controls assessed. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
3.2.1.3.6.b.2	The feasibility of the controls assessed. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
3.2.1.3.6.b.3	Compliance requirements for the controls reviewed. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response, PM-28 Risk Framing.	**Organisational evidence**
3.2.1.3.6.c	Controls selected. Organisational, non-technical. NIST SP 800-53: PL-2 System Security and Privacy Plans.	**Organisational evidence**
3.2.1.3.6.d	Residual risk identified, documented and signed off by the owner. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response, PM-9 Risk Management Strategy.	**Organisational evidence**
3.2.1.3.7	Treatment actions documented in a risk treatment plan. Organisational, non-technical. NIST SP 800-53: PM-4 Plan of Action and Milestones Process, RA-7 Risk Response.	**Organisational evidence**

3.2.1.4 Risk monitoring and review

3.2.1.4.1 Monitoring the treatment

3.2.1.4.1.a	Progress tracked against the treatment plan. Organisational, non-technical. NIST SP 800-53: PM-4 Plan of Action and Milestones Process, CA-5 Plan of Action and Milestones.	**Organisational evidence**
3.2.1.4.1.b	The agreed controls confirmed as implemented. Organisational, technical and non-technical. NIST SP 800-53: CA-5 Plan of Action and Milestones, CA-7 Continuous Monitoring.	**Organisational evidence**
3.2.1.4.2	New or changed controls reviewed for design and effectiveness. Organisational, technical and non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

3.2.2 Regulatory compliance

3.2.2.1 The compliance process

3.2.2.1.a	A process for compliance with regulation, run periodically and when new requirements take effect. Organisational, non-technical. NIST SP 800-53: PM-28 Risk Framing, CA-2 Control Assessments.	**Organisational evidence**
3.2.2.1.b	Representatives of key areas involved. Organisational, non-technical. NIST SP 800-53: PM-28 Risk Framing.	**Organisational evidence**
3.2.2.1.c	Policy, standards and procedures updated as needed. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-28 Risk Framing.	**Organisational evidence**

3.2.3 Compliance with national and international industry standards

3.2.3.1 Standards to comply with

3.2.3.1.a	PCI DSS. Organisational, technical and non-technical. NIST SP 800-53: PM-28 Risk Framing.	**Organisational evidence**
3.2.3.1.b	The EMV technical standard. Organisational, technical and non-technical. NIST SP 800-53: PM-28 Risk Framing.	**Organisational evidence**
3.2.3.1.c	SWIFT's Customer Security Controls Framework, which SAMA names in its March 2017 edition. Organisational, technical and non-technical. NIST SP 800-53: PM-28 Risk Framing.	**Organisational evidence**

3.2.4 Cyber security review

3.2.4.1	Critical information assets reviewed periodically. Organisational, technical and non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
3.2.4.2	Customer-facing and internet-facing services reviewed and penetration tested every year. Organisational, technical, outside the cluster. NIST SP 800-53: CA-2 Control Assessments, CA-8 Penetration Testing.	**Organisational evidence**
3.2.4.3	Each review's results, issues and recommended actions recorded. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
3.2.4.4	Review results reported to the business owner. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

3.2.4.5 Follow-up of a review

3.2.4.5.a	Every issue found has been addressed. Organisational, non-technical. NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**
3.2.4.5.b	Critical risks treated effectively. Organisational, non-technical. NIST SP 800-53: CA-5 Plan of Action and Milestones, PM-9 Risk Management Strategy.	**Organisational evidence**
3.2.4.5.c	Agreed actions managed continuously. Organisational, non-technical. NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**

3.2.5 Cyber security audits

3.2.5.1	Audits performed independently, to accepted auditing standards and the framework. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-2(1) Independent Assessors.	**Organisational evidence**
3.2.5.2	Audits performed under the audit manual and plan. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

3.3 Cyber security operations and technology

3.3.1 Human resources

3.3.1.1	Security requirements defined, approved and applied in the HR process. Organisational, non-technical. NIST SP 800-53: PS-1 Policy and Procedures.	**Organisational evidence**
3.3.1.2	The HR process's effectiveness monitored, measured and evaluated periodically. Organisational, non-technical. NIST SP 800-53: PS-1 Policy and Procedures, CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.1.3 What the HR process includes

3.3.1.3.a	Security duties and confidentiality clauses in staff agreements, during and after employment. Organisational, non-technical. NIST SP 800-53: PS-6 Access Agreements.	**Organisational evidence**
3.3.1.3.b	Awareness on joining and throughout employment. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.3.1.3.c	When disciplinary action applies. Organisational, non-technical. NIST SP 800-53: PS-8 Personnel Sanctions.	**Organisational evidence**
3.3.1.3.d	Screening and background checks. Organisational, non-technical. NIST SP 800-53: PS-3 Personnel Screening.	**Organisational evidence**

3.3.1.3.e After employment ends

3.3.1.3.e.1	Access rights revoked when someone leaves. Organisational, technical and non-technical. NIST SP 800-53: PS-4 Personnel Termination, AC-2 Account Management.	**Organisational evidence**
3.3.1.3.e.2	Assigned assets returned, such as badges, tokens, devices and information. Organisational, non-technical. NIST SP 800-53: PS-4 Personnel Termination.	**Organisational evidence**

3.3.2 Physical security

3.3.2.1	A physical security process, defined, approved and applied. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures.	**Organisational evidence**
3.3.2.2	The physical security process's effectiveness monitored, measured and evaluated periodically. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures, CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.2.3 What the physical security process includes

3.3.2.3.a	Physical entry controls, visitors included. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control, PE-8 Visitor Access Records.	**Organisational evidence**
3.3.2.3.b	Monitoring and surveillance, such as CCTV and sensors. Organisational, non-technical. NIST SP 800-53: PE-6 Monitoring Physical Access.	**Organisational evidence**
3.3.2.3.c	Data centres and data rooms protected. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**

3.3.2.3.d Environmental protection. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PE-13 Fire Protection, PE-14 Environmental Controls, PE-15 Water Damage Protection.

3.3.2.3.e Assets protected through their lifecycle, in transport and disposal included, against unauthorised access and leakage. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: MP-5 Media Transport, MP-6 Media Sanitization, PE-16 Delivery and Removal.

3.3.3 Asset management

3.3.3.1 An asset management process, defined, approved and applied. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CM-8 System Component Inventory, PM-5 System Inventory.

3.3.3.2 The asset management process's effectiveness monitored, measured and evaluated periodically. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CM-8 System Component Inventory, CA-7 Continuous Monitoring.

3.3.3.3 What the asset management process includes

3.3.3.3.a A single asset register. **Recorded**

Checked, coverage partial. NIST SP 800-53: CM-8 System Component Inventory, PM-5 System Inventory.

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.

3.3.3.3.b An owner and a custodian for each information asset. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CM-8 System Component Inventory, PM-5 System Inventory.

3.3.3.3.c References to the other processes that depend on asset management. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CM-8 System Component Inventory.

3.3.3.3.d Information assets classified, labelled and handled by their classification. **Pass**

Enforced, coverage partial. NIST SP 800-53: RA-2 Security Categorization, MP-3 Media Marking.

Scope of this evidence The evidence is that each namespace carries a data classification label. Handling information by its classification is the Member Organization's to evidence.

policy.namespace-classification	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries a data classification label.

3.3.3.3.e New information assets discovered. **Recorded**

Checked, coverage partial. NIST SP 800-53: CM-8 System Component Inventory, CM-8(3) Automated Unauthorized Component Detection.

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.

3.3.4 Cyber security architecture

3.3.4.1	A security architecture, defined, approved and applied. Organisational, technical, outside the cluster. NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**
3.3.4.2	Compliance with the architecture monitored. Organisational, technical, outside the cluster. NIST SP 800-53: PL-8 Security and Privacy Architectures, CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.4.3 What the architecture includes

3.3.4.3.a	A strategic outline of security capabilities and controls, from business requirements. Organisational, technical, outside the cluster. NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**
3.3.4.3.b	Approval of the architecture. Organisational, non-technical. NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**
3.3.4.3.c	Qualified security architects. Organisational, non-technical. NIST SP 800-53: PM-13 Security and Privacy Workforce.	**Organisational evidence**
3.3.4.3.d	Design principles for controls and requirements, security by design among them. Organisational, technical, outside the cluster. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, PL-8 Security and Privacy Architectures.	**Organisational evidence**
3.3.4.3.e	The architecture reviewed periodically. Organisational, technical, outside the cluster. NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**

3.3.5 Identity and access management

3.3.5.1	An identity and access management policy, with responsibilities and accountabilities, defined, approved and applied. Organisational, technical and non-technical. NIST SP 800-53: AC-1 Policy and Procedures, IA-1 Policy and Procedures.	**Organisational evidence**
3.3.5.2	Compliance with the policy monitored. Organisational, technical and non-technical. NIST SP 800-53: AC-1 Policy and Procedures, CA-7 Continuous Monitoring.	**Organisational evidence**
3.3.5.3	The policy's controls measured and evaluated periodically. Organisational, technical and non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.5.4 What the identity and access policy includes

3.3.5.4.a Access limited to what the business requires each person to have and to know. **Fail**

Checked, coverage partial. NIST SP 800-53: AC-6 Least Privilege, AC-6(1) Authorize Access to Security Functions.

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

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.

3.3.5.4.b User access management, for joiners, movers and leavers

3.3.5.4.b.1 Every user type covered, staff and third parties. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-2 Account Management.

3.3.5.4.b.2 Changes for staff started by HR. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: AC-2 Account Management, PS-5 Personnel Transfer.

3.3.5.4.b.3 Changes for external staff started by the accountable party. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: AC-2 Account Management, PS-7 External Personnel Security.

3.3.5.4.b.4 Access requests formally approved against business and compliance needs. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: AC-2 Account Management.

3.3.5.4.b.5 Access changes processed promptly. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-2 Account Management.

3.3.5.4.b.6 User access rights and profiles reviewed periodically. **Recorded**

Checked, coverage partial. NIST SP 800-53: AC-2(3) Disable Accounts, AC-6(7) Review of User Privileges.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.

3.3.5.4.b.7 An audit trail of access requests, approvals, changes and revocations. **Pass**

Platform, coverage partial. NIST SP 800-53: AC-2 Account Management, AC-2(4) Automated Audit Actions, AU-2 Event Logging. Evidence counted: platform.audit; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict concerns whether the API server's audit log records requests to the cluster, among them every grant and removal of a role binding. The trail of access requests and approvals, and of access to other systems, is the Member Organization's to evidence.

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.

3.3.5.4.c User access management supported by automation. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-2(1) Automated System Account Management.

3.3.5.4.d Identity and access management centralised. **Incomplete**

Platform, coverage partial. NIST SP 800-53: AC-2 Account Management, IA-2 Identification and Authentication (Organizational Users).

Scope of this evidence The evidence concerns sign-in to the cluster through the organisation's identity provider. Centralising identity for the organisation's other systems is the Member Organization's to evidence.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.
node.kubelet-authn	**Pass**	The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: so on all 1 node(s). Establishes: The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.
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.oidc	**Not evaluated**	The platform could not read the authentication configuration. Establishes: People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.

3.3.5.4.e Sensitive and critical systems and profiles protected by multi-factor authentication. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.

3.3.5.4.f Privileged and remote access

3.3.5.4.f.1 Granting and restricting privileged and remote access

3.3.5.4.f.1.a Multi-factor authentication for all remote access. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts, AC-17 Remote Access.

3.3.5.4.f.1.b Multi-factor authentication for privileged access to critical systems, by risk assessment. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts.

3.3.5.4.f.2 Users with privileged and remote access reviewed periodically. **Recorded**

Checked, coverage partial. NIST SP 800-53: AC-2(3) Disable Accounts, AC-6(7) Review of User Privileges.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.

3.3.5.4.f.3 Individual accountability for privileged and remote access. **Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), AC-2 Account Management.

Scope of this evidence The verdict concerns whether sign-in to the cluster is delegated to the organisation's identity provider, anonymous requests are refused and kubelets authenticate their callers; the role bindings are recorded beside it. Whether shared credentials, such as kubeadm's admin.conf, are still in use, SSH access to the nodes, and other remote access are the Member Organization's to evidence.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.
node.kubelet-authn	**Pass**	The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: so on all 1 node(s). Establishes: The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.
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.oidc	**Not evaluated**	The platform could not read the authentication configuration. Establishes: People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.

3.3.5.4.f.4 Non-personal privileged accounts

3.3.5.4.f.4.a Non-personal privileged accounts limited and monitored. **Pass**

Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation, AC-2(9) Restrictions on Use of Shared and Group Accounts.

Scope of this evidence The evidence is that the cluster's audit log records each request with its identity. The cluster's kubeadm admin.conf is a shared administrative credential that every Kubernetes cluster built with kubeadm has; limiting its use is the Member Organization's to evidence.

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.

3.3.5.4.f.4.b The passwords of non-personal privileged accounts kept confidential. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.

3.3.5.4.f.4.c Those passwords replaced often, and after every session. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.

3.3.6 Application security

3.3.6.1 Application security standards, defined, approved and applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-1 Policy and Procedures, SA-8 Security and Privacy Engineering Principles.

3.3.6.2 Compliance with the standards monitored. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.6.3 Application controls measured and evaluated periodically. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.6.4 Applications developed under the approved secure development lifecycle. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-3 System Development Life Cycle, SA-15 Development Process, Standards, and Tools.

3.3.6.5 What the application security standard includes

3.3.6.5.a Secure coding standards. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-15 Development Process, Standards, and Tools, SA-8 Security and Privacy Engineering Principles.

3.3.6.5.b The controls an application implements, such as its configuration, the events it records and keeps, and its access management. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-4 Acquisition Process, AU-2 Event Logging.

3.3.6.5.c Segregation of duties within the application, with a documented authorisation matrix. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-5 Separation of Duties.

3.3.6.5.d	Data protected by its classification against unauthorised access and leakage, customers' privacy included. Organisational, technical, outside the cluster. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.	**Organisational evidence**
3.3.6.5.e	Vulnerability and patch management of applications. Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SI-2 Flaw Remediation.	**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.
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.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.

3.3.6.5.f	Backup and recovery procedures. Organisational, technical, outside the cluster. NIST SP 800-53: CP-9 System Backup, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
3.3.6.5.g	Periodic security compliance reviews of applications. Organisational, technical, outside the cluster. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

3.3.7 Change management

3.3.7.1	A change management process, defined, approved and applied. Organisational, technical and non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
3.3.7.2	Compliance with the process monitored. Organisational, technical and non-technical. NIST SP 800-53: CM-3 Configuration Change Control, CA-7 Continuous Monitoring.	**Organisational evidence**
3.3.7.3	The process's security controls measured and evaluated periodically. Organisational, technical and non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.7.4 What the change process includes

3.3.7.4.a	Security requirements for changes: impact assessed, changes classified and reviewed. Organisational, technical and non-technical. NIST SP 800-53: CM-3 Configuration Change Control, CM-4 Impact Analyses.	**Organisational evidence**

3.3.7.4.b Security testing of a change, where applicable

3.3.7.4.b.1	Penetration testing. Organisational, technical, outside the cluster. NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**
3.3.7.4.b.2	Code review of internally developed applications. Organisational, technical, outside the cluster. NIST SP 800-53: SA-11(4) Manual Code Reviews.	**Organisational evidence**
3.3.7.4.b.3	Code review of external applications where the source is available. Organisational, technical, outside the cluster. NIST SP 800-53: SA-11(4) Manual Code Reviews.	**Organisational evidence**
3.3.7.4.b.4	A code review report or equivalent assurance where the source is not available. Organisational, technical, outside the cluster. NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
3.3.7.4.c	Changes approved by the business owner. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
3.3.7.4.d	The security function's approval before the change advisory board. Organisational, technical and non-technical. NIST SP 800-53: CM-3 Configuration Change Control, CM-3(4) Security and Privacy Representatives.	**Organisational evidence**
3.3.7.4.e	The change advisory board's approval. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
3.3.7.4.f	A review of the affected security controls after implementation. Organisational, technical, outside the cluster. NIST SP 800-53: CM-4(2) Verification of Controls.	**Organisational evidence**

3.3.7.4.g	Development, test and implementation segregated, in environments and in people.	**Fail**

Checked, coverage partial. NIST SP 800-53: CM-4(1) Separate Test Environments, SC-7 Boundary Protection, AC-4 Information Flow Enforcement, AC-5 Separation of Duties.

Scope of this evidence The evidence is that each namespace carries an environment label and has NetworkPolicies. Separate clusters or infrastructure for each environment, and segregation of the people involved, are the Member Organization's to evidence.

Fails in Namespace payments.

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-environment	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries an environment label, one of the values in namespaces.environments.
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

3.3.7.4.h	A procedure for emergency changes and fixes.	**Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CM-3 Configuration Change Control.

3.3.7.4.i	Fall-back and roll-back procedures.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control.

3.3.8 Infrastructure security

3.3.8.1	Infrastructure security standards, defined, approved and applied.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-1 Policy and Procedures, SC-1 Policy and Procedures.

3.3.8.2	Compliance with the standards monitored.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.8.3	Infrastructure controls measured and evaluated periodically. Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**
3.3.8.4	The standards cover the infrastructure in the main data centres, the disaster recovery sites and the offices. Organisational, technical, outside the cluster. NIST SP 800-53: CM-1 Policy and Procedures.	**Organisational evidence**
3.3.8.5	The standards cover every kind of infrastructure, from servers and virtual machines to firewalls, network devices and gateways. Organisational, technical, outside the cluster. NIST SP 800-53: CM-1 Policy and Procedures, CM-6 Configuration Settings.	**Organisational evidence**

3.3.8.6 What the infrastructure security standard includes

3.3.8.6.a The controls each component implements, such as configuration settings, the events recorded and kept, data leakage prevention, access management and remote maintenance. **Fail**

Checked, coverage partial. NIST SP 800-53: CM-6 Configuration Settings, CM-2 Baseline Configuration, AU-2 Event Logging.

Scope of this evidence The evidence concerns the configuration of the cluster's nodes, control plane and workloads against a hardening baseline, and the cluster's audit log. Other infrastructure, data leakage prevention and remote maintenance are the Member Organization's to evidence.

Fails in CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app.

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.
node.etcd-data	**Pass**	etcd's data directory is owned by root and closed to other users: so on all 1 node(s). Establishes: etcd's data directory on each control-plane node is owned by root and closed to other users (700).
node.file-permissions	**Pass**	Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s). Establishes: The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.
node.kubelet-hardening	**Pass**	The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s). Establishes: The kubelet keeps its read-only port closed and rotates its client certificates.
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.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
platform.mesh-cni	**Not evaluated**	The service mesh CNI plugin: the platform could not observe it. Establishes: Meshed Pods run without elevated privileges, through the mesh's CNI plugin.

platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
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.
policy.resource-limits	**Fail**	3 object(s) fail the policy. Establishes: Every container declares memory and CPU limits.
trivy.limits	**Fail**	3 object(s) fail. Establishes: Containers without CPU or memory limits.
trivy.run-as-root	**Fail**	3 object(s) fail. Establishes: Containers that run as the root user.
trivy.seccomp	**Fail**	3 object(s) fail. Establishes: Containers without the runtime's default seccomp profile.

3.3.8.6.b Segregation of duties within each component, with a documented authorisation matrix. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-5 Separation of Duties.

3.3.8.6.c Data protected by its classification against unauthorised access and leakage, customers' privacy included. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

3.3.8.6.d Only approved software and secure protocols. **Fail**

Enforced, coverage partial. NIST SP 800-53: SR-3 Supply Chain Controls and Processes, CM-14 Signed Components, SC-8 Transmission Confidentiality and Integrity, CM-7(5) Authorized Software — Allow-by-exception.

Scope of this evidence The evidence concerns the images the cluster runs outside the exempt namespaces: that they come from the registries the organisation allows, by a fixed tag or digest, and carry a signature from a configured key (an image no key covers fails); by default a failing Pod is admitted with a warning and recorded. It also concerns TLS into the cluster and to its control plane. Approved software on other infrastructure is the Member Organization's to evidence.

Fails in CronJob payments/nightly, CronJob payments/weekly, Deployment payments/ledger, Deployment payments/legacy-batch, Deployment payments/unsigned-app, Job payments/migrate-once, Job payments/nightly-now, Pod payments/nightly-now-k7cbf, Pod payments/one-off, Pod payments/unsigned-app-b5567644f-vpkpp and 1 more.

platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platf could not observe it. Establishes: Profiling is off and only AEAD TLS cipher offered by the control plane and the kubelets.
platform.image-registry	**Recorded**	The registry the control plane pulls its images from: 1x.ax/bke/kubernetes. Establishes: The platform's own images come from th registry recorded, signed.
policy.images-signed	**Fail**	11 object(s) run images that are not signed or that no key covers. Establishes: Every image outside the exempt namesp carries a signature from a configured key: Kyverno ve images that match a key's patterns, and the collector image that no key covers. A failing Pod is admitted w warning and recorded, or refused, as policies.defaultA sets (Warn by default).
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt names the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.
policy.no-latest-tag	**Pass**	Every object the policy judged passes it. Establishes: Images are referenced by a fixed tag or d never by a moving tag.
policy.registries-allowed	**Fail**	7 object(s) fail the policy. Establishes: Containers run images only from the regi customer allows.
trivy.image-sources	**Pass**	Every object outside the exempt namespaces passes Establishes: Images from public registries (AVD-KSV-0 referenced by a moving tag (AVD-KSV-0013). AVD-KS not used: its list trusts only three cloud providers' reg and policy.registries-allowed judges the registries aga own list instead. See https://tersane.bahriya.cloud/docs/charts/compliance/ the-convoy-does-not-use-and-why.

3.3.8.6.e Networks segmented. **Fail**

Enforced, coverage partial. NIST SP 800-53: AC-4 Information Flow Enforcement, SC-7 Boundary Protection.

Scope of this evidence The evidence is that each application namespace has a NetworkPolicy. Traffic is restricted by default only when the Convoy's default-deny policy is turned on (generate.defaultDenyNetworkPolicy.enabled), which is off by default. Segmentation of other networks is the Member Organization's to evidence.

Fails in Namespace payments.

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

3.3.8.6.f Protection against malicious code, with application allow-listing and protection against advanced persistent threats. **Fail**

Enforced, coverage partial. NIST SP 800-53: SI-3 Malicious Code Protection, CM-14 Signed Components, SR-3 Supply Chain Controls and Processes, CM-7(5) Authorized Software — Allow-by-exception.

Scope of this evidence Allow-listing only: the cluster runs images from the registries the organisation allows, by a fixed tag or digest, each carrying a signature from a configured key (an image no key covers fails). By default a failing Pod is admitted with a warning and recorded; it is refused only where the policy's action is Deny. Malware and advanced threat protection are the Member Organization's to evidence.

Fails in CronJob payments/nightly, CronJob payments/weekly, Deployment payments/ledger, Deployment payments/legacy-batch, Deployment payments/unsigned-app, Job payments/migrate-once, Job payments/nightly-now, Pod payments/nightly-now-k7cbf, Pod payments/one-off, Pod payments/unsigned-app-b5567644f-vpkpp and 1 more.

platform.image-registry	**Recorded**	The registry the control plane pulls its images from: 1x.ax/bke/kubernetes. Establishes: The platform's own images come from the registry recorded, signed.
policy.images-signed	**Fail**	11 object(s) run images that are not signed or that no signing key covers. Establishes: Every image outside the exempt namespaces carries a signature from a configured key: Kyverno verifies the images that match a key's patterns, and the collector fails any image that no key covers. A failing Pod is admitted with a warning and recorded, or refused, as policies.defaultAction sets (Warn by default).
policy.no-latest-tag	**Pass**	Every object the policy judged passes it. Establishes: Images are referenced by a fixed tag or digest, never by a moving tag.
policy.registries-allowed	**Fail**	7 object(s) fail the policy. Establishes: Containers run images only from the registries the customer allows.
trivy.image-sources	**Pass**	Every object outside the exempt namespaces passes. Establishes: Images from public registries (AVD-KSV-0034), or referenced by a moving tag (AVD-KSV-0013). AVD-KSV-0125 is not used: its list trusts only three cloud providers' registries, and policy.registries-allowed judges the registries against your own list instead. See https://tersane.bahriya.cloud/docs/charts/compliance/#checks-the-convoy-does-not-use-and-why.

3.3.8.6.g Vulnerability and patch management of infrastructure. **Incomplete**

Checked, coverage partial. NIST SP 800-53: CM-2 Baseline Configuration, SA-22 Unsupported System Components, SI-2 Flaw Remediation.

Scope of this evidence The verdict concerns whether the cluster's Kubernetes and Bahriya Kubernetes Engine releases are in support, whether its workloads' images run a supported operating system, and whether those images have open critical or high vulnerabilities; the versions, the inventory and the age of open vulnerabilities are recorded beside it. Patching within the Member Organization's deadlines, the nodes' operating systems and other infrastructure are the Member Organization's to evidence.

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.
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.
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.

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.

3.3.8.6.h Protection against denial of service, where applicable

3.3.8.6.h.1 A scrubbing service. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection.

3.3.8.6.h.2 The agreed bandwidth specified. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection.

3.3.8.6.h.3 Monitoring around the clock by the SOC, the service provider and the scrubbing provider. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection, SI-4 System Monitoring.

3.3.8.6.h.4 Scrubbing tested at least twice a year. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection.

3.3.8.6.h.5 Protection for the main data centres and the disaster recovery sites. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection.

3.3.8.6.i Backup and recovery procedures. **Fail**

Checked, coverage partial. NIST SP 800-53: CP-9 System Backup, CP-10 System Recovery and Reconstitution.

Scope of this evidence The verdict concerns whether Longhorn has an available backup target and a recurring backup job; each volume's last backup is recorded beside it. Recovery procedures, and the backups of other infrastructure, are the Member Organization's to evidence.

Fails in Cluster backups.

cluster.backups	**Fail**	Nothing backs the cluster up: neither Longhorn nor Velero is installed. Establishes: The cluster is backed up: Longhorn has an available backup target and a recurring backup job, or Velero has an available backup storage location and an active schedule. The last backup of each volume and schedule is recorded beside the verdict.

3.3.8.6.j Periodic security compliance reviews of infrastructure. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-2 Control Assessments.

3.3.9 Cryptography

3.3.9.1 A cryptographic standard, defined, approved and applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection.

3.3.9.2 Compliance with the standard monitored. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.9.3 Cryptographic controls measured and evaluated periodically. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.9.4 What the cryptographic standard includes

3.3.9.4.a The approved cryptographic solutions and their technical and legal restrictions. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection.

3.3.9.4.b When the approved solutions are to be used. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection, SC-8 Transmission Confidentiality and Integrity.

3.3.9.4.c Key management through the lifecycle, with archiving and recovery. **Not evaluated**

Platform, coverage partial. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

Scope of this evidence The evidence records where the cluster's encryption key for Secrets is held. Key lifecycle, archiving and recovery, and other keys, are the Member Organization's to evidence.

platform.key-provider	**Not evaluated**	The platform could not observe the encryption provider. Establishes: Where the encryption key is held (a local key, or a key management service through KMS v2).

3.3.10 Bring your own device

3.3.10.1 A standard for personal devices, defined, approved and applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems.

Scope of this evidence Applies only where the Member Organization allows personal devices to be used for business.

3.3.10.2 Compliance with the standard monitored. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

Scope of this evidence Applies only where the Member Organization allows personal devices to be used for business.

3.3.10.3 Personal device controls measured and evaluated periodically. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

Scope of this evidence Applies only where the Member Organization allows personal devices to be used for business.

3.3.10.4 What the personal device standard includes

3.3.10.4.a The user's responsibilities, with awareness training. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AC-20 Use of External Systems, AT-2 Literacy Training and Awareness.

Scope of this evidence Applies only where the Member Organization allows personal devices to be used for business.

3.3.10.4.b The restrictions on, and consequences for, staff whose devices carry the organisation's controls, as when a device is modified, lost or stolen, or employment ends. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: AC-20 Use of External Systems, PL-4 Rules of Behavior.

Scope of this evidence Applies only where the Member Organization allows personal devices to be used for business.

3.3.10.4.c	Business information kept apart from personal information, as in a container. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices. **Scope of this evidence** Applies only where the Member Organization allows personal devices to be used for business.	**Organisational evidence**
3.3.10.4.d	Corporate and approved public mobile applications regulated. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices, CM-10 Software Usage Restrictions. **Scope of this evidence** Applies only where the Member Organization allows personal devices to be used for business.	**Organisational evidence**
3.3.10.4.e	Mobile device management, with access control and encryption on the device. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices, AC-19(5) Full Device or Container-based Encryption. **Scope of this evidence** Applies only where the Member Organization allows personal devices to be used for business.	**Organisational evidence**

3.3.11 Secure disposal of information assets

3.3.11.1	A secure disposal standard and procedure, defined, approved and applied. Organisational, technical and non-technical. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
3.3.11.2	Compliance with them monitored. Organisational, technical and non-technical. NIST SP 800-53: MP-6 Media Sanitization, CA-7 Continuous Monitoring.	**Organisational evidence**
3.3.11.3	Disposal controls measured and evaluated periodically. Organisational, technical and non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**
3.3.11.4	Assets disposed of under the law, privacy law included, once no longer needed. Organisational, technical and non-technical. NIST SP 800-53: MP-6 Media Sanitization, SI-12 Information Management and Retention.	**Organisational evidence**
3.3.11.5	Sensitive information destroyed so that it cannot be recovered. Organisational, technical, outside the cluster. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
3.3.11.6	Disposal, transport and storage providers follow the standard, and their effectiveness is evaluated periodically. Organisational, non-technical. NIST SP 800-53: MP-6 Media Sanitization, SA-9 External System Services.	**Organisational evidence**
3.3.12	A payment systems security standard, defined, applied and monitored, following the SARIE information security policy and the MADA rules and standards SAMA names. Organisational, technical, outside the cluster. NIST SP 800-53: PM-28 Risk Framing. **Scope of this evidence** SAMA refers here to the SARIE and MADA standards, which the Convoy does not assess.	**Organisational evidence**

3.3.13 Electronic banking services

3.3.13.1 Security standards for electronic banking, defined, approved and applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: PL-1 Policy and Procedures, SA-8 Security and Privacy Engineering Principles.

3.3.13.2 Compliance with them monitored. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.13.3 Their effectiveness measured and evaluated periodically. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.

3.3.13.4 What the electronic banking standard covers

3.3.13.4.a Brand protection for online services, social media included. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: PM-16 Threat Awareness Program.

3.3.13.4.b Online, mobile and phone banking

3.3.13.4.b.1 In online and mobile banking, applications and websites only from official stores and sites. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program.

3.3.13.4.b.2 In online and mobile banking, malicious applications and websites detected and taken down. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program.

3.3.13.4.b.3 Sandboxing in online and mobile banking. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-39 Process Isolation.

3.3.13.4.b.4 Non-caching techniques in online and mobile banking. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-28 Protection of Information at Rest.

3.3.13.4.b.5 In online and mobile banking, communication protected against man-in-the-middle attacks. **Incomplete**

Enforced, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-23 Session Authenticity.

Scope of this evidence The evidence concerns TLS on traffic into the cluster. How the banking applications protect their own sessions is the Member Organization's to evidence.

platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.

3.3.13.4.b.6 Multi-factor authentication for customers

3.3.13.4.b.6.a Multi-factor authentication when a customer registers for electronic banking. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).

3.3.13.4.b.6.b Multi-factor authentication for every electronic banking service. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).

3.3.13.4.b.6.c Hard and soft tokens protected by a password. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.

3.3.13.4.b.6.d Customer access revoked after three incorrect passwords or PINs in a row. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-7 Unsuccessful Logon Attempts.

3.3.13.4.b.6.e A customer's mobile number changed only at a branch or an ATM. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: IA-5 Authenticator Management.

3.3.13.4.b.6.f Multi-factor authentication requested and activated through different channels. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.

3.3.13.4.b.6.g Processes that need multi-factor authentication

3.3.13.4.b.6.g.1 Multi-factor authentication at sign-on. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).

3.3.13.4.b.6.g.2 Multi-factor authentication to add or change beneficiaries. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).

3.3.13.4.b.6.g.3 Multi-factor authentication to add utility and government payments. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).

3.3.13.4.b.6.g.4 Multi-factor authentication for transactions above set limits. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).

3.3.13.4.b.6.g.5 Multi-factor authentication for a password reset. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users), IA-5 Authenticator Management.

3.3.13.4.b.7 In online and mobile banking, beneficiaries added and then activated through separate channels. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.

3.3.13.4.b.8 Electronic banking services highly available. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, SC-6 Resource Availability.

3.3.13.4.b.9	Planned downtime communicated to SAMA and customers in time. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
3.3.13.4.b.10	Customer agreements setting each party's roles, responsibilities and liabilities. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
3.3.13.4.b.11	SAMA's approval before a new electronic banking service is launched. Organisational, non-technical. NIST SP 800-53: PM-28 Risk Framing.	**Organisational evidence**

3.3.13.4.c ATMs and points of sale

3.3.13.4.c.1	Exploitation of ATM and point-of-sale weaknesses prevented and detected, such as through cables, ports or reboots. Organisational, technical, outside the cluster. NIST SP 800-53: PE-3 Physical Access Control, SI-4 System Monitoring.	**Organisational evidence**
3.3.13.4.c.2	Security measures on ATMs and points of sale, such as hardening, malware protection, masking, geo-blocking, anti-skimming, protected PIN pads, privacy screens and CCTV, and cards revoked after three invalid PINs. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings, SI-3 Malicious Code Protection, AC-7 Unsuccessful Logon Attempts.	**Organisational evidence**
3.3.13.4.c.3	ATMs stopped remotely when malicious activity is seen. Organisational, technical, outside the cluster. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**

3.3.13.4.d SMS notifications

3.3.13.4.d.1	No sensitive data in SMS messages, credit card balances excepted. Organisational, technical, outside the cluster. NIST SP 800-53: SI-12(1) Limit Personally Identifiable Information Elements.	**Organisational evidence**
3.3.13.4.d.2	An alert to both the old and the new number when a customer's mobile number changes. Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**
3.3.13.4.d.3	A notification when a new authentication mechanism is requested. Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**
3.3.13.4.d.4	A notification for every retail and personal financial transaction. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4(12) Automated Organization-generated Alerts.	**Organisational evidence**
3.3.13.4.d.5	A notification when beneficiaries are added, changed or activated. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4(12) Automated Organization-generated Alerts.	**Organisational evidence**

3.3.14 Cyber security event management

3.3.14.1	A security event management process, defined, approved and applied. Organisational, technical, outside the cluster. NIST SP 800-53: IR-1 Policy and Procedures, SI-4 System Monitoring.	**Organisational evidence**
3.3.14.2	The process's controls measured and evaluated periodically. Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.14.3 A security event monitoring standard, defined, approved and applied

3.3.14.3.a	The events every information asset must have monitored, set by its classification or risk profile. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation. **Scope of this evidence** The evidence concerns the cluster's audit policy, which records each request to the API server. The events to monitor on other assets are the Member Organization's to evidence.	**Pass**

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.

3.3.14.4 What the event management process requires

3.3.14.4.a	A team dedicated to security monitoring, a SOC. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-7 Incident Response Assistance.	**Organisational evidence**
3.3.14.4.b	Skilled, continually trained staff. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
3.3.14.4.c	A restricted area for the SOC. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
3.3.14.4.d	Resources for monitoring around the clock. Organisational, technical and non-technical. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
3.3.14.4.e	Malicious code detected and handled. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
3.3.14.4.f	Suspicious events and anomalies detected and handled. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.	**Organisational evidence**
3.3.14.4.g	Network packet analysis. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

3.3.14.4.h Logs adequately protected. **Pass**

Checked, coverage partial. NIST SP 800-53: AU-9 Protection of Audit Information.

Scope of this evidence The evidence is that only root can read or change the Kubernetes API server's audit log directory and files on each control-plane node. The logs' protection against the cluster's administrators and of copies forwarded elsewhere, and the protection of every other log, are the Member Organization's to evidence.

node.audit-log-permissions	**Pass**	The API server's audit log directory is owned by root and no more open than 700, and each file in it no more open than 600: so on all 1 node(s). Establishes: On each control-plane node, the API server's audit log directory is owned by root and no more open than 700, and each file directly in it no more open than 600, so that no user but root can change or read the audit log. Judged where the API server writes its audit log to a directory on the node, held in a host-path volume; on a Bahriya Kubernetes Engine cluster, from release 2.5.0. Where the directory cannot be examined, the check is not evaluated and states why. The node collector runs as an unprivileged user and examines modes alone: where the directory admits no other user, it cannot list the files, and that directory is the evidence for them, since on the node's local filesystem no user but root can then reach them, whatever their modes or any POSIX ACL.

3.3.14.4.i Periodic monitoring of compliance with the application and infrastructure standards. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings, CA-7 Continuous Monitoring.

Scope of this evidence The Convoy runs against the cluster's configuration every day, and its reports record that monitoring for the cluster. Monitoring compliance with the standards is the Member Organization's to evidence.

3.3.14.4.j Automated, central analysis and correlation of security logs, a SIEM. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, AU-6(3) Correlate Audit Record Repositories, SI-4 System Monitoring.

3.3.14.4.k Security incidents reported. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: IR-6 Incident Reporting.

3.3.14.4.l The SOC's effectiveness tested independently and periodically, as by red teaming. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-8 Penetration Testing, CA-8(2) Red Team Exercises.

3.3.15 Cyber security incident management

3.3.15.1 An incident management process, defined, approved, applied and aligned with enterprise incident management. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: IR-1 Policy and Procedures, IR-8 Incident Response Plan.

3.3.15.2 The process's controls measured and evaluated periodically. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CA-7 Continuous Monitoring, IR-3 Incident Response Testing.

3.3.15.3	The events, mandatory and suspicious, that require a response.	**Organisational evidence**
	Organisational, technical and non-technical. NIST SP 800-53: IR-8 Incident Response Plan.	

3.3.15.4 What the incident management process requires

3.3.15.4.a	A team dedicated to incident management.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: IR-7 Incident Response Assistance, IR-8 Incident Response Plan.	
3.3.15.4.b	Skilled, continually trained staff.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: IR-2 Incident Response Training.	
3.3.15.4.c	Enough certified forensic capacity for major incidents, in-house or contracted.	**Organisational evidence**
	Organisational, technical and non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-7 Incident Response Assistance.	
3.3.15.4.d	A restricted area for the incident response team.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control.	
3.3.15.4.e	Incidents classified.	**Organisational evidence**
	Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-8 Incident Response Plan.	
3.3.15.4.f	Incidents handled promptly, recorded and tracked.	**Organisational evidence**
	Organisational, technical and non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-5 Incident Monitoring.	
3.3.15.4.g	Relevant evidence and logs kept protected.	**Pass**
	Checked, coverage partial. NIST SP 800-53: AU-9 Protection of Audit Information, IR-4 Incident Handling.	
	Scope of this evidence The evidence is that only root can read or change the Kubernetes API server's audit log directory and files on each control-plane node. Its protection against the cluster's administrators and of copies forwarded elsewhere, and the protection of other evidence and logs kept for incidents, are the Member Organization's to evidence.	
	node.audit-log-permissions **Pass** The API server's audit log directory is owned by root and no more open than 700, and each file in it no more open than 600: so on all 1 node(s). Establishes: On each control-plane node, the API server's audit log directory is owned by root and no more open than 700, and each file directly in it no more open than 600, so that no user but root can change or read the audit log. Judged where the API server writes its audit log to a directory on the node, held in a host-path volume; on a Bahriya Kubernetes Engine cluster, from release 2.5.0. Where the directory cannot be examined, the check is not evaluated and states why. The node collector runs as an unprivileged user and examines modes alone: where the directory admits no other user, it cannot list the files, and that directory is the evidence for them, since on the node's local filesystem no user but root can then reach them, whatever their modes or any POSIX ACL.	
3.3.15.4.h	Post-incident work, such as forensics and root-cause analysis.	**Organisational evidence**
	Organisational, technical, outside the cluster. NIST SP 800-53: IR-4 Incident Handling.	

3.3.15.4.i	Suggested improvements reported to the CISO and the committee. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.4.j	An incident repository. Organisational, technical and non-technical. NIST SP 800-53: IR-5 Incident Monitoring.	**Organisational evidence**
3.3.15.5	SAMA's IT risk supervision told at once of a medium or high incident. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.6	SAMA's no-objection before speaking to the media about an incident. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**

3.3.15.7 The incident report to SAMA after recovery

3.3.15.7.a	The incident's title. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.b	Its classification, medium or high. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.c	When it occurred. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.d	When it was detected. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.e	The information assets involved. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.f	Its technical details. Organisational, technical and non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.g	Its root cause. Organisational, technical and non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.h	Corrective actions taken and planned. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.i	Its impact, such as data lost, services disrupted and customers affected. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.j	Its estimated total cost. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
3.3.15.7.k	The estimated cost of corrective action. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**

3.3.16 Threat management

3.3.16.1	A threat intelligence process, defined, approved and applied. Organisational, technical and non-technical. NIST SP 800-53: PM-16 Threat Awareness Program.	**Organisational evidence**
3.3.16.2	Its effectiveness measured and evaluated periodically. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program, CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.16.3 What the threat intelligence process includes

3.3.16.3.a	Internal sources, such as logs, IDS and IPS, security tools, the SIEM and support functions. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program, SI-4 System Monitoring.	**Organisational evidence**
3.3.16.3.b	Reliable external sources, such as SAMA, government, forums and vendors. Organisational, technical and non-technical. NIST SP 800-53: PM-16 Threat Awareness Program, SI-5 Security Alerts, Advisories, and Directives.	**Organisational evidence**
3.3.16.3.c	A method for analysing threat information periodically. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program.	**Organisational evidence**
3.3.16.3.d	Details of each threat, such as method, actors, motive and type. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program.	**Organisational evidence**
3.3.16.3.e	The intelligence's relevance and the follow-up it calls for, as for the SOC or risk management. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program.	**Organisational evidence**
3.3.16.3.f	Relevant intelligence shared with stakeholders such as SAMA and the banking sector. Organisational, non-technical. NIST SP 800-53: PM-16 Threat Awareness Program, PM-15 Security and Privacy Groups and Associations.	**Organisational evidence**

3.3.17 Vulnerability management

3.3.17.1	A vulnerability management process, defined, approved and applied. Organisational, technical, outside the cluster. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SI-2 Flaw Remediation.	**Organisational evidence**
3.3.17.2	Its effectiveness measured and evaluated periodically. Organisational, technical, outside the cluster. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**

3.3.17.3 What the vulnerability management process includes

3.3.17.3.a Every information asset covered. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

Scope of this evidence The verdict is that every workload outside the exempt namespaces is scanned. The cluster's nodes and platform, and other information assets, are the Member Organization's to evidence.

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.

3.3.17.3.b Scans as often as risk requires. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, RA-5(2) Update Vulnerabilities to Be Scanned.

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.

3.3.17.3.c Vulnerabilities classified. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

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.

3.3.17.3.d Deadlines to fix each class of vulnerability. **Recorded**

Checked, coverage partial. NIST SP 800-53: SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions.

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.

3.3.17.3.e Classified assets prioritised. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, RA-2 Security Categorization.

3.3.17.3.f Patch management and its method of deployment. **Pass**

Checked, coverage partial. NIST SP 800-53: SI-2 Flaw Remediation.

Scope of this evidence The verdict concerns the images of the workloads outside the exempt namespaces. The versions of the Bahriya Kubernetes Engine and Kubernetes are recorded beside it. Patching the nodes and other systems, and the method of deployment, are the Member Organization's to evidence.

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.
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.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.

3.4 Third party cyber security

3.4.1 Contract and vendor management

3.4.1.1	Security requirements defined, approved, applied and communicated in contract and vendor management. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SR-1 Policy and Procedures.	**Organisational evidence**
3.4.1.2	Compliance with the process monitored. Organisational, non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**
3.4.1.3	The process's controls measured and evaluated periodically. Organisational, non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**

3.4.1.4 What contract and vendor management covers

3.4.1.4.a	When the security function must take part, as in due diligence. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
3.4.1.4.b	Baseline security requirements that always apply. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
3.4.1.4.c	The right to review and audit the supplier periodically. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**

3.4.1.5 Contract management

3.4.1.5.a	A risk assessment in procurement. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SR-5 Acquisition Strategies, Tools, and Methods.	**Organisational evidence**
3.4.1.5.b	Security requirements in the tender. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
3.4.1.5.c	Vendors' replies evaluated against those requirements. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
3.4.1.5.d	The agreed requirements tested, by risk. Organisational, technical and non-technical. NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
3.4.1.5.e	How incidents are communicated and escalated. Organisational, non-technical. NIST SP 800-53: SR-8 Notification Agreements, IR-6 Incident Reporting.	**Organisational evidence**
3.4.1.5.f	Security requirements for ending or renewing a contract, escrow included where applicable. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**
3.4.1.5.g	A mutual confidentiality agreement. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SA-4 Acquisition Process.	**Organisational evidence**

3.4.1.6 Vendor management

3.4.1.6.a	Contracted security requirements reported, reviewed and evaluated periodically, as in SLAs. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SA-9(2) Identification of Functions, Ports, Protocols, and Services.	**Organisational evidence**

3.4.2 Outsourcing

3.4.2.1	Security requirements in the outsourcing policy and process, defined, approved, applied and communicated. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
3.4.2.2	Those requirements measured and evaluated periodically. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-7 Continuous Monitoring.	**Organisational evidence**

3.4.2.3 What the outsourcing process includes

3.4.2.3.a	SAMA's approval before material outsourcing. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PM-28 Risk Framing.	**Organisational evidence**
3.4.2.3.b	The security function involved. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
3.4.2.3.c	Compliance with SAMA's outsourcing circular. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PM-28 Risk Framing.	**Organisational evidence**

3.4.3 Cloud computing

3.4.3.1	Security controls in the policy for hybrid and public cloud, defined, approved, applied and communicated. Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services. **Scope of this evidence** Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.	**Organisational evidence**
3.4.3.2	Compliance with the cloud policy monitored. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-7 Continuous Monitoring. **Scope of this evidence** Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.	**Organisational evidence**
3.4.3.3	The cloud policy's controls measured and evaluated periodically. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-7 Continuous Monitoring. **Scope of this evidence** Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.	**Organisational evidence**

3.4.3.4 What the cloud policy requires

3.4.3.4.a Adopting a cloud service

3.4.3.4.a.1 The provider and its services assessed for risk and examined before adoption. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.a.2 SAMA's approval before a cloud service is used or contracted. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PM-28 Risk Framing.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.a.3 A contract with security requirements before use. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.b Where data is held

3.4.3.4.b.1 Cloud services in Saudi Arabia, or SAMA's explicit approval for any outside it. **Organisational evidence**

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

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.c Limits on the use of data

3.4.3.4.c.1 The provider does not use the organisation's data for other purposes. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PT-3 Personally Identifiable Information Processing Purposes.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.d Security at the provider

3.4.3.4.d.1 The provider applies and monitors the controls the risk assessment set for the data. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.e Segregation of data

3.4.3.4.e.1 The organisation's data logically segregated, and always distinguishable, from the provider's other data. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-9 External System Services, SC-4 Information in Shared System Resources.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.f Business continuity at the provider

3.4.3.4.f.1 Continuity requirements met as the organisation's continuity policy requires. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CP-2 Contingency Plan, SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.g Audit, review and monitoring of the provider

3.4.3.4.g.1 The right to a security review at the provider. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.g.2 The right to a security audit at the provider. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.g.3 The right to a security examination at the provider. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.h Leaving the provider

3.4.3.4.h.1 Rights to terminate. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.h.2 The provider returns the data on termination. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

3.4.3.4.h.3 The provider deletes the data irreversibly on termination. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services, MP-6 Media Sanitization.

Scope of this evidence Hybrid and public cloud only: SAMA excludes private cloud from 3.4.3, so it does not apply to a cluster on the Member Organization's own premises. It applies where the cluster or its data are on hybrid or public cloud services.

Checks

cluster.access-review Recorded

Every subject bound to a role, with what it may do, for the periodic access review.

109 role bindings to subjects; 2 to cluster-admin across the cluster.

- cluster-admin: Group kubeadm:cluster-admins (kubeadm:cluster-admins)
- cluster-admin: Group system:masters (cluster-admin)

Scope	Subject	Role
cluster	Group kubeadm:cluster-admins	ClusterRole cluster-admin
cluster	Group system:authenticated	ClusterRole calico-tiered-policy-passthrough
cluster	Group system:authenticated	ClusterRole system:basic-user
cluster	Group system:authenticated	ClusterRole system:discovery
cluster	Group system:authenticated	ClusterRole system:public-info-viewer
cluster	Group system:bootstrappers:kubeadm:default-node-token	ClusterRole kubeadm:get-nodes
cluster	Group system:bootstrappers:kubeadm:default-node-token	ClusterRole system:certificates.k8s.io:certificatesigningrequests:nodec
cluster	Group system:bootstrappers:kubeadm:default-node-token	ClusterRole system:node-bootstrapper
cluster	Group system:masters	ClusterRole cluster-admin
cluster	Group system:monitoring	ClusterRole system:monitoring
cluster	Group system:nodes	ClusterRole system:certificates.k8s.io:certificatesigningrequests:selfno
cluster	Group system:serviceaccounts	ClusterRole system:service-account-issuer-discovery
cluster	Group system:unauthenticated	ClusterRole system:public-info-viewer
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole calico-crds
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole calico-extension-apiserver-auth-access
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole calico-webhook-reader
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole system:auth-delegator

cluster	ServiceAccount calico-system/calico-cni-plugin	ClusterRole calico-cni-plugin
cluster	ServiceAccount calico-system/calico-kube-controllers	ClusterRole calico-kube-controllers
cluster	ServiceAccount calico-system/calico-node	ClusterRole calico-node
cluster	ServiceAccount calico-system/calico-typha	ClusterRole calico-typha
cluster	ServiceAccount compliance/compliance-collector	ClusterRole compliance-collector
cluster	ServiceAccount kube-system/attachdetach-controller	ClusterRole system:controller:attachdetach-controller
cluster	ServiceAccount kube-system/certificate-controller	ClusterRole system:controller:certificate-controller
cluster	ServiceAccount kube-system/clusterrole-aggregation-controller	ClusterRole system:controller:clusterrole-aggregation-cont
cluster	ServiceAccount kube-system/coredns	ClusterRole system:coredns
cluster	ServiceAccount kube-system/cronjob-controller	ClusterRole system:controller:cronjob-controller
cluster	ServiceAccount kube-system/daemon-set-controller	ClusterRole system:controller:daemon-set-controller
cluster	ServiceAccount kube-system/deployment-controller	ClusterRole system:controller:deployment-controller
cluster	ServiceAccount kube-system/device-taint-eviction-controller	ClusterRole system:controller:device-taint-eviction-controll
cluster	ServiceAccount kube-system/disruption-controller	ClusterRole system:controller:disruption-controller
cluster	ServiceAccount kube-system/endpoint-controller	ClusterRole system:controller:endpoint-controller
cluster	ServiceAccount kube-system/endpointslice-controller	ClusterRole system:controller:endpointslice-controller
cluster	ServiceAccount kube-system/endpointslicemirroring-controller	ClusterRole system:controller:endpointslicemirroring-contr
cluster	ServiceAccount kube-system/ephemeral-volume-controller	ClusterRole system:controller:ephemeral-volume-controller
cluster	ServiceAccount kube-system/expand-controller	ClusterRole system:controller:expand-controller
cluster	ServiceAccount kube-system/generic-garbage-collector	ClusterRole system:controller:generic-garbage-collector
cluster	ServiceAccount kube-system/horizontal-pod-autoscaler	ClusterRole system:controller:horizontal-pod-autoscaler
cluster	ServiceAccount kube-system/job-controller	ClusterRole system:controller:job-controller
cluster	ServiceAccount kube-system/kube-dns	ClusterRole system:kube-dns

cluster	ServiceAccount kube-system/kube-proxy	ClusterRole system:node-proxier
cluster	ServiceAccount kube-system/legacy-service-account-token-cleaner	ClusterRole system:controller:legacy-service-account-token-cleaner
cluster	ServiceAccount kube-system/namespace-controller	ClusterRole system:controller:namespace-controller
cluster	ServiceAccount kube-system/node-controller	ClusterRole system:controller:node-controller
cluster	ServiceAccount kube-system/persistent-volume-binder	ClusterRole system:controller:persistent-volume-binder
cluster	ServiceAccount kube-system/pod-garbage-collector	ClusterRole system:controller:pod-garbage-collector
cluster	ServiceAccount kube-system/pv-protection-controller	ClusterRole system:controller:pv-protection-controller
cluster	ServiceAccount kube-system/pvc-protection-controller	ClusterRole system:controller:pvc-protection-controller
cluster	ServiceAccount kube-system/replicaset-controller	ClusterRole system:controller:replicaset-controller
cluster	ServiceAccount kube-system/replication-controller	ClusterRole system:controller:replication-controller
cluster	ServiceAccount kube-system/resource-claim-controller	ClusterRole system:controller:resource-claim-controller
cluster	ServiceAccount kube-system/resourcequota-controller	ClusterRole system:controller:resourcequota-controller
cluster	ServiceAccount kube-system/root-ca-cert-publisher	ClusterRole system:controller:root-ca-cert-publisher
cluster	ServiceAccount kube-system/route-controller	ClusterRole system:controller:route-controller
cluster	ServiceAccount kube-system/selinux-warning-controller	ClusterRole system:controller:selinux-warning-controller
cluster	ServiceAccount kube-system/service-account-controller	ClusterRole system:controller:service-account-controller
cluster	ServiceAccount kube-system/service-cidrs-controller	ClusterRole system:controller:service-cidrs-controller
cluster	ServiceAccount kube-system/service-controller	ClusterRole system:controller:service-controller
cluster	ServiceAccount kube-system/statefulset-controller	ClusterRole system:controller:statefulset-controller
cluster	ServiceAccount kube-system/ttl-after-finished-controller	ClusterRole system:controller:ttl-after-finished-controller
cluster	ServiceAccount kube-system/ttl-controller	ClusterRole system:controller:ttl-controller
cluster	ServiceAccount kube-system/validatingadmissionpolicy-status-controller	ClusterRole system:controller:validatingadmissionpolicy-status-controller

cluster	ServiceAccount kube-system/volumeattributesclass-protection-controller	ClusterRole system:controller:volumeattributesclass-protec controller
cluster	ServiceAccount kyverno/engine-admission-controller	ClusterRole kyverno:admission-controller
cluster	ServiceAccount kyverno/engine-admission-controller	ClusterRole view
cluster	ServiceAccount kyverno/engine-background-controller	ClusterRole kyverno:background-controller
cluster	ServiceAccount kyverno/engine-background-controller	ClusterRole view
cluster	ServiceAccount kyverno/engine-cleanup-controller	ClusterRole kyverno:cleanup-controller
cluster	ServiceAccount kyverno/engine-reports-controller	ClusterRole kyverno:reports-controller
cluster	ServiceAccount kyverno/engine-reports-controller	ClusterRole view
cluster	ServiceAccount local-path-storage/local-path-provisioner-service-account	ClusterRole local-path-provisioner-role
cluster	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator
cluster	ServiceAccount trivy-system/trivy-operator-engine	ClusterRole trivy-operator
cluster	User kube-apiserver-kubelet-client	ClusterRole system:kubelet-api-admin
cluster	User system:kube-controller-manager	ClusterRole calico-tier-getter
cluster	User system:kube-controller-manager	ClusterRole system:kube-controller-manager
cluster	User system:kube-proxy	ClusterRole system:node-proxier
cluster	User system:kube-scheduler	ClusterRole system:kube-scheduler
cluster	User system:kube-scheduler	ClusterRole system:volume-scheduler
bahriya-system	ServiceAccount compliance/compliance-collector	ClusterRole bke-platform-reader
calico-system	ServiceAccount calico-system/goldmane	Role goldmane
calico-system	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator-secrets
compliance-node	ServiceAccount compliance/compliance-collector	Role compliance-node-collector
kube-public	ServiceAccount kube-system/bootstrap-signer	Role system:controller:bootstrap-signer
kube-public	User system:anonymous	Role kubeadm:bootstrap-signer-clusterinfo
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kube-proxy

kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kubeadm:kubelet-config
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kubeadm:nodes-kubeadm-config
kube-system	Group system:nodes	Role kubeadm:kubelet-config
kube-system	Group system:nodes	Role kubeadm:nodes-kubeadm-config
kube-system	ServiceAccount calico-system/calico-apiserver	Role extension-apiserver-authentication-reader
kube-system	ServiceAccount kube-system/bootstrap-signer	Role system:controller:bootstrap-signer
kube-system	ServiceAccount kube-system/cloud-provider	Role system:controller:cloud-provider
kube-system	ServiceAccount kube-system/kube-controller-manager	Role system::leader-locking-kube-controller-manager
kube-system	ServiceAccount kube-system/kube-scheduler	Role system::leader-locking-kube-scheduler
kube-system	ServiceAccount kube-system/leader-election-controller	Role system::leader-locking-kube-controller-manager
kube-system	ServiceAccount kube-system/token-cleaner	Role system:controller:token-cleaner
kube-system	User system:kube-controller-manager	Role extension-apiserver-authentication-reader
kube-system	User system:kube-controller-manager	Role system::leader-locking-kube-controller-manager
kube-system	User system:kube-scheduler	Role extension-apiserver-authentication-reader
kube-system	User system:kube-scheduler	Role system::leader-locking-kube-scheduler
kyverno	ServiceAccount kyverno/engine-admission-controller	Role kyverno:admission-controller
kyverno	ServiceAccount kyverno/engine-background-controller	Role kyverno:background-controller
kyverno	ServiceAccount kyverno/engine-cleanup-controller	Role kyverno:cleanup-controller
kyverno	ServiceAccount kyverno/engine-reports-controller	Role kyverno:reports-controller
local-path-storage	ServiceAccount local-path-storage/local-path-provisioner-service-account	Role local-path-provisioner-role
tigera-operator	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator-secrets
trivy-system	ServiceAccount trivy-system/trivy-operator-engine	Role trivy-operator-engine

trivy-system	ServiceAccount trivy-system/trivy-operator-engine	Role trivy-operator-engine-leader-election

cluster.backups Fail

The cluster is backed up: Longhorn has an available backup target and a recurring backup job, or Velero has an available backup storage location and an active schedule. The last backup of each volume and schedule is recorded beside the verdict.

Nothing backs the cluster up: neither Longhorn nor Velero is installed.

- no longhorn.io API group
- no velero.io API group

How to fix On a Bahriya Kubernetes Engine cluster, set components.longhorn.settings.backup.target and credentialSecret in config.yaml, and backup.daily.enabled to true, then run apply.sh --commit, which creates the recurring job bke-daily-backup. A target that is configured but not available gives its reason in the longhorn-manager log: kubectl -n longhorn-system logs -l app=longhorn-manager --tail=200 | grep -i backup. With Velero, create a backup storage location that Velero reports Available and a Schedule that is not paused, as Velero's documentation describes; kubectl get backupstoragelocations.velero.io -A gives each location's phase. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Cluster backups	neither Longhorn nor Velero is installed	`kubectl api-resources | grep -E 'longhorn.io|velero.io'`

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.audit-log-permissions Pass

On each control-plane node, the API server's audit log directory is owned by root and no more open than 700, and each file directly in it no more open than 600, so that no user but root can change or read the audit log. Judged where the API server writes its audit log to a directory on the node, held in a host-path volume; on a Bahriya Kubernetes Engine cluster, from release 2.5.0. Where the directory cannot be examined, the check is not evaluated and states why. The node collector runs as an unprivileged user and examines modes alone: where the directory admits no other user, it cannot list the files, and that directory is the evidence for them, since on the node's local filesystem no user but root can then reach them, whatever their modes or any POSIX ACL.

The API server's audit log directory is owned by root and no more open than 700, and each file in it no more open than 600: so on all 1 node(s).

- node-1: files in /var/log/kubernetes/audit not examinable: the directory admits no other user (mode 700, owner root). This is the expected, secure state: no user but root can reach the files, whatever their modes, so the directory is the evidence for them.
- node-1: audit log directory /var/log/kubernetes/audit examined

node.etcd-data Pass

etcd's data directory on each control-plane node is owned by root and closed to other users (700).

etcd's data directory is owned by root and closed to other users: so on all 1 node(s).

- node-1: 1 path(s) examined

node.file-permissions Pass

The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.

Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s).

- node-1: 33 path(s) examined

node.kubelet-authn Pass

The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.

The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: 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.

node.kubelet-hardening Pass

The kubelet keeps its read-only port closed and rotates its client certificates.

The kubelet keeps its read-only port closed and rotates its certificates: 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.
- node-1: protectKernelDefaults is false (recorded, not judged: turning it on requires kernel settings the platform does not yet apply)

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.control-plane-tls Not evaluated

Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.

The control-plane TLS and profiling settings: the platform could not observe it.

- compliance.control-plane.configured: unknown
- compliance.control-plane.observed: unknown

platform.host-firewall Not evaluated

The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.

The platform could not count the host endpoints.

- host-network.host-endpoints: unknown
- host-network.ssh-ports: unknown

platform.image-registry Recorded

The platform's own images come from the registry recorded, signed.

The registry the control plane pulls its images from: 1x.ax/bke/kubernetes.

- image-registry: 1x.ax/bke/kubernetes

platform.key-provider Not evaluated

Where the encryption key is held (a local key, or a key management service through KMS v2).

The platform could not observe the encryption provider.

- encryption.provider: unknown

platform.mesh-cni Not evaluated

Meshed Pods run without elevated privileges, through the mesh's CNI plugin.

The service mesh CNI plugin: the platform could not observe it.

- compliance.mesh-cni.configured: unknown
- compliance.mesh-cni.observed: unknown

platform.oidc Not evaluated

People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.

The platform could not read the authentication configuration.

- authentication.oidc-issuers: unknown

platform.pod-security Not evaluated

Pod Security Admission defaults are applied to namespaces, with the exemptions listed.

Pod Security admission defaults: the platform could not observe it.

- compliance.pod-security.configured: unknown
- compliance.pod-security.observed: unknown
- pod-security.defaults: unknown
- pod-security.exemptions: unknown

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.default-deny-generated Not provided

A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).

The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed.

How to fix Set generate.defaultDenyNetworkPolicy.enabled to true in the Convoy's values and upgrade the Convoy. Where the policy is present but not ready, Kyverno's own status for it says why: kubectl describe generatingpolicy tersane-compliance-default-deny. (Bahriya Tersane)

policy.images-signed Fail

Every image outside the exempt namespaces carries a signature from a configured key: Kyverno verifies the images that match a key's patterns, and the collector fails any image that no key covers. A failing Pod is admitted with a warning and recorded, or refused, as policies.defaultAction sets (Warn by default).

11 object(s) run images that are not signed or that no signing key covers.

- tersane-compliance-images-signed: ready
- tersane-compliance-images-signed-organisation: ready
- 9 object(s) passed, 6 failed
- not judged while it holds no workload: namespace default
- signing keys cover: 1x.ax/*, registry.example.com/payments/legacy-batch*

How to fix Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)

Fails (11)

Object	What is wrong	Full result
CronJob payments/nightly	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
Deployment payments/unsigned-app	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`
Job payments/nightly-now	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6a73d7cc-01f5-42d8-9d6c-462a360b517b -n payments -o yaml`
Pod payments/nightly-now-k7cbf	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 4074d46b-fb0f-4ce3-8312-15270922068d -n payments -o yaml`
Pod payments/unsigned-app-b5567644f-vpkpp	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 3f291cbb-5fdd-4171-9ead-42230533be9f -n payments -o yaml`

ReplicaSet payments/unsigned-app-b5567644f	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 9f9f8242-9449-4023-a60b-aa60653c0b24 -n payments -o yaml`
Deployment payments/ledger	no signing key covers registry.example.com/payments/checkout:3.10.1	Kyverno passes an image that no signing key covers without verifying it, so no report records it.
Deployment payments/legacy-batch	no signing key covers registry.example.com/payments/checkout:3.10.1	Kyverno passes an image that no signing key covers without verifying it, so no report records it.
CronJob payments/weekly	no signing key covers registry.example.com/payments/checkout:3.10.1	Kyverno passes an image that no signing key covers without verifying it, so no report records it.
Job payments/migrate-once	no signing key covers registry.example.com/payments/checkout:3.10.1	Kyverno passes an image that no signing key covers without verifying it, so no report records it.
Pod payments/one-off	no signing key covers registry.example.com/payments/checkout:3.10.1	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

policy.ingress-tls Nothing to check

Every Ingress serves its hosts over TLS.

The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge.

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

policy.namespace-classification Pass

Every application namespace carries a data classification label.

Every object the policy judged passes it.

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

Fails in exempt namespaces, not counted (1)

Object	What is wrong	Full result
Namespace default	holds no workload, so not judged; the namespace needs the label tersane.bahriya.cloud/data-classification, one of: top-secret, secret, restricted, public	`kubectl get clusterpolicyreport 64c20931-22c4-4dab-a1fd-bf2b33cddf86 -o yaml`

policy.namespace-environment Pass

Every application namespace carries an environment label, one of the values in namespaces.environments.

Every object the policy judged passes it.

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

Fails in exempt namespaces, not counted (1)

Object	What is wrong	Full result
Namespace default	holds no workload, so not judged; the namespace needs the label tersane.bahriya.cloud/environment, one of: production, staging, test, development	`kubectl get clusterpolicyreport 64c20931-22c4-4dab-a1fd-bf2b33cddf86 -o yaml`

policy.namespace-network-policy Fail

Every application namespace has at least one NetworkPolicy.

1 object(s) fail the policy.

- tersane-compliance-namespace-network-policy: ready
- 0 object(s) passed, 1 failed
- not judged while it holds no workload: namespace default

How to fix Add NetworkPolicies to the namespace that allow only the traffic its workloads need. To start every new namespace closed, set generate.defaultDenyNetworkPolicy.enabled to true in the Convoy's values. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Namespace payments	namespace payments holds no NetworkPolicy	`kubectl get clusterpolicyreport 1bef7dc4-e354-4b6d-bc32-e548e1af4393 -o yaml`

Fails in exempt namespaces, not counted (1)

Object	What is wrong	Full result
Namespace default	holds no workload, so not judged; namespace default holds no NetworkPolicy	`kubectl get clusterpolicyreport 64c20931-22c4-4dab-a1fd-bf2b33cddf86 -o yaml`

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

policy.no-latest-tag Pass

Images are referenced by a fixed tag or digest, never by a moving tag.

Every object the policy judged passes it.

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

policy.registries-allowed Fail

Containers run images only from the registries the customer allows.

7 object(s) fail the policy.

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

How to fix Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)

Fails (7)

Object	What is wrong	Full result
CronJob payments/nightly	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
CronJob payments/weekly	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport f95320a9-ae62-47ac-8865-9ff294efe291 -n payments -o yaml`
Deployment payments/ledger	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport dd716344-57f2-43ff-8850-cec7fbc7281f -n payments -o yaml`
Deployment payments/legacy-batch	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport cc1c8507-d6bb-4e77-8205-1a214c884777 -n payments -o yaml`
Deployment payments/unsigned-app	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`
Job payments/migrate-once	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport cdf45f25-40a7-4023-bc92-880235dc0c91 -n payments -o yaml`
Pod payments/one-off	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport 157881f3-9f3d-472c-9134-201b7cf0220e -n payments -o yaml`

policy.resource-limits Fail

Every container declares memory and CPU limits.

3 object(s) fail the policy.

- tersane-compliance-resource-limits: ready
- 4 object(s) passed, 3 failed
- not judged while it holds no workload: namespace default

How to fix Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)

Fails (3)

Object	What is wrong	Full result
CronJob payments/nightly	containers without CPU and memory limits: app	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
Deployment payments/legacy-batch	containers without CPU and memory limits: app	`kubectl get policyreport cc1c8507-d6bb-4e77-8205-1a214c884777 -n payments -o yaml`
Deployment payments/unsigned-app	containers without CPU and memory limits: app	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`

trivy.external-ip Pass

Services with external IP addresses.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0108
- 15 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

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.image-sources Pass

Images from public registries (AVD-KSV-0034), or referenced by a moving tag (AVD-KSV-0013). AVD-KSV-0125 is not used: its list trusts only three cloud providers' registries, and policy.registries-allowed judges the registries against your own list instead. See https://tersane.bahriya.cloud/docs/charts/compliance/#checks-the-convoy-does-not-use-and-why.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0013, AVD-KSV-0034
- 22 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

trivy.limits Fail

Containers without CPU or memory limits.

3 object(s) fail.

- trivy checks: AVD-KSV-0011, AVD-KSV-0018
- 13 object(s) with a passing result, 3 failing, 6 failing in exempt namespaces

How to fix AVD-KSV-0011 Set a limit value under 'containers[].resources.limits.cpu'. (trivy-operator)

How to fix AVD-KSV-0018 Set a limit value under 'containers[].resources.limits.memory'. (trivy-operator)

Fails (6)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0011: CPU not limited. Container 'app' of CronJob 'nightly' should set 'resources.limits.cpu' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
CronJob payments/nightly	AVD-KSV-0018: Memory not limited. Container 'app' of CronJob 'nightly' should set 'resources.limits.memory' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0011: CPU not limited. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'resources.limits.cpu' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0018: Memory not limited. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'resources.limits.memory' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0011: CPU not limited. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'resources.limits.cpu' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0018: Memory not limited. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'resources.limits.memory' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (30)

Object	What is wrong	Full result
APIServer calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-apiserver' of ReplicaSet 'calico-apiserver-6b7f4598c7' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-apiserver-6b7f4598c7 -n calico-system -o yaml`
APIServer calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-apiserver' of ReplicaSet 'calico-apiserver-6b7f4598c7' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-apiserver-6b7f4598c7 -n calico-system -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0011: CPU not limited. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0018: Memory not limited. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`

Goldmane calico-system/default	AVD-KSV-0011: CPU not limited. Container 'goldmane' of ReplicaSet 'goldmane-7d6f669648' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-goldmane-7d6f669648 -n calico-system -o yaml`
Goldmane calico-system/default	AVD-KSV-0018: Memory not limited. Container 'goldmane' of ReplicaSet 'goldmane-7d6f669648' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-goldmane-7d6f669648 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-kube-controllers' of ReplicaSet 'calico-kube-controllers-697bdf6d74' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-kube-controllers-697bdf6d74 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-node' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-typha' of ReplicaSet 'calico-typha-5f45dc8cf9' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-typha-5f45dc8cf9 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'install-cni' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-kube-controllers' of ReplicaSet 'calico-kube-controllers-697bdf6d74' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-kube-controllers-697bdf6d74 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-node' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`

Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-typha' of ReplicaSet 'calico-typha-5f45dc8cf9' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-typha-5f45dc8cf9 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'install-cni' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Pod compliance/reader	AVD-KSV-0011: CPU not limited. Container 'reader' of Pod 'reader' should set 'resources.limits.cpu'	`kubectl get configauditreport pod-reader -n compliance -o yaml`
Pod compliance/reader	AVD-KSV-0018: Memory not limited. Container 'reader' of Pod 'reader' should set 'resources.limits.memory'	`kubectl get configauditreport pod-reader -n compliance -o yaml`
Whisker calico-system/default	AVD-KSV-0011: CPU not limited. Container 'whisker' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0011: CPU not limited. Container 'whisker-backend' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0018: Memory not limited. Container 'whisker' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0018: Memory not limited. Container 'whisker-backend' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`

trivy.network-policy-selectors **Pass**

NetworkPolicies whose selectors select nothing.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0038
- 188 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

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.run-as-root Fail

Containers that run as the root user.

3 object(s) fail.

- trivy checks: AVD-KSV-0012, AVD-KSV-0105
- 188 object(s) with a passing result, 3 failing, 2 failing in exempt namespaces

How to fix AVD-KSV-0012 Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)

Fails (3)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0012: Runs as root user. Container 'app' of CronJob 'nightly' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (10)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0012: Runs as root user. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'calico-node' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`

Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'install-cni' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0105: Containers must not set runAsUser to 0. securityContext.runAsUser should be set to a value greater than 0	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0105: Containers must not set runAsUser to 0. securityContext.runAsUser should be set to a value greater than 0	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`

trivy.seccomp Fail

Containers without the runtime's default seccomp profile.

3 object(s) fail.

- trivy checks: AVD-KSV-0030, AVD-KSV-0104
- 18 object(s) with a passing result, 3 failing, 1 failing in exempt namespaces

How to fix AVD-KSV-0030 Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

How to fix AVD-KSV-0104 Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)

Fails (6)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
CronJob payments/nightly	AVD-KSV-0104: Seccomp policies disabled. container "app" of cronjob "nightly" in "payments" namespace should specify a seccomp profile	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`

Deployment payments/legacy-batch	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "legacy-batch-5bdd998d78" in "payments" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "unsigned-app-b5567644f" in "payments" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (2)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0104: Seccomp policies disabled. container "tigera-operator" of replicaset "tigera-operator-686489b657" in "tigera-operator" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -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-2 Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.
AC-2(1) Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
AC-2(3) Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
AC-2(4) Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.
AC-2(9) Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions].
AC-4 Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
AC-5 Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals] ; and b. Define system access authorizations to support separation of duties.
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.
AC-6(1) Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals and roles] to: (a) [Assignment: organization-defined organization-defined security functions (deployed in hardware, software, and firmware)] ; and (b) [Assignment: organization-defined security-relevant information].
AC-6(7) Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles and classes] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-7 Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period] ; and b. Automatically [Selection (one or more): lock the account or node for [Assignment: organization-defined time period] ; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm] ; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.
AC-17 Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
AC-19 Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.
AC-19(5) Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].
AC-20 Use of External Systems	a. [Selection (one or more): establish [Assignment: organization-defined terms and conditions] ; identify [Assignment: organization-defined controls asserted]] , consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organization-defined prohibited types of external systems].
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].
AT-2 Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined organization-defined events]; b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]; c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
AT-2(1) Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.

AT-3 Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined organization-defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes; b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.
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-6 Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles] ; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
AU-6(3) Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
AU-9 Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.
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-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-5 Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
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(2) Red Team Exercises	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].

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(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(1) Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
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-6 Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements] ; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

CM-7(5) Authorized Software — Allow-by-exception	(a) Identify [Assignment: organization-defined software programs]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].
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].
CM-8(3) Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined organization-defined automated mechanisms] [Assignment: organization-defined frequency] ; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by unauthorized components; isolate unauthorized components; notify [Assignment: organization-defined personnel or roles]].
CM-10 Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CM-14 Signed Components	Prevent the installation of [Assignment: organization-defined organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
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-9 System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency]; b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency]; c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency] ; and d. Protect the confidentiality, integrity, and availability of backup information.
CP-10 System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.
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].
IA-2 Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-2(1) Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.
IA-2(2) Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.
IA-5 Authenticator Management	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.

IA-8 Identification and Authentication (Non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
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-2 Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and b. Review and update incident response training content [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.
MP-3 Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt [Assignment: organization-defined types of media exempted from marking] from marking if the media remain within [Assignment: organization-defined controlled areas].
MP-5 Media Transport	a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined organization-defined controls]; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel.
MP-6 Media Sanitization	a. Sanitize [Assignment: organization-defined organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined organization-defined sanitization techniques and procedures] ; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
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].

PE-3 Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined systems or devices] ; guards]; b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]; d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances]; e. Secure keys, combinations, and other physical access devices; f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency] ; and g. Change combinations and keys [Assignment: organization-defined organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
PE-6 Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events] ; and c. Coordinate results of reviews and investigations with the organizational incident response capability.
PE-8 Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]; b. Review visitor access records [Assignment: organization-defined frequency] ; and c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].
PE-13 Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.
PE-14 Environmental Controls	a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels] ; and b. Monitor environmental control levels [Assignment: organization-defined frequency].
PE-15 Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
PE-16 Delivery and Removal	a. Authorize and control [Assignment: organization-defined organization-defined types of system components] entering and exiting the facility; and b. Maintain records of the system components.
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].

PL-2 System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization’s enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes; 4. Identify the individuals that fulfill system roles and responsibilities; 5. Identify the information types processed, stored, and transmitted by the system; 6. Provide the security categorization of the system, including supporting rationale; 7. Describe any specific threats to the system that are of concern to the organization; 8. Provide the results of a privacy risk assessment for systems processing personally identifiable information; 9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components; 10. Provide an overview of the security and privacy requirements for the system; 11. Identify any relevant control baselines or overlays, if applicable; 12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; 13. Include risk determinations for security and privacy architecture and design decisions; 14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups] ; and 15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation. b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]; c. Review the plans [Assignment: organization-defined frequency]; d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and e. Protect the plans from unauthorized disclosure and modification.
PL-4 Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior [Assignment: organization-defined frequency] ; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency] ; when the rules are revised or updated].
PL-8 Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

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-2 Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
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-4 Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-5 System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
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-13 Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.

PM-15 Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and c. To share current security and privacy information, including threats, vulnerabilities, and incidents.
PM-16 Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PM-28 Risk Framing	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel] ; and c. Review and update risk framing considerations [Assignment: organization-defined frequency].
PM-29 Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.
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].
PS-3 Personnel Screening	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with [Assignment: organization-defined organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].
PS-4 Personnel Termination	Upon termination of individual employment: a. Disable system access within [Assignment: organization-defined time period]; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by terminated individual.
PS-5 Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

PS-6 Access Agreements	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [Assignment: organization-defined frequency] ; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].
PS-7 External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements; d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period] ; and e. Monitor provider compliance with personnel security requirements.
PS-8 Personnel Sanctions	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
PS-9 Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.
PT-3 Personally Identifiable Information Processing Purposes	a. Identify and document the [Assignment: organization-defined purpose(s)] for processing personally identifiable information; b. Describe the purpose(s) in the public privacy notices and policies of the organization; c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d. Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].
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-2 Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

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-5(2) Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency] ; prior to a new scan; when new vulnerabilities are identified and reported].
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-3 System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system-development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.
SA-4 Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria.
SA-8 Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined organization-defined systems security and privacy engineering principles].
SA-9 External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].
SA-9(2) Identification of Functions, Ports, Protocols, and Services	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].
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-11 Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency to conduct] at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.
SA-11(4) Manual Code Reviews	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].

SA-15 Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined organization-defined security and privacy 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-4 Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.
SC-5 Denial-of-service Protection	a. [Selection: protect against; limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events] ; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].
SC-6 Resource Availability	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].
SC-7 Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
SC-8 Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

SC-12 Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements].
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-23 Session Authenticity	Protect the authenticity of communications sessions.
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].
SC-39 Process Isolation	Maintain a separate execution domain for each executing system process.
SI-2 Flaw Remediation	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.
SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions	(a) Measure the time between flaw identification and flaw remediation; and (b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].
SI-3 Malicious Code Protection	a. Implement [Selection (one or more): signature-based; non-signature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]] ; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

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-4(12) Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].
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-12 Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.
SI-12(1) Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].
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].

SR-3 Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls] ; and c. Document the selected and implemented supply chain processes and controls in [Selection (one or more): security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].
SR-5 Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined strategies, tools, and methods].
SR-6 Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].
SR-8 Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; [Assignment: organization-defined results of assessments or audits]].