Cyber Resilience Controls, first edition (June 2024), and Banking Reform Standards B2, B3, B7 and B9 (2025): technical evidence

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

Regime	Cyber Resilience Controls, first edition (June 2024), and Banking Reform Standards B2, B3, B7 and B9 (2025), Central Bank of Iraq (CBI)
Organisation	Example Bank
Cluster	example-production
Collected	2026-11-19T10:53:03Z
Collector	Bahriya Tersane Compliance and Assurance Convoy, collector 1.x.y

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

The Central Bank of Iraq is the source and owner of the Cyber Resilience Controls and the Banking Reform Standards. The requirement summaries in this report are Mamluk's paraphrase in English, not the CBI's text and not an official translation.

The Cyber Resilience Controls are published in Arabic only. The Standards are published in Arabic with an English reference translation, and the Arabic prevails.

The CBI publishes no mapping of these requirements to NIST SP 800-53. The mapping in this report is Mamluk's own.

Requirements labelled Controls apply to every bank and payment provider. Requirements labelled Standards come from standards B2, B3, B7 and B9 of the Banking Reform Standards 2025, which apply to private banks; a private bank is assessed on both. The function prefixes and the letters and suffixes added to the CBI's numbers are Mamluk's identifiers, not the CBI's.

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

524 requirements: 2 enforced by a policy, 37 checked, 6 provided by the platform, 479 organisational (107 technical, outside the cluster; 250 non-technical; 122 technical and non-technical).

Outcome	Requirements	Meaning
Fail	24	The cluster was checked and something does not meet the requirement. The findings say what and where.
Not provided	1	A control the requirement needs is switched off on this cluster.
Incomplete	7	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	0	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	9 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	3	Facts collected for the organisation's reviewer, such as an inventory or a list of access; no verdict.
Nothing to check	1	The cluster has nothing of this kind yet, for example no Ingress to check for TLS. Neither a pass nor a failure.
Organisational evidence	479	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

16 object(s) fail at least one check: 4 cluster-wide and 12 in 1 namespace(s). They are listed under Fix first, those that fail a requirement marked "Controls (all banks and payment providers)" first, then 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

4 object(s), most severe Critical.

ClusterRole **tigera-operator** Fails B2 B.7, ID-1.7, PR-1.2.1, PR-3.1.21, PR-8.1.1, PR-8.4.2.c, PR-8.4.2.d, PR-14.2.2 Controls (all banks and payment providers): ID-1.7, PR-1.2.1, PR-3.1.21, PR-8.1.1, PR-8.4.2.c, PR-8.4.2.d, PR-14.2.2

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 B2 B.7, ID-1.7, PR-1.2.1, PR-3.1.21, PR-8.1.1, PR-8.4.2.c, PR-8.4.2.d, PR-14.2.2 Controls (all banks and payment providers): ID-1.7, PR-1.2.1, PR-3.1.21, PR-8.1.1, PR-8.4.2.c, PR-8.4.2.d, PR-14.2.2

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 PR-1.2.9.c, RS-3.1, RS-3.2 Controls (all banks and payment providers): PR-1.2.9.c, RS-3.1, RS-3.2

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'`

Cluster **log shipping** Fails DE-1.4, PR-1.2.4 Controls (all banks and payment providers): DE-1.4, PR-1.2.4

MEDIUM	no log shipper runs on the cluster Check cluster.log-forwarding. **How to fix** On a Bahriya Kubernetes Engine cluster, set components.fluent-bit.settings.output.config in config.yaml to an [OUTPUT] section naming the central store, then run apply.sh --commit. Keep the store's password out of config.yaml, as the Logging with Fluent Bit guide describes. On another cluster, install a log shipper, such as Fluent Bit, that sends the logs to a central store. Where records do not arrive, the Pod named in the finding logs each failed delivery: check that the store can be reached from the cluster and that its credentials are accepted. (Bahriya Tersane)
Full result	`kubectl get daemonsets,deployments -A`

Namespace payments

12 object(s), most severe High.

CronJob **nightly** Fails ID-1.13, ID-1.14, PR-1.2.9.a, PR-3.1.1, PR-3.1.2 Controls (all banks and payment providers): ID-1.13, ID-1.14, PR-1.2.9.a, PR-3.1.1, PR-3.1.2

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14, PR-1.2.9.a, PR-3.1.1, PR-3.1.2 Controls (all banks and payment providers): ID-1.13, ID-1.14, PR-1.2.9.a, PR-3.1.1, PR-3.1.2	
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 ID-1.13, ID-1.14, PR-1.2.9.a, PR-3.1.1, PR-3.1.2 Controls (all banks and payment providers): ID-1.13, ID-1.14, PR-1.2.9.a, PR-3.1.1, PR-3.1.2

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 ID-1.13, ID-1.14 Controls (all banks and payment providers): ID-1.13, ID-1.14

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 B2 B.6, PR-2.2.3, PR-3.1.3, PR-3.1.6, PR-3.1.9, PR-14.1.6 Controls (all banks and payment providers): PR-2.2.3, PR-3.1.3, PR-3.1.6, PR-3.1.9, PR-14.1.6

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

GV Governance

GV-BOD Roles and responsibilities of the Board of Directors

GV-BOD.a	The Board approves the IT strategy and policy documents. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-1 Information Security Program Plan, PL-1 Policy and Procedures.	**Organisational evidence**
GV-BOD.b	The Board makes sure that management has put an effective planning process in place. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy, PL-2 System Security and Privacy Plans.	**Organisational evidence**
GV-BOD.c	The Board confirms that the IT strategy is aligned with the business strategy. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-11 Mission and Business Process Definition.	**Organisational evidence**
GV-BOD.d	The Board makes sure that the IT organisation structure complements and fits the business model and its direction. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
GV-BOD.e	The Board makes sure that IT investment balances risks, benefits and acceptable budgets. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-3 Information Security and Privacy Resources.	**Organisational evidence**

GV-BOD.f	The Board ascertains the state of compliance with the cybersecurity policy. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring, CA-2 Control Assessments.	**Organisational evidence**

GV-ITSC Roles and responsibilities of the IT Steering Committee

GV-ITSC.0	An IT Steering Committee formed with representatives of IT, risk management, human resources, internal audit, legal and the other relevant departments. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
GV-ITSC.a	The committee monitors management's methods for setting and achieving strategic objectives. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
GV-ITSC.b	The committee members are aware of the IT risk exposure and of its controls. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
GV-ITSC.c	The committee gives direction on risk, funding and its sources. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-9 Risk Management Strategy.	**Organisational evidence**
GV-ITSC.d	The committee confirms project priorities and assesses the feasibility of IT proposals. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-2 Allocation of Resources, PM-3 Information Security and Privacy Resources.	**Organisational evidence**
GV-ITSC.e	The committee makes sure that every critical project includes project risk management. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-3 System Development Life Cycle, RA-3 Risk Assessment.	**Organisational evidence**
GV-ITSC.f	The committee advises on the choice of technologies within the standards. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
GV-ITSC.g	The committee makes sure that vulnerability assessments of new technologies are completed. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation, RA-5 Vulnerability Monitoring and Scanning.	**Organisational evidence**
GV-ITSC.h	The committee makes sure of compliance with regulatory and legal requirements. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
GV-ITSC.i	The committee directs that the IT architecture design complies with legislative and regulatory requirements, and confirms that it does. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**

GV-CSC Information security governance: roles and responsibilities of the Cybersecurity Committee

GV-CSC.0	A Cybersecurity Committee formed with representatives of IT, information and cybersecurity, risk management, the internal complaints committee and the other relevant departments. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
GV-CSC.a	The committee makes sure that cybersecurity objectives, and the related policies and procedures, are developed and put into effect. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-1 Information Security Program Plan, PL-1 Policy and Procedures.	**Organisational evidence**
GV-CSC.b	The committee gives continuing management support to information security operations. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-3 Information Security and Privacy Resources.	**Organisational evidence**
GV-CSC.c	The committee makes sure of continuing compliance with business objectives and with the regulatory and legal requirements on cybersecurity. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
GV-CSC.d	The committee supports the drafting of the IT risk management framework or process and sets the risk appetite. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
GV-CSC.e	The committee reviews changes to cybersecurity processes periodically and approves them. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-1 Information Security Program Plan.	**Organisational evidence**

GV-POL IT policies, standards and procedures

GV-POL.a	A cybersecurity policy, consistent with the CBI's cybersecurity directives and approved by the Board. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
GV-POL.b	The policy covers end-user computers and devices, data, the network, applications and other technical resources; controls are adopted to protect the information system; senior management shows its commitment through continuing awareness and training for every level of staff and for the parties concerned. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures, AT-2 Literacy Training and Awareness.	**Organisational evidence**

GV-POL.c	The policy is updated regularly for changes in the institution's IT environment and in the financial and banking sector. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures.	**Organisational evidence**
GV-POL.d	Cybersecurity specialists employed in the information security department to handle security events, document policies and treat technical risks. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-13 Security and Privacy Workforce.	**Organisational evidence**
GV-POL.e	For a case of non-compliance, a compliance plan submitted to the CBI to request an exception, which is for a fixed period. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-4 Plan of Action and Milestones Process.	**Organisational evidence**

GV-DOC Documentation

GV-DOC.a	An up-to-date organisation structure for the IT department. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
GV-DOC.b	An IT support unit in the organisation structure of the branches. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
GV-DOC.c	A job description, with a named backup person, for everyone who works in the IT department. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-9 Position Descriptions.	**Organisational evidence**
GV-DOC.d	Segregation of duties kept for IT tasks. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-5 Separation of Duties.	**Organisational evidence**
GV-DOC.e	Detailed design documents kept for all critical IT systems and services, such as the data centre, network and data centre power designs. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-2 System Security and Privacy Plans, PL-8 Security and Privacy Architectures.	**Organisational evidence**
GV-DOC.f	A schedule set in advance for sensitive IT tasks, such as end-of-day processing, network monitoring, data centre physical security and ATM monitoring. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-2 System Security and Privacy Plans.	**Organisational evidence**
GV-DOC.g	Up-to-date operating procedures for all IT functions, such as backup, database and network administration, job scheduling, start-up, shutdown, restart and recovery. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-5 System Documentation.	**Organisational evidence**

GV-DOC.h	Requisition and acknowledgement forms for the various IT requests, operations and services. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures.	**Organisational evidence**
GV-DOC.i	A user guide for every application, for internal and external users. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-5 System Documentation.	**Organisational evidence**

IM 1. IT and Security Infrastructure Management

IM-1	The performance of cybersecurity governance and of the technical controls measured with at least the 96 key performance indicators the Controls list, from governance meetings and policy reviews to incidents, vulnerabilities, penetration tests, backups, access and third parties. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**

RM 2. Risk Management

RM-2	A cyber resilience framework that sets objectives and identifies, validates and manages cyber risks, reviewed and updated periodically and adopted by the Board and senior management. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy, RA-1 Policy and Procedures.	**Organisational evidence**
RM-2.1	Business functions and their supporting processes identified, their risks assessed, and each classified by sensitivity and criticality to set the priorities for protection, investigation, response and recovery. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2(8) Identify Critical Assets, RA-9 Criticality Analysis, PM-11 Mission and Business Process Definition.	**Organisational evidence**
RM-2.2	Measures to prevent and reduce the risks that arise from connected entities, with the cyber resilience level and controls part of every agreement with them (contracts, service level agreements), and those agreements subject to periodic audit and cyber risk assessment. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, CA-3 Information Exchange, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
RM-2.3	Risk assessments of vendors, suppliers, service providers and other external parties, with controls to detect and prevent intrusions and attacks linked to them. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SR-6 Supplier Assessments and Reviews, SA-9 External System Services, RA-3(1) Supply Chain Risk Assessment.	**Organisational evidence**

RM-2.4 2.4 IT Risk Governance

RM-2.4.1	An IT risk management committee that governs all IT risks and their mitigation. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

RM-2.4.2	The risk appetite defined, by the frequency and size of loss the institution will accept, such as financial loss and reputational harm. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.3	The risk tolerance defined after approval by the Board or the risk management committee, and communicated clearly to all stakeholders. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.4	Changes in risk appetite and tolerance reviewed and approved over time, in particular for new technologies, structures and strategies, with the risk profile reassessed at regular intervals. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy, RA-3 Risk Assessment.	**Organisational evidence**
RM-2.4.5	Risk responsibilities assigned to individuals. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.6	Risk accountability assigned to those who hold the resources and the authority to approve or accept an outcome, with ownership of a risk kept by the owner or custodian best placed to mitigate it. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.7	All risks acknowledged and made known through risk awareness, as the means of managing them. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.8	The actual IT risk exposure made clear to executive management through open communication. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.9	Internal stakeholders made aware of the importance of integrating risk and opportunity into their daily work. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy, AT-2 Literacy Training and Awareness.	**Organisational evidence**
RM-2.4.10	Transparency towards external stakeholders on the actual level of risk and the processes used to manage it. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.4.11	A risk-aware culture set from the top by the Board and the executives. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

RM-2.4.12	The information security department reports the state of IT security risks to the IT security committee and the risk management committee periodically, as the policy sets. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy, PM-6 Measures of Performance.	**Organisational evidence**

RM-2.5 2.5 IT Risk Assessment

RM-2.5.a	IT teams understand how IT failures and events can affect the institution's objectives and cause direct or indirect loss. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
RM-2.5.b	Business teams understand how IT failures and events can affect key services and operations. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
RM-2.5.1	A business impact analysis, to understand the effects of adverse events. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-9 Criticality Analysis, CP-2(8) Identify Critical Assets.	**Organisational evidence**
RM-2.5.2	Risk scenarios developed and used to identify the significant risks, with their frequency and impact assessed. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
RM-2.5.3	The risk factors that affect the frequency or impact of the risk scenarios identified. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
RM-2.5.4	Risk factors interpreted as causes of a scenario or as weaknesses. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
RM-2.5.5	The information security department assesses the IT risks of IT assets (processes and systems) periodically and recommends mitigation to the risk owners. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

RM-2.6 2.6 IT Risk Response

RM-2.6.1	A set of metrics used as risk indicators, with the key risk indicators (KRIs) among them. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-6 Measures of Performance, PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.6.2	The various indicators of equal sensitivity applied, measured and reported. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**

RM-2.6.3	KRIs chosen to give early warning of high risks, review risk events, document trends, indicate the risk appetite and tolerance, support the strategic objectives and improve risk governance; the risk response set after analysis to bring risks within the appetite. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-6 Measures of Performance, PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.6.4	IT risk management practices strengthened through adequate risk management processes. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
RM-2.6.5	Measures that limit any adverse event or its effect on the business. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-9 Risk Management Strategy, RA-7 Risk Response.	**Organisational evidence**

ID Identify

ID-1 1. Assets Management

ID-1.1	A compatibility assessment against the existing systems before any new IT asset is bought. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
ID-1.2	Every purchase of IT assets follows the institution's procurement policy. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-4 Acquisition Process, SA-1 Policy and Procedures.	**Organisational evidence**
ID-1.3	Every IT asset assigned to a custodian, a person or entity responsible for its development, maintenance, use and security. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-8(4) Accountability Information.	**Organisational evidence**
ID-1.4	Every IT asset identified and clearly labelled, with the label showing the asset's classification. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-5 System Inventory.	**Organisational evidence**
ID-1.5	An inventory of IT assets with their important details, such as owner, custodian, purchase date, location, licence number and configuration. Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-8 System Component Inventory. **Scope of this evidence** The inventory of the cluster's namespaces, workloads and images is recorded. The inventory of other IT assets, with their owners, purchase dates, locations and licences, is the institution's to evidence. cluster.workload-inventory — **Recorded** — 13 namespaces, 21 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.	**Recorded**

ID-1.6 The IT asset inventory reviewed and updated periodically. **Recorded**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-8 System Component Inventory, CM-8(1) Updates During Installation and Removal.

Scope of this evidence The inventory of the cluster's workloads and images is recorded at every run. The periodic review of the institution's whole IT asset inventory is the institution's to evidence.

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

ID-1.7 Information system assets adequately protected from unauthorised access, misuse, modification, insertion, deletion, substitution, cancellation or disclosure. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege, SC-28 Protection of Information at Rest.

Scope of this evidence The evidence concerns the cluster: role-based access control, anonymous access refused, service account tokens and the encryption of Kubernetes Secrets at rest. The protection of the institution's other information system assets is the institution's to evidence.

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

node.kubelet-authz	**Pass**	The kubelet authorises requests through the API server: so on all 1 node(s). Establishes: The kubelet authorises requests through the API server (Webhook mode).
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
platform.secret-encryption	**Not evaluated**	The platform could not observe Secret encryption. Establishes: Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.
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.

ID-1.8 A disposal policy, with all data on equipment and its storage media destroyed or overwritten before the equipment is sold, disposed of or reissued. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-6 Media Sanitization.

ID-1.9 Guidance on the use of portable devices, in particular outside the workplace. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-19 Access Control for Mobile Devices.

ID-1.10 A policy for the return of the institution's assets by employees and external parties at the end of their employment, contract or agreement. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-4 Personnel Termination.

ID-1.11 The terms of every software licence respected, and no software used that was not bought or obtained lawfully. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-10 Software Usage Restrictions.

ID-1.12 External software used in production covered by a support agreement with its vendor. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services.

ID-1.13 Only an approved list of software used on any IT device. **Fail**

Enforced, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-7(5) Authorized Software — Allow-by-exception.

Scope of this evidence In the cluster, the images admitted to run are limited to the allowed registries and, where configured, to signed images. The list of approved software on the institution's other IT devices is the institution'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.

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.registries-allowed	**Fail**	7 object(s) fail the policy. Establishes: Containers run images only from the registries the customer allows.

ID-1.14 Unauthorised or pirated software strictly prohibited. **Fail**

Enforced, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-7(5) Authorized Software — Allow-by-exception, CM-10 Software Usage Restrictions.

Scope of this evidence In the cluster, images from registries that are not allowed are refused, and, where configured, unsigned images. Licensing and piracy are the institution'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.

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.registries-allowed	**Fail**	7 object(s) fail the policy. Establishes: Containers run images only from the registries the customer allows.

ID-2 2. Software Assets

ID-2.1 All software bought and installed legally licensed, with records kept by the department concerned. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-10 Software Usage Restrictions.

ID-2.2 A separate test environment for full functional testing of software before implementation. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-4(1) Separate Test Environments.

Scope of this evidence The evidence is that each application namespace carries an environment label. A separate test environment outside the cluster, and the testing itself, are the institution's to evidence.

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.

ID-2.3 User acceptance testing carried out and signed off by the business departments concerned before go-live. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.

ID-2.4 The regulatory compliance requirements of banking procedures and practice and the relevant laws of the Government of Iraq taken into account. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.

ID-2.5 Errors or faults caused by design defects escalated promptly to higher levels in the software suppliers' organisations. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services.

ID-2.6	Support agreements, with confidentiality agreements, kept in force with the suppliers of the software and applications used in production. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, PS-6 Access Agreements.	**Organisational evidence**

ID-3 3. Capacity Management

ID-3.1	Indicators such as performance, capacity and utilisation of IT systems and infrastructure monitored and reviewed. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-5 Response to Audit Logging Process Failures, PM-6 Measures of Performance.	**Organisational evidence**
ID-3.2	Monitoring processes with thresholds to plan and provide additional resources for operational and business needs. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CP-2(2) Capacity Planning.	**Organisational evidence**

ID-4 4. Data Classification

ID-4.a	Data classified at four levels: public, restricted, secret and top secret, each defined by the harm its disclosure would cause. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
ID-4.b	Staff authorised to handle classified information: restricted information classified by staff; awareness sessions before authorisation; clear desk and clear screen; a short, approved list of staff for secret information who sign non-disclosure terms; vetting for top secret, and a register of everyone who saw it. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-3 Personnel Screening, PS-6 Access Agreements, AT-2 Literacy Training and Awareness.	**Organisational evidence**
ID-4.c	Creating, printing and copying: restricted information not printed or copied outside the institution or sent over social media or instant messaging; secret information printed or copied only with approval; the staff who may create or handle top secret information identified. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-2 Media Access.	**Organisational evidence**
ID-4.d	Storage: restricted information only on the institution's devices or authorised external ones, with removable media encrypted; secret information only on the institution's own assets; top secret information always encrypted when stored electronically, on removable media only with approval, and never on non-government cloud services. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-4 Media Storage, SC-28 Protection of Information at Rest, SA-9 External System Services.	**Organisational evidence**

ID-4.e	Access and remote access: identity and access management and data loss prevention applied to restricted information; no remote access to secret information; time-limited access, granted and reviewed with prior written approval; approval for non-Iraqi individuals only by exception under international agreements. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement, AC-17 Remote Access, SC-7(10) Prevent Exfiltration.	**Organisational evidence**
ID-4.f	Electronic transfer: restricted information emailed only through the institution's own email system; secret information encrypted and password-protected in transit, with the password sent by another channel and no revealing subject line; top secret information never sent electronically. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, AC-4 Information Flow Enforcement.	**Organisational evidence**
ID-4.g	Destruction and disposal: restricted information erased from media to be reused; media holding secret information destroyed completely; disposal of media holding top secret information recorded in a register approved and signed by the committee concerned. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
ID-4.h	Meetings: restricted material disposed of after meetings; secret matters discussed in a secure room with a defined, verified attendance list; top secret meetings with approved attendees and no connected or recording devices without approval. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-2 Physical Access Authorizations, PE-19 Information Leakage.	**Organisational evidence**
ID-4.i	Disclosure: restricted information disclosed only with the institution's formal permission, and secret and top secret information only with the proper approvals. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-6 Access Agreements, AC-21 Information Sharing.	**Organisational evidence**
ID-4.j	Reporting a breach or leak: the CBI informed directly by official letter or email with the facts and type of event; for top secret information, an urgent confidential notice and a letter stating what was leaked. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
ID-4.k	Physical transport: restricted information encrypted on flash storage when travelling; permission to carry secret information; travel media holding top secret information destroyed and recorded in an approved register. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-5 Media Transport.	**Organisational evidence**

ID-4.I	Portable devices: classified information carried on travel kept on external storage registered to the employee, never opened on a public device; top secret information never created, moved, processed or stored on portable devices. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-19 Access Control for Mobile Devices, MP-7 Media Use.	**Organisational evidence**

PR Protect

PR-1 1. Endpoint Controls

PR-1.1 1.1 Desktop and Laptop Security Controls

PR-1.1.1	Computers connected to an uninterruptible power supply to prevent damage to data and hardware. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-11 Emergency Power.	**Organisational evidence**
PR-1.1.2	Users lock their workstation before leaving it unattended, and it locks automatically under the institution's policy if they do not. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-11 Device Lock.	**Organisational evidence**
PR-1.1.3	Confidential or sensitive information stored on laptops encrypted. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-28(1) Cryptographic Protection, MP-5 Media Transport.	**Organisational evidence**
PR-1.1.4	Desktops, laptops and screens switched off at the end of each working day. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-11 Device Lock.	**Organisational evidence**
PR-1.1.5	Laptops and storage media holding sensitive information kept in a safe place or locked cabinet when not in use. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-4 Media Storage.	**Organisational evidence**
PR-1.1.6	Access to the USB ports of desktops and laptops controlled. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: MP-7 Media Use.	**Organisational evidence**
PR-1.1.7	Other media holding confidential data, such as paper, files and tapes, kept in a safe place or locked cabinet when not in use. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-4 Media Storage.	**Organisational evidence**
PR-1.1.8	Users do not install or download software or executable files on any desktop or laptop without prior permission. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-11 User-installed Software.	**Organisational evidence**

PR-1.1.9	Users do not write, compile, copy, spread, run or try to introduce code designed to replicate itself, cause damage or degrade a system, such as viruses or malware. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
PR-1.1.10	Any virus reported at once. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
PR-1.1.11	User identification and a password required to log on to every desktop and laptop at start-up or restart. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2(5) Individual Authentication with Group Authentication.	**Organisational evidence**
PR-1.1.12	Standard, approved antivirus software installed on every desktop and laptop, set to scan files on read and to scan the system routinely. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
PR-1.1.13	Desktops and laptops set to log every significant security event, such as password guessing, unauthorised log-on attempts and changes to applications or system software. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-2 Event Logging.	**Organisational evidence**
PR-1.1.14	Every computer placed above floor level and away from windows. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-18 Location of System Components.	**Organisational evidence**

PR-1.2 1.2 Server Security Controls

PR-1.2.1 Users given specific authorisation to access servers, with a defined set of privileges. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege.

Scope of this evidence The evidence concerns access to the cluster: the roles and bindings that grant privileges, the kubelet's authorisation, anonymous access refused, and service account tokens. Access to the institution's other servers is the institution's to evidence.

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

node.kubelet-authz	**Pass**	The kubelet authorises requests through the API server: so on all 1 node(s). Establishes: The kubelet authorises requests through the API server (Webhook mode).
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
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.

PR-1.2.2 An additional authentication mechanism to control users' remote access. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.

PR-1.2.3 An inactive session expires after a set period of inactivity. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-12 Session Termination, AC-11 Device Lock.

PR-1.2.4 System administrators' activities logged; servers holding sensitive and confidential data may send their activity logs to a central log host. **Fail**

Platform, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation, AU-4 Audit Log Storage Capacity.

Scope of this evidence The evidence is the API server's audit log, which records the requests of every authenticated user, administrators included, and the forwarding of the cluster's logs to a central store. Administrators' activity on the institution's other servers is the institution's to evidence.

Fails in Cluster log shipping.

cluster.log-forwarding	**Fail**	No log shipper runs on the cluster, so its logs stay on its nodes. Establishes: The cluster's logs leave its nodes and arrive: Fluent Bit sends them to a central store (an output with a host, or an s3 output with a bucket), and its own counters show records delivered there since the last run with no error, failed retry or dropped record; or another log shipper runs, which is named and whose destination the organisation evidences.
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.

PR-1.2.5 Test servers to test configuration settings, new updates and service packs before they are applied to production. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-4(1) Separate Test Environments.

Scope of this evidence The evidence is that each application namespace carries an environment label, so that test and production workloads are told apart. Test servers outside the cluster, and the testing itself, are the institution's to evidence.

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.

PR-1.2.6 File sharing secured, with file and print sharing disabled where not needed or kept to a minimum. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-7 Least Functionality.

PR-1.2.7 Every unnecessary service on a production server disabled, and no new service run on a production server without prior testing. **Incomplete**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-7 Least Functionality.

Scope of this evidence The evidence concerns the cluster's workloads and nodes: Pods that use the host's namespaces, ports or paths, Services on external addresses, and the nodes' host firewall. The services on the institution's other production servers, and the testing of new ones, are the institution's to evidence.

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.no-host-namespaces	**Pass**	Every object the policy judged passes it. Establishes: No Pod shares the host's network, process or IPC namespace, outside named namespaces.
policy.no-host-path	**Pass**	Every object the policy judged passes it. Establishes: No Pod mounts a host path, outside named namespaces.
policy.no-host-ports	**Pass**	Every object the policy judged passes it. Establishes: No container binds a host port, outside named namespaces.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.host-access	**Pass**	Every object outside the exempt namespaces passes. Establishes: Workloads that use the host's namespaces, paths or ports.

PR-1.2.8 Every unnecessary program uninstalled from production servers. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-7 Least Functionality.

PR-1.2.9 1.2.9 Virtualisation

PR-1.2.9.a A planned limit on the resources (processors, memory, disk space and virtual network interfaces) each virtual machine may use. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-6 Configuration Settings. Evidence counted: policy.resource-limits, trivy.limits; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence Read for containers: the evidence is that each workload declares its processor and memory requests and limits. Limits on the institution's virtual machines, and on disk space and network interfaces, are the institution's to evidence.

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

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.

PR-1.2.9.b Host and guest operating systems of virtual servers, and the virtualisation software, updated with new and required security updates. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SI-2 Flaw Remediation.

Scope of this evidence The evidence is that running images have no open critical or high vulnerabilities, with the age of open vulnerabilities and the platform's versions recorded. Updates to the hosts and hypervisors of the institution's virtual machines are the institution'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.

PR-1.2.9.c Virtual servers backed up regularly, as physical servers are. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup.

Scope of this evidence The evidence is that the cluster's volumes are backed up to a backup target on a schedule. Backups of the institution's virtual servers outside the cluster are the institution'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.

PR-1.2.9.d Host and guest virtual servers use synchronised time. **Not provided**

Platform, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AU-8 Time Stamps, SC-45 System Time Synchronization.

Scope of this evidence The evidence is that the cluster's nodes synchronise their clocks with configured time servers. The clocks of the institution's other hosts and guests are the institution's to evidence.

node.time-sync	**Not evaluated**	The platform names no time servers, so there is nothing to compare the nodes with. Establishes: Each node runs a time service configured with the servers the platform names.
platform.time-servers	**Not provided**	No time servers are set for the cluster; each node keeps its own. Establishes: The time servers each node synchronises with.

PR-1.2.9.e File sharing between host and guest operating systems not allowed unless needed. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-4 Information in Shared System Resources.

PR-2 2. Data Center Controls

PR-2.1 2.1 Physical Security

PR-2.1.1 Physical security applied to the data centre: entry restricted to authorised staff on a need basis, and revoked at once when no longer needed. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control.

PR-2.1.2 Entry authorisation applied strictly to vendors, service providers, support staff and cleaners, with visitors always escorted by an authorised employee. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control, PE-8 Visitor Access Records.

PR-2.1.3 The list of people authorised to enter the data centre kept and reviewed periodically. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-2 Physical Access Authorizations.

PR-2.1.4 Every physical entry to sensitive areas recorded with its purpose. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-8 Visitor Access Records.

PR-2.1.5 The perimeter, building and equipment room secured and monitored, with physical, human and procedural controls around the clock, such as guards, card entry and surveillance. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control, PE-6 Monitoring Physical Access.

PR-2.1.6 The emergency exit door available. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-12 Emergency Lighting.

PR-2.1.7	A named custodian or manager of the data centre, responsible for authorisation and for compliance with the policy. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-2 Physical Access Authorizations.	**Organisational evidence**
PR-2.1.8	An inventory of all technical and related equipment and consumables in the data centre, kept by the manager or a delegate. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-8 System Component Inventory.	**Organisational evidence**
PR-2.1.9	Where an external supplier runs the data centre, the contract requires compliance with the physical security policy and keeps the institution's right to review physical security at any time. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, PE-3 Physical Access Control.	**Organisational evidence**
PR-2.1.10	Where an external supplier runs the facility, physical security is the supplier's, but access to the dedicated facilities is reviewed and authorised by the institution. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, PE-2 Physical Access Authorizations.	**Organisational evidence**

PR-2.2 2.2 Environmental Security

PR-2.2.1	The data centre designed and protected against fire, flood, explosion and other disasters; a data centre or disaster recovery site in a multi-tenant building is advised against. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13 Fire Protection, PE-15 Water Damage Protection, PE-23 Facility Location.	**Organisational evidence**
PR-2.2.2	The data centre layout, including power and network connections, properly documented. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-9 Power Equipment and Cabling, PL-2 System Security and Privacy Plans.	**Organisational evidence**

PR-2.2.3 Development and test environments separated from production. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-4(1) Separate Test Environments, AC-4 Information Flow Enforcement.

Scope of this evidence The evidence is that each application namespace carries an environment label and has network policies governing its traffic, each of which selects workloads. Separate physical environments, and environments outside the cluster, are the institution's to evidence.

Fails in Namespace payments.

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.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

PR-2.2.4 Separate conduits for data and power cables, to prevent interference or damage. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-4 Access Control for Transmission, PE-9 Power Equipment and Cabling.

PR-2.2.5 Water detectors under a raised floor, where there is one. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-15 Water Damage Protection.

PR-2.2.6 No unrelated or out-of-service equipment stored in the data centre, with a separate store for unused and spare IT equipment. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-16 Delivery and Removal.

PR-2.2.7 Closed-circuit television cameras installed in suitable places covering every direction. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-6 Monitoring Physical Access.

PR-2.2.8 A sign forbidding eating, drinking and smoking. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13 Fire Protection.

PR-2.2.9 Dedicated emergency vehicles always on site, and public transport avoided when moving critical equipment off the premises. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-16 Delivery and Removal, MP-5 Media Transport.

PR-2.2.10	A dedicated telephone line for the data centre. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-8 Telecommunications Services.	**Organisational evidence**
PR-2.2.11	The addresses and telephone numbers of everyone who may need to be contacted in an emergency (fire service, police, providers, vendors, all IT staff) available. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, IR-8 Incident Response Plan.	**Organisational evidence**
PR-2.2.12	The power supply and other support units separated from the production site and placed in a secure area. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-9 Power Equipment and Cabling, PE-11 Emergency Power.	**Organisational evidence**
PR-2.2.13	Power from the main distributor or generator dedicated to the data centre, with its outlets restricted from other equipment and monitored against overload. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-9 Power Equipment and Cabling.	**Organisational evidence**
PR-2.2.14	Environmental controls installed: uninterruptible power with redundant units, a backup power source, temperature and humidity meters, water leak alarms, air conditioning with redundant units, emergency power cut-off switches, emergency lighting, regularly tested dehumidifiers, and a maintenance contract covering 24 hours a day, 7 days a week. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-10 Emergency Shutoff, PE-11 Emergency Power, PE-12 Emergency Lighting, PE-14 Environmental Controls, PE-15 Water Damage Protection.	**Organisational evidence**

PR-2.3 2.3 Fire Prevention

PR-2.3.1	The data centre's walls, ceiling and door fire-resistant. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13 Fire Protection.	**Organisational evidence**
PR-2.3.2	Fire suppression equipment installed and tested periodically. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13(2) Suppression Systems — Automatic Activation and Notification.	**Organisational evidence**
PR-2.3.3	An automatic fire and smoke alarm installed and tested periodically. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13(1) Detection Systems — Automatic Activation and Notification.	**Organisational evidence**
PR-2.3.4	Fire detectors under a raised floor, where there is one, and above the false ceiling. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13(1) Detection Systems — Automatic Activation and Notification.	**Organisational evidence**
PR-2.3.5	The quality of power and data cables in the data centre maintained, and the cables concealed. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-4 Access Control for Transmission, PE-9 Power Equipment and Cabling.	**Organisational evidence**

PR-2.3.6	No combustible materials such as paper, wood or plastic stored in the data centre. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13 Fire Protection.	**Organisational evidence**

PR-2.4 2.4 Servers, Network Room and Rack Controls

PR-2.4.1	Racks with lockable glass doors, their keys held by a responsible employee. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
PR-2.4.2	Physical access to the server room restricted, with a visitor log kept. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control, PE-8 Visitor Access Records.	**Organisational evidence**
PR-2.4.3	The list of people authorised to enter kept and reviewed regularly. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-2 Physical Access Authorizations.	**Organisational evidence**
PR-2.4.4	Procedures to replace servers and network devices as quickly as possible after a disaster. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
PR-2.4.5	A power generator to keep operating during a power cut. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-11(1) Alternate Power Supply — Minimal Operational Capability.	**Organisational evidence**
PR-2.4.6	An uninterruptible power supply for the servers and devices that need it. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-11 Emergency Power.	**Organisational evidence**
PR-2.4.7	Care taken to avoid overloading power outlets that feed many devices. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-9 Power Equipment and Cabling.	**Organisational evidence**
PR-2.4.8	A conduit so that power and data cables are connected tidily and safely. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-4 Access Control for Transmission, PE-9 Power Equipment and Cabling.	**Organisational evidence**
PR-2.4.9	The addresses and telephone numbers of everyone who may need to be contacted in an emergency available. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, IR-8 Incident Response Plan.	**Organisational evidence**
PR-2.4.10	A fire extinguisher in a visible place outside the server room, maintained and inspected every year. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-13 Fire Protection.	**Organisational evidence**

PR-3 3. Network Security Management

PR-3.1 3.1 Local Area Network Control Guidelines

PR-3.1.1 Baseline standards for the security of operating systems, databases, network equipment and mobile devices, consistent with the institution's policy. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-6 Configuration Settings.

Scope of this evidence The evidence is the cluster's configuration against its baseline: Pod Security, control-plane TLS, the service mesh, the kubelet's hardening, file permissions on the nodes, etcd's data directory, containers running as root, seccomp and resource limits. Baselines for operating systems, databases, network equipment and mobile devices outside the cluster are the institution's to evidence.

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

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.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.
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.

PR-3.1.2 Regular checks that the baseline standards are applied uniformly, with non-compliance found and raised for investigation. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-6 Configuration Settings.

Scope of this evidence Each run checks the cluster's configuration against its baseline and reports every departure. Checks of the institution's systems outside the cluster, and the investigation of what is found, are the institution's to evidence.

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

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.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.
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.

PR-3.1.3 Network design and its security configuration carried out under a documented plan, with distinct security zones defined. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection.

Scope of this evidence The evidence concerns traffic into and within the cluster: NetworkPolicies that deny by default in each namespace, the nodes' host firewall, and Services exposed on external addresses. The documented network plan, and security zones outside the cluster, are the institution'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.

PR-3.1.4 Every cable, including UTP, fibre and power, labelled for corrective or preventive maintenance. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-4 Access Control for Transmission.

PR-3.1.5 The physical security of all network equipment ensured. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control, PE-4 Access Control for Transmission.

PR-3.1.6 Groups of information services, users and information systems separated on the network, for example with VLANs. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-4 Information Flow Enforcement, SC-7 Boundary Protection.

Scope of this evidence The evidence is that each namespace's traffic is governed by NetworkPolicies that deny by default and select workloads, and that the nodes' host firewall is active. Separation on the institution's networks outside the cluster is the institution'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.

PR-3.1.7 Unauthorised access and change strictly controlled, with a mechanism to encrypt and decrypt sensitive data crossing the wide area network or a public network. **Incomplete**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, CM-6 Configuration Settings. Evidence counted: platform.control-plane-tls, platform.mesh-cni, policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is TLS on the Kubernetes control plane, TLS on Ingresses, and the service mesh that encrypts traffic between Pods. The Controls name no algorithm, so this verdict does not state that any algorithm is approved. Encryption on the institution's wide area and public network links is the institution'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.
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.
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.

PR-3.1.8 Network security devices, such as firewalls and intrusion detection and prevention systems, at the critical levels of the IT infrastructure to protect the network perimeter. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection, SI-4 System Monitoring.

PR-3.1.9 Firewalls and other security layers inside the internal networks, to limit the effect of exposures from external parties and systems and from the trusted internal network. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection.

Scope of this evidence The evidence concerns the cluster: NetworkPolicies that deny by default in each namespace, the nodes' host firewall, and Services exposed on external addresses. Firewalls in the institution's internal networks outside the cluster are the institution'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.

PR-3.1.10 Secure log-in, such as SSH, enabled on network devices for remote administration, and any unencrypted log-in, such as Telnet, disabled. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-17(2) Protection of Confidentiality and Integrity Using Encryption.

PR-3.1.11 The rules on network security devices backed up and reviewed regularly to confirm they are still appropriate. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection, CM-6 Configuration Settings.

PR-3.1.12 Backup communication channels for external wide area network connectivity. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CP-8 Telecommunications Services.

PR-3.1.13 An institution with a wireless LAN aware of its risks, with secure protocols between access points and wireless users. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-18 Wireless Access.

PR-3.1.14 Syslog servers may be set up, depending on the size of the network, to monitor the logs and events of network devices. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting.

PR-3.1.15 Authentication, authorisation and accounting (AAA) servers may be set up, depending on the size of the network, to manage network devices. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-3 Device Identification and Authentication.

PR-3.1.16 Role-based or time-based access control lists on routers to control the flow of data within the network. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-4 Information Flow Enforcement.

PR-3.1.17 A real-time monitoring system may be applied to watch all network equipment and servers. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-4 System Monitoring.

PR-3.1.18 Connection of personal laptops, or other personal wireless devices, to the office network or to the institution's computers restricted and secured. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems.

PR-3.1.19 Every default password of network devices changed. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.

PR-3.1.20 Every unused port of network access devices closed. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-7 Least Functionality. Evidence counted: policy.no-host-ports, trivy.external-ip; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence Read for the cluster: the evidence is that no Pod binds a port on its node and that no Service is exposed on an external address. Unused ports on the institution's switches and other network access devices are the institution's to evidence.

policy.no-host-ports	**Pass**	Every object the policy judged passes it. Establishes: No container binds a host port, outside named namespaces.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.

PR-3.1.21	Role-based administration of servers.	**Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-6 Least Privilege.

Scope of this evidence The evidence is the cluster's role-based access control: roles and bindings that grant broad privileges or exec into Pods, and service account tokens. Role-based administration of the institution's other servers is the institution's to evidence.

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.

PR-4 4. ATM and POS Transactions

PR-4.1	Anti-skimming solutions on ATMs to detect unknown devices placed over or near the card slot.	**Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control.

PR-4.2	Detection mechanisms that alert the appropriate staff to respond.	**Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-4 System Monitoring.

PR-4.3	Tamper-resistant keypads.	**Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control.

PR-4.4	Measures to prevent shoulder surfing of customers' PINs.	**Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-18 Location of System Components.

PR-4.5	Biometric finger-vein sensing may be applied to prevent PIN compromise.	**Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).

PR-4.6	Video surveillance of the machines 24 hours a day, with footage of good quality kept for at least one year.	**Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-6 Monitoring Physical Access.

PR-4.7	Adequate physical security measures at ATMs verified.	**Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control.

PR-4.8	All ATMs and POS devices inspected frequently for standard practices (environment, anti-skimming devices, tampering), with the verification record kept centrally and on site. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-3 Physical Access Control, CA-7 Continuous Monitoring.	**Organisational evidence**
PR-4.9	The activities of third-party cash replenishment suppliers monitored continuously, and their cash sorting centres visited regularly. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
PR-4.10	Merchants trained and given documentation on the security practices for handling POS devices, such as signature checks, tampering or replacement attempts and changing default passwords. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
PR-4.11	Customers made aware of the security measures they must follow in ATM and POS transactions. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

PR-5 5. Malicious Code Protection

PR-5.1	Servers and end-user devices protected from malware with approved endpoint protection installed. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
PR-5.2	Users aware of the arrangements to prevent and detect the introduction of malware. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
PR-5.3	Software and data supporting critical business activities scanned regularly for malicious code. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
PR-5.4	Files received on electronic media or from unknown networks scanned for malware before use. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
PR-5.5	Email attachments scanned for malicious code before use. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection, SI-8 Spam Protection.	**Organisational evidence**
PR-5.6	Antivirus definitions updated by an automated, timely process. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**

PR-5.7	Every computer on the network receives updated antivirus signatures automatically from a dedicated server. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
PR-5.8	Automatic virus protection enabled to scan storage units, discs and other media. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
PR-5.9	Staff aware of virus hoaxes and do not forward them. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
PR-5.10	Processes to manage malicious code attacks include procedures to report them and recover from them. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-4 Incident Handling, IR-6 Incident Reporting.	**Organisational evidence**
PR-5.11	An awareness programme on computer viruses and their prevention may be organised for end users. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

PR-6 6. Internet Access Management

PR-6.1	Staff given internet access under the approved internet access policy. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-1 Policy and Procedures, PL-4 Rules of Behavior.	**Organisational evidence**
PR-6.2	Internet access and use from the institution's premises secure, without putting its information security at risk. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
PR-6.3	Internet access from the institution's premises and systems routed through secure gateways. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-7(8) Route Traffic to Authenticated Proxy Servers.	**Organisational evidence**
PR-6.4	Any direct local internet connection from the institution's premises or systems, desktops and laptops included, prohibited unless information security approves it. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection, AC-20 Use of External Systems.	**Organisational evidence**
PR-6.5	Staff prohibited from setting up their own internet connection using the institution's systems or premises. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-20 Use of External Systems.	**Organisational evidence**
PR-6.6	Internet access provided by the institution not used for business that is not the institution's, or for the personal business of staff or others. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**

PR-6.7	Internet access provided by the institution not used for any activity that knowingly breaks a law, with disciplinary action for any such activity. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior, PS-8 Personnel Sanctions.	**Organisational evidence**
PR-6.8	Every application and system that connects to the internet, third-party or public networks subject to a formal risk analysis during development and before production use, with all required security mechanisms in place. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**

PR-7 7. Email Management

PR-7.1	The email system used under the institution's policy. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
PR-7.2	Access to the email system only on a formal request. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management.	**Organisational evidence**
PR-7.3	Confidential information sent to external parties by email only when encrypted with approved encryption. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-8(1) Cryptographic Protection.	**Organisational evidence**
PR-7.4	Staff consider the confidentiality and sensitivity of email content before forwarding or replying to external parties. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
PR-7.5	Email not defamatory, offensive, racially abusive or harmful to the institution's reputation or to anyone, with disciplinary action for deliberate sending. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
PR-7.6	The email system provided mainly for work, with personal use only at management's discretion and with permission, which may be withdrawn. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
PR-7.7	The institution's email address not used on social networks, blogs, groups or forums without management's approval. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4(1) Social Media and External Site/Application Usage Restrictions.	**Organisational evidence**
PR-7.8	Every email sent to external domains carries a disclaimer protecting the confidentiality of its content. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**

PR-7.9 Email services reviewed and monitored regularly by the department concerned. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-4 System Monitoring, SI-8 Spam Protection.

PR-7.10 Staff careful opening attachments from unknown senders. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.

PR-8 8. Identity and Access Control of Information Systems

PR-8.1 8.1 User Access Management

PR-8.1.1 Users given access to IT systems and networks only on a need-to-use basis, and only for the period it is needed. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-6 Least Privilege.

Scope of this evidence The evidence concerns the cluster: roles and bindings that grant broad privileges or exec into Pods, and service account tokens. Access to the institution's other systems and networks, and its time limits, are the institution's to evidence.

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.

PR-8.1.2 Non-employees (contractors, external staff, vendor staff) closely monitored with respect to access restrictions. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-7 External Personnel Security.

PR-8.1.3 Every user has a unique user ID and a valid password. **Incomplete**

Platform, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).

Scope of this evidence The evidence is that users sign in to the cluster through an identity provider, that anonymous requests are refused, and that the kubelet authenticates its callers. Unique IDs in the institution's other systems, and the passwords the identity provider holds, are the institution's to evidence.

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.

PR-8.1.4 The user ID form, with its access privileges, approved by the competent authority. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management.

PR-8.1.5 User access disabled after unsuccessful log-in attempts. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-7 Unsuccessful Logon Attempts.

PR-8.1.6 User access privileges kept up to date with every change in the user's employment status. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management, PS-5 Personnel Transfer.

PR-8.1.7 User log-ins uniquely identified and recorded for audit and review. **Incomplete**

Platform, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), AU-2 Event Logging, AU-3 Content of Audit Records, AU-9 Protection of Audit Information.

Scope of this evidence The evidence is that users sign in to the cluster through an identity provider and that anonymous requests are refused, and the API server's audit log, with the user, time and source of each request, kept with restricted permissions on the control-plane nodes. Log-ins to the institution's other systems are the institution'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.
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.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.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.

PR-8.1.8	Regular reviews of user access privileges to confirm they are appropriate. Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-6(7) Review of User Privileges. **Scope of this evidence** The roles and bindings that grant access to the cluster are recorded at every run, for the review. The review itself, and access to the institution's other systems, are the institution'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.	**Recorded**

PR-8.2 8.2 Password Management

PR-8.2.1	Strong password controls enforced on user log-in. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-8.2.2	Password controls include a change of password at first log-in. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-8.2.3	A minimum password length kept under the institution's policy, at least 8 characters. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-8.2.4	Passwords combine at least three of upper-case letters, lower-case letters, special characters and digits. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-8.2.5	A maximum password age no longer than the institution's policy allows, at most 90 days. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-8.2.6	The maximum number of invalid log-in attempts set under the institution's policy, at most 3 in a row. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-7 Unsuccessful Logon Attempts.	**Organisational evidence**
PR-8.2.7	A password history kept so that a password can be reused only after at least three others. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-8.2.8	Administrative passwords of operating systems, databases and business applications kept in a sealed envelope in a safe place. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**

PR-8.2.9	Staff access revoked on retirement, resignation or termination. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-4 Personnel Termination.	**Organisational evidence**

PR-8.3 8.3 Data Input Control

PR-8.3.1	A session time-out set for users under the institution's policy. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-12 Session Termination.	**Organisational evidence**
PR-8.3.2	A schedule of the times users may enter data in banking applications, under the regulations unless the competent authority allows otherwise. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-2(11) Usage Conditions.	**Organisational evidence**
PR-8.3.3	An audit trail with the user ID and a date and time stamp kept for every data entry, deletion and change. Platform, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AU-3 Content of Audit Records, AU-12 Audit Record Generation. **Scope of this evidence** The evidence is the API server's audit log, which records the user, verb, object and time of every change made through the Kubernetes API. Audit trails of data entered in banking applications are the institution'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.	**Pass**
PR-8.3.4	The software does not let the same user both enter and check the same transaction, unless the competent authority allows it in critical cases. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-5 Separation of Duties.	**Organisational evidence**
PR-8.3.5	Management approval obtained for delegating authority. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-5 Separation of Duties.	**Organisational evidence**
PR-8.3.6	Access to sensitive data and fields of banking applications restricted. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement.	**Organisational evidence**

PR-8.4 8.4 Privileged Access Management (PAM)

PR-8.4.1	Strict selection criteria and thorough screening for staff appointed to critical operations and security functions. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-3 Personnel Screening.	**Organisational evidence**
PR-8.4.2.a	Privileged users: strong authentication mechanisms. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts.	**Organisational evidence**

PR-8.4.2.b Privileged users: strong controls on remote access. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-17 Remote Access.

PR-8.4.2.c Privileged users: their number limited. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-6(5) Privileged Accounts. Evidence counted: trivy.rbac-privilege; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is the cluster's roles and bindings that grant broad privileges. The number of privileged users in the institution's other systems is the institution's to evidence.

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

trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

PR-8.4.2.d Privileged users: privileged access granted on a need-to-access basis. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-6 Least Privilege.

Scope of this evidence The evidence concerns the cluster: roles and bindings that grant broad privileges or exec into Pods, and service account tokens. Privileged access to the institution's other systems is the institution's to evidence.

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.

PR-8.4.2.e Privileged users: their activities reviewed in good time. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, AC-6(9) Log Use of Privileged Functions.

PR-8.4.2.f Privileged users: sharing of privileged accounts prohibited. **Incomplete**

Platform, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).

Scope of this evidence The evidence is that each user signs in to the cluster individually through an identity provider, that anonymous requests are refused, and that the kubelet authenticates its callers. Whether a privileged account is shared, in the cluster's identity provider or in other systems, is the institution's to evidence.

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.

PR-9 9. Patch Management

PR-9.1a Patch management procedures that identify, classify and prioritise security patches, with a timeframe set for applying each class of security patch. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SI-2 Flaw Remediation.

Scope of this evidence The evidence is that running images have no open critical or high vulnerabilities, with the age of open vulnerabilities by severity and the platform's versions recorded. The classes and their timeframes are the institution's own and are not judged here; patching outside the cluster is the institution'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.

PR-9.1b	Security patches tested thoroughly before they are applied in production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-4(1) Separate Test Environments, SI-2 Flaw Remediation.	**Organisational evidence**

PR-10 10. IT Service Delivery Management

PR-10.1 10.1 Change Management

PR-10.1.1	Changes to information processing facilities and systems controlled. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
PR-10.1.2	A business requirements document (BRD) covering the requirements of a system change and its effect on operations, the security matrix, reporting and interfaces. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control, SA-4 Acquisition Process.	**Organisational evidence**
PR-10.1.3	Every change to a business application in production goes through a formal, documented process with the details of the change. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
PR-10.1.4	Audit records kept for business applications. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-12 Audit Record Generation.	**Organisational evidence**
PR-10.1.5	A recovery plan for unexpected events. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
PR-10.1.6	User acceptance testing of application changes and updates before they are implemented. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
PR-10.1.7	User verification testing may be carried out after implementation. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-4(2) Verification of Controls.	**Organisational evidence**

PR-11 11. Mobile Financial Services

PR-11.1	Security standards followed in proportion to the complexity of the mobile services offered. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
PR-11.2	The risks of each type of mobile service identified clearly in the risk management process. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

PR-11.3	Measures to reduce risk, such as transaction limits, limits on transaction frequency, fraud checks and anti-money-laundering checks, unless the regulator provides otherwise. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
PR-11.4	Mobile services consistent with the security principles and practices of transaction authentication. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2(8) Access to Accounts — Replay Resistant.	**Organisational evidence**
PR-11.5	Periodic risk analysis and security assessment of mobile financial service operations, with measures taken accordingly. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment, CA-2 Control Assessments.	**Organisational evidence**
PR-11.6	Compliance with the state's regulatory compliance requirements. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
PR-11.7	The security practices, guidelines, methods and procedures of these mobile services documented and kept up to date. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-5 System Documentation.	**Organisational evidence**

PR-12 12. Database Security

PR-12.1 12.1 General Statements

PR-12.1.1	The institution's database management systems identified and documented, in an environment that protects them from operational and environmental risks. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-8 System Component Inventory, PE-14 Environmental Controls.	**Organisational evidence**
PR-12.1.2	Technical security standards for the database management systems developed and applied by the database administrators. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
PR-12.1.3	Direct access to a database limited to database administrators; other users reach it only through applications. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege.	**Organisational evidence**
PR-12.1.4	Database access granted under the identity and access management policy. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management.	**Organisational evidence**

PR-12.1.5	Migrating or moving the database of a critical system from production to any other environment prohibited. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-4 Information Flow Enforcement, CM-4(1) Separate Test Environments.	**Organisational evidence**

PR-12.2 12.2 DBMS Hosting Security Requirements

PR-12.2.1	For a hosted database management system, the business continuity and disaster recovery requirements set out clearly in the hosting contract, with each party's roles for backups, incident response and the recovery plan. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, CP-2 Contingency Plan.	**Organisational evidence**
PR-12.2.2	The institution's databases logically separated from other hosted databases. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-4 Information in Shared System Resources, SA-9 External System Services.	**Organisational evidence**
PR-12.2.3	Administrators' access to the database management system secured and encrypted with a strong mechanism such as SSH, VPN or SSL/TLS, under the institution's encryption policy. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-17(2) Protection of Confidentiality and Integrity Using Encryption.	**Organisational evidence**

PR-12.3 12.3 DBMS Change Management Requirements

PR-12.3.1	Changes to the database management system, such as migration into production, follow the institution's change management process. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
PR-12.3.2	The database management system updated under the institution's patch management policy. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-2 Flaw Remediation.	**Organisational evidence**
PR-12.3.3	Only licensed and authorised database management systems used. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-10 Software Usage Restrictions.	**Organisational evidence**
PR-12.3.4	A disaster recovery plan and procedures for the database management system. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
PR-12.3.5	Service level agreements kept with the vendors of the production database management systems. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**

PR-12.3.6	Stored databases encrypted under the institution's encryption and classification policies. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-28 Protection of Information at Rest, SC-28(1) Cryptographic Protection.	**Organisational evidence**

PR-12.4 12.4 DBMS Event Logs Monitoring

PR-12.4.1	Database management system event logs enabled and kept under the institution's security event log management and monitoring policy. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-2 Event Logging, SI-12 Information Management and Retention.	**Organisational evidence**
PR-12.4.2	The database event logs of critical systems and user behaviour monitored. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, SI-4 System Monitoring.	**Organisational evidence**
PR-12.4.3	The event logs and behaviour of the database administrators of critical systems monitored and reviewed regularly. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, AC-6(9) Log Use of Privileged Functions.	**Organisational evidence**

PR-12.5 12.5 Operational Requirements

PR-12.5.1	Suitable operational conditions for databases, such as a secure environment and physical access restricted to authorised staff. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control.	**Organisational evidence**
PR-12.5.2	The operational components of databases monitored by IT for performance, availability and storage capacity. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AU-5 Response to Audit Logging Process Failures, SI-4 System Monitoring.	**Organisational evidence**

PR-12.6 12.6 Other Requirements

PR-12.6.1	Key performance indicators used for continual improvement of database security. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**
PR-12.6.2	The cybersecurity requirements for database management systems reviewed at least once a year, or when the relevant legal and regulatory requirements change. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures.	**Organisational evidence**

PR-13 13. Third Party Security

PR-13.1 13.1 General Statement

PR-13.1.1	Standard, approved procedures documented for managing relationships with third parties before, during and after the contract. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, SR-1 Policy and Procedures.	**Organisational evidence**
PR-13.1.2	Third-party service providers chosen carefully under the institution's policies, its procedures and the relevant legal and regulatory requirements. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SR-5 Acquisition Strategies, Tools, and Methods, SA-9 External System Services.	**Organisational evidence**
PR-13.1.3	Risk assessments of third parties and their services, through review of their projects in the institution and periodic review of their security event logs, where they exist, before and during the contract. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SR-6 Supplier Assessments and Reviews, RA-3(1) Supply Chain Risk Assessment.	**Organisational evidence**
PR-13.1.4	Contracts and agreements with third parties commit them to the institution's cybersecurity requirements and policies and to the relevant legal and regulatory requirements. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**
PR-13.1.5	Contracts and agreements with third parties reviewed so that their terms bind during the agreement and the third party is legally liable for any breach. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
PR-13.1.6	Contracts and agreements include non-disclosure terms and the secure deletion of the institution's information by the third party at the end of the service. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-6 Access Agreements, SA-9 External System Services.	**Organisational evidence**
PR-13.1.7	Third-party cybersecurity requirements reviewed periodically. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
PR-13.1.8	The cybersecurity risk management policy reviewed every year, with changes documented and approved. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-1 Policy and Procedures, PM-9 Risk Management Strategy.	**Organisational evidence**

PR-13.2 13.2 Cybersecurity Requirements for IT Outsourcing and Third-Party Managed Services

PR-13.2.1.1	Outsourcing: a cybersecurity risk assessment and the control activities carried out before contracts with third parties are signed, and on relevant changes in requirements, laws and regulations. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SR-6 Supplier Assessments and Reviews, RA-3(1) Supply Chain Risk Assessment.	**Organisational evidence**
PR-13.2.1.2	Outsourcing: services for critical information and technology assets consistent with the relevant legal and regulatory requirements. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
PR-13.2.2.1	Third-party personnel: external companies, outsourced and managed service staff, and staff working on critical systems vetted and screened. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-3 Personnel Screening, PS-7 External Personnel Security.	**Organisational evidence**
PR-13.2.2.2	Third-party personnel: cybersecurity responsibilities and non-disclosure terms in their contracts, in force during and after the working relationship. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-6 Access Agreements, PS-7 External Personnel Security.	**Organisational evidence**
PR-13.2.3.1	Third-party access: a formal, documented process to grant and revoke access to every system that processes, transmits or stores the institution's information. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management, PS-7 External Personnel Security.	**Organisational evidence**
PR-13.2.3.2	Third-party access: access to and processing of the institution's information provided in a secure, controlled way. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement, SA-9 External System Services.	**Organisational evidence**
PR-13.2.3.3	Third-party access: password controls applied to every user with access to the institution's information. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
PR-13.2.3.4	Third-party access: multi-factor authentication for access to critical systems that process, transmit or store the institution's information. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.	**Organisational evidence**
PR-13.2.3.5	Third-party access: access rights revoked when a third-party employee leaves, or when a change of role ends the need for access. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PS-4 Personnel Termination, PS-7 External Personnel Security.	**Organisational evidence**

PR-13.2.3.6	Third-party access: access rights reviewed regularly by the third party under the institution's cybersecurity policies. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-6(7) Review of User Privileges, PS-7 External Personnel Security.	**Organisational evidence**
PR-13.2.3.7	Third-party access: all audit records stored, kept and made available on the institution's request. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, SI-12 Information Management and Retention.	**Organisational evidence**

PR-14 14. Application Security

PR-14.1 14.1 Web Application Design and Architecture

PR-14.1.1	Important web applications, built or bought, follow a multi-tier architecture with at least three layers, such as presentation, business logic and database. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SC-2 Separation of System and User Functionality.	**Organisational evidence**
PR-14.1.2	Web applications use secure communication protocols only, such as HTTPS, SFTP and TLS. Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, CM-6 Configuration Settings. Evidence counted: platform.control-plane-tls, platform.mesh-cni, policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster. **Scope of this evidence** The evidence is TLS on the cluster's Ingresses and on its control plane, and the service mesh that encrypts traffic between Pods. The Controls name no algorithm, so this verdict does not state that any algorithm is approved. Protocols used by applications outside the cluster are the institution's to evidence.	**Incomplete**

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.
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.

PR-14.1.3	External web applications protected from external attack by a web application firewall (WAF). Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-7 Boundary Protection, SI-4 System Monitoring.	**Organisational evidence**

PR-14.1.4 Multi-factor authentication for every web application used by staff or customers and reachable over the internet. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.

PR-14.1.5 Web applications that transmit, process or store protected information do so securely with approved encryption tools and protocols, such as SFTP, FTPS and AS2. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection.

PR-14.1.6 Secure environments for development and testing, separated and isolated from production. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CM-4(1) Separate Test Environments, AC-4 Information Flow Enforcement.

Scope of this evidence The evidence is that each application namespace carries an environment label and has network policies governing its traffic, each of which selects workloads. Separate development and test environments outside the cluster are the institution's to evidence.

Fails in Namespace payments.

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.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

PR-14.1.7 Web applications use standard ports and services. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-7 Least Functionality.

PR-14.1.8 Web applications bought from external vendors meet the institution's requirements and cybersecurity policies. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-4 Acquisition Process.

PR-14.1.9 Developers use suitable security controls, such as operating system authentication, approved vendor software and encryption under the institution's encryption standard. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SA-15 Development Process, Standards, and Tools.

PR-14.1.10 Important web applications are recommended to take account of the controls and prevention techniques for the OWASP Top 10 application security risks. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.

PR-14.2 14.2 Restricted Access and Segregation of Duties

PR-14.2.1 Session management controls, including session authentication, log-out and time-out, defined and applied to every web application. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-12 Session Termination.

PR-14.2.2 Access to production systems limited and monitored according to job responsibilities. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AC-6 Least Privilege, AU-2 Event Logging.

Scope of this evidence The evidence concerns the cluster: roles and bindings that grant broad privileges or exec into Pods, service account tokens, and the API server's audit log. Access to the institution's other production systems is the institution's to evidence.

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

platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.
policy.no-default-token	**Pass**	Every object the policy judged passes it. Establishes: Pods say whether they mount a service account token, so that none receives one by default.
trivy.rbac-exec	**Pass**	Every object outside the exempt namespaces passes. Establishes: Roles that allow executing into Pods or impersonating privileged groups.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.
trivy.token-automount	**Pass**	Every object outside the exempt namespaces passes. Establishes: Pods that mount a service account token.

PR-14.2.3 Where important protected information is needed outside production, its protected elements removed, masked or deleted after use. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-3(2) Use of Live or Operational Data, PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research.

PR-14.2.4 The amount of important protected information used outside production limited to what testing needs. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research.

PR-14.2.5	Access to protected information in non-production environments restricted. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-3 Access Enforcement, PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research.	**Organisational evidence**
PR-14.2.6	Developers not allowed to change production source code or production data. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-5 Access Restrictions for Change, AC-5 Separation of Duties.	**Organisational evidence**
PR-14.2.7	Developers restricted from changing system settings unless approved. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-5 Access Restrictions for Change.	**Organisational evidence**
PR-14.2.8	Test accounts used outside production removed before the application moves to production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management, CM-3 Configuration Change Control.	**Organisational evidence**
PR-14.2.9	Test accounts and test data not allowed in production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-2 Account Management, PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research.	**Organisational evidence**
PR-14.2.10	Web application users warned of, and informed about, the secure use policy. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: AC-8 System Use Notification, PL-4 Rules of Behavior.	**Organisational evidence**

PR-14.3 14.3 Risk Management Requirements

PR-14.3.1	Risk assessments of web applications in development or bought, to set the controls that bring their risk within acceptable limits. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: RA-3 Risk Assessment, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
PR-14.3.2	Outsourced software development subject to the same risk assessment as in-house development. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-9 External System Services, RA-3 Risk Assessment.	**Organisational evidence**
PR-14.3.3	Web applications that rely on macro or scripting languages or third-party tools follow the approved change management process before installation in production. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**

PR-14.4 14.4 Web Application Testing

PR-14.4.1	Cybersecurity controls tested for conformity with the cybersecurity requirements before release to production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**

PR-14.4.2	The security features of new applications, or of significant changes to existing web applications, tested, documented and reviewed before promotion to production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation, CM-4 Impact Analyses.	**Organisational evidence**
PR-14.4.3	Web application security features and the results of security verification tests reviewed and treated with the application owners before installation. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
PR-14.4.4	Evidence of security verification tests documented and classified under the institution's data classification policy. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
PR-14.4.5	The evidence names who tested, the nature of the tests, their results and any remediation required or carried out. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
PR-14.4.6	Web application test data protected against unauthorised access to protected information. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-3(2) Use of Live or Operational Data, PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research.	**Organisational evidence**
PR-14.4.7	Web applications tested to confirm that segregation of duties controls work. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: AC-5 Separation of Duties, SA-11 Developer Testing and Evaluation.	**Organisational evidence**
PR-14.4.8	Web applications tested for vulnerabilities or updates before implementation in production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation, RA-5 Vulnerability Monitoring and Scanning.	**Organisational evidence**
PR-14.4.9	Vulnerability scans carried out, and the vulnerabilities found remediated, before a web application is implemented in production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SA-11 Developer Testing and Evaluation.	**Organisational evidence**
PR-14.4.10	New web applications, and those that have had a major update, scanned for vulnerabilities. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.	**Organisational evidence**
PR-14.4.11	Web applications given independent penetration tests periodically. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**

PR-14.4.12	The security controls of new in-house web applications reviewed and approved before implementation in production. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SA-11 Developer Testing and Evaluation, CA-6 Authorization.	**Organisational evidence**
PR-14.4.13	Existing web applications reassessed and reapproved after a major change or after a set period. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-6 Authorization, CA-2 Control Assessments.	**Organisational evidence**
PR-14.4.14	Every security issue found in source code security review fixed before implementation in production. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-11(1) Static Code Analysis, SA-11(4) Manual Code Reviews.	**Organisational evidence**

PR-14.5 14.5 Maintenance

PR-14.5.1	Every necessary update to a web application installed in good time under the institution's patch management policy. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-2 Flaw Remediation.	**Organisational evidence**
PR-14.5.2	Version control numbering used to show when updated releases were installed. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
PR-14.5.3	Every downtime request follows the change management process. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
PR-14.5.4	Web applications given source code and security reviews after major release changes or after a set period. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SA-11(4) Manual Code Reviews.	**Organisational evidence**
PR-14.5.5	Changes to configuration parameters within a web application tested where possible. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control, CM-4 Impact Analyses.	**Organisational evidence**
PR-14.5.6	Installations in production controlled to reduce the risk of disrupting production. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CM-3 Configuration Change Control, CM-5 Access Restrictions for Change.	**Organisational evidence**

PR-14.6 14.6 Disposal

PR-14.6.1	At the end of a web application's life, the equipment that hosted, developed or maintained it decommissioned under the asset management policy. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

PR-14.6.2	All data used or kept by a retired web application destroyed, or kept securely, as the asset management policy sets. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-6 Media Sanitization, SI-12 Information Management and Retention.	**Organisational evidence**
PR-14.6.3	The source code of a retired web application archived so that it can be retrieved if needed. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: SI-12 Information Management and Retention.	**Organisational evidence**

PR-14.7 14.7 Monitoring and Improvement

PR-14.7.1	The cybersecurity requirements for web applications reviewed periodically. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**

DE Detect

DE-1 1. Security Monitoring

DE-1.1	Security monitoring systems and processes for prompt detection of unauthorised or malicious activity by internal and external parties. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
DE-1.2	Network and security monitoring with network security devices, such as intrusion detection and prevention systems, that protect against network intrusion and alert when it happens. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-4 System Monitoring, SI-4(5) System-generated Alerts.	**Organisational evidence**
DE-1.3	Security monitoring tools may be used to detect changes to critical IT resources such as databases, system files, data and programs, to identify unauthorised changes. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity.	**Organisational evidence**

DE-1.4 The security logs of systems, applications and network devices reviewed regularly for anomalies, and the logs protected and kept for a set period to support later investigation. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: AU-4 Audit Log Storage Capacity, AU-9 Protection of Audit Information, AU-6 Audit Record Review, Analysis, and Reporting.

Scope of this evidence The evidence is that the API server's audit log is kept with restricted permissions on the control-plane nodes and forwarded with the cluster's logs to a central store. The review of the logs, the retention period, and the logs of systems outside the cluster are the institution's to evidence.

Fails in Cluster log shipping.

cluster.log-forwarding	**Fail**	No log shipper runs on the cluster, so its logs stay on its nodes. Establishes: The cluster's logs leave its nodes and arrive: Fluent Bit sends them to a central store (an output with a host, or an s3 output with a bucket), and its own counters show records delivered there since the last run with no error, failed retry or dropped record; or another log shipper runs, which is named and whose destination the organisation evidences.
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.

DE-1.5 Continuous real-time or near real-time monitoring to detect unknown and abnormal activity or incidents, such as a security operations centre (SOC), tested and maintained continuously. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: SI-4 System Monitoring, IR-4(14) Security Operations Center.

DE-2 2. Audits

DE-2.1 2.1 Internal Audits

DE-2.1.1 The internal audit of information systems carried out by the institution's internal audit department. **Organisational evidence**

Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.

DE-2.1.2	The internal audit of information systems carried out by staff with enough experience and skill in information systems audit. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
DE-2.1.3	An annual audit plan covering the main technology-based services and operations and the IT infrastructure, operational branches included. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
DE-2.1.4	The internal audit of information systems carried out at least once a year, its report kept for the regulators, and audit issues tracked, recorded, followed up and corrected. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-2 Control Assessments, CA-5 Plan of Action and Milestones.	**Organisational evidence**
DE-2.1.5	Suitable measures taken to treat the recommendations of external and internal audit reports. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**
DE-2.2	The cybersecurity of the institution's information assets subject to comprehensive, independent and regular information security audits. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CA-2(1) Independent Assessors, CA-7 Continuous Monitoring.	**Organisational evidence**

DE-2.3 2.3 Regulatory Compliance

DE-2.3.1	A process to ensure compliance with the regulatory requirements that affect cybersecurity, carried out periodically and when new regulatory requirements take effect. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring, CA-2 Control Assessments.	**Organisational evidence**
DE-2.3.2	The compliance process involves representatives of the institution's main areas. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
DE-2.3.3	The compliance process leads to updates of the cybersecurity policy, standards and procedures to take in any necessary changes. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PL-1 Policy and Procedures, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**

DE-2.4 2.4 Compliance with International Industry Standards

DE-2.4.1	Compliance with the Payment Card Industry Data Security Standard (PCI DSS), under the CBI's regulations and instructions. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**

DE-2.4.2	Compliance with the EMV technical standard (Europay, MasterCard, Visa), under the CBI's regulations and instructions. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
DE-2.4.3	Compliance with the SWIFT Customer Security Programme (CSP), under the CBI's regulations and instructions. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**

RS Respond

RS-1 1. Incident Management

RS-1.1	An incident management framework to restore normal IT services as quickly as possible with the least effect on operations, with the roles of the staff who record, analyse, treat and monitor incidents defined. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-1 Policy and Procedures, IR-8 Incident Response Plan.	**Organisational evidence**
RS-1.2	Incidents given the right severity; technical support may be delegated to set severity and is trained to recognise high-severity incidents; the criteria for severity set and documented. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-4 Incident Handling, IR-2 Incident Response Training.	**Organisational evidence**
RS-1.3	Escalation and resolution procedures, with resolution timeframes in proportion to severity. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-4 Incident Handling, IR-8 Incident Response Plan.	**Organisational evidence**
RS-1.4	The predefined escalation and response plan for security incidents tested periodically. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-3 Incident Response Testing.	**Organisational evidence**
RS-1.5	An IT emergency response team of internal staff with the technical and operational skills to handle incidents. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-7 Incident Response Assistance, IR-4(11) Integrated Incident Response Team.	**Organisational evidence**
RS-1.6	Senior management kept informed as a major incident develops so that the disaster recovery plan can be activated in time, and the CBI informed as soon as possible of any disaster. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-6 Incident Reporting, CP-2 Contingency Plan.	**Organisational evidence**
RS-1.7	Customers kept informed of any major incident. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-6 Incident Reporting, IR-7 Incident Response Assistance.	**Organisational evidence**

RS-1.8	Root cause and impact analysis of incidents that disrupt IT services, with corrective action to prevent similar incidents. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-4 Incident Handling, IR-4(4) Information Correlation.	**Organisational evidence**
RS-1.9	The root cause and impact analysis report covers the cause (when, where, why and how, recurrence, lessons), the impact (scope, size, losses, customers, reputation, regulatory breaches) and corrective and preventive measures, with every incident treated within its timeframe and monitored until resolved. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: IR-4 Incident Handling, IR-5 Incident Monitoring, IR-8 Incident Response Plan.	**Organisational evidence**

RS-2 2. Business Continuity and Disaster Recovery Management

RS-2.1 2.1 Business Continuity Plan (BCP)

RS-2.1.1	An approved business continuity plan that addresses disaster recovery so that the institution can continue to work. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
RS-2.1.2	The approved plan circulated to all stakeholders concerned, each receiving the amended plan after every change. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2(1) Coordinate with Related Plans.	**Organisational evidence**
RS-2.1.3	Business continuity documents kept in a secure place away from the main and alternate sites as well as at the main site, with one copy in the office for reference. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-6 Alternate Storage Site.	**Organisational evidence**
RS-2.1.4	The business continuity plan coordinated with and supported by the business impact analysis and the disaster recovery plan, considering system, operational and interdependency requirements. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2(1) Coordinate with Related Plans, RA-9 Criticality Analysis.	**Organisational evidence**
RS-2.1.5.a	The business continuity plan covers the action plan to restore operations. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
RS-2.1.5.b	The business continuity plan covers emergency contacts, with the addresses and telephone numbers of staff, vendors and agencies. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
RS-2.1.5.c	The business continuity plan lists items such as backups, laptops and portable storage media. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**

RS-2.1.5.d	The business continuity and disaster recovery plans tested and reviewed at least once a year. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-4 Contingency Plan Testing.	**Organisational evidence**

RS-2.2 2.2 Disaster Recovery Plan (DRP)

RS-2.2.1	An approved disaster recovery plan built on scenario analysis, covering major system outages from system, hardware, operating or security failures and the complete loss of the main data centre. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
RS-2.2.2	A disaster recovery site geographically separated from the main site, to restore critical systems and resume operations if the main site fails. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-7 Alternate Processing Site, CP-7(1) Separation from Primary Site.	**Organisational evidence**
RS-2.2.3	Where the disaster recovery site is not properly separated geographically, a third site in a different region may be set up as the far disaster recovery site, with the near site configured accordingly. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-7(1) Separation from Primary Site.	**Organisational evidence**
RS-2.2.4	The disaster recovery site and the near data centre equipped with compatible hardware and communications to support critical business services in a disaster. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-7 Alternate Processing Site, CP-8 Telecommunications Services.	**Organisational evidence**
RS-2.2.5	The physical and environmental security of the disaster recovery site and the near data centre maintained. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-7 Alternate Processing Site, PE-3 Physical Access Control.	**Organisational evidence**
RS-2.2.6	Priorities for system recovery and business resumption, with a recovery time objective (RTO) and recovery point objective (RPO) for IT systems and applications. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
RS-2.2.7	The interdependencies of critical systems considered in the recovery plan and in contingency tests. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-4 Contingency Plan Testing.	**Organisational evidence**
RS-2.2.8	Recovery strategies and technologies, such as on-site availability and real-time data replication, may be used to strengthen recovery capability. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2(5) Continue Mission and Business Functions, CP-9(6) Redundant Secondary System.	**Organisational evidence**

RS-2.2.9	Information security properly maintained throughout recovery. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-10(4) Restore Within Time Period, CP-2 Contingency Plan.	**Organisational evidence**
RS-2.2.10	An up-to-date, tested copy of the disaster recovery plan kept securely away from the main and alternate sites as well as at the main site, with one copy in the office for reference. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-2 Contingency Plan, CP-6 Alternate Storage Site.	**Organisational evidence**
RS-2.2.11	The disaster recovery arrangements, and the staff's ability to carry out emergency and recovery procedures, tested at least once a year. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-4 Contingency Plan Testing, CP-3 Contingency Training.	**Organisational evidence**
RS-2.2.12	Staff involved in designing and running comprehensive test cases that confirm the recovered systems work correctly. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-4 Contingency Plan Testing.	**Organisational evidence**
RS-2.2.13	Disaster recovery test documents include at least the scope, plan and results, with the test report sent to management and other stakeholders and kept. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-4 Contingency Plan Testing.	**Organisational evidence**

RS-3 3. Data Backup and Restore Management

RS-3.1	A data backup and restore policy, with a planned, scheduled and documented backup strategy for every business application, including online and offline backups moved to secure off-site storage. Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup. **Scope of this evidence** The evidence is that the cluster's volumes are backed up to a backup target on a schedule. The policy, the strategy for each business application, and off-site storage are the institution's to evidence. Fails in Cluster backups.	**Fail**

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.

RS-3.2 A detailed backup schedule for every business application, in line with its classification, stating the type of backup (full, partial, incremental, differential), with real-time monitoring of every detail of the schedule. **Fail**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup.

Scope of this evidence The evidence is that the cluster's volumes are backed up on a schedule and that recent backups completed. The schedule for each business application, its type and its monitoring are the institution'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.

RS-3.3 Backup frequency set in line with the information's classification and each application's business continuity requirements. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup.

RS-3.4 The schedule for each business application includes the retention period of backed-up or archived information, consistent with local legal and regulatory requirements. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup, SI-12 Information Management and Retention.

RS-3.5 All backup media labelled with their content, backup cycle, serial identifier and date. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: MP-3 Media Marking.

RS-3.6 Backup inventory documents and records kept, verified and signed by the person responsible. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup.

RS-3.7 Backup data on units or media holding sensitive or confidential information encrypted before it is moved off site. **Nothing to check**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: CP-9(8) Cryptographic Protection.

Scope of this evidence The evidence is that the cluster's volume backups are encrypted. Encryption of the institution's other backup media is the institution's to evidence.

cluster.backup-encryption	**Nothing to check**	Neither Longhorn nor Velero is installed, so no backup leaves the site. Establishes: Every backed-up Longhorn volume is encrypted, so that its backups leave the site encrypted.

RS-3.8 At least one backup copy kept on site for time-critical delivery. **Organisational evidence**

Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-9 System Backup.

RS-3.9	The process to restore information from on-site and off-site backup storage documented. Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CP-10 System Recovery and Reconstitution.	**Organisational evidence**
RS-3.10	Periodic tests of restoring from backups, assessing whether they are adequate and effective for the institution's recovery. Organisational, technical and non-technical. Controls (all banks and payment providers). NIST SP 800-53: CP-9(1) Testing for Reliability and Integrity, CP-4 Contingency Plan Testing.	**Organisational evidence**

AW Awareness

AW-1 1. Awareness Program

AW-1.1	The needs of the target audience identified, suitable budgets obtained and priorities set. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-1 Policy and Procedures, PM-3 Information Security and Privacy Resources.	**Organisational evidence**
AW-1.2	An action plan stating the main activities, with the resources, timelines and main objectives. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-1 Policy and Procedures, PM-13 Security and Privacy Workforce.	**Organisational evidence**
AW-1.3	Suitable content created and published. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
AW-1.4	The programme's common objectives: information on fraud risks and controls for those who need it, helping customers recognise fraud attempts and their responsibilities, encouraging good practice, a stronger security culture, and fewer and smaller incidents. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
AW-1.5	The right message delivered to the right audience through the most effective channels. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
AW-1.6	Awareness may take forms such as leaflets, text messages, safety tips, educational material, ATM and POS receipts, screensavers, electronic newsletters, case-study DVDs and recorded messages on hold. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
AW-1.7	More than one channel may be used to reach customers, such as print and television campaigns, ATM screens, email and text messages, a shared website, social media, online shops, billboards, online training, help lines and meetings with specialists. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

AW-1.8	A well-tested feedback strategy designed and put into effect, for continual improvement of the programme. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness, PM-6 Measures of Performance.	**Organisational evidence**

AW-2 2. Security Awareness and Training

AW-2.1	All staff concerned receive suitable training, education, updates and awareness on the cybersecurity activities of their roles. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
AW-2.2	A minimum of basic business training for IT staff. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
AW-2.3	Security awareness training or workshops for all staff. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
AW-2.4	Adequate training and awareness for the information systems audit team, taking account of new banking services and technical changes. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
AW-3	Customer education: customers equipped to bank safely by themselves, with awareness raised among customers and among other stakeholders, such as bank staff, law enforcement and the media. Organisational, non-technical. Controls (all banks and payment providers). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

TS Testing

TS-1 1. Vulnerability Assessment and Penetration Testing

TS-1.1 Vulnerability assessments carried out regularly to find security vulnerabilities in the IT environment. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

Scope of this evidence The evidence is that the cluster's running images are scanned for known vulnerabilities, that the scans are recent, and that no critical or high vulnerability is open, with the age of open vulnerabilities recorded. Vulnerability assessment of the rest of the IT environment is the institution'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.

TS-1.2 A mix of automated and manual techniques for a comprehensive vulnerability assessment, with common application vulnerabilities, such as SQL injection and cross-site scripting, in scope for application-based systems. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning. Evidence counted: cluster.scan-freshness, trivy.vulnerabilities; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is the automated scanning of the cluster's running images for known vulnerabilities, kept recent. Manual techniques and the assessment of application vulnerabilities such as SQL injection and cross-site scripting are the institution'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.
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.

TS-1.3 Processes to remediate the issues the vulnerability assessment finds, then validation that each vulnerability has been fully remediated. **Pass**

Checked, coverage partial. Controls (all banks and payment providers). NIST SP 800-53: SI-2 Flaw Remediation, RA-5 Vulnerability Monitoring and Scanning.

Scope of this evidence Each run rescans the cluster's images, so a remediated vulnerability no longer shows as open, and the age of open vulnerabilities is recorded. The remediation process, and remediation outside the cluster, are the institution'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.
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.

TS-1.4 Penetration tests that simulate real attacks for an in-depth assessment, run on the network infrastructure and internet-facing systems periodically or as needed. **Organisational evidence**

Organisational, technical, outside the cluster. Controls (all banks and payment providers). NIST SP 800-53: CA-8 Penetration Testing.

B2 Standard B2.1: Core Banking System

B2 B.1 An integrated suite of systems providing the critical functionalities, from reputable, internationally recognised providers. **Organisational evidence**

Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-4 Acquisition Process.

B2 B.2 Critical functionalities defined as the processes needed to deliver core products and services securely, compliantly and efficiently, with up-to-date access to data and, where possible, a single authoritative source for each data element. **Organisational evidence**

Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: PM-11 Mission and Business Process Definition, SA-8 Security and Privacy Engineering Principles.

B2 B.3 The systems fully integrated with the national and CBI-mandated platforms, such as RTGS, ACH, the National Switch, AML systems, the CBI reporting interfaces, SWIFT, the credit bureau, card networks, BSRS, the instant payment scheme and the government payments gateway. **Organisational evidence**

Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CA-3 Information Exchange, PM-14 Testing, Training, and Monitoring.

B2 B.4 Integrations with external systems follow ISO 20022 for payment messages, OpenAPI for APIs, and internationally recognised codes such as IBAN, BIC and ISIC. **Organisational evidence**

Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: SA-4 Acquisition Process, CA-3 Information Exchange.

B2 B.5 Well-structured data that can be exported for analytics, reporting, logging and archiving, following the BCBS 239 principles for risk reporting. **Organisational evidence**

Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SI-12 Information Management and Retention.

B2 B.6 A secure, isolated test environment where system upgrades and patches are tested before deployment to the live environment. **Fail**

Checked, coverage partial. Standards (private banks). NIST SP 800-53: CM-4(1) Separate Test Environments, AC-4 Information Flow Enforcement.

Scope of this evidence Where the system runs in the cluster, the evidence is that each application namespace carries an environment label and has network policies governing its traffic, each of which selects workloads. A test environment outside the cluster, and the testing of upgrades and patches, are the bank's to evidence.

Fails in Namespace payments.

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.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

B2 B.7 The systems support and enforce role-based access control for all users, in particular for sensitive operations. **Fail**

Checked, coverage partial. Standards (private banks). NIST SP 800-53: AC-6 Least Privilege.

Scope of this evidence The evidence concerns the Kubernetes cluster on which the systems run: roles and bindings that grant broad privileges or exec into Pods, and service account tokens. Role-based access control within the core banking system itself, for its users and operations, is the bank's to evidence.

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.

B2 B.8 The systems support and enforce multi-factor authentication for all customers, with a second factor or biometrics for read-only access, an additional factor for transactions to existing payees, and full biometric validation or a re-challenge for changes of details or new payees. **Organisational evidence**

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

B2 B.9 Access by unauthorised bank users to critical data and core banking functions strictly restricted, with roles and authorities clearly delineated and access given only where necessary. **Organisational evidence**

Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: AC-3 Access Enforcement, AC-5 Separation of Duties.

B2 B.10 A tiered notification framework: security-critical alerts, such as failed log-ins, blocks, password changes and suspicious activity, by SMS or automated voice call; general notifications by push, email or other channels the customer chooses. **Organisational evidence**

Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: SI-4 System Monitoring.

B2 B.11 Electronic onboarding and digital KYC with automated data capture (OCR, barcode, NFC), biometrics and facial recognition, liveness detection, and safeguards against deepfakes and synthetic identities. **Organisational evidence**

Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: IA-12 Identity Proofing.

B2 B.12	A detailed list of the systems and modules integrated with the core banking system, with each module's function and technical configuration. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CM-8 System Component Inventory, PL-8 Security and Privacy Architectures.	**Organisational evidence**
B2 B.13	Availability of at least 99.5%, measured monthly per customer, for all critical IT infrastructure and core banking services, excluding notified planned maintenance, met for at least 95% of active customers. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
B2 B.14a	The standards of ISO 27001, ISO 22301, ISO 20000 and ISO 25011 maintained. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
B2 B.15a	The required ISO and other international standards implemented in phases, with an analysis of cost and expected timelines. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
B2 B.16a	A binding long-term support and maintenance contract with each core banking vendor, with measurable service levels by severity, preventive maintenance and upgrades tested first in the isolated test environment, an escalation matrix and quarterly reviews, knowledge transfer and documentation, and business continuity support. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-9 External System Services, SA-5 System Documentation.	**Organisational evidence**
B2 B.14b	A dedicated senior official, suitably certified and reporting to executive leadership, appointed to oversee the implementation, maintenance and compliance of the core banking system. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
B2 B.15b	The core banking system hosted in data centres located within Iraq, subject to the CBI's data sovereignty requirements. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-9(5) Processing, Storage, and Service Location.	**Organisational evidence**
B2 B.16b	The CBI notified at least 14 calendar days before major enhancements, launches or policy changes to the core banking system, and of security incidents, breaches or customer data exposures within 48 hours of discovery. Organisational, non-technical. Standards (private banks). NIST SP 800-53: IR-6 Incident Reporting, CM-3 Configuration Change Control.	**Organisational evidence**

B2 C.1	Detailed technical documentation of the core banking system submitted to a third-party IT assurance company: name and version, providers and implementation date, architecture and integration diagrams, modules, user access and security features, test environments and disaster recovery. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors, SA-5 System Documentation.	**Organisational evidence**
B2 C.2	A third-party audit report from a CBI-approved IT assurance firm on integration, performance and uptime, encryption and storage, security and authentication, test environments and failover, reporting accuracy and the ISO standards. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
B2 C.3	Annual assurance reviews of the core banking system by a CBI-approved third-party firm, with the report submitted to the Board and the CBI within 60 days of the financial year end. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors, CA-7 Continuous Monitoring.	**Organisational evidence**
B2 C.4	A remediation plan, developed with the assurance provider, submitted to the Board and the CBI within 180 days of the financial year end and carried out on its timelines. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**
B2 C.5	The bank supports the CBI's supplementary audits, demonstrations of functionality, inspection of system logs and interviews with administrators or vendors. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

B3 Standard B3.1: Online Banking

B3 B.1	Web and mobile digital banking for all retail account holders, and at least web banking for corporate account holders, with continuous access to core services, meeting the CBI's availability and cybersecurity standards, in Arabic and English. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
B3 B.2	Online banking delivered through a secure website and a mobile application on iOS and Android, integrated with the core banking system and processing transactions in real time. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, CA-3 Information Exchange.	**Organisational evidence**
B3 B.3	The relevant digital channels available to corporate clients holding the different types of corporate account. Organisational, non-technical. Standards (private banks). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**

B3 B.4	The website and the mobile application each available at least 98% of each month, excluding scheduled maintenance, with unplanned outages over 4 hours reported to the CBI within 24 hours. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, IR-6 Incident Reporting.	**Organisational evidence**
B3 B.5	Core retail functions on both channels: balance and 90-day history, transfers, personal details updates, self-registration and digital KYC, electronic statements, and branch locator and FAQs. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
B3 B.6	Core corporate functions online: balance and 180-day history, transfers with bulk payments and payroll, multi-level approval workflows, statements and reports, and service requests. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-4 Acquisition Process, AC-5 Separation of Duties.	**Organisational evidence**
B3 B.7	Two-factor authentication on every online banking platform for log-in and for sensitive transactions, by OTP over SMS or email, authenticator applications or biometrics. Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.	**Organisational evidence**
B3 B.8	The interface in Arabic and English, easy to navigate and meeting basic WCAG 2.2 accessibility standards. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
B3 B.9	Self-service digital onboarding for existing retail customers with secure identity verification, and acceptance of the terms of service and privacy policy at onboarding. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: IA-12 Identity Proofing, PT-4 Consent.	**Organisational evidence**
B3 B.10	Immediate SMS or email notice to the customer of every online transaction involving account access, transfers, card services or profile changes. Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
B3 B.11	An auditable digital activity log kept for at least 6 months and made available to the CBI on request. Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: AU-12 Audit Record Generation, SI-12 Information Management and Retention.	**Organisational evidence**
B3 B.12	A clear escalation process and support framework for digital banking issues, with response times disclosed in the application or website and complaints trackable by reference number. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: IR-7 Incident Response Assistance.	**Organisational evidence**

B3 B.13	The CBI notified at least 14 calendar days before major enhancements, launches or policy changes to online banking, and of security incidents, breaches or customer data exposures within 48 hours of discovery. Organisational, non-technical. Standards (private banks). NIST SP 800-53: IR-6 Incident Reporting, CM-3 Configuration Change Control.	**Organisational evidence**
B3 C.1	A CBI-approved third-party specialist firm assesses the availability, functionality and security of the online banking channels at least once a year. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
B3 C.2	The assessment reviews uptime and incident logs, simulates user journeys, verifies two-factor authentication and alerts, and reviews onboarding, language accessibility and complaint handling. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors, CA-8 Penetration Testing.	**Organisational evidence**
B3 C.3	The bank cooperates with spot audits and targeted reviews, giving access to back-end dashboards, audit trails and compliance documentation on request. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

B7 Standard B7.1: Infrastructure and Data

B7 B.1	A secure, resilient and scalable IT infrastructure protecting sensitive financial, personal and transactional data across core and peripheral systems, with high availability, fault-tolerant architecture and disaster recovery arrangements. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, CP-2 Contingency Plan, CP-11 Alternate Communications Protocols.	**Organisational evidence**

B7 B.2 A data classification and tiering framework, with Tier 0 and Tier 1 data (customer master, authentication, contact, static, product and transaction data) encrypted at rest and in transit, Tier 2 data encrypted in transit, and Tier 3 encryption optional. **Incomplete**

Checked, coverage partial. Standards (private banks). NIST SP 800-53: SC-28 Protection of Information at Rest, SC-8 Transmission Confidentiality and Integrity, CM-6 Configuration Settings. Evidence counted: platform.control-plane-tls, platform.mesh-cni, platform.secret-encryption, policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is that Kubernetes Secrets are encrypted at rest, and TLS on the control plane and on Ingresses, with the service mesh encrypting traffic between Pods. The tiering framework, and the encryption of data in databases, applications and backups, are the bank'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.
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.secret-encryption	**Not evaluated**	The platform could not observe Secret encryption. Establishes: Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.
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.

B7 B.3 A multi-layered cybersecurity defence, for example WAF, next-generation firewall, IDS/IPS, SIEM/SOC, PAM, IAM and EDR/NDR/XDR, from reputable, recognised providers. **Organisational evidence**

Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: SC-7 Boundary Protection, SI-4 System Monitoring, SC-3 Security Function Isolation.

B7 B.4 Availability of at least 99.5% for critical IT infrastructure and core banking services, excluding scheduled downtime. **Organisational evidence**

Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.

B7 B.5 Tier 0 and Tier 1 data, on premises, in the cloud or in off-site backups, protected by layered controls including intrusion prevention, access control and multi-factor authentication, and accessible only to authorised personnel. **Organisational evidence**

Organisational, technical, outside the cluster. Standards (private banks). NIST SP 800-53: AC-3 Access Enforcement, IA-2(1) Multi-factor Authentication to Privileged Accounts, SI-4 System Monitoring.

B7 B.6	Physical data centres and servers inside Iraq, with access control devices, full camera coverage kept 6 months, raised floors or smart racks with fire suppression, FM200 suppression, gas extinguishers, environmental sensors, backup power and primary and backup cooling, meeting the Uptime Institute's Tier 3 specifications. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SA-9(5) Processing, Storage, and Service Location, PE-3 Physical Access Control, PE-6 Monitoring Physical Access, PE-13 Fire Protection, PE-14 Environmental Controls.	**Organisational evidence**
B7 B.7	A detailed inventory of all data storage and processing systems, showing where and how customer data is stored, encrypted, replicated and destroyed, with the classification, retention, geographic location and contingency access policies. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CM-12 Information Location, SA-9(5) Processing, Storage, and Service Location.	**Organisational evidence**
B7 B.8	Documented data deletion policies: deletion only when retention has expired, on a verified request, on clearance of holds or in approved processes; covering all data types; with an auditable log of every deletion (type, reason, time, system, actor) kept at least 5 years. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: SI-12 Information Management and Retention, SI-12(3) Information Disposal, MP-6 Media Sanitization.	**Organisational evidence**
B7 B.9	The requirements of ISO 27001, ISO 20000, ISO 22301, ISO 25011 and PCI DSS followed. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
B7 B.10	The required ISO and other international standards implemented in phases, with an analysis of cost and expected timelines. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
B7 B.11	A detailed incident response plan for cybersecurity breaches, updated every year. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: IR-8 Incident Response Plan.	**Organisational evidence**
B7 B.12	A third party to which data processing is outsourced complies with security standards no less strict than the bank's own. Organisational, non-technical. Standards (private banks). NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
B7 B.13	A third party to which data processing or a core banking function is outsourced signs a non-disclosure agreement with the bank. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PS-6 Access Agreements, SA-9 External System Services.	**Organisational evidence**

B7 B.14	A senior executive appointed to oversee cybersecurity, data security governance and infrastructure compliance, keeping infrastructure, encryption standards and storage policies aligned with the CBI's directives and best practice. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
B7 B.15	All other CBI circulars, regulations and directives on cybersecurity, data and technology infrastructure followed. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
B7 B.16	Full compliance with the COBIT 2019 IT governance framework and with the CBI's Cyber Resilience Controls and related instructions. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-14 Testing, Training, and Monitoring, PM-1 Information Security Program Plan.	**Organisational evidence**
B7 C.1	Documentation submitted of the infrastructure architecture, encryption configurations and storage policies, with system diagrams, technical specifications, encryption protocols and a register of key management procedures without key material. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
B7 C.2	A third-party audit report from a CBI-approved IT assurance firm on infrastructure, security, encryption, classification, access control and data centre compliance, dated within 12 months and with an attestation of independence. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
B7 C.3	Annual independent validation, by a CBI-approved firm, of compliance with the infrastructure and encryption specifications through audit and testing of actual configurations, with a report of gaps and recommendations to the Board and the CBI. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors, CA-8 Penetration Testing.	**Organisational evidence**
B7 C.4	The annual assurance report submitted to the Board and the CBI within 60 days of the close of the financial year. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
B7 C.5	Where material gaps or risks are found, a remediation plan developed with the assurance company shared with the Board and the CBI within 180 days of the close of the financial year, with timelines and owners. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**

B7 C.6	The bank's teams supervised by the CBI, through on-site visits and meetings, until every element of the remediation plan is actioned. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-5 Plan of Action and Milestones, CA-7 Continuous Monitoring.	**Organisational evidence**
B7 C.7	Testing logs, penetration test summaries or vulnerability assessment results provided on the CBI's request, with interviews of the responsible executives or technical leads. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**
B7 C.8	The assurance process is in addition to, not in place of, the data storage and processing obligations of Article 38 of the 2004 Banking Law, and both are met. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-14 Testing, Training, and Monitoring.	**Organisational evidence**

B9 Standard B9.1: Business and Operational Resilience

B9 B.1	A Board-approved business continuity plan, reviewed and updated every year, with business impact analysis, risk assessment, critical process mapping and maximum tolerable downtime, under clauses 8.2 and 6.1.2 of ISO 22301. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, RA-9 Criticality Analysis.	**Organisational evidence**
B9 B.2	The business continuity plan includes alternate work arrangements, internal and external communication, staffing continuity, crisis governance, a scenario testing schedule and post-incident review. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-4 Contingency Plan Testing.	**Organisational evidence**
B9 B.3	The business continuity plan reflects ISO 22301 clause 8.4 on recovery strategy, clause 9 on performance evaluation and clause 10 on continual improvement. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
B9 B.4	A Board-approved disaster recovery plan, reviewed and updated every year, with critical ICT infrastructure mapping, restoration sequencing, fallback strategies and RTO and RPO alignment, under sections 6 and 7 of ISO/IEC 27031. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
B9 B.5	At least one disaster recovery site inside Iraq, able to recover all critical ICT and banking services. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-7 Alternate Processing Site, SA-9(5) Processing, Storage, and Service Location.	**Organisational evidence**

B9 B.6	The disaster recovery site has secure access control with multi-factor authentication, digital access logs kept at least one year, and full-room surveillance with video kept at least three months. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: PE-3 Physical Access Control, PE-6 Monitoring Physical Access, PE-8 Visitor Access Records.	**Organisational evidence**
B9 B.7	The disaster recovery site at least 75 kilometres from the primary data sites. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-7(1) Separation from Primary Site.	**Organisational evidence**
B9 B.8	The disaster recovery site has access control devices, full camera coverage kept 3 months, raised floors or smart racks with fire suppression, FM200 suppression, gas extinguishers, environmental sensors, backup power and primary and backup cooling, meeting the Uptime Institute's Tier 3 specifications. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PE-3 Physical Access Control, PE-6 Monitoring Physical Access, PE-13 Fire Protection, PE-14 Environmental Controls.	**Organisational evidence**
B9 B.9	The disaster recovery plan identifies critical systems and data, real-time or scheduled backup procedures, tiered restoration priorities, fallback infrastructure (hot, warm or cold sites) and failover and restoration procedures. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
B9 B.10	The disaster recovery plan names the systems and data critical for restoration, at least core banking, transaction records, customer data, real-time payments, communication channels and user authentication services. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-2(8) Identify Critical Assets.	**Organisational evidence**
B9 B.11	The disaster recovery plan aligned with section 8 of ISO/IEC 27031 on performance assessment, recovery maturity and corrective measures. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
B9 B.12	On a disruption of critical services, a customer and regulatory communication protocol: proactive notice to customers by SMS, email, website and social media with recovery times and alternatives, and immediate notice to the CBI with regular updates. Organisational, non-technical. Standards (private banks). NIST SP 800-53: IR-6 Incident Reporting, CP-2 Contingency Plan.	**Organisational evidence**
B9 B.13	A disruption of critical banking services resolved within at most 24 hours. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-10 System Recovery and Reconstitution, IR-4 Incident Handling.	**Organisational evidence**

B9 B.14	A disruption triggers these protocols when it is expected to exceed 4 hours or continues one hour without known cause, affects more than 10% of customers or threatens stability, trust or compliance, risks regulatory breach, or is caused by a cyberattack, compromise or major data centre failure. Organisational, non-technical. Standards (private banks). NIST SP 800-53: IR-8 Incident Response Plan, CP-2 Contingency Plan.	**Organisational evidence**
B9 B.15	Annual testing of the business continuity and disaster recovery plans, with simulations and failover drills, and the outcomes, gaps and corrective actions documented and reported to the Board. Organisational, technical and non-technical. Standards (private banks). NIST SP 800-53: CP-4 Contingency Plan Testing.	**Organisational evidence**
B9 B.16	A senior executive, such as the Chief Risk Officer, designated to oversee the continuity and recovery frameworks, reporting regularly to the Board. Organisational, non-technical. Standards (private banks). NIST SP 800-53: PM-2 Information Security Program Leadership Role, CP-2 Contingency Plan.	**Organisational evidence**
B9 B.17	Internal audit reviews the continuity and recovery frameworks every year and reports its findings to the Audit Committee and the Board. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2 Control Assessments, CP-4 Contingency Plan Testing.	**Organisational evidence**
B9 B.18	Fallback infrastructure from a third party follows the CBI's outsourcing guidelines, with the bank keeping full responsibility for continuity and compliance. Organisational, non-technical. Standards (private banks). NIST SP 800-53: SA-9 External System Services, CP-7 Alternate Processing Site.	**Organisational evidence**
B9 C.1	The latest Board-approved continuity and recovery plans submitted, with change logs for the past two years, test results and records of corrective actions. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan, CP-4 Contingency Plan Testing.	**Organisational evidence**
B9 C.2	Board resolutions or minutes confirming formal approval of the continuity and recovery plans included in the submission. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
B9 C.3	An annual third-party audit of the continuity and recovery plans by a CBI-approved firm, covering governance, infrastructure readiness, alignment with ISO 22301 and ISO/IEC 27031, and testing effectiveness. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
B9 C.4	The audit report includes the auditor's credentials, a formal opinion of compliance, detailed findings, remediation recommendations and a statement of independence. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**

B9 C.5	The audit report submitted to the Board and the CBI within 60 days of the end of the financial year. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
B9 C.6	Where material gaps or risks are found, a remediation plan developed with the audit firm within 180 days of the end of the financial year, with timelines and owners. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**
B9 C.7	The bank supports the CBI's site visits, failover demonstrations, interviews and inspection of documentation to validate the disaster recovery site and the continuity framework. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-2 Control Assessments, CP-4 Contingency Plan Testing.	**Organisational evidence**
B9 C.8	The bank carries out the remediation plan under the CBI's monitoring, including any further directives, re-testing or supervisory actions. Organisational, non-technical. Standards (private banks). NIST SP 800-53: CA-5 Plan of Action and Milestones, CA-7 Continuous Monitoring.	**Organisational evidence**

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-st 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.backup-encryption Nothing to check

Every backed-up Longhorn volume is encrypted, so that its backups leave the site encrypted.

Neither Longhorn nor Velero is installed, so no backup leaves the site.

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.log-forwarding Fail

The cluster's logs leave its nodes and arrive: Fluent Bit sends them to a central store (an output with a host, or an s3 output with a bucket), and its own counters show records delivered there since the last run with no error, failed retry or dropped record; or another log shipper runs, which is named and whose destination the organisation evidences.

No log shipper runs on the cluster, so its logs stay on its nodes.

- no Fluent Bit DaemonSet or Deployment in namespace logging
- no other log shipper found: Fluent Bit, Vector, Fluentd, Promtail, Grafana Alloy, Filebeat, OpenTelemetry Collector, Datadog Agent

How to fix On a Bahriya Kubernetes Engine cluster, set components.fluent-bit.settings.output.config in config.yaml to an [OUTPUT] section naming the central store, then run apply.sh --commit. Keep the store's password out of config.yaml, as the Logging with Fluent Bit guide describes. On another cluster, install a log shipper, such as Fluent Bit, that sends the logs to a central store. Where records do not arrive, the Pod named in the finding logs each failed delivery: check that the store can be reached from the cluster and that its credentials are accepted. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Cluster log shipping	no log shipper runs on the cluster	`kubectl get daemonsets,deployments -A`

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-authz Pass

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

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

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

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)

node.time-sync Not evaluated

Each node runs a time service configured with the servers the platform names.

The platform names no time servers, so there is nothing to compare the nodes with.

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.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.secret-encryption Not evaluated

Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.

The platform could not observe Secret encryption.

- encryption.observed: unknown
- encryption.resources.configured: unknown

platform.time-servers Not provided

The time servers each node synchronises with.

No time servers are set for the cluster; each node keeps its own.

- compliance.time-servers.configured: unknown

How to fix Name the organisation's time servers in compliance.time.servers in /etc/bke/config.yaml and run apply.sh --commit, then upgrade.sh --node-settings --commit on every node. That command moves no version and restarts only the time service. (Bahriya Tersane)

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-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-host-namespaces Pass

No Pod shares the host's network, process or IPC namespace, outside named namespaces.

Every object the policy judged passes it.

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

policy.no-host-path Pass

No Pod mounts a host path, outside named namespaces.

Every object the policy judged passes it.

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

policy.no-host-ports Pass

No container binds a host port, outside named namespaces.

Every object the policy judged passes it.

- tersane-compliance-no-host-ports: 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.host-access Pass

Workloads that use the host's namespaces, paths or ports.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0008, AVD-KSV-0009, AVD-KSV-0010, AVD-KSV-0023, AVD-KSV-0024
- 22 object(s) with a passing result, 0 failing, 3 failing in exempt namespaces

Fails in exempt namespaces, not counted (7)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0009: Access to host network. ReplicaSet 'tigera-operator-686489b657' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0023: hostPath volumes mounted. ReplicaSet 'tigera-operator-686489b657' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Installation calico-system/default	AVD-KSV-0009: Access to host network. DaemonSet 'calico-node' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0009: Access to host network. ReplicaSet 'calico-typha-5f45dc8cf9' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport replicaset-calico-typha-5f45dc8cf9 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0023: hostPath volumes mounted. DaemonSet 'calico-node' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0023: hostPath volumes mounted. DaemonSet 'csi-node-driver' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Job compliance-node/node-facts-gtn4z	AVD-KSV-0023: hostPath volumes mounted. Job 'node-facts-gtn4z' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport job-node-facts-gtn4z -n compliance-node -o yaml`

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(11) Usage Conditions	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].
AC-3 Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
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(5) Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
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-6(9) Log Use of Privileged Functions	Log the execution of privileged functions.
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-8 System Use Notification	a. Display [Assignment: organization-defined system use notification] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that: 1. Users are accessing a U.S. Government system; 2. System usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. Use of the system indicates consent to monitoring and recording; b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and c. For publicly accessible systems: 1. Display system use information [Assignment: organization-defined conditions] , before granting further access to the publicly accessible system; 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system.
AC-11 Device Lock	a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended] ; and b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.
AC-12 Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events].
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-17(2) Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
AC-18 Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless 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-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].
AC-21 Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions for [Assignment: organization-defined information-sharing circumstances] ; and b. Employ [Assignment: organization-defined automated mechanisms] to assist users in making information sharing and collaboration decisions.

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-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-3 Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.
AU-4 Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].

AU-5 Response to Audit Logging Process Failures	a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and b. Take the following additional actions: [Assignment: organization-defined additional actions].
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-8 Time Stamps	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.
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-3 Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; non-disclosure agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [Assignment: organization-defined frequency].

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-6 Authorization	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; e. Update the authorizations [Assignment: organization-defined frequency].
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].
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-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-5 Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to 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 Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission-essential capabilities] ; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].
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(1) Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.
CM-8(4) Accountability Information	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role] , individuals responsible and accountable for administering those components.
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-11 User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods] ; and c. Monitor policy compliance [Assignment: organization-defined frequency].
CM-12 Information Location	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

CP-2 Contingency Plan	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by [Assignment: organization-defined organization-defined personnel or roles]; b. Distribute copies of the contingency plan to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system [Assignment: organization-defined frequency]; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
CP-2(1) Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.
CP-2(2) Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
CP-2(5) Continue Mission and Business Functions	Plan for the continuance of [Selection: all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.
CP-2(8) Identify Critical Assets	Identify critical system assets supporting [Selection: all; essential] mission and business functions.
CP-3 Contingency Training	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and b. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-4 Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
CP-6 Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

CP-7 Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site.
CP-7(1) Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.
CP-8 Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
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-9(1) Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined organization-defined frequency] to verify media reliability and information integrity.
CP-9(6) Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.
CP-9(8) Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined 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.
CP-10(4) Restore Within Time Period	Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.
CP-11 Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.
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-2(5) Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.
IA-2(8) Access to Accounts — Replay Resistant	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].
IA-3 Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.
IA-5(1) Password-based Authentication	For password-based authentication: (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly; (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a); (c) Transmit passwords only over cryptographically-protected channels; (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash; (e) Require immediate selection of a new password upon account recovery; (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; (g) Employ automated tools to assist the user in selecting strong password authenticators; and (h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].
IA-12 Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.
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-4(4) Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
IR-4(11) Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].
IR-4(14) Security Operations Center	Establish and maintain a security operations center.
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-2 Media Access	Restrict access to [Assignment: organization-defined organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined organization-defined personnel or roles].
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-4 Media Storage	a. Physically control and securely store [Assignment: organization-defined organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined organization-defined controlled areas] ; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
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.
MP-7 Media Use	a. [Selection: restrict; prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls] ; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.
PE-2 Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency] ; and d. Remove individuals from the facility access list when access is no longer required.
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-4 Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].
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-9 Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.
PE-10 Emergency Shutoff	a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations; b. Place emergency shutoff switches or devices in [Assignment: organization-defined location] to facilitate access for authorized personnel; and c. Protect emergency power shutoff capability from unauthorized activation.
PE-11 Emergency Power	Provide an uninterruptible power supply to facilitate [Selection: an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.
PE-11(1) Alternate Power Supply — Minimal Operational Capability	Provide an alternate power supply for the system that is activated [Selection: manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.
PE-12 Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
PE-13 Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.
PE-13(1) Detection Systems — Automatic Activation and Notification	Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.
PE-13(2) Suppression Systems — Automatic Activation and Notification	(a) Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] ; and (b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.
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.
PE-18 Location of System Components	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.
PE-19 Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.
PE-23 Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

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-4(1) Social Media and External Site/Application Usage Restrictions	Include in the rules of behavior, restrictions on: (a) Use of social media, social networking sites, and external sites/applications; (b) Posting organizational information on public websites; and (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

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-11 Mission and Business Process Definition	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c. Review and revise the mission and business processes [Assignment: organization-defined frequency].
PM-13 Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.
PM-14 Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures [Assignment: organization-defined organization-defined frequency].
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-4 Consent	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.
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-3(1) Supply Chain Risk Assessment	(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services] ; and (b) Update the supply chain risk assessment [Assignment: organization-defined frequency] , when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
RA-5 Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-7 Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
RA-9 Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].

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-2 Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.
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-3(2) Use of Live or Operational Data	(a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and (b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.
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-5 System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b. Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and d. Distribute documentation to [Assignment: organization-defined personnel or roles].
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(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(1) Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.
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].
SC-2 Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.
SC-3 Security Function Isolation	Isolate security functions from nonsecurity functions.
SC-4 Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.
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-7(8) Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.
SC-7(10) Prevent Exfiltration	(a) Prevent the exfiltration of information; and (b) Conduct exfiltration tests [Assignment: organization-defined frequency].
SC-8 Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-8(1) Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.
SC-13 Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses] ; and b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography].
SC-28 Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-28(1) Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].
SC-45 System Time Synchronization	Synchronize system clocks within and between systems and system components.

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-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(5) System-generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].
SI-7 Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined organization-defined software, firmware, and information] ; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined organization-defined actions].
SI-8 Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
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(3) Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined organization-defined techniques].

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-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].