Technology Risks (January 2018): technical evidence

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

Regime	Technology Risks (January 2018), Qatar Central Bank (QCB), State of Qatar
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.

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

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

516 requirements: 6 enforced by a policy, 30 checked, 26 provided by the platform, 454 organisational (188 technical, outside the cluster; 248 non-technical; 18 technical and non-technical).

Outcome	Requirements	Meaning
Fail	17	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	11	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	2	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	21 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	9	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	454	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

10 object(s) fail at least one check: 6 cluster-wide and 4 in 1 namespace(s). They are listed under Fix first, the most severe first.

Fix first

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

Cluster-wide

6 object(s), most severe Critical.

ClusterRole **`tigera-operator`** Fails 2.1.9, 8.10.1.2, 9.7.1.2, 10.10.6	
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 2.1.9, 8.10.1.2, 9.7.1.2, 10.10.6

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 8.7.2

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 8.4.10

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
```

Node **node-1** Fails 9.1.1.12, 9.2.2.2, 9.6.1.1, 9.6.1.4

MEDIUM no cipher suites are set, so the defaults, which include CBC suites, are offered

Check node.kubelet-ciphers.

How to fix On a Bahriya Kubernetes Engine cluster, set compliance.controlPlane.enabled to true in config.yaml (the default) and upgrade each node with upgrade.sh, which writes tlsMinVersion and tlsCipherSuites into every kubelet's configuration. Elsewhere, set tlsMinVersion to VersionTLS12 and tlsCipherSuites to AES-GCM suites only in the kubelet's configuration, then restart the kubelet. (Bahriya Tersane)

MEDIUM the minimum TLS version is not set, which allows TLS 1.0

Check node.kubelet-ciphers.

How to fix On a Bahriya Kubernetes Engine cluster, set compliance.controlPlane.enabled to true in config.yaml (the default) and upgrade each node with upgrade.sh, which writes tlsMinVersion and tlsCipherSuites into every kubelet's configuration. Elsewhere, set tlsMinVersion to VersionTLS12 and tlsCipherSuites to AES-GCM suites only in the kubelet's configuration, then restart the kubelet. (Bahriya Tersane)

What was read on the node is in this run's snapshot.json, under nodes.

Platform **API server audit log** Fails 8.4.7	
MEDIUM	kept at most 30 days before rotation; the regime requires 180 Check platform.audit-rotation. **How to fix** Keep the audit log for at least the period the regime requires. On BKE, which always limits the number of audit log files, forward the log to a central log store that keeps it that long, and give that store's retention setting to your assessor as evidence: from BKE 2.6.1, Fluent Bit collects the audit log on the control-plane nodes under the tag audit.*, and an output that matches that tag sends it to your store; on earlier versions, forward it with your own collector. On another cluster, either forward the log in the same way, or set --audit-log-maxage to at least that period and leave --audit-log-maxbackup unset or 0 on each API server's static Pod manifest, with enough disk on each control-plane node to hold that period. (Bahriya Tersane)
Full result	`kubectl -n bahriya-system get configmap bke-platform -o jsonpath='{.data.audit\.rotation}'`

Namespace payments

4 object(s), most severe Medium.

CronJob **nightly** Fails 9.1.1.8	
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.

Deployment **legacy-batch** Fails 9.1.1.8	
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.

Deployment **unsigned-app** Fails 9.1.1.8	
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.

Namespace **payments** Fails 8.1.7, 8.10.1.9, 9.1.1.3, 9.1.1.7, 9.7.1.2, 9.7.2.1	
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

1 Cyber security within the organisation

1.1 Managing cyber security risk

1.1.1	A cyber security function and framework, approved by the board or its committee. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-1 Information Security Program Plan.	**Organisational evidence**
1.1.2	Senior management reviews the adequacy of cyber security controls against new threats at least annually, and justifies material gaps to the board. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, CA-2 Control Assessments.	**Organisational evidence**
1.1.3	Board oversight of technology and cyber risk, an approved cyber risk appetite, and board expertise to exercise it. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing.	**Organisational evidence**
1.1.4	A board-approved cyber security policy. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
1.1.5	A board-approved cyber security strategy and budget, with contingency. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-9 Risk Management Strategy.	**Organisational evidence**
1.1.6	A cyber security function with representatives of IT, risk, security, HR, continuity, legal and compliance. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**
1.1.7	Policies, standards and procedures reviewed and updated at least annually. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**

1.2 Policy and organisation

1.2.1	Board and management oversight of technology risk, IT policies, standards and procedures within the framework, and committees for IT strategy, IT steering and technology risk. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PL-1 Policy and Procedures.	**Organisational evidence**
1.2.2	A security organisation that designs, operates and improves the security programme in line with leading practice. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PM-2 Information Security Program Leadership Role.	**Organisational evidence**
1.2.3	The security programme's minimum content: policies, roles and accountability, a control framework, risk assessment, awareness, monitoring and incident handling. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
1.2.4	A board-approved policy setting the strategy against cyber threats for the bank's complexity and risk appetite. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PL-1 Policy and Procedures.	**Organisational evidence**
1.2.5	An information security function separate from IT, with segregation of duties between the two. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, AC-5 Separation of Duties.	**Organisational evidence**
1.2.6	The information security function sized to the bank's activities and channels. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-3 Information Security and Privacy Resources.	**Organisational evidence**
1.2.7	A CISO who leads the security function and reports independently of the CIO or CTO. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
1.2.8	A security forum of senior executives, the CEO and CFO among them, facilitated by the CISO. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**
1.2.9	The information security committee's duties: policy implementation within risk appetite, approval and monitoring of initiatives, and reporting. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**
1.2.10	The security function adequately staffed, skilled and equipped. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-13 Security and Privacy Workforce.	**Organisational evidence**

1.2.11	The CISO's responsibilities: security plans and procedures, advice on systems, monitoring, incident handling and reporting. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PL-2 System Security and Privacy Plans.	**Organisational evidence**

1.3 Preparedness indicators

1.3.1	Indicators that measure cyber resilience and preparedness. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance.	**Organisational evidence**
1.3.2	The indicators assessed by independent, qualified compliance checks or audits. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.	**Organisational evidence**
1.3.3	The board monitors the key cyber indicators at least every six months, with a remedial plan for deviations. Organisational, non-technical. NIST SP 800-53: PM-6 Measures of Performance, CA-7 Continuous Monitoring.	**Organisational evidence**

2 Cyber security in human resources

2.1 Personnel security

2.1.1	HR policies aligned with the security policy, stating the security duties of staff, contractors and third parties. Organisational, non-technical. NIST SP 800-53: PS-1 Policy and Procedures, PS-7 External Personnel Security.	**Organisational evidence**
2.1.2	Security responsibilities written into roles and job descriptions and monitored throughout employment. Organisational, non-technical. NIST SP 800-53: PS-9 Position Descriptions, PM-13 Security and Privacy Workforce.	**Organisational evidence**
2.1.3	HR policies available to all staff, who know and follow their security obligations. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior, PS-1 Policy and Procedures.	**Organisational evidence**
2.1.4	A disciplinary process, enforced and known to staff. Organisational, non-technical. NIST SP 800-53: PS-8 Personnel Sanctions.	**Organisational evidence**
2.1.5	Terms and a confidentiality agreement signed on joining and on a change of role. Organisational, non-technical. NIST SP 800-53: PS-6 Access Agreements.	**Organisational evidence**
2.1.6	Personal information about personnel handled as the privacy law requires. Organisational, non-technical. NIST SP 800-53: PT-2 Authority to Process Personally Identifiable Information, PM-18 Privacy Program Plan.	**Organisational evidence**
2.1.7	Visitors and vendors logged, badged and identifiable as visitors on the premises, briefed on their obligations and escorted in secure areas. Organisational, non-technical. NIST SP 800-53: PE-8 Visitor Access Records, PE-2 Physical Access Authorizations.	**Organisational evidence**

2.1.8	HR raises a change request on a change of duties or departure, so assets are returned and access amended or removed. Organisational, non-technical. NIST SP 800-53: PS-4 Personnel Termination, PS-5 Personnel Transfer, AC-2 Account Management.	**Organisational evidence**
2.1.9	Access limited to what each person needs for the job, by least privilege. Checked, coverage partial. NIST SP 800-53: AC-6 Least Privilege, AC-6(1) Authorize Access to Security Functions. Fails in ClusterRole tigera-operator, ClusterRole tigera-operator-secrets.	**Fail**

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.

2.1.10	Controls against unauthorised disclosure, misuse or corruption of information by staff, vendors and visitors. Organisational, non-technical. NIST SP 800-53: PS-6 Access Agreements, PL-4 Rules of Behavior.	**Organisational evidence**
2.1.11	Insider threats considered in risk assessment. Organisational, non-technical. NIST SP 800-53: PM-12 Insider Threat Program, RA-3 Risk Assessment.	**Organisational evidence**

2.2 Competence and training

2.2.1	A funded security awareness programme. Organisational, non-technical. NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.	**Organisational evidence**
2.2.2	Training content reviewed at least annually for new threats, systems and law. Organisational, non-technical. NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.	**Organisational evidence**
2.2.3	Training covers the bank's security, legal and regulatory requirements, discipline, incident reporting and acceptable use. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, AT-3 Role-based Training.	**Organisational evidence**
2.2.4	Training material and security policies available to all staff and long-term on-site contractors. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, PL-4 Rules of Behavior.	**Organisational evidence**
2.2.5	All staff and long-term contractors trained in the policies relevant to their roles. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**

2.2.6	Awareness training at induction and at least annually, including recognising social engineering. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, AT-2(3) Social Engineering and Mining.	**Organisational evidence**
2.2.7	Training assessed for effectiveness, with attendance and acknowledgement recorded, and the board and senior management briefed on cyber threats. Organisational, non-technical. NIST SP 800-53: AT-4 Training Records, AT-3 Role-based Training.	**Organisational evidence**
2.2.8	Customers, vendors and other stakeholders made aware of the bank's cyber resilience objectives. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
2.2.9	Consider an awareness programme on attackers' methods, updated annually and mandatory for all staff. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

3 Cyber security in legal and compliance

3.1.1	A security and governance programme that addresses legal and compliance requirements. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PL-1 Policy and Procedures.	**Organisational evidence**
3.1.2	Compliance with current and future laws and regulations. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, CA-2 Control Assessments.	**Organisational evidence**
3.1.3	An audit of information systems, people and processes at least annually and after a significant change, with findings remediated within defined timelines. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-5 Plan of Action and Milestones.	**Organisational evidence**
3.1.4	Reassessment when a change or finding invalidates the current assessment, and in full for a major design change. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.	**Organisational evidence**
3.1.5	All infrastructure, people and processes in the audit's scope, with any exemption justified to QCB. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
3.1.6	An organisation for legal and compliance enforcement, with the board's risk forum addressing cyber-law risk. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.7	Legal risks reported to management and the board, covering applicable legislation, intellectual property, records, privacy and cryptography. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, PM-18 Privacy Program Plan.	**Organisational evidence**

3.1.8	Compliance with PCI DSS and the payment application standard. Organisational, technical and non-technical. NIST SP 800-53: CA-2 Control Assessments, PM-1 Information Security Program Plan.	**Organisational evidence**
3.1.9	An audit charter for the information security audit: mandate, responsibility and authority. Organisational, non-technical. NIST SP 800-53: CA-1 Policy and Procedures, CA-2 Control Assessments.	**Organisational evidence**
3.1.10	A structured, risk-based audit programme for IT risk management, controls and compliance. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.	**Organisational evidence**
3.1.11	An IT and security audit function whose reporting lines preserve its independence. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-2(1) Independent Assessors.	**Organisational evidence**
3.1.12	An audit cycle set by risk: at most 6 to 12 months for very high and high risk, 18 months for medium and 36 months for low, and never open-ended. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.	**Organisational evidence**
3.1.13	An annual assessment of the legal impact of cyber incidents, with remedial actions approved by the board. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.14	Application control audits, risk-based, focused on data integrity. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, SI-10 Information Input Validation.	**Organisational evidence**
3.1.15	A defined risk assessment methodology for the internal audit strategy. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, RA-3 Risk Assessment.	**Organisational evidence**

4 Cyber security in procurement

4.1.1	A procurement policy with vendor selection criteria and contractual and security requirements. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SR-5 Acquisition Strategies, Tools, and Methods.	**Organisational evidence**
4.1.2	Vendors assessed for reliability and risk at the start of procurement. Organisational, non-technical. NIST SP 800-53: SR-6 Supplier Assessments and Reviews, SA-9 External System Services.	**Organisational evidence**
4.1.3	Vendor contracts with confidentiality, security and right-to-audit clauses, responsibilities and the standards to meet. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**

4.1.4	The bank's security requirements passed on to its contractors in the agreement. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PS-7 External Personnel Security.	**Organisational evidence**
4.1.5	Vendors with access to premises or systems audited at least annually, or their self-assessment evaluated. Organisational, non-technical. NIST SP 800-53: SR-6 Supplier Assessments and Reviews, SA-9 External System Services.	**Organisational evidence**
4.1.6	Vendor devices hardened, with default and insecure settings removed. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings, SA-9 External System Services.	**Organisational evidence**

5 Cyber security in risk management

5.1 Risk management framework

5.1.1	A technology risk management framework: roles, asset identification, threat and vulnerability assessment, treatment and monitoring. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, RA-1 Policy and Procedures.	**Organisational evidence**
5.1.2	Risk management practices and controls tested periodically and monitored for effect. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.	**Organisational evidence**
5.1.3	An asset protection policy that sets each asset's criticality and its protection. Organisational, non-technical. NIST SP 800-53: RA-2 Security Categorization, PM-5 System Inventory.	**Organisational evidence**
5.1.4	An up-to-date inventory of information assets, classified by sensitivity. Checked, coverage partial. NIST SP 800-53: CM-8 System Component Inventory, RA-2 Security Categorization. **Scope of this evidence** The inventory of the cluster's namespaces, workloads and images is recorded, and the verdict is that each namespace outside the exempt namespaces carries a classification label. The inventory and classification of other information assets are the bank's to evidence.	**Pass**

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

5.1.5	Each inventory record identifies the asset, its location, classification, group, owner and custodian. Checked, coverage partial. NIST SP 800-53: CM-8 System Component Inventory.	**Recorded**

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.

5.2 Risk assessment

5.2.1	A risk assessment process and methodology covering networks, systems, applications, interfaces, operations and people. Organisational, non-technical. NIST SP 800-53: RA-1 Policy and Procedures, RA-3 Risk Assessment.	**Organisational evidence**
5.2.2	Identified risks analysed for their impact on the business. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
5.2.3	A threat and vulnerability matrix to prioritise risks. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-16 Threat Awareness Program.	**Organisational evidence**
5.2.4	A threat register including denial of service, sabotage and malware, monitored. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-16 Threat Awareness Program.	**Organisational evidence**
5.2.5	The risk appetite defined in the risk assessment process. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
5.2.6	A risk treatment plan, with high residual risks accepted by senior management. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response, PM-9 Risk Management Strategy.	**Organisational evidence**
5.2.7	Risk assessment built into business processes and repeated when the business or regulation changes. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-9 Risk Management Strategy.	**Organisational evidence**

5.3 Risk monitoring and reporting

5.3.1	A procedure to confirm that controls stay effective as circumstances change. Organisational, non-technical. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**
5.3.2	A risk register, reviewed periodically, with the highest risks monitored closely. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, RA-3 Risk Assessment.	**Organisational evidence**
5.3.3	A risk matrix showing the systems and processes most exposed. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

5.3.4	Internal and external threat intelligence used to address new risks. Organisational, non-technical. NIST SP 800-53: PM-16 Threat Awareness Program, SI-5 Security Alerts, Advisories, and Directives.	**Organisational evidence**

6 Business continuity management

6.1 Continuity and recovery

6.1.1	Business continuity per QCB's continuity instructions, aligned with a standard such as ISO 22301. Organisational, non-technical. NIST SP 800-53: CP-1 Policy and Procedures, CP-2 Contingency Plan.	**Organisational evidence**
6.1.2	An emergency response plan: evacuation, command centre and communications. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, PE-15 Water Damage Protection.	**Organisational evidence**
6.1.3	Natural and man-made threat scenarios, cyber included, with incident procedures. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, IR-1 Policy and Procedures.	**Organisational evidence**
6.1.4	A senior head of business continuity, responsible for the plan and its upkeep, an annual business impact analysis, risk assessment and test, and advice on declaring a crisis. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, PM-2 Information Security Program Leadership Role.	**Organisational evidence**
6.1.5	A cross-functional committee that exercises, maintains and invokes the continuity plans. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, CP-4 Contingency Plan Testing.	**Organisational evidence**
6.1.6	Continuity teams for response, IT, damage assessment, logistics and support, at each location as needed. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, CP-3 Contingency Training.	**Organisational evidence**
6.1.7	A crisis communication strategy for regulators, customers, partners and media. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, IR-7 Incident Response Assistance.	**Organisational evidence**
6.1.8	Continuity plans tested and updated at least annually, with at least four unplanned drills a year (one hot, three cold), tests from alternate sites, internal audit review of the testing and an annual independent external audit. Organisational, non-technical. NIST SP 800-53: CP-4 Contingency Plan Testing, CA-2 Control Assessments.	**Organisational evidence**
6.1.9	Annual tests include table-top, simulation and technical recovery. Organisational, technical and non-technical. NIST SP 800-53: CP-4 Contingency Plan Testing.	**Organisational evidence**
6.1.10	The approved continuity plan and test summary sent to QCB annually. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**

6.1.11	Recovery procedures for critical systems and their infrastructure, describing assets, data and recovery mechanisms. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
6.1.12	Recovery capabilities that meet cyber resilience objectives and defined recovery time objectives. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
6.1.13	A cyber crisis management plan covering detection, response, recovery and containment. Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, CP-2 Contingency Plan.	**Organisational evidence**
6.1.14	Measures to prevent and promptly detect cyber attacks, including zero-day, remote access and targeted attacks. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.	**Organisational evidence**
6.1.15	Effective measures to prevent and detect cyber intrusions. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.	**Organisational evidence**
6.1.16	No remote working for critical functions; privileged remote access only with prior approval when needed. Organisational, technical and non-technical. NIST SP 800-53: AC-17 Remote Access, PS-6 Access Agreements.	**Organisational evidence**

7 Compliance with the circular

7.1 Reporting compliance

7.1.1	A reporting framework for the circular, with a compliance report to QCB at least annually. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, CA-2 Control Assessments.	**Organisational evidence**
7.1.2	Material control gaps remediated under board guidance, an action plan shared with QCB for advisory requirements not met, and the report signed by the board or its committee. Organisational, non-technical. NIST SP 800-53: CA-5 Plan of Action and Milestones, PM-4 Plan of Action and Milestones Process.	**Organisational evidence**
7.1.3	QCB may audit the bank's compliance at any time. Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**

7.2 Exceptions

7.2.1	An exception to a mandatory requirement justified and approved by the board or its committee. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, CA-5 Plan of Action and Milestones.	**Organisational evidence**

8 IT operations

8.1 Change management

8.1.1	A change management policy covering major, minor and emergency changes, each documented with a rollback procedure and its business impact assessed beforehand. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control, CM-1 Policy and Procedures, CM-4 Impact Analyses.	**Organisational evidence**
8.1.2	Changes classified so that resources match each change. Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
8.1.3	A cross-functional change committee that includes security and risk. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control, CM-3(4) Security and Privacy Representatives.	**Organisational evidence**
8.1.4	Changes affecting the security posture reassessed, with risk analysis to keep residual risk acceptable. Organisational, technical, outside the cluster. NIST SP 800-53: CM-4 Impact Analyses, RA-3 Risk Assessment.	**Organisational evidence**
8.1.5	Changes tested to a documented plan and accepted by users before production. Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control, CM-3(2) Testing, Validation, and Documentation of Changes.	**Organisational evidence**
8.1.6	The requester of a change is not its implementer, and implementers are competent. Organisational, technical, outside the cluster. NIST SP 800-53: AC-5 Separation of Duties, CM-5 Access Restrictions for Change.	**Organisational evidence**

8.1.7 Separate physical and logical environments for development, test, staging and production. **Fail**

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

Fails in Namespace payments.

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

8.1.8 A change made in production also made in the disaster recovery environment. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control, CP-2 Contingency Plan.

8.1.9 Processes and system documentation updated after a change. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control, CM-9 Configuration Management Plan.

8.1.10 A change verified after implementation for its objective and side effects. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-4(2) Verification of Controls.

8.1.11	Activities during a change logged; a six-monthly review of the change process is recommended. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation, CM-3 Configuration Change Control. 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**

8.2 Incident management

8.2.1	An incident management framework, policy and procedures to protect against, detect, evaluate and respond to incidents. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures, IR-8 Incident Response Plan.	**Organisational evidence**
8.2.2	Dedicated incident resources with defined roles for recording, analysis, remediation and monitoring. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures, IR-4(11) Integrated Incident Response Team.	**Organisational evidence**
8.2.3	An owner of the incident programme and point of contact for security communications. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures, PM-2 Information Security Program Leadership Role.	**Organisational evidence**
8.2.4	Every incident handled and monitored within its resolution timeframe. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-5 Incident Monitoring.	**Organisational evidence**
8.2.5	Incidents classified by criticality, with escalation and resolution times set by severity. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-8 Incident Response Plan.	**Organisational evidence**
8.2.6	Root cause and impact analysis of major incidents, with remediation. Organisational, technical and non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
8.2.7	Incident evidence collected and kept to the rules of evidence where legal action may follow. Organisational, technical and non-technical. NIST SP 800-53: IR-4 Incident Handling, AU-9 Protection of Audit Information.	**Organisational evidence**
8.2.8	A plan for reporting incidents internally and to QCB and other authorities. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting, IR-7 Incident Response Assistance.	**Organisational evidence**
8.2.9	Users trained to report incidents and to respond to certain ones. Organisational, non-technical. NIST SP 800-53: IR-2 Incident Response Training, AT-2 Literacy Training and Awareness.	**Organisational evidence**
8.2.10	Critical incidents reported to QCB and the authorities within one hour. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**

8.2.11	The incident escalation and response plan tested annually against scenarios such as ransomware and denial of service. Organisational, non-technical. NIST SP 800-53: IR-3 Incident Response Testing.	**Organisational evidence**
8.2.12	Incidents documented and lessons learned used to improve handling. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, IR-5 Incident Monitoring.	**Organisational evidence**
8.2.13	Customers' security awareness raised through notices and announcements. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
8.2.14	QCB and the Ministry of Interior kept informed of large-scale incidents. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
8.2.15	An ITIL framework considered for incident management. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures.	**Organisational evidence**

8.3 Patch management

8.3.1	A patch management process: roles, sourcing and validating patches, impact assessment and failed deployments. Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation, CM-3 Configuration Change Control.	**Organisational evidence**
8.3.2	Operating systems, devices and software patched regularly under the patch process. Checked, coverage partial. NIST SP 800-53: SI-2 Flaw Remediation. **Scope of this evidence** The verdict concerns the software in the images of the workloads outside the exempt namespaces. The versions of the Bahriya Kubernetes Engine and Kubernetes are recorded beside it. Patching the nodes' operating systems, and other systems and devices, are the bank's to evidence.	**Pass**

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.

8.3.3 Vendor releases monitored, and patches for publicly known vulnerabilities applied promptly. **Pass**

Checked, coverage partial. NIST SP 800-53: SI-2 Flaw Remediation, RA-5 Vulnerability Monitoring and Scanning, SI-5 Security Alerts, Advisories, and Directives.

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.

8.3.4 Critical patches tested before production, with other mitigations where a patch breaks a critical application. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation, CM-4 Impact Analyses.

8.3.5 Compensating protection where no patch exists for a vulnerability. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation, RA-7 Risk Response.

8.3.6 The delay in patching new vulnerabilities measured against the bank's baseline. **Recorded**

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

cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.

8.4 Logging and security monitoring

8.4.1 A logging and monitoring policy naming the assets and processes to be monitored and logged. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AU-1 Policy and Procedures, SI-4 System Monitoring.

8.4.2 Continuous monitoring of applications, devices and servers, with responsibilities assigned. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, CA-7 Continuous Monitoring, AU-12 Audit Record Generation.

8.4.3 Monitoring set by criticality, under a four-eyes principle. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, AC-5 Separation of Duties.

8.4.4 Logging enabled on infrastructure and applications handling critical information, with logs protected from change or deletion. **Pass**

Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation, AU-9 Protection of Audit Information.

Scope of this evidence The evidence is the cluster's API audit log: that it is enabled, and that only root can read or change its directory and files on each control-plane node. Logging by applications and other infrastructure, the continuous monitoring of the logs' integrity, their protection against the cluster's administrators and of copies forwarded elsewhere, and the protection of every other log are the bank'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.
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.

8.4.5 A security operations centre operating around the clock, on site or in Qatar. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.

8.4.6 Audit trails of administrators and privileged users reviewed on an alert or incident. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting.

8.4.7 Logs kept for at least six months, recording date, time, command, address and authentication, monitored automatically and by the SOC, with significant logs reviewed by hand. **Fail**

Platform, coverage partial. NIST SP 800-53: AU-11 Audit Record Retention, AU-3 Content of Audit Records, AU-2 Event Logging.

Fails in Platform API server audit log.

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.audit-rotation	**Fail**	The API server keeps its audit log for at most 30 days, fewer than the 180 the regime requires. A log collected to a central store may meet the requirement; that store is the customer's to evidence. Establishes: How long the API server keeps its audit log on the node. The API server deletes a rotated file at its age limit or its file-count limit, whichever comes first, so the age limit is an upper bound: it is the retention only where no file-count limit applies. An absent --audit-log-maxbackup is taken as Kubernetes' documented default, 0, no limit on the number of files. Where a file-count limit applies, the days kept depend on how much is logged, and the regime's period is evidenced by the central log store the audit log is forwarded to.

8.4.8 User access reviewed every six months, with unneeded accounts disabled or removed. **Recorded**

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

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

8.4.9 A SIEM that collects, correlates and analyses events and alerts on suspicious activity. **Organisational evidence**

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

8.4.10 An enterprise log repository for managing and keeping logs. **Fail**

Checked, coverage partial. NIST SP 800-53: AU-4 Audit Log Storage Capacity, AU-6 Audit Record Review, Analysis, and Reporting.

Scope of this evidence The verdict concerns whether the cluster's logs leave its nodes: Fluent Bit sending them to a central store, or another log shipper, named, whose destination the bank evidences. The repository itself, and how it manages and keeps logs, are the bank'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.

8.4.11 Incident information obtained from, and recommendations acted on from, an outsourced security provider. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services, IR-4 Incident Handling.

8.4.12 Logs holding personal information protected as privacy law requires. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AU-9 Protection of Audit Information, PT-2 Authority to Process Personally Identifiable Information.

8.4.13 Monitoring and logging lawful under the applicable frameworks. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AU-1 Policy and Procedures, PM-18 Privacy Program Plan.

8.4.14 Security logs classified by criticality and protected from unauthorised access and tampering. **Pass**

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

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

8.4.15 Monitoring integrated with incident handling, with exceptions recorded and acted on. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.

8.4.16 Network surveillance with intrusion detection and prevention. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, SC-7 Boundary Protection.

8.5 Capacity management

8.5.1 A capacity management policy: utilisation thresholds, performance and a capacity plan. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, SC-5 Denial-of-service Protection.

8.5.2	System performance monitored continuously against agreed targets. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
8.5.3	Capacity planning for sudden peaks in transactions and for performance incidents. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
8.5.4	The effect of changes on capacity and performance assessed. Organisational, technical, outside the cluster. NIST SP 800-53: CM-4 Impact Analyses.	**Organisational evidence**
8.5.5	CPU, network and memory use monitored continuously by tools on each system. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
8.5.6	Capacity planning extended to backup and disaster recovery environments. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, CP-7 Alternate Processing Site.	**Organisational evidence**

8.6 Problem management

8.6.1	A problem management framework: root causes, known errors, workarounds and permanent fixes. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling, SI-2 Flaw Remediation.	**Organisational evidence**
8.6.2	Problem management roles, and problems handled within service levels. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
8.6.3	A helpdesk for first-line technology support. Organisational, technical, outside the cluster. NIST SP 800-53: IR-7 Incident Response Assistance.	**Organisational evidence**
8.6.4	Root causes found and recurrence prevented. Organisational, technical, outside the cluster. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
8.6.5	An ITIL framework considered for problem management. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**

8.7 Backup

8.7.1	A backup and archiving process: frequency, media, access and classification, in line with local regulation. Organisational, technical, outside the cluster. NIST SP 800-53: CP-9 System Backup.	**Organisational evidence**

8.7.2 Backup and archiving in place, with copies kept off site. **Fail**

Checked, coverage partial. NIST SP 800-53: CP-9 System Backup, CP-6 Alternate Storage Site.

Scope of this evidence The verdict concerns whether Longhorn has an available backup target, which is outside the cluster, and a recurring backup job, or Velero an available storage location, also outside it, and an active schedule; the last backup of each volume or schedule is recorded beside it. Archiving, and the backups of other systems, are the bank'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.

8.7.3 Backups holding sensitive information encrypted before they leave the site. **Nothing to check**

Checked, coverage partial. NIST SP 800-53: CP-9(8) Cryptographic Protection.

Scope of this evidence The verdict concerns whether each backed-up Longhorn volume outside the exempt namespaces is encrypted, so that its backups leave the site encrypted. The backups of other systems are the bank'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.

8.7.4 Recovery from backup tested and validated every six months. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-9(1) Testing for Reliability and Integrity, CP-4 Contingency Plan Testing.

8.8 Technology refresh

8.8.1 A management-approved refresh policy: standards, cycles, acquisition and disposal. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-22 Unsupported System Components, PM-1 Information Security Program Plan.

8.8.2 An up-to-date inventory of hardware and software in production and disaster recovery, with support details. **Recorded**

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

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

8.8.3 A refresh plan so outdated and unsupported systems are replaced or upgraded in time. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-22 Unsupported System Components.

8.8.4 End-of-life and end-of-support dates tracked, with outdated systems phased out or risk-assessed. **Incomplete**

Checked, coverage partial. NIST SP 800-53: SA-22 Unsupported System Components, RA-3 Risk Assessment.

Scope of this evidence The verdict covers the cluster's Kubernetes release, judged against the end-of-life dates the Kubernetes project publishes; its Bahriya Kubernetes Engine release, judged against Mamluk's published support policy; and the operating systems of the images outside the exempt namespaces, judged against trivy's end-of-life data. A release or an image out of support fails, and the versions are recorded. The nodes' operating systems and other systems, and phasing out or risk-assessing what is outdated, are the bank's to evidence.

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

8.8.5 An inventory of hardware and software in acceptance, test, staging and stock. **Recorded**

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

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

8.9 Cloud computing

8.9.1	A management-approved, periodically reviewed cloud policy naming what may be hosted in cloud and its risks. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PL-1 Policy and Procedures.	**Organisational evidence**
8.9.2	Minimum terms in a cloud agreement, among them costs, data leakage, unauthorised access, encryption controls, a migration plan to another provider, a rollback plan, exit, and notice when a government or third party asks for the data. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SA-4 Acquisition Process.	**Organisational evidence**
8.9.3	The cloud policy considers where hosted and backed-up data physically resides. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SA-9(5) Processing, Storage, and Service Location.	**Organisational evidence**
8.9.4	Periodic security compliance reports obtained from the cloud provider. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-2 Control Assessments.	**Organisational evidence**
8.9.5	Independent assurance reports obtained on the provider's controls. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-2 Control Assessments.	**Organisational evidence**
8.9.6	Cloud use does not transfer the bank's responsibility for risk controls; its risks are considered. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, RA-3 Risk Assessment.	**Organisational evidence**
8.9.7	The provider's security domains evidenced before contracting. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
8.9.8	Critical data kept out of cloud the bank does not control, with a bank-controlled private facility as the alternative. Organisational, non-technical. NIST SP 800-53: SA-9(5) Processing, Storage, and Service Location, SA-9 External System Services.	**Organisational evidence**
8.9.9	Key security controls written into the cloud agreement. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SA-4 Acquisition Process.	**Organisational evidence**
8.9.10	Due diligence on sovereignty, multi-tenancy, recoverability, compliance, audit and data offshoring. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
8.9.11	The contractual right to penetration-test the provided machine images and instances. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-8 Penetration Testing.	**Organisational evidence**

8.9.12	The contractual right and means to destroy the bank's data at the provider on exit. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, MP-6 Media Sanitization.	**Organisational evidence**
8.9.13	The contractual right to test and audit the provider's network layer serving the bank. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-8 Penetration Testing.	**Organisational evidence**
8.9.14	The provider's ability to recover services within the recovery time objective verified before contracting. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CP-2 Contingency Plan.	**Organisational evidence**

8.10 Access control

8.10.1 General principles

8.10.1.1	An access control policy and procedures for identifying, authenticating and authorising users. Organisational, non-technical. NIST SP 800-53: AC-1 Policy and Procedures, IA-1 Policy and Procedures.	**Organisational evidence**
8.10.1.2	Logical access based on roles, least privilege, need to know and need to have. Checked, coverage partial. NIST SP 800-53: AC-6 Least Privilege, AC-6(1) Authorize Access to Security Functions. Fails in ClusterRole tigera-operator, ClusterRole tigera-operator-secrets.	**Fail**

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.

8.10.1.3	Segregation of duties and a four-eyes principle, through role-based privileges. Organisational, technical, outside the cluster. NIST SP 800-53: AC-5 Separation of Duties.	**Organisational evidence**
8.10.1.4	Job rotation and cross-training. Organisational, non-technical. NIST SP 800-53: AC-5 Separation of Duties, PS-1 Policy and Procedures.	**Organisational evidence**
8.10.1.5	A process for lost, stolen or compromised passwords, known to users. Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**

8.10.1.6 Accounts handling critical information audited periodically against current roles. **Recorded**

Checked, coverage partial. NIST SP 800-53: AC-2(3) Disable Accounts.

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.

8.10.1.7 Access rights set by an access control matrix owned by the information or system owner. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement, AC-2 Account Management.

8.10.1.8 Sensitive security tasks divided so that no one person controls a critical process. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AC-5 Separation of Duties.

8.10.1.9 Logical access to networks controlled and restricted to authorised devices and services. **Fail**

Enforced, coverage partial. NIST SP 800-53: AC-4 Information Flow Enforcement, SC-7 Boundary Protection, IA-3 Device Identification and Authentication.

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.

8.10.1.10 Logon banners on authorised use, monitoring, acceptable use and the consequences of misuse. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-8 System Use Notification.

8.10.1.11 Controls against bypassing access control, with any bypass approved and attempts investigated. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement.

8.10.1.12 No one holds concurrent access to production and backup systems, and backup access is authorised for a purpose and time. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-5 Separation of Duties, CP-9 System Backup.

8.10.2 Identification and authentication

8.10.2.1 Every user identified by a unique identifier and accountable for its use. **Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), IA-4 Identifier Management, AC-2 Account Management.

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

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

8.10.2.2 Anonymous and shared accounts avoided, and tightly controlled where unavoidable. **Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), AC-2 Account Management, AC-2(9) Restrictions on Use of Shared and Group Accounts.

Scope of this evidence The verdict concerns whether anonymous requests are refused and sign-in to the cluster is delegated to the bank's identity provider; the role bindings are recorded beside it. Whether shared credentials, such as kubeadm's admin.conf, are still in use and how they are controlled, and accounts on other systems, are the bank's to evidence.

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

8.10.2.3 Default accounts renamed and their default passwords changed, where feasible. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management, CM-6 Configuration Settings.

Scope of this evidence The cluster's kubeadm admin.conf is a shared administrative credential that every Kubernetes cluster built with kubeadm has; the bank accounts for who holds it and how it is kept.

8.10.2.4 All accounts, privileged ones included, monitored and logged. **Pass**

Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.

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.

8.10.2.5 Shared identifiers, where unavoidable, tied to authorised users by time and place. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), AC-2 Account Management.

8.10.2.6 No account for anyone who is not staff, a contractor or a third party, save by approved exception. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-2 Account Management, PS-7 External Personnel Security.

8.10.2.7 Access through an appropriate authentication mechanism, with multi-factor authentication by sensitivity. **Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), IA-2(1) Multi-factor Authentication to Privileged Accounts.

Scope of this evidence The evidence is that sign-in to the cluster is delegated to the organisation's identity provider. Whether that provider requires multi-factor authentication, and authentication to other systems, are the bank'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.

8.10.2.8 Rights to create, read, update, delete or send information set by the owners' access control matrix. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement.

8.10.2.9 Authentication data protected in use against replay, interception and session hijacking. **Incomplete**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-23 Session Authenticity, IA-2(8) Access to Accounts — Replay Resistant.

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

8.10.2.10 A password policy enforcing strong passwords and considering two-factor authentication. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5(1) Password-based Authentication, IA-2(1) Multi-factor Authentication to Privileged Accounts.

8.10.2.11 Passwords changed at least every 60 days with a minimum age of one day, and changed at logon after expiry or reset. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-5(1) Password-based Authentication.

8.10.2.12 Screens locked as the bank's policy requires. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-11 Device Lock.

8.10.2.13	Access suspended after three failed attempts, for at least 30 minutes. Organisational, technical, outside the cluster. NIST SP 800-53: AC-7 Unsuccessful Logon Attempts.	**Organisational evidence**
8.10.2.14	A policy for verifying users of locked accounts before a helpdesk reset. Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**
8.10.2.15	Accounts inactive for more than 60 days suspended, and deleted when no longer needed. Organisational, technical, outside the cluster. NIST SP 800-53: AC-2(3) Disable Accounts.	**Organisational evidence**
8.10.2.16	An audit trail of successful and failed logins for accounts handling highly classified information, reviewed on an alert. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.	**Pass**

platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

8.10.3 System access

8.10.3.1	Procedures stating who may access which data, when, and by which method and location. Organisational, non-technical. NIST SP 800-53: AC-1 Policy and Procedures, AC-3 Access Enforcement.	**Organisational evidence**
8.10.3.2	An approval process for system access. Organisational, technical, outside the cluster. NIST SP 800-53: AC-2 Account Management.	**Organisational evidence**
8.10.3.3	System users vetted as the personnel security requirements require. Organisational, non-technical. NIST SP 800-53: PS-3 Personnel Screening.	**Organisational evidence**
8.10.3.4	Users told their responsibilities and acceptable use before access is granted. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior, AT-2 Literacy Training and Awareness.	**Organisational evidence**

8.10.4 Privileged access

8.10.4.1	The activities of privileged accounts logged, including maintenance, backup, recovery and out-of-hours work. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.	**Pass**

platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

8.10.4.2	Administrators use a separate account for ordinary work, and privileged activity is supervised, logged and reviewed.	**Pass**

Checked, coverage partial. NIST SP 800-53: AC-6(2) Non-privileged Access for Nonsecurity Functions, AC-6(7) Review of User Privileges, AU-6 Audit Record Review, Analysis, and Reporting, AU-2 Event Logging.

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.
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.

8.10.4.3	Changes to privileged accounts approved by the director and the information security officer.	**Organisational evidence**

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

8.10.4.4	The information security officer keeps the master list of privileged users and their access boundaries up to date.	**Recorded**

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

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

8.10.4.5	Privileged users cannot reach the logs of their own activity, and privileged accounts are never shared.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AU-9(4) Access by Subset of Privileged Users, AC-2 Account Management.

8.10.5 Remote access

8.10.5.1	Remote access only where the business requires it, authorised and risk-assessed.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-17 Remote Access.

8.10.5.2	Two-factor authentication for remote access to critical systems.	**Organisational evidence**

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

8.10.5.3	Remote sessions encrypted end to end, authentication included.	**Incomplete**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, AC-17 Remote Access.

Scope of this evidence The evidence is TLS into the cluster and to its control plane, the host firewall, and sign-in delegated to the bank's identity provider. Authentication and encryption of SSH access to the nodes, and other remote sessions, 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.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.
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.
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.

8.10.5.4	Remote access only from devices protected by a firewall and anti-malware.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-17 Remote Access, SI-3 Malicious Code Protection.

8.10.5.5	Security software on remote access systems kept patched.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation.

8.10.5.6	No split tunnelling or dual homing on remote access systems.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-7(7) Split Tunneling for Remote Devices.

8.11 Acceptable use

8.11.1.1	Users responsible for the assets given to them, used as the acceptable use policy allows.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.

8.11.1.2	Bank resources, internet access included, for business use only.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.

8.11.1.3	An acceptable use policy for information assets, the internet and email. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
8.11.1.4	Controls protecting information systems against cyber attack. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection, SC-7 Boundary Protection.	**Organisational evidence**
8.11.1.5	A policy on social media and forums. Organisational, non-technical. NIST SP 800-53: PL-4(1) Social Media and External Site/Application Usage Restrictions.	**Organisational evidence**
8.11.1.6	Users, contractors and third parties trained in acceptable use of assets, the internet and email. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
8.11.1.7	No public web email used from the bank's systems. Organisational, technical and non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
8.11.1.8	External parties agree to the handling of classified data, under confidentiality agreements and a risk assessment. Organisational, non-technical. NIST SP 800-53: PS-6 Access Agreements, CA-3 Information Exchange.	**Organisational evidence**
8.11.1.9	Controls against unauthorised websites and unauthorised software on workstations. Organisational, technical, outside the cluster. NIST SP 800-53: CM-11 User-installed Software, SC-7 Boundary Protection.	**Organisational evidence**
8.11.1.10	Web access through secure proxies and filtering gateways. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
8.11.1.11	Email protected against malware, phishing and spam by a filtering gateway. Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection, SI-3 Malicious Code Protection.	**Organisational evidence**
8.11.1.12	Users taught basic security hygiene, such as logging off and not running unknown software. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
8.11.1.13	Email use on public and non-work sites restricted, and emails classified. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**

9 Enterprise security

9.1 Network and infrastructure security

9.1.1 Network and infrastructure devices

9.1.1.1	High-level and detailed diagrams of the network and security architecture, reviewed on every significant change or quarterly. Organisational, technical, outside the cluster. NIST SP 800-53: PL-8 Security and Privacy Architectures, CM-2 Baseline Configuration.	**Organisational evidence**

9.1.1.2 A detailed inventory of network devices, servers and workstations. **Recorded**

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

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

9.1.1.3 Defence-in-depth network design: physical and VLAN segregation, port security, no single points of failure, a separate management network, a quarterly review of device configurations, network access control, IDS and IPS, a 24/7 network SOC, MFA for device management and an AAA server. **Fail**

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

Scope of this evidence Network segmentation only: the cluster's host firewall and its network policies. The other measures are the bank'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.

9.1.1.4 Audit trails of daily activity on critical devices, reviewed on an alert or incident. **Pass**

Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.

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.

9.1.1.5 Infrastructure and network devices tested for vulnerabilities and by penetration testing twice a year. **Recorded**

Checked, coverage partial. NIST SP 800-53: CM-2 Baseline Configuration, CA-8 Penetration Testing.

Scope of this evidence The evidence is the versions of the Bahriya Kubernetes Engine and Kubernetes the cluster runs, and its inventory, recorded for review. The scans of the workloads' images do not reach the control plane or the platform, so they are not evidence of this statement. Testing the infrastructure and network devices for vulnerabilities, and penetration testing, are the bank'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.
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.

9.1.1.6 Default accounts disabled or removed and default passwords changed. **Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-5 Authenticator Management, CM-6 Configuration Settings, AC-3 Access Enforcement, AC-6 Least Privilege. Evidence counted: platform.anonymous, policy.no-default-token; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict concerns whether anonymous requests are refused and whether Pods receive the default service account's token. Shared credentials such as kubeadm's admin.conf, and default accounts and passwords on other systems, are the bank's to evidence.

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.

9.1.1.7 A risk analysis for each application needing network access, and unneeded connections to critical networks closed. **Fail**

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

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.

9.1.1.8 A minimum hardening baseline for servers, virtual machines and network devices, based on industry practice and reviewed twice a year. **Fail**

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

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

cluster.workload-inventory	**Recorded**	13 namespaces, 21 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.
node.etcd-data	**Pass**	etcd's data directory is owned by root and closed to other users: so on all 1 node(s). Establishes: etcd's data directory on each control-plane node is owned by root and closed to other users (700).
node.file-permissions	**Pass**	Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s). Establishes: The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.
node.kubelet-hardening	**Pass**	The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s). Establishes: The kubelet keeps its read-only port closed and rotates its client certificates.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
platform.mesh-cni	**Not evaluated**	The service mesh CNI plugin: the platform could not observe it. Establishes: Meshed Pods run without elevated privileges, through the mesh's CNI plugin.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.

policy.resource-limits	**Fail**	3 object(s) fail the policy. Establishes: Every container declares memory and CPU limits.
trivy.limits	**Fail**	3 object(s) fail. Establishes: Containers without CPU or memory limits.
trivy.run-as-root	**Fail**	3 object(s) fail. Establishes: Containers that run as the root user.
trivy.seccomp	**Fail**	3 object(s) fail. Establishes: Containers without the runtime's default seccomp profile.

9.1.1.9 Administrators' access to the network and infrastructure monitored and reviewed. **Pass**

Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AC-17(1) Monitoring and Control, AU-6 Audit Record Review, Analysis, and Reporting.

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.

9.1.1.10 Logs protected from change or deletion, reviewed and backed up. **Pass**

Checked, coverage partial. NIST SP 800-53: AU-9 Protection of Audit Information, AU-6 Audit Record Review, Analysis, and Reporting.

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

9.1.1.11 Additions and changes to network infrastructure assessed for security. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CM-4 Impact Analyses.

9.1.1.12	Strong encryption of data in transit, at the application and the network layer. Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection. Fails in Node node-1.	**Fail**

node.kubelet-ciphers	**Fail**	The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 1 node(s). Establishes: The kubelet offers TLS 1.2 or later with AEAD cipher suites only.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.

9.1.2 Communications

9.1.2.1	Separate cabling and routing for systems handling highly sensitive information. Organisational, non-technical. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
9.1.2.2	A register of data cables, inspected periodically. Organisational, non-technical. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
9.1.2.3	Remote activation of conferencing equipment disabled. Organisational, technical, outside the cluster. NIST SP 800-53: SC-15 Collaborative Computing Devices and Applications.	**Organisational evidence**
9.1.2.4	Fax and multifunction devices encrypted end to end where applicable. Organisational, technical, outside the cluster. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**
9.1.2.5	Cables protected in conduit against tampering and damage. Organisational, non-technical. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
9.1.2.6	Redundant communication paths. Organisational, technical, outside the cluster. NIST SP 800-53: CP-8 Telecommunications Services.	**Organisational evidence**
9.1.2.7	Conduits in public areas not labelled in a way that reveals their purpose. Organisational, non-technical. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**

9.1.3 Virtual LANs

9.1.3.1	Administrative and network control traffic on a separate management network, with the default VLAN unused. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SC-7(29) Separate Subnets to Isolate Functions.	**Organisational evidence**

9.1.3.2	Control and administrative traffic prioritised and run in its own spanning tree instance. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
9.1.3.3	VLANs pruned on trunk interfaces. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
9.1.3.4	Voice traffic segregated, with its own quality of service. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**

9.1.4 Multifunction devices

9.1.4.1	A hardening baseline for multifunction devices, and users trained in their use. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
9.1.4.2	Authentication, encryption and auditing enabled on multifunction devices. Organisational, technical, outside the cluster. NIST SP 800-53: IA-3 Device Identification and Authentication, AU-2 Event Logging.	**Organisational evidence**
9.1.4.3	Multifunction devices physically protected against theft. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
9.1.4.4	Multifunction device firmware versions reviewed. Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation.	**Organisational evidence**

9.1.5 DNS

9.1.5.1	DNS zones signed, with the integrity of zone transfers protected. Organisational, technical, outside the cluster. NIST SP 800-53: SC-20 Secure Name/Address Resolution Service (Authoritative Source), SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver).	**Organisational evidence**
9.1.5.2	A DNS firewall against malware that uses DNS to reach its controllers. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SI-4 System Monitoring.	**Organisational evidence**
9.1.5.3	Redundant, separated internal and external DNS, with public DNS hardened in a DMZ. Organisational, technical, outside the cluster. NIST SP 800-53: SC-22 Architecture and Provisioning for Name/Address Resolution Service.	**Organisational evidence**

9.1.6 Internet

9.1.6.1	Firewalls and content filtering that scan files downloaded from the internet. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SI-3 Malicious Code Protection.	**Organisational evidence**
9.1.6.2	Internet gateways deny by default and are hardened. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7(5) Deny by Default — Allow by Exception, CM-6 Configuration Settings.	**Organisational evidence**

9.1.6.3	Internal and external traffic monitored to understand its patterns. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

9.1.7 Email

9.1.7.1	Mail servers configured with sender authentication against spoofing. Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection.	**Organisational evidence**
9.1.7.2	Distribution lists and automatic replies restricted. Organisational, technical, outside the cluster. NIST SP 800-53: AC-22 Publicly Accessible Content.	**Organisational evidence**
9.1.7.3	Redundant email servers. Organisational, technical, outside the cluster. NIST SP 800-53: CP-7 Alternate Processing Site.	**Organisational evidence**
9.1.7.4	Email servers hardened. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
9.1.7.5	An anti-spam gateway, and scanning and content filtering of email. Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection, SI-3 Malicious Code Protection.	**Organisational evidence**

9.1.8 Wireless

9.1.8.1	Wireless networks risk-assessed beforehand, authenticated and encrypted, with access points registered and approved, and kept isolated from the bank's infrastructure. Organisational, technical, outside the cluster. NIST SP 800-53: AC-18 Wireless Access, RA-3 Risk Assessment.	**Organisational evidence**
9.1.8.2	Current wireless encryption and strong client authentication; no WEP. Organisational, technical, outside the cluster. NIST SP 800-53: AC-18(1) Authentication and Encryption.	**Organisational evidence**
9.1.8.3	An encrypted VPN for confidential data over wireless. Organisational, technical, outside the cluster. NIST SP 800-53: AC-18 Wireless Access, SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**
9.1.8.4	An inventory of wireless devices, with keys changed when one is lost. Organisational, technical, outside the cluster. NIST SP 800-53: CM-8 System Component Inventory, AC-18 Wireless Access.	**Organisational evidence**
9.1.8.5	Periodic scans for rogue or misconfigured wireless devices, with quarterly wireless penetration tests and audits. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4(14) Wireless Intrusion Detection, CA-8 Penetration Testing.	**Organisational evidence**
9.1.8.6	Wireless access points hardened, with default settings changed at installation. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**

9.1.8.7	A firewall between wireless access points and the internal network. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, AC-18 Wireless Access.	**Organisational evidence**

9.1.9 Clock synchronisation

9.1.9.1	Time servers hardened. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
9.1.9.2	Time synchronisation authenticated, with no answer to unauthenticated requests. Organisational, technical, outside the cluster. NIST SP 800-53: SC-45 System Time Synchronization.	**Organisational evidence**
9.1.9.3	Devices synchronised to a time server that follows an agreed reference time, with drift from the reference tested. Platform, coverage partial. NIST SP 800-53: AU-8 Time Stamps, SC-45 System Time Synchronization.	**Not provided**

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.

9.1.10 VPN

9.1.10.1	VPN access restricted to approved business need, with remote devices monitored and VPN user access reconciled monthly. Organisational, technical, outside the cluster. NIST SP 800-53: AC-17 Remote Access, AC-2 Account Management.	**Organisational evidence**
9.1.10.2	Two-factor authentication before a VPN tunnel is established. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, AC-17 Remote Access.	**Organisational evidence**
9.1.10.3	No split tunnelling without compensating controls. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7(7) Split Tunneling for Remote Devices.	**Organisational evidence**
9.1.10.4	Uniform, documented cryptographic standards for VPNs. Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection, AC-17 Remote Access.	**Organisational evidence**
9.1.10.5	Posture checks on computers connecting by VPN. Organisational, technical, outside the cluster. NIST SP 800-53: AC-17 Remote Access, CM-6 Configuration Settings.	**Organisational evidence**
9.1.10.6	VPN sessions time out after inactivity. Organisational, technical, outside the cluster. NIST SP 800-53: SC-10 Network Disconnect.	**Organisational evidence**
9.1.10.7	VPN access logged and monitored. Organisational, technical, outside the cluster. NIST SP 800-53: AC-17(1) Monitoring and Control.	**Organisational evidence**

9.1.10.8	Modems disabled by default. Organisational, technical, outside the cluster. NIST SP 800-53: CM-7 Least Functionality.	**Organisational evidence**
9.1.10.9	VPN concentrators in a DMZ behind a firewall and intrusion prevention. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**

9.1.11 Information exchange

9.1.11.1	A risk assessment, including cascaded connections, before connecting to another network. Organisational, technical and non-technical. NIST SP 800-53: CA-3 Information Exchange, RA-3 Risk Assessment.	**Organisational evidence**
9.1.11.2	Trusted couriers and protection for physical media in transit. Organisational, non-technical. NIST SP 800-53: MP-5 Media Transport.	**Organisational evidence**
9.1.11.3	Information exchanged electronically protected against unauthorised access and interruption. Organisational, technical, outside the cluster. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, CA-3 Information Exchange.	**Organisational evidence**
9.1.11.4	A trained spokesperson for information released to the media. Organisational, non-technical. NIST SP 800-53: IR-7 Incident Response Assistance.	**Organisational evidence**
9.1.11.5	Agreements signed before information is exchanged, stating responsibilities. Organisational, non-technical. NIST SP 800-53: CA-3 Information Exchange, PS-6 Access Agreements.	**Organisational evidence**

9.1.12 Gateways

9.1.12.1	Administration of gateways under dual control by trained staff. Organisational, technical, outside the cluster. NIST SP 800-53: AC-5 Separation of Duties.	**Organisational evidence**
9.1.12.2	Gateways hardened before production. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
9.1.12.3	Gateways integrated with logging and real-time monitoring. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, AU-2 Event Logging.	**Organisational evidence**
9.1.12.4	Gateways integrated with analytics and threat intelligence, as recommended. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

9.1.13 Virtualisation

9.1.13.1	The legal and operational risks of virtualisation assessed. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
9.1.13.2	Virtual machines, hypervisors and their management systems hardened. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**

9.1.13.3	Physical and logical controls against unauthorised access to the virtual environment. Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement, IA-2 Identification and Authentication (Organizational Users).	**Organisational evidence**
9.1.13.4	Changes to the virtual environment under change management, and virtual machines patched. Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation.	**Organisational evidence**
9.1.13.5	Logging enabled, monitored and kept for virtual machines. Organisational, technical, outside the cluster. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.	**Organisational evidence**

9.1.14 Databases

9.1.14.1	Databases hardened, with default passwords and insecure settings changed at installation. Organisational, technical, outside the cluster. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
9.1.14.2	Database access by least privilege and roles, with stored information classified. Organisational, technical, outside the cluster. NIST SP 800-53: AC-6 Least Privilege, RA-2 Security Categorization.	**Organisational evidence**
9.1.14.3	Database access controls cannot be bypassed, for example by direct file access. Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement.	**Organisational evidence**
9.1.14.4	Individual accounts recommended for database administrators; a group account allowed only for automated jobs. Organisational, technical, outside the cluster. NIST SP 800-53: AC-2 Account Management, IA-2 Identification and Authentication (Organizational Users).	**Organisational evidence**
9.1.14.5	Database access logged, reviewed periodically and archived centrally. Organisational, technical, outside the cluster. NIST SP 800-53: AU-2 Event Logging, AU-6 Audit Record Review, Analysis, and Reporting.	**Organisational evidence**
9.1.14.6	Databases with critical or confidential information encrypted, with documented key management. Organisational, technical, outside the cluster. NIST SP 800-53: SC-28 Protection of Information at Rest, SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**

9.1.14.7	Databases patched promptly. Checked, coverage partial. NIST SP 800-53: SI-2 Flaw Remediation. **Scope of this evidence** The verdict concerns databases that run as workloads in the cluster, outside the exempt namespaces. Other databases are the bank's to evidence.	**Pass**

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.

9.2 Data security

9.2.1 Classification and labelling

9.2.1.1	An information classification policy based on industry standards, by sensitivity and impact. Organisational, non-technical. NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
9.2.1.2	Unlabelled or damaged-label assets treated as confidential by default. Organisational, non-technical. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
9.2.1.3	Information treated as private unless made for public release. Organisational, non-technical. NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
9.2.1.4	Process owners identify and classify the data their processes hold. Organisational, non-technical. NIST SP 800-53: RA-2 Security Categorization, PM-5 System Inventory.	**Organisational evidence**
9.2.1.5	Classified information marked by its confidentiality, integrity and availability ratings. Enforced, coverage partial. NIST SP 800-53: RA-2 Security Categorization, MP-3 Media Marking.	**Pass**

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

9.2.1.6	Staff and partners aware of labelling and need to know. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

9.2.1.7	Network details, configurations and personal data stored safely and encrypted.	**Not evaluated**

Platform, coverage partial. NIST SP 800-53: SC-28 Protection of Information at Rest.

platform.secret-encryption	**Not evaluated**	The platform could not observe Secret encryption. Establishes: Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.

9.2.1.8	Information made available on request and approval, on a need-to-know basis.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege.

9.2.2 Data leakage prevention

9.2.2.1	Procedures for handling and reporting the theft, loss or leakage of customer data.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, PM-18 Privacy Program Plan.

9.2.2.2	Sensitive data sent to external parties encrypted with strong standards.	**Fail**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection.

Scope of this evidence The evidence concerns TLS on traffic into the cluster and to its control plane and kubelets. Encryption of the data the bank's applications send to external parties is the bank's to evidence.

Fails in Node node-1.

node.kubelet-ciphers	**Fail**	The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 1 node(s). Establishes: The kubelet offers TLS 1.2 or later with AEAD cipher suites only.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.

9.2.2.3	Detection of suspicious access, change or transfer of data.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.

9.2.2.4	Endpoint data leakage prevention against copying customer data to portable media.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: MP-7 Media Use, SC-7 Boundary Protection.

9.2.2.5	Portable media ports disabled, with media used only in an isolated environment.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: MP-7 Media Use.

9.2.2.6	Outsourcing providers holding customer data bound to equivalent protection. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PS-7 External Personnel Security.	**Organisational evidence**

9.2.3 Data migration

9.2.3.1	A migration policy and method that verify the completeness and integrity of migrated data. Organisational, technical, outside the cluster. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SI-7 Software, Firmware, and Information Integrity.	**Organisational evidence**
9.2.3.2	Pre- and post-migration activities, responsibilities and timelines. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
9.2.3.3	Owners sign off each stage of a migration. Organisational, non-technical. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**
9.2.3.4	An audit trail of the conversion, including mappings and transformations. Organisational, technical, outside the cluster. NIST SP 800-53: AU-2 Event Logging, CM-3 Configuration Change Control.	**Organisational evidence**

9.2.4 Retention and archiving

9.2.4.1	Access rights to archived information defined to protect it. Organisational, technical, outside the cluster. NIST SP 800-53: AC-3 Access Enforcement.	**Organisational evidence**
9.2.4.2	Integrity tools on information and media, with procedures for backup, archive and recovery. Organisational, technical, outside the cluster. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity, CP-9 System Backup.	**Organisational evidence**
9.2.4.3	Archiving frequency and retention periods set by law and regulation, with financial transaction records kept at least 15 years and personal data retained as the privacy law requires. Organisational, non-technical. NIST SP 800-53: SI-12 Information Management and Retention.	**Organisational evidence**

9.3 Portable devices

9.3.1	Mobile device management that keeps corporate data in an encrypted container. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**
9.3.2	A policy on personal devices. Organisational, non-technical. NIST SP 800-53: AC-19 Access Control for Mobile Devices, PL-4 Rules of Behavior.	**Organisational evidence**
9.3.3	Personal device rules set by classification and risk, covering data, storage, recovery and training. Organisational, non-technical. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**

9.4 Threat and vulnerability management

9.4.1 Threat and vulnerability risk assessment

9.4.1.1	Risk assessment for each asset of the threats and vulnerabilities that could affect it. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
9.4.1.2	Each year, a gap analysis and risk assessment of whether controls and response plans suffice, with a roadmap to close the gaps promptly. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, CA-5 Plan of Action and Milestones.	**Organisational evidence**
9.4.1.3	The risk assessment programme's minimum content, from asset valuation to controls. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PM-9 Risk Management Strategy.	**Organisational evidence**
9.4.1.4	A risk management function with formal acknowledgement of technology risk. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
9.4.1.5	Events that could disrupt operations, reputation or earnings identified, with regulatory compliance assessed. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

9.4.2 Web applications

9.4.2.1	A web application firewall in front of applications. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
9.4.2.2	Security testing of web and mobile applications before and after implementation and after major changes. Checked, coverage partial. NIST SP 800-53: SA-11 Developer Testing and Evaluation, RA-5 Vulnerability Monitoring and Scanning.	**Pass**

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

9.4.2.3 Vulnerability assessment, code review and penetration testing of the application infrastructure at least twice a year. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, CA-8 Penetration Testing, SA-11(4) Manual Code Reviews.

Scope of this evidence The evidence is the scanning of the images of the workloads outside the exempt namespaces for known vulnerabilities. Code review, penetration testing, and the assessment of the cluster's nodes and platform, are the bank'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.

9.4.2.4 Secure development guidelines following OWASP, CERT and CWE. **Organisational evidence**

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

9.4.2.5 Information in web applications protected at rest, in transit and in use. **Incomplete**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

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.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.

9.4.3 Vulnerability assessment and penetration testing

9.4.3.1 Automated and manual vulnerability assessment at least twice a year, each compared with the last to confirm remediation. **Pass**

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

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

9.4.3.2 An action plan for identified vulnerabilities, shared with senior management. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-5 Plan of Action and Milestones, RA-5 Vulnerability Monitoring and Scanning.

9.4.3.3 Penetration testing at least twice a year. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-8 Penetration Testing.

9.4.3.4 Accepted vulnerabilities reviewed every six months. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: RA-7 Risk Response, CA-5 Plan of Action and Milestones.

9.4.4 Phishing

9.4.4.1 Domains protected and monitored against look-alike registrations. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, PM-16 Threat Awareness Program.

9.4.4.2 Email and DNS hardened against phishing with sender authentication and signing. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection.

9.4.4.3 Customers informed about phishing, with an address to report it, and QCB told of every phishing incident. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness, IR-6 Incident Reporting.

9.4.4.4 Evidence of phishing attacks kept for prosecution. **Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: IR-4 Incident Handling.

9.4.5 Malware

9.4.5.1 Malware detection and mitigation at host, network and user level. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection.

9.4.5.2	Anti-malware software and signatures kept up to date. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
9.4.5.3	Auto-run disabled, and removable media scanned when inserted. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection, MP-7 Media Use.	**Organisational evidence**
9.4.5.4	Attachments filtered at the email gateway. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection, SI-8 Spam Protection.	**Organisational evidence**
9.4.5.5	Firewall, intrusion prevention, DNS and proxy logs reviewed daily for indicators of compromise. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, AU-6 Audit Record Review, Analysis, and Reporting.	**Organisational evidence**

9.4.6 Denial of service

9.4.6.1	Bottlenecks and single points of failure exposed to denial of service identified. Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection.	**Organisational evidence**
9.4.6.2	Denial-of-service protection considered when choosing an internet provider. Organisational, non-technical. NIST SP 800-53: SC-5 Denial-of-service Protection.	**Organisational evidence**
9.4.6.3	A validated incident response framework for denial-of-service attacks. Organisational, technical, outside the cluster. NIST SP 800-53: IR-8 Incident Response Plan, SC-5 Denial-of-service Protection.	**Organisational evidence**

9.4.7 Intrusion detection

9.4.7.1	Intrusion prevention at both the internal and the external level. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
9.4.7.2	Suspicious activity on servers, networks and endpoints detected, alerted and blocked. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
9.4.7.3	A network traffic baseline, with deviations treated as priorities. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
9.4.7.4	A breach response plan for cyber intrusions. Organisational, technical and non-technical. NIST SP 800-53: IR-8 Incident Response Plan.	**Organisational evidence**
9.4.7.5	An intrusion investigated for its extent, impact and the vulnerabilities exploited. Organisational, technical, outside the cluster. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**

9.5 Physical and environmental security

9.5.1	Physical spaces zoned by security requirement, set by risk assessment at design. Organisational, non-technical. NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control.	**Organisational evidence**

9.5.2	Environmental conditions such as fire, smoke, temperature, water and dust monitored. Organisational, non-technical. NIST SP 800-53: PE-13 Fire Protection, PE-14 Environmental Controls, PE-15 Water Damage Protection.	**Organisational evidence**
9.5.3	Protection against power failure and interference, such as UPS and a generator. Organisational, non-technical. NIST SP 800-53: PE-11 Emergency Power.	**Organisational evidence**
9.5.4	Facilities and equipment protected by barriers, entry controls and physical security. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control, PE-6 Monitoring Physical Access.	**Organisational evidence**
9.5.5	Physical access approved as the access control rules require, visitors included. Organisational, non-technical. NIST SP 800-53: PE-2 Physical Access Authorizations, PE-8 Visitor Access Records.	**Organisational evidence**
9.5.6	A site security plan and procedures for secure areas. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures, PE-3 Physical Access Control.	**Organisational evidence**
9.5.7	Alarms for environmental, access, power, communication and server failures. Organisational, non-technical. NIST SP 800-53: PE-6 Monitoring Physical Access, PE-14 Environmental Controls.	**Organisational evidence**

9.6 Cryptography

9.6.1.1	A cryptographic policy based on industry standards, using established, well-tested algorithms. Platform, coverage partial. NIST SP 800-53: SC-13 Cryptographic Protection. Fails in Node node-1.	**Fail**

node.kubelet-ciphers	**Fail**	The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 1 node(s). Establishes: The kubelet offers TLS 1.2 or later with AEAD cipher suites only.
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.

9.6.1.2	A key management standard governing the whole lifecycle of cryptographic keys. Platform, coverage partial. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Not evaluated**

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

9.6.1.3 Confidential information protected by encryption in transit, at rest and in use, as risk assessment determines. **Incomplete**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

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.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.

9.6.1.4 Secure practices for web traffic, file transfer, remote access, email, hashing and disk encryption. **Fail**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest, SC-13 Cryptographic Protection.

Fails in Node node-1.

node.kubelet-ciphers	**Fail**	The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 1 node(s). Establishes: The kubelet offers TLS 1.2 or later with AEAD cipher suites only.
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.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.

9.6.1.5	Passwords protected at rest and in transit, with privileged passwords escrowed securely off site.	**Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-5 Authenticator Management, SC-28 Protection of Information at Rest.

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.
platform.secret-encryption	**Not evaluated**	The platform could not observe Secret encryption. Establishes: Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.
trivy.config-secrets	**Pass**	Every object outside the exempt namespaces passes. Establishes: ConfigMaps that hold secrets.

9.6.1.6	A hardware security module for key management and cryptographic processing.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-12(1) Availability, SC-13 Cryptographic Protection.

9.6.1.7	State-licensed digital certificates in production, with online revocation checking.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-17 Public Key Infrastructure Certificates.

9.7 Software development and acquisition

9.7.1 Software security

9.7.1.1	A secure development lifecycle following OWASP, CERT and CWE.	**Organisational evidence**

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

9.7.1.2 Test and development isolated from production, with access only for a business need. **Fail**

Checked, coverage partial. NIST SP 800-53: CM-4(1) Separate Test Environments, SC-7 Boundary Protection, AC-4 Information Flow Enforcement, AC-6 Least Privilege.

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

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-environment	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries an environment label, one of the values in namespaces.environments.
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
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.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.
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.

9.7.1.3 Applications classified under the national classification policy. **Pass**

Enforced, coverage partial. NIST SP 800-53: RA-2 Security Categorization.

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

9.7.1.4 Source code reviewed for vulnerabilities and malicious code. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-11(4) Manual Code Reviews.

9.7.1.5 Source code of custom critical applications held by the bank, or in escrow. **Organisational evidence**

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

9.7.1.6 Security requirements specified with the system requirements. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-4 Acquisition Process, SA-8 Security and Privacy Engineering Principles.

9.7.2 Applications

9.7.2.1 Applications reviewed for the external connections they attempt. **Fail**

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

Scope of this evidence Workloads' outbound connections are restricted only when the Convoy's default-deny network policy is turned on (generate.defaultDenyNetworkPolicy.enabled), which is off by default. Reviewing the connections each application attempts is the bank's.

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.

9.7.2.2	Integrity checks on backups and replicated systems to detect compromise or faulty changes. Organisational, technical, outside the cluster. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity, CP-9 System Backup.	**Organisational evidence**
9.7.2.3	Servers exposed to public networks hosted in a DMZ. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
9.7.2.4	Undocumented changes handled as security incidents. Organisational, technical, outside the cluster. NIST SP 800-53: IR-4 Incident Handling, CM-3 Configuration Change Control.	**Organisational evidence**

9.7.3 End-user development

9.7.3.1	The importance of office macros and user-built applications assessed. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
9.7.3.2	User-developed macros and scripts reviewed and tested before use. Organisational, technical, outside the cluster. NIST SP 800-53: CM-3 Configuration Change Control, SA-11 Developer Testing and Evaluation.	**Organisational evidence**

9.8 Media

9.8.1 Classification and labelling

9.8.1.1	Media classified by the information they hold and protected accordingly. Organisational, technical and non-technical. NIST SP 800-53: MP-3 Media Marking, RA-2 Security Categorization.	**Organisational evidence**
9.8.1.2	Media visibly labelled under a uniform documented scheme and protected against tampering. Organisational, non-technical. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**

9.8.2 Sanitisation and disposal

9.8.2.1	Media sanitisation procedures and tools, tested regularly. Organisational, technical, outside the cluster. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
9.8.2.2	Only authorised staff repair or maintain classified media. Organisational, non-technical. NIST SP 800-53: MA-5 Maintenance Personnel.	**Organisational evidence**
9.8.2.3	Documented procedures for destroying and disposing of media. Organisational, non-technical. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
9.8.2.4	Media destroyed by degaussing and physical destruction. Organisational, technical and non-technical. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
9.8.2.5	Destruction of media supervised by staff. Organisational, non-technical. NIST SP 800-53: MP-6(1) Review, Approve, Track, Document, and Verify.	**Organisational evidence**
9.8.2.6	Disposal that does not draw attention to the waste. Organisational, non-technical. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

9.8.2.7	Media with classified information, faulty media included, sanitised before disposal. Organisational, technical, outside the cluster. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
9.8.2.8	Disposal contractors bound to acceptable procedures. Organisational, non-technical. NIST SP 800-53: MP-6 Media Sanitization, SA-9 External System Services.	**Organisational evidence**

9.9 Data centres

9.9.1 Resilience

9.9.1.1	Data centres resilient and physically secure against internal and external threats. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control, CP-7 Alternate Processing Site.	**Organisational evidence**
9.9.1.2	Each data centre's perimeter, surroundings and building in the risk assessment. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, PE-23 Facility Location.	**Organisational evidence**
9.9.1.3	Redundancy of power, cooling, fire suppression and communications assessed. Organisational, non-technical. NIST SP 800-53: PE-11 Emergency Power, CP-8 Telecommunications Services.	**Organisational evidence**
9.9.1.4	Fire protection and suppression. Organisational, non-technical. NIST SP 800-53: PE-13 Fire Protection.	**Organisational evidence**
9.9.1.5	Uninterruptible and backup power at each data centre. Organisational, non-technical. NIST SP 800-53: PE-11 Emergency Power.	**Organisational evidence**

9.9.2 Physical security

9.9.2.1	Data centre access restricted to authorised staff. Organisational, non-technical. NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control.	**Organisational evidence**
9.9.2.2	Physical access revoked as soon as it is no longer needed. Organisational, non-technical. NIST SP 800-53: PE-2 Physical Access Authorizations.	**Organisational evidence**
9.9.2.3	Temporary access for vendors notified, approved and escorted. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control, MA-5 Maintenance Personnel.	**Organisational evidence**
9.9.2.4	The perimeter, building and equipment rooms secured and monitored. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control, PE-6 Monitoring Physical Access.	**Organisational evidence**
9.9.2.5	Physical, human and procedural controls in combination. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures.	**Organisational evidence**
9.9.2.6	Surveillance recording activity in the data centre. Organisational, non-technical. NIST SP 800-53: PE-6 Monitoring Physical Access.	**Organisational evidence**

9.9.2.7	Systems, racks, devices and tapes physically protected against unauthorised access. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control, PE-18 Location of System Components.	**Organisational evidence**

9.10 Outsourcing

9.10.1 Outsourcing IT

9.10.1.1	The board and senior management govern outsourced processes and set the framework for them. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PM-9 Risk Management Strategy.	**Organisational evidence**
9.10.1.2	QCB's prior approval before an outsourcing agreement, with its scope submitted. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
9.10.1.3	Risk assessment and due diligence of providers, with data jurisdiction clarified. Organisational, non-technical. NIST SP 800-53: SR-6 Supplier Assessments and Reviews, SA-9 External System Services.	**Organisational evidence**
9.10.1.4	Outsourced work formalised by a contract of service. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**
9.10.1.5	Approval required for significant subcontracting by the provider. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SR-3 Supply Chain Controls and Processes.	**Organisational evidence**
9.10.1.6	The right of internal and external auditors and QCB to audit providers. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
9.10.1.7	Independent assurance reports required from outsourcing providers. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-2 Control Assessments.	**Organisational evidence**
9.10.1.8	Provider reports monitored and audited against service levels. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-7 Continuous Monitoring.	**Organisational evidence**

9.10.1.9	Third-party remote access over channels encrypted end to end.	**Incomplete**

Platform, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, AC-17 Remote Access.

Scope of this evidence The evidence is TLS into the cluster and to its control plane, the host firewall, and sign-in delegated to the bank's identity provider. Third parties' SSH access to the nodes, and their remote access to other systems, 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.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.
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.
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.

9.10.1.10	Providers subject to the bank's change management for code changes, with their developers confined to test environments.	**Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CM-3 Configuration Change Control, SA-10 Developer Configuration Management.

9.10.1.11	In-house skills kept for outsourced technology as a contingency.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, PM-13 Security and Privacy Workforce.

9.10.1.12	No legal obstacle to obtaining source code developed by a third party.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process.

9.10.1.13	Providers report regularly on security posture and incidents.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, IR-6 Incident Reporting.

9.10.1.14	Providers able to operate through exceptional events such as loss of communication. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, SA-9 External System Services.	**Organisational evidence**
9.10.1.15	Group intermediaries and representative offices abroad have no access to the bank's IT systems in Qatar. Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services, AC-3 Access Enforcement.	**Organisational evidence**
9.10.1.16	Providers' controls at least as stringent as the bank's own. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PS-7 External Personnel Security.	**Organisational evidence**
9.10.1.17	The national information assurance baseline written into third-party contracts and subcontracts. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**

9.10.2 Data centre and technology providers

9.10.2.1	Due diligence on a data centre or technology provider's viability, capability and finances. Organisational, non-technical. NIST SP 800-53: SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
9.10.2.2	Applications and data hosted at providers located physically in Qatar. Organisational, non-technical. NIST SP 800-53: SA-9(5) Processing, Storage, and Service Location.	**Organisational evidence**
9.10.2.3	The bank's change control and monitoring apply to its technology providers, and their service quality and availability are kept under review. Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services, CM-3 Configuration Change Control.	**Organisational evidence**
9.10.2.4	Risk assessment of providers across several jurisdictions. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, RA-3 Risk Assessment.	**Organisational evidence**
9.10.2.5	Contracts that do not hinder audits by the bank or the regulator, with QCB notified first if those rights may be impeded. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
9.10.2.6	Approval required for significant subcontracting by the provider. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SR-3 Supply Chain Controls and Processes.	**Organisational evidence**
9.10.2.7	Agreements covering performance, service levels, availability, compliance, audit, security and exit. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SA-4 Acquisition Process.	**Organisational evidence**
9.10.2.8	Providers maintain and test a disaster recovery framework. Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan, SA-9 External System Services.	**Organisational evidence**

9.10.2.9	Disaster recovery plans reviewed and tested against credible worst cases. Organisational, technical, outside the cluster. NIST SP 800-53: CP-4 Contingency Plan Testing.	**Organisational evidence**
9.10.2.10	Providers' controls at least as stringent as the bank's, monitored by the bank. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, CA-7 Continuous Monitoring.	**Organisational evidence**
9.10.2.11	QCB's prior approval before engaging such providers. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**

10 Business applications

10.1 Internal fraud

10.1.1	Policies, procedures and controls to prevent fraud by employees. Organisational, non-technical. NIST SP 800-53: AC-5 Separation of Duties, PS-8 Personnel Sanctions.	**Organisational evidence**
10.1.2	An internal control framework against fraud, with periodic reviews of systems and controls. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy, CA-7 Continuous Monitoring.	**Organisational evidence**
10.1.3	A senior fraud review group that meets at least quarterly. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
10.1.4	Systems monitoring suspicious transactions. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
10.1.5	Media with card and account data stored securely to prevent card fraud, with card production kept physically apart from PIN generation. Organisational, non-technical. NIST SP 800-53: MP-4 Media Storage, SC-28 Protection of Information at Rest.	**Organisational evidence**

10.2 External fraud

10.2.1	Online, ATM and point-of-sale transactions monitored for fraud and money laundering by a real-time system. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
10.2.2	Counter-fraud measures acted on after alarms, such as velocity checks. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.	**Organisational evidence**
10.2.3	ATM and point-of-sale fraud and embezzlement reported to the Ministry of Interior, and QCB notified of these and of hacking, penetration, fake websites and forged cards. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
10.2.4	Fraud monitoring with online authorisation decisions, queries and tailored rules. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

10.3 Fraud risk management

10.3.1	Fraud vulnerability assessments across every channel. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
10.3.2	New products and processes analysed for fraud before launch, with loss limits. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
10.3.3	Residual fraud risks covered by monitored loss limits, reviewed with the business when losses reach 90 per cent of a limit. Organisational, non-technical. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
10.3.4	Cards, cheque books and passwords delivered to customers securely. Organisational, non-technical. NIST SP 800-53: MP-5 Media Transport.	**Organisational evidence**
10.3.5	Internet banking with transaction passwords, two-factor authentication, payee controls, limits and alerts. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts.	**Organisational evidence**
10.3.6	Access to information and transaction validation only for employees who need it. Organisational, technical, outside the cluster. NIST SP 800-53: AC-6 Least Privilege, AC-3 Access Enforcement.	**Organisational evidence**
10.3.7	Know-your-customer and know-your-employee and vendor due diligence. Organisational, non-technical. NIST SP 800-53: PS-3 Personnel Screening, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
10.3.8	A dedicated team for the security of the physical infrastructure. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures.	**Organisational evidence**
10.3.9	Regular fraud awareness for staff and customers. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
10.3.10	A strong internal control framework against fraud, kept under review. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

10.4 Fraud detection

10.4.1	Channels for reporting fraud, including system triggers and customer and employee alerts. Organisational, technical and non-technical. NIST SP 800-53: IR-6 Incident Reporting, SI-4 System Monitoring.	**Organisational evidence**
10.4.2	Mechanisms to report and investigate disputes, exceptions and suspicions, including a well-publicised whistle-blowing mechanism. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting, IR-4 Incident Handling.	**Organisational evidence**
10.4.3	A dedicated email address, telephone number and team for reports of fraud. Organisational, non-technical. NIST SP 800-53: IR-7 Incident Response Assistance.	**Organisational evidence**

10.5 Fraud investigation

10.5.1	Continuous training of the fraud team. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
10.5.2	Investigation reports shared within the bank and tracked to closure. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
10.5.3	Forensic techniques and data analysis tools, by risk appetite. Organisational, technical, outside the cluster. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**

10.6 Fraud reporting

10.6.1	Fraud in merchant acquiring reported to QCB. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
10.6.2	In a shared ATM network, the acquirer reports fraud and seeks the issuer's help in recovery. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
10.6.3	Data requested by the police shared, even where the bank only received fraudulent funds. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**

10.7 Customer fraud awareness

10.7.1	Continuous fraud awareness for customers. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

10.8 Employee fraud awareness

10.8.1	Fraud prevention training for employees by the fraud team. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

10.9 Customer education

10.9.1	Board commitment and resources for customer education. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources.	**Organisational evidence**
10.9.2	Customer awareness of cyber risks, with customers encouraged to report phishing. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
10.9.3	Ongoing customer awareness activities through several channels. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

10.10 Online systems

10.10.1	A security strategy for the confidentiality, integrity and availability of data and systems. Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan, PL-2 System Security and Privacy Plans.	**Organisational evidence**
10.10.2	Internet systems use established, well-scrutinised encryption algorithms. Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection.	**Organisational evidence**

10.10.3	Two-factor authentication to sign online banking transactions. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts.	**Organisational evidence**
10.10.4	Risk-assessed, token-based authorisation of transactions for institutional and corporate customers. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), RA-3 Risk Assessment.	**Organisational evidence**
10.10.5	Customers assured that online login and transactions are protected and authenticated. Organisational, technical, outside the cluster. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-23 Session Authenticity.	**Organisational evidence**
10.10.6	Physical and logical access limited to authorised staff, with processing and transmission controls. Platform, coverage partial. NIST SP 800-53: AC-3 Access Enforcement, SC-8 Transmission Confidentiality and Integrity. Fails in ClusterRole tigera-operator, ClusterRole tigera-operator-secrets.	**Fail**

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.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

10.10.7	Monitoring that alerts on abnormal activity, transmission errors and unusual transactions, with an action plan. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

10.10.8	Vulnerability assessment and penetration testing of online banking against attacks such as man-in-the-middle.	**Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, CA-8 Penetration Testing.

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.

10.10.9	High resilience and availability of online systems and the systems behind them.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, SC-5 Denial-of-service Protection.

10.11 Mobile services and payments

10.11.1	Security measures for mobile services and payments.	**Organisational evidence**

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

10.11.2	Fraud scenarios for mobile payments assessed and countered.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.

10.11.3	Sensitive information used by mobile services and payments protected.	**Organisational evidence**

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

10.11.4	Customers educated to protect their own mobile devices.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.

10.11.5	3-D Secure for cardholder authentication, with customers informed.	**Organisational evidence**

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

10.12 Payment cards

10.12.1	Compliance with PCI DSS and related payment standards.	**Organisational evidence**

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

10.12.2	Annual reporting of that compliance to QCB.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments.

10.12.3	EMV chips and terminals and strong card authentication. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).	**Organisational evidence**
10.12.4	Magnetic stripes protected. Organisational, technical, outside the cluster. NIST SP 800-53: MP-4 Media Storage.	**Organisational evidence**
10.12.5	Online authorisation only for ATM transactions, with PINs verified securely. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).	**Organisational evidence**
10.12.6	Security controls on payment card systems and networks. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
10.12.7	New cards activated only on the customer's instruction. Organisational, technical, outside the cluster. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**
10.12.8	Two-factor authentication, such as one-time passwords, for card-not-present payments online. Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts.	**Organisational evidence**
10.12.9	Prompt alerts to cardholders for transactions above their thresholds. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
10.12.10	Fraud detection with behavioural scoring and correlation. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
10.12.11	Transactions that depart from a cardholder's usual pattern investigated and authorised by the cardholder. Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

10.13 ATMs and kiosks

10.13.1	Measures against attacks on ATMs and kiosks, such as anti-skimming. Organisational, technical, outside the cluster. NIST SP 800-53: PE-3 Physical Access Control, SI-4 System Monitoring.	**Organisational evidence**
10.13.2	Regular customer awareness of ATM risks. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
10.13.3	Merchants contractually barred from swiping or storing card data in clear text. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
10.13.4	Point-of-sale terminals that meet PIN entry security standards. Organisational, technical, outside the cluster. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
10.13.5	Receipts that do not disclose card details. Organisational, technical, outside the cluster. NIST SP 800-53: SI-15 Information Output Filtering.	**Organisational evidence**

10.14 Cheques

10.14.1	Sensitive cheque information kept in a secure area. Organisational, non-technical. NIST SP 800-53: MP-4 Media Storage.	**Organisational evidence**

10.14.2	Digitally signed cheque data protected cryptographically. Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection.	**Organisational evidence**
10.14.3	Customer identification in line with know-your-customer practice. Organisational, non-technical. NIST SP 800-53: IA-12 Identity Proofing.	**Organisational evidence**

10.15 Core banking

10.15.1	Reliable, resilient core banking servers and infrastructure, managed under the network guidelines. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, SC-7 Boundary Protection.	**Organisational evidence**
10.15.2	Core banking applications and databases secured under the software and data security rules. Organisational, technical, outside the cluster. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SC-28 Protection of Information at Rest.	**Organisational evidence**
10.15.3	Vulnerability assessment and penetration testing of applications linked to core banking. Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, CA-8 Penetration Testing.	**Pass**

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

10.15.4	Core banking systems follow the cryptography and key management rules. Organisational, technical, outside the cluster. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management, SC-13 Cryptographic Protection.	**Organisational evidence**
10.15.5	Core banking resilient through continuity mechanisms, with security events archived as Qatari retention law requires, integrity controls on core data, versioned application changes, sensitive core records encrypted and role-based access. Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, SI-7 Software, Firmware, and Information Integrity, SC-28 Protection of Information at Rest, AC-3 Access Enforcement.	**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-controlle
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-ciphers Fail

The kubelet offers TLS 1.2 or later with AEAD cipher suites only.

The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 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: minimum not set, suites not set

How to fix On a Bahriya Kubernetes Engine cluster, set compliance.controlPlane.enabled to true in config.yaml (the default) and upgrade each node with upgrade.sh, which writes tlsMinVersion and tlsCipherSuites into every kubelet's configuration. Elsewhere, set tlsMinVersion to VersionTLS12 and tlsCipherSuites to AES-GCM suites only in the kubelet's configuration, then restart the kubelet. (Bahriya Tersane)

Fails (2)

Object	What is wrong	Full result
Node node-1	the minimum TLS version is not set, which allows TLS 1.0	`What was read on the node is in this run's snapshot.json, under nodes.`
Node node-1	no cipher suites are set, so the defaults, which include CBC suites, are offered	`What was read on the node is in this run's snapshot.json, under nodes.`

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.audit-rotation Fail

How long the API server keeps its audit log on the node. The API server deletes a rotated file at its age limit or its file-count limit, whichever comes first, so the age limit is an upper bound: it is the retention only where no file-count limit applies. An absent --audit-log-maxbackup is taken as Kubernetes' documented default, 0, no limit on the number of files. Where a file-count limit applies, the days kept depend on how much is logged, and the regime's period is evidenced by the central log store the audit log is forwarded to.

The API server keeps its audit log for at most 30 days, fewer than the 180 the regime requires. A log collected to a central store may meet the requirement; that store is the customer's to evidence.

- audit.rotation: maxage=30 maxbackup=10 maxsize=100
- the regime's log-retention-days: 180

How to fix Keep the audit log for at least the period the regime requires. On BKE, which always limits the number of audit log files, forward the log to a central log store that keeps it that long, and give that store's retention setting to your assessor as evidence: from BKE 2.6.1, Fluent Bit collects the audit log on the control-plane nodes under the tag audit.*, and an output that matches that tag sends it to your store; on earlier versions, forward it with your own collector. On another cluster, either forward the log in the same way, or set --audit-log-maxage to at least that period and leave --audit-log-maxbackup unset or 0 on each API server's static Pod manifest, with enough disk on each control-plane node to hold that period. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Platform API server audit log	kept at most 30 days before rotation; the regime requires 180	`kubectl -n bahriya-system get configmap bke-platform -o jsonpath='{.data.audit\.rotation}'`

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.key-provider Not evaluated

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

The platform could not observe the encryption provider.

- encryption.provider: unknown

platform.mesh-cni Not evaluated

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

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

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

platform.oidc Not evaluated

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

The platform could not read the authentication configuration.

- authentication.oidc-issuers: unknown

platform.pod-security Not evaluated

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

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

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

platform.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.version-support Pass

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

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

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

platform.versions Recorded

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

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

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

policy.default-deny-generated Not provided

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

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

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

policy.ingress-tls Nothing to check

Every Ingress serves its hosts over TLS.

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

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

policy.namespace-classification Pass

Every application namespace carries a data classification label.

Every object the policy judged passes it.

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

Fails in exempt namespaces, not counted (1)

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

policy.namespace-environment Pass

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

Every object the policy judged passes it.

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

Fails in exempt namespaces, not counted (1)

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

policy.namespace-network-policy Fail

Every application namespace has at least one NetworkPolicy.

1 object(s) fail the policy.

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

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

Fails (1)

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

Fails in exempt namespaces, not counted (1)

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

policy.no-default-token Pass

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

Every object the policy judged passes it.

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

policy.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.config-secrets Pass

ConfigMaps that hold secrets.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0109
- 29 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

ConfigMap trivy-system/trivy-operator	AVD-KSV-0109: ConfigMap with secrets. ConfigMap 'trivy-operator' in 'trivy-system' namespace stores secrets in key(s) or value(s) '{"node.collector.imagePullSecret"}'	`kubectl get configauditreport configmap-trivy-operator -n trivy-system -o yaml`
ConfigMap trivy-system/trivy-operator-config	AVD-KSV-0109: ConfigMap with secrets. ConfigMap 'trivy-operator-config' in 'trivy-system' namespace stores secrets in key(s) or value(s) '{"OPERATOR_ACCESS_GLOBAL_SECRETS_SERVICE_ACCOUNTS", "OPERATOR_EXPOSED_SECRET_SCANNER_ENABLED", "OPERATOR_METRICS_EXPOSED_SECRET_INFO_ENABLED", "OPERATOR_PRIVATE_REGISTRY_SCAN_SECRETS_NAMES"}'	`kubectl get configauditreport configmap-trivy-operator-config -n trivy-system -o yaml`
ConfigMap trivy-system/trivy-operator-trivy-config	AVD-KSV-0109: ConfigMap with secrets. ConfigMap 'trivy-operator-trivy-config' in 'trivy-system' namespace stores secrets in key(s) or value(s) '{"trivy.imagePullSecret"}'	`kubectl get configauditreport configmap-trivy-operator-trivy-config -n trivy-system -o yaml`

trivy.external-ip Pass

Services with external IP addresses.

Every object outside the exempt namespaces passes.

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

trivy.image-os-support Not evaluated

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

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

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

trivy.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(3) Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
AC-2(9) Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions].
AC-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(1) Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals and roles] to: (a) [Assignment: organization-defined organization-defined security functions (deployed in hardware, software, and firmware)] ; and (b) [Assignment: organization-defined security-relevant information].
AC-6(2) Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.
AC-6(7) Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles and classes] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
AC-7 Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period] ; and b. Automatically [Selection (one or more): lock the account or node for [Assignment: organization-defined time period] ; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm] ; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.
AC-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-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(1) Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.
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-18(1) Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.
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-22 Publicly Accessible Content	a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.
AT-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c. Review and update the current awareness and training: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AT-2 Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined organization-defined events]; b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]; c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
AT-2(3) Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.
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.
AT-4 Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for [Assignment: organization-defined time period].

AU-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c. Review and update the current audit and accountability: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AU-2 Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined organization-defined event types (subset of the event types defined in [AU-2a.](#au-2_smt.a)) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
AU-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-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-9(4) Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].
AU-11 Audit Record Retention	Retain audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-12 Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in [AU-2a](#au-2_smt.a) on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in [AU-2c](#au-2_smt.c) that include the audit record content defined in [AU-3](#au-3).
CA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and c. Review and update the current assessment, authorization, and monitoring: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CA-2 Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined assessment frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
CA-2(1) Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.
CA-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-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-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c. Review and update the current configuration management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CM-2 Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances] ; and 3. When system components are installed or upgraded.
CM-3 Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency] ; when [Assignment: organization-defined configuration change conditions]].
CM-3(2) Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(4) Security and Privacy Representatives	Require [Assignment: organization-defined organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].

CM-4 Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(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-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-9 Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by [Assignment: organization-defined personnel or roles] ; and e. Protects the configuration management plan from unauthorized disclosure and modification.
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].

CP-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c. Review and update the current contingency planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-2 Contingency Plan	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by [Assignment: organization-defined organization-defined personnel or roles]; b. Distribute copies of the contingency plan to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system [Assignment: organization-defined frequency]; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
CP-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-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(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.
IA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and c. Review and update the current identification and authentication: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IA-2 Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-2(1) Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.

IA-2(2) Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.
IA-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-4 Identifier Management	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for [Assignment: organization-defined time period].
IA-5 Authenticator Management	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.
IA-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(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-5 Incident Monitoring	Track and document incidents.
IR-6 Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period] ; and b. Report incident information to [Assignment: organization-defined authorities].
IR-7 Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

IR-8 Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency] ; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined organization-defined incident response personnel (identified by name and/or by role) and organizational elements] ; and e. Protect the incident response plan from unauthorized disclosure and modification.
MA-5 Maintenance Personnel	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
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-6(1) Review, Approve, Track, Document, and Verify	Review, approve, track, document, and verify media sanitization and disposal actions.

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-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c. Review and update the current physical and environmental protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PE-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-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-13 Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.
PE-14 Environmental Controls	a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels] ; and b. Monitor environmental control levels [Assignment: organization-defined frequency].
PE-15 Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
PE-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-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-12 Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
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-16 Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PM-18 Privacy Program Plan	a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; 3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; 4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; 5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and 6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and b. Update the plan [Assignment: organization-defined frequency] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.
PM-28 Risk Framing	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel] ; and c. Review and update risk framing considerations [Assignment: organization-defined frequency].
PM-29 Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.
PS-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c. Review and update the current personnel security: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

PS-3 Personnel Screening	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with [Assignment: organization-defined organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].
PS-4 Personnel Termination	Upon termination of individual employment: a. Disable system access within [Assignment: organization-defined time period]; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by terminated individual.
PS-5 Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].
PS-6 Access Agreements	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [Assignment: organization-defined frequency] ; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].
PS-7 External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements; d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period] ; and e. Monitor provider compliance with personnel security requirements.
PS-8 Personnel Sanctions	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
PS-9 Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.
PT-2 Authority to Process Personally Identifiable Information	a. Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.

RA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
RA-2 Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
RA-3 Risk Assessment	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles] ; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
RA-5 Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-5(2) Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency] ; prior to a new scan; when new vulnerabilities are identified and reported].

RA-7 Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
SA-4 Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria.
SA-8 Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined organization-defined systems security and privacy engineering principles].
SA-9 External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].
SA-9(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-10 Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].
SA-11 Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency to conduct] at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.
SA-11(4) Manual Code Reviews	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].

SA-15 Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined organization-defined security and privacy requirements].
SA-22 Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].
SC-5 Denial-of-service Protection	a. [Selection: protect against; limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events] ; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].
SC-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(5) Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].
SC-7(7) Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].
SC-7(29) Separate Subnets to Isolate Functions	Implement [Selection: physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].
SC-8 Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-10 Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.
SC-12 Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements].
SC-12(1) Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.
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-15 Collaborative Computing Devices and Applications	a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed] ; and b. Provide an explicit indication of use to users physically present at the devices.
SC-17 Public Key Infrastructure Certificates	a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
SC-22 Architecture and Provisioning for Name/Address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.
SC-23 Session Authenticity	Protect the authenticity of communications sessions.
SC-28 Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-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-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions	(a) Measure the time between flaw identification and flaw remediation; and (b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].

SI-3 Malicious Code Protection	a. Implement [Selection (one or more): signature-based; non-signature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]] ; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
SI-4 System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives] ; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
SI-4(14) Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.
SI-5 Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles] ; [Assignment: organization-defined elements] ; [Assignment: organization-defined external organizations]] ; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
SI-7 Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined organization-defined software, firmware, and information] ; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined organization-defined actions].
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-10 Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs].

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-15 Information Output Filtering	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].
SR-3 Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls] ; and c. Document the selected and implemented supply chain processes and controls in [Selection (one or more): security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].
SR-5 Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined strategies, tools, and methods].
SR-6 Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].