National Information Assurance Standard, version 2.1 (May 2023): technical evidence

Neither Mamluk LLC-FZ nor its products are affiliated with or endorsed by the National Cyber Security Agency (Qatar).

Regime	National Information Assurance Standard, version 2.1 (May 2023), National Cyber Security Agency (NCSA), 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.

NCSA is the source and owner of the National Information Assurance Standard. The requirement summaries in this report are Mamluk's paraphrase, not the standard's text.

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

The standard marks its baseline controls, which apply to every asset rated I1, A1 or C1 or above. Its other controls are additional: after a risk assessment, one or more in each applicable domain are chosen and implemented for assets rated at level 2, and two or more for assets at level 3 or above.

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

356 requirements: 7 enforced by a policy, 8 checked, 17 provided by the platform, 324 organisational (145 technical, outside the cluster; 122 non-technical; 57 technical and non-technical).

Outcome	Requirements	Meaning
Fail	11	The cluster was checked and something does not meet the requirement. The findings say what and where.
Not provided	2	A control the requirement needs is switched off on this cluster.
Incomplete	7	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	2	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	8 of which with exception: 0	Every check behind the requirement passed on this run's date. Where coverage is partial, the pass covers the cluster's part only.
Recorded	2	Facts collected for the organisation's reviewer, such as an inventory or a list of access; no verdict.
Nothing to check	0	The cluster has nothing of this kind yet, for example no Ingress to check for TLS. Neither a pass nor a failure.
Organisational evidence	324	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

16 object(s) fail at least one check: 4 cluster-wide and 12 in 1 namespace(s). They are listed under Fix first, those that fail a requirement marked "Baseline control" first, then the most severe first.

Fix first

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

Cluster-wide

4 object(s), most severe Critical.

Platform **`API server audit log`** Fails SM 7 Baseline control: SM 7

MEDIUM kept at most 30 days before rotation; the regime requires 120

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}'
```

ClusterRole **tigera-operator** Fails AM 1, AM 2, AM 31, PS 8

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 AM 1, AM 2, AM 31, PS 8

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 DR 4

HIGH neither Longhorn nor Velero is installed

Check cluster.backups.

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

Full result

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

Namespace payments

12 object(s), most severe High.

Namespace **payments** Fails NS 5, SS 4, SS 21, SS 23 Baseline control: NS 5, SS 4, SS 21

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.

CronJob **`nightly`** Fails PR 7

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

Check policy.images-signed.

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

Full result

```
kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml
```

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

CronJob **`weekly`** Fails PR 7

HIGH no signing key covers registry.example.com/payments/checkout:3.10.1

Check policy.images-signed.

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

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

Deployment **`ledger`** Fails PR 7

HIGH no signing key covers registry.example.com/payments/checkout:3.10.1

Check policy.images-signed.

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

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

Deployment **`legacy-batch`** Fails PR 7

HIGH no signing key covers registry.example.com/payments/checkout:3.10.1

Check policy.images-signed.

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

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

Deployment **`unsigned-app`** Fails PR 7

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

Check policy.images-signed.

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

Full result

```
kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml
```

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

Job **`migrate-once`** Fails PR 7

HIGH no signing key covers registry.example.com/payments/checkout:3.10.1

Check policy.images-signed.

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

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

Job **nightly-now** Fails PR 7

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

Check policy.images-signed.

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

Full result

```
kubectl get policyreport 6a73d7cc-01f5-42d8-9d6c-462a360b517b -n payments -o yaml
```

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

Pod **nightly-now-k7cbf** Fails PR 7

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

Check policy.images-signed.

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

Full result

```
kubectl get policyreport 4074d46b-fb0f-4ce3-8312-15270922068d -n payments -o yaml
```

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

Pod **one-off** Fails PR 7

HIGH no signing key covers registry.example.com/payments/checkout:3.10.1

Check policy.images-signed.

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

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

Pod **unsigned-app-b5567644f-vpkpp** Fails PR 7

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

Check policy.images-signed.

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

Full result

```
kubectl get policyreport 3f291cbb-5fdd-4171-9ead-42230533be9f -n payments -o yaml
```

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

ReplicaSet **unsigned-app-b5567644f** Fails PR 7

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

Check policy.images-signed.

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

Full result

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

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

Requirements

4 Security governance and processes

IG Security governance

IG 1	A Security Manager appointed to own the information security programme and run it. Organisational, non-technical. Baseline control. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
IG 2	A budget sufficient to staff and run the information security programme. Organisational, non-technical. Baseline control. NIST SP 800-53: PM-3 Information Security and Privacy Resources.	**Organisational evidence**
IG 3	The Security Manager reports to senior management, for example through the risk or internal audit function. Organisational, non-technical. Baseline control. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
IG 4	The head of the organisation gives documented, continuing support to building, running and maintaining ICT security processes and infrastructure. Organisational, non-technical. Baseline control. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-3 Information Security and Privacy Resources.	**Organisational evidence**
IG 5	Anyone the head delegates to approve variations from the standard holds more authority than the Security Manager. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
IG 6	Security responsibilities defined for the Security Manager, management, staff and third parties. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PS-7 External Personnel Security.	**Organisational evidence**
IG 7	The Security Manager has executive support, security knowledge, working knowledge of the organisation's systems or the resources for it, and the capacity for the role. Organisational, non-technical. Baseline control. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-13 Security and Privacy Workforce.	**Organisational evidence**
IG 8	The Security Manager's role includes recommending security improvements, bringing security into change management, coordinating security documentation, and reporting incidents to NCSA and taking part in their investigation. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PM-2 Information Security Program Leadership Role, IR-6 Incident Reporting.	**Organisational evidence**

IG 9	The Security Manager answers for security plans and procedures, technical advice across the system life cycle, system security standards, certification where it applies, the awareness programme, and regular review of system security, audit trails and the integrity of configurations. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PL-2 System Security and Privacy Plans, AU-6 Audit Record Review, Analysis, and Reporting.	**Organisational evidence**
IG 10	The Security Manager knows the systems' security operating procedures and the roles of their managers, administrators and users. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-13 Security and Privacy Workforce.	**Organisational evidence**

RM Risk management

RM 1	A process to assess the threats to, and the vulnerabilities of, critical information assets, those whose aggregate security level is Medium or High. Organisational, non-technical. Baseline control. NIST SP 800-53: RA-3 Risk Assessment, RA-1 Policy and Procedures.	**Organisational evidence**
RM 2	A risk treatment plan based on the assessment. Organisational, non-technical. Baseline control. NIST SP 800-53: RA-7 Risk Response, PM-9 Risk Management Strategy.	**Organisational evidence**
RM 3	Treatment plans and residual risk for assets rated High vetted by senior management. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PM-9 Risk Management Strategy, RA-7 Risk Response.	**Organisational evidence**
RM 4	The controls chosen under RM 2 and RM 3 monitored periodically for effectiveness. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CA-7 Continuous Monitoring.	**Organisational evidence**
RM 5	Risk assessment built into business processes and repeated on change, including changes in the business or in law and regulation. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

TM Third-party security management

TM 1	Outsourced areas and services remain the organisation's accountability for governance, compliance and risk. Organisational, non-technical. Baseline control. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
TM 2	The risks of outsourcing understood and acknowledged. Organisational, non-technical. Baseline control. NIST SP 800-53: SA-9 External System Services, RA-3 Risk Assessment.	**Organisational evidence**
TM 3	This standard's controls written into third-party contracts, and binding on the third party's subcontractors. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**

TM 4	Third parties bound by contract to report regularly on the security of the outsourced service, incidents included. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-9 External System Services, IR-6 Incident Reporting.	**Organisational evidence**
TM 5	Third parties' services, reports and records monitored and reviewed continuously, and audited at set intervals. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**

DL Data labelling

DL 1	The organisation acts as the labelling authority for the data it collects or holds. Organisational, non-technical. Baseline control. NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
DL 2	Every information asset given a classification rating, and assets rated C1 to C4 marked Internal, Restricted, Secret or Top Secret. Enforced, coverage partial. Baseline control. NIST SP 800-53: RA-2 Security Categorization, MP-3 Media Marking. **Scope of this evidence** The verdict is that each namespace outside the exempt namespaces carries a classification label from the values the organisation configures. Rating and marking each information asset, in the cluster and outside it, are the organisation's to evidence. policy.namespace-classification — **Pass** Every object the policy judged passes it. Establishes: Every application namespace carries a data classification label.	**Pass**
DL 3	Information assets labelled Internal by default, unless meant for public release or rated higher. Organisational, non-technical. Baseline control. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
DL 4	The labelling system supports need to know, protecting information from unauthorised disclosure and use. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
DL 5	Staff and contractors taught about data labelling. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

CM Change management

CM 1	A documented change management process, followed, with categories such as planned major changes, maintenance and minor changes, and emergency changes. Organisational, non-technical. Baseline control. NIST SP 800-53: CM-3 Configuration Change Control, CM-1 Policy and Procedures.	**Organisational evidence**
CM 2	A cross-functional change committee, with the security and risk functions represented. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CM-3(4) Security and Privacy Representatives.	**Organisational evidence**
CM 3	Every proposed change documented and approved by the committee. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**

CM 4	After a change that may affect security, the need for re-certification assessed; the system still meets the baseline controls, with risk analysis where needed. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: CM-4 Impact Analyses, CA-6 Authorization.	**Organisational evidence**
CM 5	System documentation updated to reflect each change. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CM-3 Configuration Change Control, SA-5 System Documentation.	**Organisational evidence**
CM 6	Emergency changes may go ahead on the verbal approval of the committee's head and the process owner, then be documented and risk-analysed afterwards. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CM-3 Configuration Change Control.	**Organisational evidence**

PS Personnel security

PS 1	HR processes aligned with the organisation's security policies. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PS-1 Policy and Procedures.	**Organisational evidence**
PS 2	Security requirements and obligations set out in an HR standard that all staff can read. Organisational, non-technical. Baseline control. NIST SP 800-53: PS-1 Policy and Procedures, PL-4 Rules of Behavior.	**Organisational evidence**
PS 3	Information about personnel collected, managed and kept with care, as the personal data protection law requires. Organisational, non-technical. Baseline control. NIST SP 800-53: PT-1 Policy and Procedures, PT-2 Authority to Process Personally Identifiable Information.	**Organisational evidence**
PS 4	Security responsibilities written into job descriptions and applied throughout employment. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PS-9 Position Descriptions.	**Organisational evidence**
PS 5	Candidates and contractors, subcontracted workers included, screened for integrity; existing staff may be screened again where needed. Organisational, non-technical. Baseline control. NIST SP 800-53: PS-3 Personnel Screening.	**Organisational evidence**
PS 6	Staff sign an agreement of their security obligations, confidentiality and non-disclosure included, on joining and on a change of role. Organisational, non-technical. Baseline control. NIST SP 800-53: PS-6 Access Agreements.	**Organisational evidence**
PS 7	Controls that stop staff, vendors, contractors and visitors disclosing, misusing or corrupting information without authority. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PS-6 Access Agreements, PL-4 Rules of Behavior.	**Organisational evidence**

PS 8	Access rights limited to what each user's job needs, by least privilege and need to have.	**Fail**

Checked, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AC-6 Least Privilege, AC-6(1) Authorize Access to Security Functions.

Scope of this evidence The verdict covers the cluster's RBAC: subjects and workloads with privileged, exec or Secret access, and service account tokens. Access rights in other systems are the organisation's to evidence.

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

policy.no-default-token	**Pass**	Every object the policy judged passes it. Establishes: Pods say whether they mount a service account token, so that none receives one by default.
trivy.rbac-exec	**Pass**	Every object outside the exempt namespaces passes. Establishes: Roles that allow executing into Pods or impersonating privileged groups.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.
trivy.token-automount	**Pass**	Every object outside the exempt namespaces passes. Establishes: Pods that mount a service account token.

PS 9	Sensitive security tasks split under the four-eyes principle, so no one person controls a critical process.	**Organisational evidence**

Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-5 Separation of Duties.

PS 10	A disciplinary process defined, communicated and enforced, and documented in the HR standard.	**Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: PS-8 Personnel Sanctions.

PS 11	Visitors and vendors logged with identity, time and purpose, badged and visibly marked as visitors, told of their obligations and escorted in secure areas.	**Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: PE-8 Visitor Access Records, PE-2 Physical Access Authorizations.

PS 12	HR raises a change request on any change of duties or departure, so that assets are returned and physical and logical access changed or removed.	**Organisational evidence**

Organisational, technical and non-technical. Baseline control. NIST SP 800-53: PS-4 Personnel Termination, PS-5 Personnel Transfer, AC-2 Account Management.

SA Security awareness

SA 1	A defined security awareness programme with a budget.	**Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.

SA 2	Training covers at least this standard's baseline, the organisation's requirements, legal duties, business controls, acceptable use, discipline, and whom to ask and how to report incidents.	**Organisational evidence**

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

SA 3	All staff, and contractors and third parties where relevant, trained in the organisation's policies as their role requires. Organisational, non-technical. Baseline control. NIST SP 800-53: AT-2 Literacy Training and Awareness, AT-3 Role-based Training.	**Organisational evidence**
SA 4	Staff trained to recognise social engineering and not to give information away in social or public settings. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-2(3) Social Engineering and Mining.	**Organisational evidence**
SA 5	Training content reviewed and updated for new trends and threats, changes in infrastructure, and changes in law. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.	**Organisational evidence**
SA 6	Awareness training at induction, with periodic refreshers. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
SA 7	Training followed by an assessment of its effectiveness, with attendance recorded. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-4 Training Records.	**Organisational evidence**
SA 8	Posters, the intranet, email and similar media may support the programme. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

IM Incident management

IM 1	A person appointed to own the incident management programme, with a point of contact for security communications. Organisational, non-technical. Baseline control. NIST SP 800-53: IR-8 Incident Response Plan, IR-7 Incident Response Assistance.	**Organisational evidence**
IM 2	An incident response capability, based on the classification policy, that assesses the risk to data, processes, systems and networks periodically. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IR-4 Incident Handling, RA-3 Risk Assessment.	**Organisational evidence**
IM 3	Procedures for detecting, evaluating and responding to incidents. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
IM 4	Procedures for reporting, managing and recovering from incidents, internally, with NCSA, and with others such as law enforcement. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IR-6 Incident Reporting, IR-4 Incident Handling.	**Organisational evidence**
IM 5	Staff made aware that they should report incidents. Organisational, non-technical. Baseline control. NIST SP 800-53: IR-6 Incident Reporting, AT-2 Literacy Training and Awareness.	**Organisational evidence**

IM 6	Incidents categorised and prioritised by the kind of attack and how critical the affected systems are. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
IM 7	A record of the organisation's incidents, kept in coordination with NCSA. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IR-5 Incident Monitoring.	**Organisational evidence**
IM 8	Critical incidents reported to NCSA within two hours of being identified. Organisational, non-technical. Baseline control. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
IM 9	An annual security assurance plan, run by the incident management coordinator, which may include penetration tests, audits of procedures and incident exercises. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CA-2 Control Assessments, CA-8 Penetration Testing, IR-3 Incident Response Testing.	**Organisational evidence**

BC Business continuity management

BC 1	A person appointed to own the business continuity programme. Organisational, non-technical. Baseline control. NIST SP 800-53: CP-1 Policy and Procedures, CP-2 Contingency Plan.	**Organisational evidence**
BC 2	A business continuity plan to keep critical processes and essential services going, based on recovery time and recovery point objectives for each process. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
BC 3	The plan covers the possible disaster scenarios and includes disaster recovery. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
BC 4	The plan kept current, with the relevant parts shared with the team, staff and service providers. Organisational, non-technical. Baseline control. NIST SP 800-53: CP-2 Contingency Plan.	**Organisational evidence**
BC 5	A current copy of the plan, with backup media, kept in a fire- and tamper-proof safe, and another off site, preferably in a different geographic zone from the primary data centre. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CP-9 System Backup, CP-6 Alternate Storage Site.	**Organisational evidence**
BC 6	Alternate recovery sites identified, hot, warm or cold according to the recovery time objectives. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CP-7 Alternate Processing Site.	**Organisational evidence**
BC 7	Strong controls in contracts that outsource business, IT or continuity functions. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-9 External System Services, CP-2 Contingency Plan.	**Organisational evidence**

BC 8 The plan tested at least yearly, and after significant change in the business or in law and regulation. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CP-4 Contingency Plan Testing.

BC 9 Staff made aware of the plan. **Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: CP-3 Contingency Training.

SM Logging and security monitoring

SM 1 Logging and continuous monitoring of access, changes and command execution on information assets. **Pass**

Platform, coverage partial. Baseline control. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation, SI-4 System Monitoring.

Scope of this evidence The evidence is the API server's audit log: who did what to the cluster, and when. Logging on other assets, and the continuous monitoring of the logs, are the organisation's to evidence.

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

SM 2 Monitoring set by the criticality of infrastructure, data and applications, with round-the-clock monitoring recommended for assets rated at level 3 and duties separated as PS 9 requires. **Organisational evidence**

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

SM 3 Monitoring kept within legal and regulatory limits, privacy law included, and covering the use of and access to systems. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SI-4 System Monitoring, PT-2 Authority to Process Personally Identifiable Information.

SM 4 Logging enabled on all infrastructure, equipment and applications that handle information rated C2 or above. **Pass**

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

Scope of this evidence The evidence is the API server's audit log. Logging on the nodes' operating systems, in the applications in the cluster, and on other equipment, is the organisation's to evidence.

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

SM 5 Security logs classified C3, and application and system logs at the rating of their system. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AU-9 Protection of Audit Information, RA-2 Security Categorization.

SM 6 Logs that hold personal information protected as privacy law requires. **Organisational evidence**

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

SM 7 Logs kept for at least 120 days, up to a maximum set by criticality and by sector law and regulation. **Fail**

Platform, coverage partial. Baseline control. NIST SP 800-53: AU-11 Audit Record Retention.

Scope of this evidence The verdict is whether the API server keeps its own audit log for at least the 120 days the standard requires. A log collected to a central store may meet the requirement; that store, and the retention of other logs, are the organisation's to evidence.

Fails in Platform API server audit log.

platform.audit-rotation	**Fail**	The API server keeps its audit log for at most 30 days, fewer than the 120 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.

SM 8 Audit logs that record date, time, authentication with unique user and system identifiers, failures and changes, and commands and their output, enough to reconstruct an incident and restore the system. **Pass**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AU-3 Content of Audit Records, AU-12 Audit Record Generation.

Scope of this evidence The evidence is the API server's audit policy, BKE's or the customer's, which records the user, the verb, the source address and the time of each request. Commands run on the nodes or in containers, their output, and logging on other systems are the organisation's to evidence.

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

SM 9 Exceptions identified and reported under the incident handling policy (IM). **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IR-6 Incident Reporting, AU-6 Audit Record Review, Analysis, and Reporting.

DR Data retention and archival

DR 1 Retention periods set and documented for information assets, critical ones included, governed at least by policy, regulation and law. **Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: SI-12 Information Management and Retention.

DR 2 Retained data stored so that its confidentiality, integrity and availability are kept and it can be reached for its purpose. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-12 Information Management and Retention, SC-28 Protection of Information at Rest.

DR 3	Personal and sensitive information kept no longer than needed, as privacy law requires. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SI-12 Information Management and Retention, PT-2 Authority to Process Personally Identifiable Information.	**Organisational evidence**
DR 4	Backup, archival and recovery processes have procedures that keep the data's integrity and confidentiality. Checked, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: CP-9 System Backup. **Scope of this evidence** The verdict concerns whether Longhorn has an available backup target and a recurring backup job; each volume's last backup is recorded beside it. The procedures, the integrity and confidentiality of backups, archival, recovery and other systems are the organisation'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.	**Fail**
DR 5	Archived data keeps its classification markings and is protected accordingly. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: MP-3 Media Marking, MP-4 Media Storage.	**Organisational evidence**
DR 6	Archiving technology reviewed for obsolescence, and archives kept recoverable. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: CP-9 System Backup.	**Organisational evidence**

DC Documentation

DC 1	An organisational security policy that takes in this standard's requirements. Organisational, non-technical. Baseline control. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
DC 2	A system security plan for every critical system, with security operating procedures where needed. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-2 System Security and Privacy Plans.	**Organisational evidence**
DC 3	System security standards and procedures consistent with the security policy and its objectives. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-2 System Security and Privacy Plans, PL-1 Policy and Procedures.	**Organisational evidence**
DC 4	ICT security documentation classified at least C3 (Restricted) by default. Organisational, non-technical. Baseline control. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
DC 5	Documentation reviewed and updated periodically. Organisational, non-technical. Baseline control. NIST SP 800-53: PL-1 Policy and Procedures, PL-2 System Security and Privacy Plans.	**Organisational evidence**

AC Audit and certification

AC 1	A programme of governance and security improvement in line with the classification policy and this standard. Organisational, non-technical. Baseline control. NIST SP 800-53: PM-1 Information Security Program Plan, PM-14 Testing, Training, and Monitoring.	**Organisational evidence**
AC 2	Compliance with applicable laws and regulations, as they stand and as amended or added. Organisational, non-technical. Baseline control. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures.	**Organisational evidence**
AC 3	Audited by the accredited audit organisation NCSA designates. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**
AC 4	The information system, its infrastructure, people and processes, audited at least yearly and after any change that may affect security. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
AC 5	The audit's scope approved by NCSA, and covering all information assets, people and processes. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
AC 6	Recertification wherever a change or finding calls the accreditation into question: full for major changes to a system's security design, partial for moderate changes or those that affect two or more security requirements. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-6 Authorization.	**Organisational evidence**
AC 7	Every non-conformance fixed within a defined timeline. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-5 Plan of Action and Milestones.	**Organisational evidence**
AC 8	Exemptions approved by the competent department of NCSA. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-6 Authorization.	**Organisational evidence**

5 Security controls

CS Communications security

CS 1	Users told the highest classification allowed in internal and external telephone conversations, judged from the internal telephone system and any encryption on external lines. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
CS 2	Separate cabling distribution for systems handling information rated C4 and above. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**

CS 3	Conduits in public or visitor areas not labelled in a way that draws attention to them. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
CS 4	A cable register recording at least each cable's identifier, classification, source, destination and floor plan. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
CS 5	Cables inspected regularly against the register. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
CS 6	Redundant communication paths may be provided to keep connectivity. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: CP-8 Telecommunications Services.	**Organisational evidence**
CS 7	Users told the highest classification allowed in internal and external telephone conversations, as CS 1 also requires. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
CS 8	Speakerphones off in calls where information rated C3 or above may be discussed and overheard. Organisational, non-technical. Baseline control. NIST SP 800-53: SC-42 Sensor Capability and Data.	**Organisational evidence**
CS 9	Remote activation of conferencing equipment disabled in sensitive locations. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-15 Collaborative Computing Devices and Applications.	**Organisational evidence**
CS 10	Rooms used for sensitive conversations or meetings protected against sound leaking out. Organisational, non-technical. Baseline control. NIST SP 800-53: PE-19 Information Leakage.	**Organisational evidence**
CS 11	Fax machines at both ends secured with encryption devices when sending information rated C2 or above. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**
CS 12	Fax standards for the classification met at both ends, with the receiver collecting faxes promptly and telling the sender if one does not arrive in the agreed time. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-5 Access Control for Output Devices.	**Organisational evidence**

NS Network security

NS 1	Details of the internal network, system configuration, directories and other sensitive technology neither disclosed publicly nor open to enumeration. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: AC-22 Publicly Accessible Content.	**Organisational evidence**

NS 2	Default accounts such as root or administrator removed or disabled, or their passwords changed as SS requires.	**Incomplete**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AC-2 Account Management, IA-5 Authenticator Management, 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 organisation'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.

NS 3	Network configuration controlled by the network manager, with every change approved through change control, documented in line with the network policy and security plan, and reviewed regularly; earlier configurations kept.	**Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CM-3 Configuration Change Control.

NS 4	For each managed network, a high-level diagram of all its connections and a logical diagram of all its devices, updated as the network changes and dated.	**Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: PL-2 System Security and Privacy Plans, CM-8 System Component Inventory.

NS 5 Networks designed to limit unauthorised access to traffic, for example with switches and port security, unused ports disabled, segregation by firewalls and routers on a need-to-know basis, encryption, configuration comparison, edge authentication, device filtering, intrusion detection and time-of-day restriction. **Fail**

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

Scope of this evidence Network segmentation only: the cluster's host firewall and its network policies. The verdict can be Pass only when the Convoy's generated default-deny network policy is turned on (it is off by default). The other measures are the organisation'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.

NS 6	Management networks separated, by a dedicated VLAN or physical infrastructure, and reached over secure channels such as a VPN or SSH.	**Not evaluated**

Platform, coverage partial. Baseline control. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, AC-17 Remote Access. Evidence counted: platform.control-plane-tls, platform.host-firewall; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is TLS to the control plane and the kubelets, and the host firewall on the nodes. A separate management network, and SSH access to the nodes, are the organisation'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.

NS 7	In business-critical networks, IP telephony kept on VLANs of its own.	**Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.

NS 8	Administrative access only from a VLAN to one of the same or a lower classification.	**Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement.

NS 9	Switches secured with every measure the risk assessment recommends and the vendor's hardening guidance.	**Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-6 Configuration Settings.

NS 10	No trunking or port mirroring on switches that carry VLANs of different classifications.	**Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-7 Boundary Protection.

NS 11	Network multifunction devices not used to copy documents of a higher classification than their network.	**Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement.

NS 12	A multifunction device that can send information through a gateway to another network identifies, authenticates and audits its users as strongly as a workstation does, and the gateway filters what it sends under the data export rules; the standard marks the filtering as baseline.	**Organisational evidence**
	Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), AU-2 Event Logging, AC-4 Information Flow Enforcement.	
NS 13	No direct connection from a multifunction device to a telephone network of lower classification unless the device has been evaluated for flow control, blocking export by classification, authentication and audit.	**Organisational evidence**
	Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement, SC-7 Boundary Protection.	
NS 14	Multifunction devices deployed only under policies, plans and procedures for their use.	**Organisational evidence**
	Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	
NS 15	Information rated C1 or above not kept permanently in a multifunction device, and cleared from its memory once a job is done.	**Organisational evidence**
	Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-4 Information in Shared System Resources.	
NS 16	Multifunction devices sanitised as MS requires.	**Organisational evidence**
	Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	
NS 17	A separate internal DNS server, on the internal network, for domain information not disclosed to the Internet.	**Organisational evidence**
	Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-22 Architecture and Provisioning for Name/Address Resolution Service.	
NS 18	Public DNS information served from a secured, locally hosted bastion server; government organisations may use the Government DNS as their primary.	**Organisational evidence**
	Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-20 Secure Name/Address Resolution Service (Authoritative Source).	
NS 19	DNS servers without single points of failure, hardened, and kept secure.	**Organisational evidence**
	Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-22 Architecture and Provisioning for Name/Address Resolution Service, CM-6 Configuration Settings.	
NS 20	Zone files signed, and zone transfers and dynamic updates mutually authenticated and protected for integrity.	**Organisational evidence**
	Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-20 Secure Name/Address Resolution Service (Authoritative Source).	
NS 21	The origin and integrity of DNS data assured by cryptography.	**Organisational evidence**
	Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-20 Secure Name/Address Resolution Service (Authoritative Source), SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver).	

NS 22	DNS services, zone transfers included, provided to authorised users only. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-22 Architecture and Provisioning for Name/Address Resolution Service.	**Organisational evidence**
NS 23	The cryptography for NS 20 and NS 21 uses a hardware security module for key management and processing, as CY requires. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**
NS 24	Software and files from the Internet screened for malicious software, HTTP traffic included. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
NS 25	The Internet gateway denies every service that has not been specifically enabled. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-7 Boundary Protection. **Scope of this evidence** The Internet gateway is the organisation's to evidence. The cluster's own controls, the host firewall on its nodes and the generated default-deny network policy for its workloads (off by default), support it and are evidenced under NS 5 and SS 21.	**Organisational evidence**
NS 26	Web browsers on workstations configured and kept up to date, for example with active content limited, current versions, no saved passwords, pop-ups blocked, caches cleared and plug-in installation off. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
NS 27	The capability to monitor traffic and infer its patterns and use, as SM describes. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
NS 28	Email servers hardened and run as bastion servers, with details of internal systems kept out of email headers where feasible. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
NS 29	TLS used with the SMTP mail server, as CY requires. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**
NS 30	The Sender Policy Framework implemented, with bounces sent only to senders SPF can verify. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-8 Spam Protection.	**Organisational evidence**
NS 31	Internal distribution lists protected from external access, to reduce unsolicited email. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-8 Spam Protection.	**Organisational evidence**

NS 32	Email gateways scan all mail in and out for compliance with policy and for malicious code. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection, SI-8 Spam Protection.	**Organisational evidence**
NS 33	Wireless LANs used only with adequate authentication, encryption and security management. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-18 Wireless Access.	**Organisational evidence**
NS 34	Strong wireless protocols such as WPA2 and EAP-TLS, not relied on alone: dynamic key exchange and a VPN over wireless for data rated C3 or above, and WEP never used. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-18(1) Authentication and Encryption.	**Organisational evidence**
NS 35	An inventory of devices with wireless interfaces, with a change of keys and SSID considered when one goes missing. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-8 System Component Inventory, AC-18 Wireless Access.	**Organisational evidence**
NS 36	Regular scans for unauthorised wireless access points. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-4(14) Wireless Intrusion Detection.	**Organisational evidence**
NS 37	Access points placed to limit tapping from public areas. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: PE-18 Location of System Components.	**Organisational evidence**
NS 38	Client-side 802.1X settings secured, for example by validating the server certificate against a chosen CA and not prompting users to trust new servers. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-18(1) Authentication and Encryption.	**Organisational evidence**
NS 39	Default network names, keys, SNMP community strings and other insecure settings changed at installation, with SSIDs that name no department, system or product. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-6 Configuration Settings, AC-18 Wireless Access.	**Organisational evidence**
NS 40	For private access points, keys changed regularly and SSID broadcast off, with MAC filtering considered. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-18 Wireless Access.	**Organisational evidence**
NS 41	A firewall or router between access points and the network, passing only the ports needed from the wireless segment. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-7 Boundary Protection, AC-18 Wireless Access.	**Organisational evidence**
NS 42	Wireless intrusion detection or prevention recommended for networks rated at level 3. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-4(14) Wireless Intrusion Detection.	**Organisational evidence**

NS 43 Separate SSIDs for different VLANs and user groups, such as guests limited to the Internet. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-18 Wireless Access.

NS 44 NTP servers secured according to good practice. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-45 System Time Synchronization.

NS 45 Devices with real-time clocks set to an agreed standard, such as UTC or local time, with a procedure to find and correct drift. **Not provided**

Platform, coverage partial. Baseline control. NIST SP 800-53: AU-8 Time Stamps, SC-45 System Time Synchronization.

Scope of this evidence The evidence is that the cluster's nodes keep their clocks synchronised to the time servers configured for them. Other devices, and the procedure for correcting drift, are the organisation's to evidence.

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

NS 46 Government organisations may use the Qatari Government time server as their primary NTP server. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-45 System Time Synchronization.

NS 47 All servers and network devices synchronised with the organisation's NTP server, itself set as NS 45 and NS 46 describe. **Not provided**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AU-8 Time Stamps, SC-45 System Time Synchronization.

Scope of this evidence The evidence is that the cluster's nodes synchronise to the time servers configured for them. Whether those are the organisation's NTP server, and the synchronisation of other servers and devices, are the organisation's to evidence.

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

NS 48 VPNs carrying data rated C3 or above use two-factor authentication: a one-time password or key pair, and a username and password checked by an external authentication server. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.

Scope of this evidence This concerns VPNs. Sign-in to the cluster is under AM 36.

NS 49	VPN sessions ended after a set period of inactivity, with sign-in needed to reconnect. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-10 Network Disconnect.	**Organisational evidence**
NS 50	Split tunnelling not allowed without suitable controls, preferably one network connection at a time. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-7(7) Split Tunneling for Remote Devices.	**Organisational evidence**
NS 51	Computers on the VPN run security software, current patches and anti-malware with current signatures, always active. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
NS 52	Gateway firewalls control traffic from VPN clients to authorised systems. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection, AC-17 Remote Access.	**Organisational evidence**
NS 53	Voice and data on separate networks, physically or by VLAN, with the voice gateway keeping VoIP protocols off the data network. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
NS 54	VoIP gateways and other suitable security mechanisms in use. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
NS 55	Secure protocols such as SRTP evaluated and used, and unneeded voice protocols disabled. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, CM-7 Least Functionality.	**Organisational evidence**
NS 56	Physical countermeasures protecting the VoIP infrastructure. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
NS 57	Call logs monitored adequately. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting.	**Organisational evidence**
NS 58	Soft phones, where allowed, used only over a secure connection such as a VPN. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, AC-17 Remote Access.	**Organisational evidence**
NS 59	Backup power for PoE VoIP phones. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: PE-11 Emergency Power.	**Organisational evidence**
NS 60	Strong authentication and access control protecting the voice gateway. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), AC-3 Access Enforcement.	**Organisational evidence**

NS 61	IPsec or SSH for all remote management and audit access to the voice systems. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-17 Remote Access, SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**
NS 62	Contingency plans for voice calls if VoIP becomes unavailable. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CP-8 Telecommunications Services.	**Organisational evidence**
NS 63	Port security on the switches that connect VoIP devices. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-7 Least Functionality.	**Organisational evidence**
NS 64	A risk assessment of IPv4 and IPv6, with IPv6 deployment to be considered. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
NS 65	A risk assessment before running a dual-stack network. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
NS 66	Recertification requested when IPv6 is deployed. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CA-6 Authorization.	**Organisational evidence**

IE Information exchange

IE 1	Before cross-domain connections, the other domains' structure, security and risks evaluated and accepted, with the review documented. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CA-3 Information Exchange.	**Organisational evidence**
IE 2	Before connecting to another secured network, the networks it connects to obtained and examined for unintended cascaded connections, and their risks weighed, especially links to untrusted networks. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: CA-3 Information Exchange.	**Organisational evidence**
IE 3	Agreements, confidentiality ones included, in place before information is exchanged, setting out responsibilities, notification, transmission standards, couriers, liability, ownership and controls; a formal NDA for vendors and third parties. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CA-3 Information Exchange, PS-6 Access Agreements.	**Organisational evidence**
IE 4	Media used for exchange protected against unauthorised access, tampering or misuse, inside and outside the organisation. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-5 Media Transport.	**Organisational evidence**

IE 5	Information received from another organisation keeps its classification and protection. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-21 Information Sharing.	**Organisational evidence**
IE 6	Media in transit physically protected and packed against hazards that would make it unreadable. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-5 Media Transport.	**Organisational evidence**
IE 7	Only reliable couriers, from a list of known and authorised ones, used. Organisational, non-technical. Baseline control. NIST SP 800-53: MP-5 Media Transport.	**Organisational evidence**
IE 8	Information exchanged by electronic messaging protected from unauthorised access, change and disruption. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**
IE 9	Secure messaging, signed or encrypted with S/MIME or better, for information rated C3 or above, as CY requires. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection.	**Organisational evidence**
IE 10	An email disclaimer, such as the one the standard provides, on all outgoing email. Organisational, non-technical. Baseline control. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
IE 11	Due care that information sent or received is free of malicious code. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
IE 12	Information exchanged between systems protected against misuse, unauthorised access and corruption, with authenticated and encrypted channels for information rated C2, I2 or above, as CY requires. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection.	**Organisational evidence**
IE 13	Only sanitised, approved information released to the public, through a designated and trained spokesperson. Organisational, non-technical. Baseline control. NIST SP 800-53: AC-22 Publicly Accessible Content.	**Organisational evidence**

GS Gateway security

GS 1	Networks protected from one another by gateways, with data flows controlled. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
GS 2	Gateways to other networks, public ones included, use a suitable device to control every data flow, and sit in a secured server room. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection, PE-3 Physical Access Control.	**Organisational evidence**

GS 3	Only authorised, trained staff manage and maintain gateways. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
GS 4	Administrative access to gateways handling information rated C3 or above only under dual control and the four-eyes principle. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: AC-5 Separation of Duties.	**Organisational evidence**
GS 5	Information passing through gateways labelled under the classification policy and protected, with each gateway classified at the level of what it carries. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-16 Security and Privacy Attributes.	**Organisational evidence**
GS 6	Demilitarised zones, separated by firewalls, between externally reachable systems and both public and internal networks. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
GS 7	Gateways are the only routes in and out of internal networks, deny all connections by default and allow only those authorised, are managed over an isolated secure path, and audit and raise real-time alarms on breaches and intrusion attempts. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection, AU-2 Event Logging. **Scope of this evidence** The cluster is not the gateway. Its own default-deny controls are evidenced under NS 5 and SS 21.	**Organisational evidence**
GS 8	Gateways hardened before production, and protected against malicious code, misconfiguration, account compromise, rogue monitoring, denial of service and data leakage. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-6 Configuration Settings, SC-5 Denial-of-service Protection.	**Organisational evidence**
GS 9	Gateways monitored and supervised, with threat prevention, logging, alerts and surveillance, as SM describes. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
GS 10	Gateways block content a filter marks as suspicious, at least malware, denial of service, offensive material and the categories of content the law prohibits; the standard marks offensive material and prohibited content as baseline. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection, SC-7 Boundary Protection.	**Organisational evidence**
GS 11	Users accountable for the data they export, and told to check its marking, content and metadata before export. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-21 Information Sharing.	**Organisational evidence**

GS 12	Data exported only under approved procedures, or with the information security manager's individual approval. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-21 Information Sharing.	**Organisational evidence**
GS 13	Export to a less classified system filtered, at least by classification labels. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement.	**Organisational evidence**
GS 14	Exports checked by keyword search of all text, with unidentified data held until a trusted person other than its originator approves its release. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement.	**Organisational evidence**
GS 15	Users accountable for the data they import, and told to check its marking, content and metadata. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-4 Information Flow Enforcement.	**Organisational evidence**
GS 16	Data imported only under approved procedures, or with the information security manager's individual approval. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement.	**Organisational evidence**
GS 17	Imported data scanned for malicious and active content. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**

PR Product security

PR 1	Products selected with due diligence, keeping product and vendor independent. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
PR 2	Products classified and labelled under the classification policy. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: RA-2 Security Categorization.	**Organisational evidence**
PR 3	Vendors identified and screened against defined criteria: status, location and ownership, finances, references, and their ability to maintain the controls a risk assessment requires. Organisational, non-technical. Baseline control. NIST SP 800-53: SR-6 Supplier Assessments and Reviews, SA-4 Acquisition Process.	**Organisational evidence**
PR 4	Products tested to confirm they do what the vendor claims, so that confidentiality, integrity and availability are not lost. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**

PR 5 Products evaluated for security on a dedicated configuration, with functional tests, security tests and patching. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SA-11 Developer Testing and Evaluation.

PR 6 Products delivered in line with the organisation's practice for secure delivery. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SR-3 Supply Chain Controls and Processes.

PR 7 Secure delivery includes measures to detect tampering or masquerading. **Fail**

Enforced, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: CM-14 Signed Components. Evidence counted: policy.images-signed; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict covers the images outside the exempt namespaces: that each carries a signature from a configured key (an image no key covers fails). By default a failing Pod is admitted with a warning and recorded; it is refused only where the policy's action is Deny. The delivery of other products is the organisation's to evidence.

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

policy.images-signed	**Fail**	11 object(s) run images that are not signed or that no signing key covers. Establishes: Every image outside the exempt namespaces carries a signature from a configured key: Kyverno verifies the images that match a key's patterns, and the collector fails any image that no key covers. A failing Pod is admitted with a warning and recorded, or refused, as policies.defaultAction sets (Warn by default).

PR 8 Products bought from developers committed to maintaining their assurance. **Organisational evidence**

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

PR 9 Processes to patch and update products, with updates under change management (CM). **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-2 Flaw Remediation, CM-3 Configuration Change Control.

SS Software security

SS 1 Security built into every phase of the development life cycle and every development or implementation project. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-3 System Development Life Cycle, SA-8 Security and Privacy Engineering Principles.

SS 2	Every application classified under the classification policy and protected as its confidentiality, integrity and availability ratings require.	**Pass**

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

Scope of this evidence The verdict is that each namespace outside the exempt namespaces carries a classification label. Classifying each application, and protecting it as its ratings require, are the organisation's to evidence.

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

SS 3	Functional, technical and assurance security requirements developed and built in with the system requirements.	**Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-4 Acquisition Process.

SS 4 Test and development systems and data separate from production, with information flow between them limited by a documented policy, access only for a business need, and no write access to the authoritative copy. **Fail**

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

Scope of this evidence The verdict covers the cluster: each namespace outside the exempt namespaces labelled with its environment, and the network controls between them (network policies, the host firewall and external IPs). It can be Pass only when the Convoy's generated default-deny network policy is turned on (it is off by default). Separate infrastructure and data for test and development, access by business need, and the protection of the authoritative copy are the organisation's to evidence.

Fails in Namespace payments.

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

SS 5 Applications enter production only after quality and security assurance tests show they meet their security requirements. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SA-11 Developer Testing and Evaluation, CA-2 Control Assessments.

Scope of this evidence The scans of the running workloads' images are evidenced under SS 14. Tests before production are the organisation's to evidence.

SS 6	Secure programming practices, such as following the MITRE top 25, least privilege, deny by default, checking the returns of system calls and validating input. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SA-15 Development Process, Standards, and Tools.	**Organisational evidence**
SS 7	Software reviewed or tested for vulnerabilities before production use, preferably by an independent party rather than its developer. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
SS 8	Systems comply with legal requirements such as licences, copyright and intellectual property. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CM-10 Software Usage Restrictions.	**Organisational evidence**
SS 9	All systems adequately documented. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: SA-5 System Documentation.	**Organisational evidence**
SS 10	Source code of custom critical applications available, with escrow considered for commercial applications that serve critical processes. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
SS 11	Applications certified as AC requires before they are commissioned. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: CA-6 Authorization.	**Organisational evidence**
SS 12	The security objectives and mechanisms of servers and workstations documented in the system security plan. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-2 System Security and Privacy Plans.	**Organisational evidence**
SS 13	Workstations run a hardened standard environment: unwanted software removed, unused functions disabled, minimum access, host firewalls, and logs sent to a central server. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-6 Configuration Settings, CM-7 Least Functionality.	**Organisational evidence**

SS 14 Vulnerabilities in standard environments and systems reduced: unneeded file shares and input and output functions removed, patching kept current, unused accounts removed, and default accounts renamed and their passwords replaced. **Pass**

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

Scope of this evidence The verdict concerns whether critical and high vulnerabilities in the images of the workloads outside the exempt namespaces are patched, with the age of each open vulnerability and the platform's versions recorded. The nodes' operating systems, file shares, input and output functions, and accounts are the organisation's to evidence.

cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

SS 15 High-risk servers reachable from public networks kept functionally separate, with communication between them minimised and access limited to what is needed. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection, AC-6 Least Privilege.

SS 16 The integrity of critical and high-risk servers checked, from a trusted environment where possible. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity.

SS 17 Integrity information stored securely off the server. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity.

SS 18 Integrity information updated after every legitimate change. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity.

SS 19 Stored integrity information compared with the current state as part of the audit schedule, to find compromise or flawed changes. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity.

SS 20 Detected changes resolved under the ICT incident procedures. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity, IR-4 Incident Handling.

SS 21 Every application reviewed for the external connections it attempts; a risk-based decision should be made to allow or deny automatic outbound connections. **Fail**

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

Scope of this evidence The verdict covers the cluster's network controls: network policies in each namespace outside the exempt namespaces, the host firewall, and external IPs. Workloads' outbound connections are denied by default 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, and the decision on each, are the organisation'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.

SS 22 All active content on web servers reviewed for security; OWASP's guidance should be followed. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SA-11 Developer Testing and Evaluation.

SS 23	Connectivity and access between the components of each web application minimised.	**Fail**

Enforced, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AC-4 Information Flow Enforcement, SC-7 Boundary Protection.

Scope of this evidence The verdict covers the cluster's network controls: network policies in each namespace outside the exempt namespaces, the host firewall, and external IPs. It can be Pass only when the Convoy's generated default-deny network policy is turned on (it is off by default). Whether connectivity between each application's components is minimal is the organisation'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.

SS 24 Personal and sensitive information protected by suitable cryptography in storage and in transmission. **Incomplete**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

Scope of this evidence The evidence is TLS on ingress and to the control plane and kubelets, and Kubernetes Secrets encrypted at rest. Encryption of personal and sensitive data by the applications and in their storage is the organisation'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.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.

SS 25 Critical-sector websites that need strong authentication use certificates from a certificate service provider licensed in Qatar. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-17 Public Key Infrastructure Certificates.

SS 26 A web application firewall for applications rated medium risk or higher. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.

SS 27 Database information that could be exported, or that mixes classifications or handling, carries a classification. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-16 Security and Privacy Attributes.

SS 28 Classifications in databases granular enough to define the handling of anything retrieved or exported. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-16 Security and Privacy Attributes.

SS 29 Database files protected against any access that goes around the database's own access controls. **Organisational evidence**

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

SS 30 Databases able to audit their users' actions. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AU-12 Audit Record Generation.

SS 31	Users without the privilege to see database contents cannot see their metadata in search results; otherwise results are sanitised to their privilege. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-3 Access Enforcement, AC-4 Information Flow Enforcement.	**Organisational evidence**
SS 32	Sensitive data rated C3 and above masked in databases. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-28 Protection of Information at Rest.	**Organisational evidence**

SU System usage security

SU 1	Users responsible for the assets given to them, which they handle with care and under the acceptable use policy. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
SU 2	Users browse with due diligence under the organisation's rules, which decide whether forums and social networks are allowed. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
SU 3	Assets protected from web threats by preventing downloads of software and active content and visits to non-business sites. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-18 Mobile Code.	**Organisational evidence**
SU 4	Web access only through filtering gateways and secure proxies, as GS requires. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
SU 5	Staff know what content is permitted and what is restricted, with monitoring of encrypted channels considered. Organisational, non-technical. Baseline control. NIST SP 800-53: AT-2 Literacy Training and Awareness, SI-4 System Monitoring.	**Organisational evidence**
SU 6	Email used with care and labelled for the classification of its content and attachments. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
SU 7	Email protected against viruses, trojans, spam, forgery and social engineering. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection, SI-8 Spam Protection.	**Organisational evidence**
SU 8	Staff know that public web email may not be used from the organisation's systems. Organisational, non-technical. Baseline control. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
SU 9	Staff know that confidential information is emailed to named recipients, not to groups or lists. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**

SU 10	Staff know that automatic forwarding depends on sensitivity, and that email rated C2 or above is never forwarded automatically outside the organisation's systems. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
SU 11	External parties understand and agree to how classified data is used, as IE requires. Organisational, non-technical. Baseline control. NIST SP 800-53: CA-3 Information Exchange.	**Organisational evidence**

MS Media security

MS 1	Hardware that contains media given a classification no lower than that of the information on the media. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
MS 2	Non-volatile media classified at the highest classification of the information stored on it. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
MS 3	Volatile media with a continuous power supply classified at the highest classification it holds while powered; once power is removed it may be treated as C1. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
MS 4	Media reclassified when more highly classified information is copied to it, or when its information is upgraded. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
MS 5	Media may be declassified once its information is declassified by the originator, or once it has been sanitised as MS requires. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 6	Media that cannot be sanitised cannot be declassified, and is destroyed. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 7	Every medium's classification visible at a glance, preferably through a protective marking of its highest classification. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
MS 8	Where markings are not textual, for operational security, the scheme documented and staff trained in it. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MP-3 Media Marking.	**Organisational evidence**
MS 9	Documented procedures for sanitising media, tested regularly. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

MS 10	Media types that cannot be reliably sanitised, such as microfiche, optical discs, printer ribbons, PROM and ROM, and faulty media, destroyed before disposal if they hold information rated C1 or above. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 11	Volatile media sanitised by removing power for at least 10 minutes, or by overwriting every location and reading it back. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 12	Non-volatile magnetic media sanitised by overwriting with verification, three times for older or smaller media and once for newer or larger, or by degaussing. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 13	EPROM erased to the manufacturer's specification with three times the ultraviolet time, then overwritten once; sanitisation of media rated C3 and above should be documented. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 14	Flash memory sanitised by overwriting twice with a random pattern and reading back. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 15	Repairs and maintenance on hardware holding classified information done by vetted and briefed staff. Organisational, non-technical. Baseline control. NIST SP 800-53: MA-5 Maintenance Personnel.	**Organisational evidence**
MS 16	Repairs on systems holding information rated C3 or above supervised. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MA-5 Maintenance Personnel.	**Organisational evidence**
MS 17	Documented procedures for sanitising media, tested regularly, as MS 9 also requires. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 18	Media destroyed by degaussing magnetic media, breaking it up, or burning or melting it. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 19	Staff supervise destruction until it is complete, with destruction of media rated C3 and above documented. Organisational, non-technical. Baseline control. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
MS 20	Media holding classified information, faulty media included, sanitised as far as possible before disposal. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

MS 21	Media and media waste disposed of without drawing attention. Organisational, non-technical. Baseline control. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

AM Access control security

AM 1	Access granted by least privilege, on a need-to-know or need-to-have basis. Checked, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AC-6 Least Privilege, AC-6(1) Authorize Access to Security Functions. **Scope of this evidence** The verdict covers the cluster's RBAC: subjects and workloads with privileged, exec or Secret access, and service account tokens. Access rights in other systems are the organisation's to evidence. 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.

AM 2 Access governed by technical access controls, by identifying and authenticating users, and by audit trails suited to the information's sensitivity, with each request authorised by the user's supervisor or manager. **Fail**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AC-3 Access Enforcement, IA-2 Identification and Authentication (Organizational Users), AU-2 Event Logging.

Scope of this evidence The evidence is sign-in delegated to the organisation's identity provider, anonymous and unauthenticated kubelet access refused, RBAC, and the API server's audit log. Authorisation of access requests, and access to other systems, are the organisation's to evidence.

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

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.
node.kubelet-authz	**Pass**	The kubelet authorises requests through the API server: so on all 1 node(s). Establishes: The kubelet authorises requests through the API server (Webhook mode).
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.
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.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

AM 3 Rights to create, read, update, delete or send information based on a hierarchical matrix of rights, set by business rules from the information's owners. **Organisational evidence**

Organisational, technical and non-technical. Baseline control. NIST SP 800-53: AC-3 Access Enforcement.

AM 4 A process that updates system access on any change of role or status, departure included. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PS-5 Personnel Transfer, AC-2 Account Management.

AM 5 Users who need access that bypasses security mechanisms get formal authorisation from the Security Manager. **Organisational evidence**

Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-6 Least Privilege.

AM 6 Any unauthorised attempt to get round access control treated as a security incident, under the incident and HR procedures. **Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: IR-4 Incident Handling, PS-8 Personnel Sanctions.

AM 7 Audit logs enabled and kept so that compliance can be monitored and incidents investigated. **Pass**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.

Scope of this evidence The evidence is the API server's audit log. Audit logs of other systems are the organisation's to evidence.

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

AM 8 Logical access to the organisation's networks controlled technically, for example by network admission control. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-4 Information Flow Enforcement.

Scope of this evidence Admission of devices to the organisation's networks is the organisation's to evidence. The cluster's own network segmentation is under NS 5.

AM 9 Secure records of every authorised user, their identifier, who authorised their access and when, kept for the life of the system. **Recorded**

Checked, coverage partial. Baseline control. NIST SP 800-53: AC-2 Account Management. Evidence counted: cluster.access-review; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is the cluster's role bindings, recorded each day. The record of who authorised each user and when, kept for the life of the system, is the organisation'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.

AM 10 A logon banner before access, covering authorised use, agreement to policy, possible monitoring, acceptable use and the consequences of misuse, with acknowledgement where possible. **Organisational evidence**

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

AM 11 Central authentication stores, such as LDAP, protected from denial of service, reached over secure authenticated channels, and logging unauthorised access, activity times, user identities, sign-on and sign-off, and sessions. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: IA-5 Authenticator Management, SC-5 Denial-of-service Protection, AU-2 Event Logging.

Scope of this evidence The organisation's identity provider and directories are outside the cluster.

AM 12 Policies, plans and procedures for identifying, authenticating and authorising users, derived from the classification policy. **Organisational evidence**

Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IA-1 Policy and Procedures, AC-1 Policy and Procedures.

AM 13 Users taught the organisation's policies and procedures. **Organisational evidence**

Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AT-2 Literacy Training and Awareness.

AM 14 Every user uniquely identifiable, and authenticated each time access to a system is granted. **Incomplete**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).

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

AM 15 No account or privileges for anyone who is not an employee, contractor or consultant, unless the Security Manager approves after checking agreements, clearance and forms. **Organisational evidence**

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

AM 16 Another way of identifying the user wherever shared or generic accounts are used. **Organisational evidence**

Organisational, technical and non-technical. Baseline control. NIST SP 800-53: IA-2(5) Individual Authentication with Group Authentication.

AM 17	Unprotected authentication information that grants access to a system, or decrypts a device, not kept on or with that system or device.	**Pass**

Checked, coverage partial. Baseline control. NIST SP 800-53: IA-5 Authenticator Management. Evidence counted: trivy.config-secrets; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict concerns whether ConfigMaps outside the exempt namespaces hold secrets, such as passwords and keys, in plain text. The standard's text says such information 'is located' on or with the system; the summary reads its evident intent. Authentication information on other systems and devices is the organisation's to evidence.

trivy.config-secrets	**Pass**	Every object outside the exempt namespaces passes. Establishes: ConfigMaps that hold secrets.

AM 18	Authentication data in use resistant to replay, session hijacking and interception by a man in the middle.	**Incomplete**

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

Scope of this evidence The evidence is TLS on the control plane, the kubelets and ingress. Protection of authentication in the applications and in other systems is the organisation's to evidence.

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

AM 19	A password policy requiring at least 12 characters, or at least seven drawn from three of lowercase letters, uppercase letters, digits and special characters.	**Organisational evidence**

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

AM 20	Passwords changed at least every 90 days.	**Organisational evidence**

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

AM 21	Passwords changed no more than once a day, with a change forced at first logon and after expiry or reset.	**Organisational evidence**

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

AM 22	New passwords checked against predictable resets, reuse across accounts, reuse within eight changes, and sequences.	**Organisational evidence**

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

AM 23 Screen and session locks after at most 15 minutes of inactivity, available on demand, concealing the screen without seeming to turn it off, needing re-authentication, and not able to be disabled by users. **Organisational evidence**

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

AM 24 Access suspended after a set number of failed logons, and as soon as possible once it is no longer needed. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-7 Unsuccessful Logon Attempts, AC-2 Account Management.

AM 25 Lost, stolen or compromised passwords reported at once to the Security Manager, the account suspended, and the password changed after the user's identity is verified. **Organisational evidence**

Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: IA-5 Authenticator Management, IR-6 Incident Reporting.

AM 26 Accounts inactive for more than three months suspended. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-2(3) Disable Accounts.

Scope of this evidence The cluster's role bindings are recorded under AM 9 and AM 27; they do not show when each account was last used. Suspending inactive accounts, in the identity provider and in other systems, is the organisation's to evidence.

AM 27 Every six months, accounts reviewed for currency on systems that process information at C2, I2 or A2 and above. **Recorded**

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

Scope of this evidence The cluster's role bindings are recorded each day for the review. The review itself, and accounts on other systems, are the organisation'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.

AM 28 Security policies set out the clearances, briefings and other requirements for access to each system. **Organisational evidence**

Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.

AM 29 Users vetted as PS requires before they are given access. **Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: PS-3 Personnel Screening.

AM 30 Users given any briefings they need before they are given access. **Organisational evidence**

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

AM 31 Privileged accounts documented, controlled, accountable and kept to a minimum, and used only for administration. **Fail**

Checked, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: AC-6 Least Privilege, AC-6(5) Privileged Accounts. Evidence counted: policy.no-default-token, trivy.rbac-exec, trivy.rbac-privilege, trivy.token-automount; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict covers the cluster's RBAC: roles and bindings that grant broad rights or exec access, and service account tokens. Documenting privileged accounts, their accountability, and their use for administration only are the organisation's to evidence.

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

policy.no-default-token	**Pass**	Every object the policy judged passes it. Establishes: Pods say whether they mount a service account token, so that none receives one by default.
trivy.rbac-exec	**Pass**	Every object outside the exempt namespaces passes. Establishes: Roles that allow executing into Pods or impersonating privileged groups.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.
trivy.token-automount	**Pass**	Every object outside the exempt namespaces passes. Establishes: Pods that mount a service account token.

AM 32 System administrators given an individual account for their administration work. **Incomplete**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users).

Scope of this evidence The evidence is that sign-in to the cluster is delegated to the organisation's identity provider, which gives each administrator an identity of their own. Whether shared credentials, such as kubeadm's admin.conf, are still in use, and accounts on other systems, are the organisation'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.

AM 33 Privileged access to systems that hold information classified C4 and above limited to Qatari nationals, unless an exemption is explicitly authorised. **Organisational evidence**

Organisational, non-technical. Baseline control. NIST SP 800-53: PS-3 Personnel Screening.

AM 34	A system management log recording sanitisation, start-up and shutdown, failures, maintenance, backup and archival, recovery, and special or out-of-hours work. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AU-2 Event Logging, MA-2 Controlled Maintenance.	**Organisational evidence**
AM 35	Remote access only with the department head's explicit authorisation, for a business need, after its risks are analysed and controls put in place. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-17 Remote Access.	**Organisational evidence**
AM 36	Two-factor authentication, by hardware token, biometrics or similar, for access to systems processing data classified C3 or above. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.	**Organisational evidence**
AM 37	Remote access sessions secured with suitable end-to-end encryption, as CY requires. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, AC-17 Remote Access.	**Organisational evidence**
AM 38	Remote access computers run a personal firewall and anti-malware, always active. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-3 Malicious Code Protection, AC-17 Remote Access.	**Organisational evidence**
AM 39	Software on remote access computers, security software included, patched and kept current. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-2 Flaw Remediation.	**Organisational evidence**
AM 40	No access to internal systems from public computers, such as internet cafés, and no printing on them. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-20 Use of External Systems.	**Organisational evidence**
AM 41	Vendor remote access only where there is no alternative, initiated, controlled and monitored by the organisation, and limited to the task's duration. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: MA-4 Nonlocal Maintenance.	**Organisational evidence**

CY Cryptographic security

CY 1	Cryptographic algorithms, encryption products, key management and digital signatures meet the list approved under the Electronic Commerce and Transactions Law (Law No. 16 of 2010). Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-13 Cryptographic Protection.	**Organisational evidence**

CY 2 Key lifetimes set by the application and its infrastructure, and keys revoked and replaced at once if compromise is known or suspected. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

CY 3 Information assets classified C3 encrypted and protected from disclosure in storage and in transit, whatever the format or medium. **Incomplete**

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

Scope of this evidence The evidence is TLS on the control plane, the kubelets and ingress, and Kubernetes Secrets encrypted at rest. Encryption of the applications' data in storage and in transit, and of other media, is the organisation'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.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.

CY 4 The integrity of information assets classified I3 assured by cryptographic hashing. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SI-7 Software, Firmware, and Information Integrity.

CY 5 Data classified C3 secured in transit with TLS, SFTP, SSH version 2 or IPsec, and S/MIME version 3 or better, using algorithms the Qatar National Cryptographic Standard approves. **Organisational evidence**

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

CY 6 Passwords always encrypted or hashed in storage and in transit, with privileged passwords encrypted and stored off site with the backups after each change. **Incomplete**

Platform, coverage partial. Baseline control. NIST SP 800-53: IA-5 Authenticator Management, SC-28 Protection of Information at Rest. Evidence counted: platform.secret-encryption, trivy.config-secrets; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is that Kubernetes Secrets are encrypted at rest, and that no ConfigMap holds a secret. How the applications and other systems store passwords, and the off-site copies of privileged passwords, are the organisation's to evidence.

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.

CY 7 Hardware security modules, where used, certified to at least FIPS 140-2 Level 2 or Common Criteria EAL4. **Organisational evidence**

Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-12(1) Availability.

CY 8 Cryptographic keys moved physically only in hardware security modules that meet the standard's requirements for them. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

CY 9 Key management processes under ISO/IEC 11770 for the whole life of each key: custodians, generation, dual control and split knowledge, storage, use, distribution, backup and recovery, status checks, compromise, revocation and destruction, and audit trails. **Not evaluated**

Platform, coverage partial. Additional control, chosen by risk assessment. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

Scope of this evidence The evidence is where the key that encrypts Kubernetes Secrets is held. The management of every other key's life cycle is the organisation's to evidence.

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

CY 10 Digital certificates meet the standards of the certification service providers' policy management authority (CSP-PMA) at MCIT, with online revocation checking used. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-17 Public Key Infrastructure Certificates.

CY 11 Token and smartcard provisioning by certificate service providers meets CWA 14167-1. **Organisational evidence**

Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-17 Public Key Infrastructure Certificates.

CY 12	Every digital certificate in a production system issued by a certificate service provider licensed in Qatar. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: SC-17 Public Key Infrastructure Certificates. **Scope of this evidence** The cluster's own certificate authorities issue its control-plane and kubelet certificates; they are not issued by a certificate service provider licensed in Qatar. Whether this falls under the requirement, any exemption (AC 8), and the certificates of other production systems are the organisation's to settle and evidence.	**Organisational evidence**

OS Portable devices and working off site

OS 1	Policies on whether and how mobile devices and laptops may be used. Organisational, non-technical. Baseline control. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**
OS 2	No classified conversations on mobile devices or laptops while Bluetooth peripherals are in use. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**
OS 3	Bluetooth serial ports disabled on devices that will hold classified information. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-19 Access Control for Mobile Devices, CM-7 Least Functionality.	**Organisational evidence**
OS 4	Mobile devices that can record kept out of high-risk areas without the Security Manager's approval. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-19 Access Control for Mobile Devices, PE-3 Physical Access Control.	**Organisational evidence**
OS 5	Laptops and mobile devices encrypt the information they carry and are password protected. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-19(5) Full Device or Container-based Encryption.	**Organisational evidence**
OS 6	Devices kept under direct supervision in use and secured when not. Organisational, non-technical. Baseline control. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**
OS 7	Devices the organisation does not own or control not used with its systems unless managed and accredited like its own; its own devices may join other networks only behind a suitable firewall. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: AC-20 Use of External Systems, AC-19 Access Control for Mobile Devices.	**Organisational evidence**
OS 8	Unaccredited devices neither connect to the organisation's systems nor store its information, though temporary connections segregated by a firewall are allowed. Organisational, technical and non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: AC-20 Use of External Systems.	**Organisational evidence**
OS 9	Loss or theft of a device reported at once to the information security office and to law enforcement, and handled as an incident (IM). Organisational, non-technical. Baseline control. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**

OS 10	An emergency plan to destroy, lock or wipe any mobile device or laptop remotely. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**

PH Physical security

PH 1	Physical protection set by risk assessment, at the design stage for new buildings and through ongoing risk management for existing ones. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-1 Policy and Procedures, RA-3 Risk Assessment. **Scope of this evidence** The standard prints this statement as a second PH 2; it has no PH 1.	**Organisational evidence**
PH 2	Physical spaces zoned by security need, each zone given a level: minimal, baseline, medium or high protection. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
PH 3	Each zone has the physical controls its level requires, as the normative Appendix A sets out, with one further class of control for medium protection and two for high. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-3 Physical Access Control, PE-6 Monitoring Physical Access. **Scope of this evidence** Appendix A's controls for each protection level have no numbers of their own and are carried by this requirement. The statement itself carries no baseline mark, but Appendix A marks its minimal and baseline controls as all mandatory for zones at those levels.	**Organisational evidence**
PH 4	A policy of clean desks and clean screens. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
PH 5	Server and data rooms meet at least medium protection. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
PH 6	Cabling for information at levels C1 to C3 physically separate, fibre included, and in separate ducting from cabling for nationally classified information. Organisational, non-technical. Baseline control. NIST SP 800-53: PE-4 Access Control for Transmission.	**Organisational evidence**
PH 7	A site security plan, and procedures where needed, for each secure area, covering at least the risk assessment, roles, access control and alarm systems, keys and enrolment, clearances and training, review of audit trails, end-of-day checks and incident reporting. Organisational, non-technical. Additional control, chosen by risk assessment. NIST SP 800-53: PE-1 Policy and Procedures, PL-2 System Security and Privacy Plans.	**Organisational evidence**

VL Virtualisation

VL 1	The risks of virtualisation evaluated, against law and regulation, and for how it changes the infrastructure and its risk posture. Organisational, technical and non-technical. Baseline control. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

VL 2	The hypervisor, its administrative layer, the virtual machines and related components hardened to accepted practice and the vendor's guidance. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-6 Configuration Settings. **Scope of this evidence** This concerns the virtualisation layer beneath the cluster. The cluster's own hardening checks do not read the hypervisor, its administrative layer or the virtual machines.	**Organisational evidence**
VL 3	Least privilege and separation of duties in managing the virtual environment: granular administrator roles, limited direct access to the hypervisor, and multi-factor authentication or split administrator passwords considered according to risk. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: AC-6 Least Privilege, AC-5 Separation of Duties.	**Organisational evidence**
VL 4	Physical security against unauthorised access to the virtualisation environment. Organisational, non-technical. Baseline control. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
VL 5	Third-party security technology layered over the virtualisation environment's own controls. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: PL-8 Security and Privacy Architectures.	**Organisational evidence**
VL 6	Virtual machines segregated by the classification of the data they process or store. Organisational, technical, outside the cluster. Additional control, chosen by risk assessment. NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**
VL 7	Change management covers the virtualisation environment, with virtual machine profiles kept current, the integrity of images maintained, and dormant machines kept up to date. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: CM-3 Configuration Change Control, SI-7 Software, Firmware, and Information Integrity.	**Organisational evidence**
VL 8	Logs from the virtualisation environment collected and monitored with those of the rest of the infrastructure, as SM requires. Organisational, technical, outside the cluster. Baseline control. NIST SP 800-53: AU-2 Event Logging, AU-6 Audit Record Review, Analysis, and Reporting. **Scope of this evidence** This concerns the virtualisation layer beneath the cluster. The cluster's own audit log is evidenced under SM 1 and SM 4.	**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-toke 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.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.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

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.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 120 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: 120

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 120	`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.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.secret-encryption Not evaluated

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

The platform could not observe Secret encryption.

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

platform.time-servers Not provided

The time servers each node synchronises with.

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

- compliance.time-servers.configured: unknown

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

platform.versions Recorded

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

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

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

policy.default-deny-generated Not provided

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

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

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

policy.images-signed Fail

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

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

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

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

Fails (11)

Object	What is wrong	Full result
CronJob payments/nightly	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
Deployment payments/unsigned-app	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`
Job payments/nightly-now	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6a73d7cc-01f5-42d8-9d6c-462a360b517b -n payments -o yaml`
Pod payments/nightly-now-k7cbf	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 4074d46b-fb0f-4ce3-8312-15270922068d -n payments -o yaml`
Pod payments/unsigned-app-b5567644f-vpkpp	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 3f291cbb-5fdd-4171-9ead-42230533be9f -n payments -o yaml`
ReplicaSet payments/unsigned-app-b5567644f	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 9f9f8242-9449-4023-a60b-aa60653c0b24 -n payments -o yaml`
Deployment payments/ledger	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
Deployment payments/legacy-batch	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
CronJob payments/weekly	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
Job payments/migrate-once	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
Pod payments/one-off	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`

policy.ingress-tls Nothing to check

Every Ingress serves its hosts over TLS.

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

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

policy.namespace-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

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.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.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-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(5) Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
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-16 Security and Privacy Attributes	a. Provide the means to associate [Assignment: organization-defined organization-defined types of security and privacy attributes] with [Assignment: organization-defined organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission; b. Ensure that the attribute associations are made and retained with the information; c. Establish the following permitted security and privacy attributes from the attributes defined in [AC-16a](#ac-16_smt.a) for [Assignment: organization-defined organization-defined systems]: [Assignment: organization-defined organization-defined security and privacy attributes]; d. Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges]; e. Audit changes to attributes; and f. Review [Assignment: organization-defined organization-defined security and privacy attributes] for applicability [Assignment: organization-defined organization-defined frequency].
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-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-19(5) Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].
AC-20 Use of External Systems	a. [Selection (one or more): establish [Assignment: organization-defined terms and conditions] ; identify [Assignment: organization-defined controls asserted]] , consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organization-defined prohibited types of external systems].
AC-21 Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions for [Assignment: organization-defined information-sharing circumstances] ; and b. Employ [Assignment: organization-defined automated mechanisms] to assist users in making information sharing and collaboration decisions.
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-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-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-6 Authorization	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; e. Update the authorizations [Assignment: organization-defined frequency].
CA-7 Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to [Assignment: organization-defined organization-defined personnel or roles] [Assignment: organization-defined organization-defined frequency].
CA-8 Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined system(s) or system components].
CM-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-3 Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency] ; when [Assignment: organization-defined configuration change conditions]].
CM-3(4) Security and Privacy Representatives	Require [Assignment: organization-defined organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].

CM-4 Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(1) Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-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-10 Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CM-14 Signed Components	Prevent the installation of [Assignment: organization-defined organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
CP-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-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(5) Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.
IA-2(8) Access to Accounts — Replay Resistant	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].

IA-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].
IR-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-3 Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].
IR-4 Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
IR-5 Incident Monitoring	Track and document incidents.

IR-6 Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period] ; and b. Report incident information to [Assignment: organization-defined authorities].
IR-7 Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
IR-8 Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency] ; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined organization-defined incident response personnel (identified by name and/or by role) and organizational elements] ; and e. Protect the incident response plan from unauthorized disclosure and modification.
MA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c. Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
MA-2 Controlled Maintenance	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information]; e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].

MA-4 Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintain records for nonlocal maintenance and diagnostic activities; and e. Terminate session and network connections when nonlocal maintenance is completed.
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-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and c. Review and update the current media protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
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.

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-5 Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.
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-18 Location of System Components	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.
PE-19 Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.
PL-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and c. Review and update the current planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PL-2 System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization’s enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes; 4. Identify the individuals that fulfill system roles and responsibilities; 5. Identify the information types processed, stored, and transmitted by the system; 6. Provide the security categorization of the system, including supporting rationale; 7. Describe any specific threats to the system that are of concern to the organization; 8. Provide the results of a privacy risk assessment for systems processing personally identifiable information; 9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components; 10. Provide an overview of the security and privacy requirements for the system; 11. Identify any relevant control baselines or overlays, if applicable; 12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; 13. Include risk determinations for security and privacy architecture and design decisions; 14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups] ; and 15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation. b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]; c. Review the plans [Assignment: organization-defined frequency]; d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and e. Protect the plans from unauthorized disclosure and modification.
PL-4 Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior [Assignment: organization-defined frequency] ; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency] ; when the rules are revised or updated].

PL-8 Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.
PM-1 Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and c. Protect the information security program plan from unauthorized disclosure and modification.
PM-2 Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
PM-3 Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.
PM-9 Risk Management Strategy	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.
PM-13 Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.
PM-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.

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-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] personally identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and c. Review and update the current personally identifiable information processing and transparency: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
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-7 Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
SA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SA-3 System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system-development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.
SA-4 Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria.

SA-5 System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b. Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and d. Distribute documentation to [Assignment: organization-defined personnel or roles].
SA-8 Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined organization-defined systems security and privacy engineering principles].
SA-9 External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].
SA-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-15 Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined organization-defined security and privacy requirements].

SC-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business-process-level; system-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and c. Review and update the current system and communications protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SC-4 Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.
SC-5 Denial-of-service Protection	a. [Selection: protect against; limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events] ; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].
SC-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(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-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-18 Mobile Code	a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.
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-42 Sensor Capability and Data	a. Prohibit [Selection (one or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems] ; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]] ; and b. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].
SC-45 System Time Synchronization	Synchronize system clocks within and between systems and system components.
SI-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and c. Review and update the current system and information integrity: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

SI-2 Flaw Remediation	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.
SI-3 Malicious Code Protection	a. Implement [Selection (one or more): signature-based; non-signature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]] ; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
SI-4 System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives] ; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
SI-4(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-7 Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined organization-defined software, firmware, and information] ; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined organization-defined actions].
SI-8 Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
SI-12 Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

SR-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SR-3 Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls] ; and c. Document the selected and implemented supply chain processes and controls in [Selection (one or more): security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].
SR-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].