ASIRI Trust Assurance Pack

Owner: Compliance Operations
Status: Readiness
Current review month: May 2026
Next review: 2026-06-30

Scope

This pack summarizes ASIRI’s company and platform trust assurance readiness across NDPA operating evidence, ISO 27001 readiness, SOC 2 readiness, GDPR and cross-border transfer posture, PCI DSS responsibility boundary, AI governance readiness, vendor assurance, security controls, and procurement security.

This pack is intended for internal management review, customer procurement review, external auditor preparation, DPCO review, QSA scoping, legal review, and certification-body readiness discussions. It does not certify ASIRI under any external framework.

Framework Register Summary

Framework area - Current status - Evidence
NDPA operating program - Readiness - ../asiri-ndpa-audit-readiness/auditor-pack.md, ../asiri-ndpa-audit-readiness/audit-matrix.json
ISO 27001 readiness - Readiness - iso-27001-readiness.md, security-control-register.md, management-action-plan.md
SOC 2 readiness - Readiness - soc-2-readiness.md, security-control-register.md, management-action-plan.md
GDPR and cross-border transfer posture - Readiness - gdpr-transfer-privacy-posture.md, ../asiri-ndpa-audit-readiness/cross-border-transfer-assessment.md
PCI DSS responsibility boundary - Documented - pci-dss-responsibility-boundary.md, vendor-assurance-register.md
AI governance readiness - Readiness - ai-governance-readiness.md, ../asiri-ndpa-audit-readiness/dpia-regulatory-intelligence.md
Vendor assurance - Documented - vendor-assurance-register.md, ../asiri-ndpa-audit-readiness/subprocessor-register.md
Enterprise procurement security - Readiness - procurement-questionnaire.md, evidence-index.md

Control Summary

ASIRI maintains a control-family register covering governance, access control, encryption, tenant isolation, logging and auditability, incident response, backup and recovery, vendor assurance, cross-border transfers, payment boundary, AI governance, secure SDLC, privacy rights, and retention.

Control statuses are intentionally conservative. A documented or readiness status means ASIRI has a record or operating approach, but additional operating evidence or independent review may still be required.

Evidence Index

Primary trust assurance evidence:

- framework-register.json
- control-matrix.json
- evidence-index.md
- iso-27001-readiness.md
- soc-2-readiness.md

- gdpr-transfer-privacy-posture.md
- pci-dss-responsibility-boundary.md
- ai-governance-readiness.md
- vendor-assurance-register.md
- security-control-register.md
- procurement-questionnaire.md
- management-action-plan.md

Primary NDPA evidence reference:

- docs/compliance/asiri-ndpa-audit-readiness/auditor-pack.md

Certification and Report Boundaries

ISO/IEC 27001 certification language should not be used unless an accredited certification body has issued a certificate.

ASIRI does not claim an issued SOC 2 examination outcome unless an independent CPA firm has issued the applicable report.

ASIRI does not use PCI DSS outcome language unless a future scoped PCI assessment supports that statement.

ASIRI does not make a blanket GDPR outcome claim.

External auditor, certification body, DPCO, QSA, or legal validation is still required before ASIRI may claim an externally reviewed compliance outcome.

Security operating evidence for encryption, tenant isolation, access control, audit logs, incident response, backup/restore, disaster recovery, monitoring, and vulnerability management is tracked in docs/compliance/asiri-audit-remediation/security-operating-evidence-request-2026-05.md. Until dated samples are attached, ASIRI should describe these as documented or readiness controls, not operating-effectiveness conclusions.

Vendor contracts, DPAs, vendor assurance artifacts, AI provider retention/training settings, region evidence, and transfer risk acceptances are tracked in docs/compliance/asiri-audit-remediation/vendor-ai-evidence-request-2026-05.md. Until those artifacts are attached, ASIRI should describe vendor and AI governance as readiness-bounded.

External ISO certification-body engagement, SOC 2 CPA scoping, GDPR/cross-border counsel review, PCI scope assessment, and public claim sign-off are tracked in docs/compliance/asiri-audit-remediation/external-assurance-engagement-request-2026-05.md. Until qualified external artifacts are attached, ASIRI must keep ISO, SOC 2, GDPR, and PCI language at readiness or responsibility-boundary level.

Security and Privacy Controls

Security controls are summarized in security-control-register.md. Current records cover encryption, tenant isolation, access control, MFA, audit logs, vulnerability management, SDLC, incident response, backup/restore, disaster recovery, and monitoring.

Privacy operating evidence remains anchored in the NDPA audit-readiness pack. This trust assurance pack references the NDPA records for RoPA, lawful basis, DPIA, DSR, breach, retention, sub-processor, transfer, vendor, access, training, DPO reporting, and management action evidence.

AI Governance

ASIRI Regulatory Intelligence is governed as draft assistance. Controls include human review, source citation expectations, prompt minimisation, retention boundaries, model-provider review, monitoring, and no-legal-advice disclaimers.

Regulatory Intelligence outputs remain draft assistance for qualified human review and do not create legal, auditor, DPCO, regulator, or customer-counsel conclusions.

PCI Responsibility Boundary

ASIRI relies on third-party payment processors for raw cardholder-data handling. ASIRI application records should be limited to billing contact details, transaction metadata, invoices, subscription status, processor identifiers, and payment status.

ASIRI application records are intended to stay outside raw cardholder-data handling unless a future PCI scope assessment changes that boundary.

Cross-Border Transfer Summary

ASIRI's primary cloud posture references AWS af-south-1 where claimed, with documented exceptions for selected edge, analytics, email, payment, AI, and customer-selected integration paths. Transfer safeguards may include DPAs, Standard Contractual Clauses where applicable, transfer impact review, regional configuration, minimisation, encryption, access control, and vendor review.

Counsel or DPCO review remains required before ASIRI expands public transfer assurance claims.

Management Action Plan

Open action areas include external ISO audit, SOC 2 auditor engagement, PCI SAQ direction, GDPR transfer counsel review, AI model-provider quarterly evidence, penetration-test summary attachment, IAM evidence, backup/restore evidence, vendor contract evidence, and public trust page alignment.

The detailed action plan is maintained in management-action-plan.md.

Review Boundary

This pack is a readiness and evidence-summary artifact. It should be reviewed before external sharing to confirm that evidence paths, vendor names, dates, and customer-specific answers are current.

No statement in this pack should be used as legal advice, certification, attestation, regulator approval, QSA determination, CPA report, certification-body finding, or guarantee of compliance.