

IT & Tech Compliance — 54 tools

All tools · at-a-glance descriptions · Generated 15 Oct 2026

This is the full list of AiSevak tools in this industry, each with a short description of what it produces. Open any tool on aisevak.in to run it.

SOC 2 / ISO 27001

SOC 2 / ISO 27001 Gap Analysis

Runs a SOC 2 / ISO 27001 gap analysis against your chosen framework — an overall estimate, severity-rated gaps with remediation and effort, draft policies and an audit-readiness timeline. Use this to find your compliance gaps; for the full ISO policy set use the ISMS Policy Pack Generator, and for a risk inventory use the Risk Register Builder.

ISMS Policy Pack Generator

Generates an ISMS policy pack — the full ISO 27001 Annex A policy set with purpose and key clauses per policy, plus the ISMS core documents (scope, SoA, risk methodology, objectives). Use this for the policy set; for a gap analysis first use the SOC 2 / ISO 27001 Gap Analysis.

Risk Register Builder

Builds an information-security risk register aligned to ISO 27005 — asset, threat, vulnerability, likelihood, impact, score and treatment. Use this for the risk inventory; for the applicability mapping use the Statement of Applicability.

Statement of Applicability

Drafts an ISO 27001 Statement of Applicability — each Annex A (2022) control marked applicable or not, with justification and implementation status. Use this after your risk assessment; for the risk register use the Risk Register Builder.

Internal Audit Checklist

Produces a pre-certification internal audit checklist — clauses and controls to test, evidence to sample, and nonconformity grading — for ISO 27001 / SOC 2 readiness. Use this before certification; for the evidence mapping use the Control Evidence Tracker.

Control Evidence Tracker

Builds a control-to-evidence mapping — for each control, the evidence type, owner, frequency and where it lives — for audit readiness. Use this to prepare evidence; for the audit checklist use the Internal Audit Checklist.

Security Questionnaires

Security Questionnaire Auto-Response

Drafts professional answers to a customer security questionnaire (CAIQ/SIG/custom) from your described security posture, flagging items that need human review. Use this for a filled-in questionnaire; for a reusable buyer-facing trust page use the Security Whitepaper Generator.

CAIQ Filler

Drafts accurate, defensible answers to CAIQ (Cloud Security Alliance) items from your stated security posture, flagging where answers reveal a gap. Use this for the CAIQ; for a bespoke customer set use the Custom Questionnaire Responder.

SIG / VSAQ Filler

Drafts responses to a standard vendor security questionnaire (SIG/VSAQ) from your stated posture, kept consistent with your policies. Use this for SIG/VSAQ; for the cloud-specific CAIQ use the CAIQ Filler.

Custom Questionnaire Responder

Drafts professional, defensible answers to a bespoke customer security questionnaire from your stated posture, and predicts likely follow-up questions. Use this for a custom set; for the standard CAIQ or SIG use those fillers.

Security Whitepaper Generator

Writes a customer-facing security whitepaper / trust page — overview, data protection, access, infrastructure, compliance and incident response — from your program summary. Only claim controls you actually have. Use this for a buyer-facing page; to fill a specific questionnaire use the Security Questionnaire Auto-Response.

IT Policy Library

IT Policy Library Generator

Drafts your IT policy library — either the full standard set or a specific policy — with scope, review frequency and an acknowledgement form. Use this for the policy documents; for the ISO 27001-mapped ISMS pack use the ISMS Policy Pack Generator.

Acceptable Use Policy

Drafts an IT Acceptable Use Policy — permitted and prohibited use, email/internet, software, monitoring and privacy, and consequences — for your organisation. Use this for the AUP; for the full policy set use the IT Policy Library Generator.

Password / Access Policy

Drafts a password and access-control policy — complexity/passphrases, MFA, SSO, least privilege, joiner-mover-leaver, and privileged access — aligned to NIST/ISO. Use this for the access policy; for the full set use the IT Policy Library Generator.

BYOD / Device Policy

Drafts a device/BYOD policy — enrolment, MDM, encryption, patching, lost-device, data separation and offboarding wipe — for your organisation. Use this for the device policy; for the full set use the IT Policy Library Generator.

Data Classification Policy

Drafts a data classification policy — tiers (Public/Internal/Confidential/Restricted) with examples and handling, storage, sharing and retention rules — for your organisation. Use this for classification; for records of processing use the RoPA Builder.

Backup / Retention Policy

Drafts a backup and retention policy — scope, frequency, RPO, retention periods, encryption, testing and restoration — for your systems. Use this for backups; for the recovery steps use the Disaster Recovery Runbook.

Change Management Policy

Drafts a change management policy — change types, request and approval, testing, deployment, rollback, emergency change and records — aligned to SOC 2/ITIL. Use this for change control; for a deployment runbook use the Runbook / SOP Writer.

Vendor Risk

Vendor Risk Assessment

Produces a vendor risk assessment report — risk tier, data classification, domain-by-domain risks, a due-diligence checklist, an approval recommendation and contract requirements. Use this to approve a vendor; to vet many vendors consistently use the Vendor Tiering Framework, and for the questionnaire use the Vendor Security Questionnaire.

Vendor Security Questionnaire

Builds a vendor security questionnaire scaled to risk — sections for security, privacy (DPDPA), compliance, sub-processors, incident and BCP — to vet a vendor. Use this to vet vendors; for a full risk report use the Vendor Risk Assessment.

Vendor Tiering Framework

Builds a vendor tiering framework — criteria, tiers, and the due-diligence depth and review cadence per tier — to classify your vendor landscape. Use this to standardise vendor management; for a single vendor use the Vendor Risk Assessment.

Sub-Processor Risk Review

Assesses sub-processor (fourth-party) risk — data flows, the controls a vendor should hold over its sub-processors, and DPDPA cross-border transfer concerns. Use this for fourth-party risk; for the vendor itself use the Vendor Risk Assessment.

Vendor Offboarding Checklist

Builds a secure vendor offboarding checklist — access revocation, data return and deletion, deletion certificate, integrations, knowledge transfer and final invoices. Use this to exit a vendor; for the exit clauses in the contract use the Renewal / Exit Terms Reviewer.

Data Privacy

Data Privacy Impact Assessment

Produces a Data Privacy Impact Assessment (DPIA/PIA) — necessity/proportionality, risk-by-risk analysis with mitigations, legal basis and an overall risk rating. Use this for a high-risk processing activity; for overall India readiness use the DPDPA Readiness Assessment, and for records use the RoPA Builder.

RoPA Builder

Builds Records of Processing Activities (RoPA) aligned to DPDPA/GDPR — per activity: purpose, data categories, subjects, recipients, transfers, retention and safeguards. Use this for the processing record; for a single high-risk activity use the Data Privacy Impact Assessment.

DPDPA Readiness Assessment

Assesses your India DPDPA readiness — notice/consent, data-principal rights, security, breach process, governance — with a score, gap actions and Significant Data Fiduciary flags. Use this for overall readiness; for a specific high-risk activity use the Data Privacy Impact Assessment.

Consent Management Design

Designs consent management flows aligned to DPDPA — granular purposes, capture UX, easy withdrawal, consent records and re-consent triggers. Use this for consent design; for the wider readiness view use the DPDPA Readiness Assessment.

Data-Subject-Request Workflow

Designs a data-subject / data-principal request workflow (DPDPA/GDPR) — intake, identity verification, locating data across systems, fulfilment, SLA and records. Use this to handle rights requests; for the processing record use the RoPA Builder.

Business Continuity

Business Continuity Plan

Drafts a practical business continuity / disaster recovery plan — critical-systems inventory with RTO/RPO, incident response per scenario, backup strategy and a testing schedule. Use this for the overall BCP; for step-by-step recovery use the Disaster Recovery Runbook, and to set targets use the RTO / RPO Calculator.

Disaster Recovery Runbook

Builds a disaster recovery runbook — per scenario (region outage, data loss, ransomware, provider outage): step-by-step recovery, validation, roles and communication. Use this for recovery procedures; for the overall plan use the Business Continuity Plan and to drill it use the Tabletop Exercise Designer.

RTO / RPO Calculator

Helps set RTO and RPO per system by criticality, with the architecture and cost implications of each target. Use this to define targets; for the recovery steps use the Disaster Recovery Runbook and for impact analysis use the Business Impact Analysis.

Business Impact Analysis

Performs a business impact analysis — critical processes, dependencies, impact over time, maximum tolerable downtime and recovery priorities. Use this to prioritise recovery; to then set targets use the RTO / RPO Calculator.

Tabletop Exercise Designer

Designs a tabletop exercise — scenario, escalating injects, discussion questions, objectives and evaluation criteria — for DR/incident readiness, with a debrief template. Use this to drill your team; for the plan it tests use the Business Continuity Plan or Incident Response Plan.

Technical Documentation

Technical Documentation

Creates professional technical documentation (API reference, architecture doc, user guide, runbook, release notes, etc.) in Markdown, with a review checklist. Use this for a general doc; for a focused API reference use the API Reference Generator and for an operational runbook use the Runbook / SOP Writer.

API Reference Generator

Generates clean API reference documentation — overview, authentication, and per-endpoint method, path, parameters, request/response examples and errors. Use this for an API; for a broader technical doc use the Technical Documentation tool.

Architecture Decision Record

Writes an Architecture Decision Record — context, decision, options considered with pros/cons, and consequences — in standard ADR format. Use this to record a technical decision; for broader docs use the Technical Documentation tool.

User Guide / Manual

Writes an end-user guide — getting started, feature sections with step-by-step tasks, FAQ and troubleshooting. Use this for end users; for API docs use the API Reference Generator.

Release Notes Generator

Turns a changelog into polished release notes — highlights, new features, improvements, fixes and breaking changes with migration notes. Use this per release; for full user docs use the User Guide / Manual.

Runbook / SOP Writer

Writes an operational runbook/SOP — purpose, prerequisites, precise step-by-step, verification, rollback and escalation. Use this for an ops procedure; for a threat-specific incident playbook use the Incident Runbook.

SaaS Contract Review

SaaS Contract Review (Data & Security)

Reviews a SaaS agreement/DPA focused on data and security terms — data ownership, deletion, sub-processors, audit rights, breach notification, liability and exit — with suggested language and must-negotiate points. Use this for a data-focused review; for commercial terms use the MSA / Order-Form Reviewer and for a pure DPA use the DPA Reviewer.

MSA / Order-Form Reviewer

Reviews a SaaS MSA/order form from your side — pricing and escalation, term and auto-renewal, liability cap, indemnity, warranties, termination and IP — with fixes and top negotiation points. Use this for commercial terms; for data terms use the DPA Reviewer or the SaaS Contract Review.

DPA Reviewer

Reviews a Data Processing Addendum for DPDPA/GDPR alignment — roles, purpose limitation, security, sub-processors, breach notification, cross-border transfer, deletion and audit — with fixes. Use this for a DPA; for commercial terms use the MSA / Order-Form Reviewer.

SLA Analyzer

Analyses a SaaS SLA — uptime definition and measurement, support tiers, service credits and exclusions — and flags weak terms with negotiation points. Use this for an SLA; for renewal/exit terms use the Renewal / Exit Terms Reviewer.

Renewal / Exit Terms Reviewer

Reviews SaaS renewal and exit terms for lock-in risk — auto-renewal, notice period, price escalation, data export/portability, transition assistance and termination fees — with fixes. Use this to assess exit risk; for the full commercial terms use the MSA / Order-Form Reviewer.

Incident Response

Incident Response Plan

Drafts a complete incident response plan — roles, incident classification, per-threat playbooks, a notification matrix (incl. CERT-In/DPDPA timelines) and communication templates. Use this for the overall IRP; for a single-threat playbook use the Incident Runbook, and for breach notices use the Breach Notification Drafter.

Breach Notification Drafter

Drafts data-breach notifications — to the regulator (Data Protection Board / CERT-In 6-hour reporting) and to affected individuals — aligned to DPDPA and CERT-In directions. Legal review is required and timelines are strict. For the overall plan use the Incident Response Plan.

Post-Incident / RCA Report

Writes a blameless post-incident / RCA report — summary, timeline, root cause, contributing factors, impact, resolution and owned action items. Use this after an incident; for a per-threat playbook use the Incident Runbook.

Incident Runbook (per threat)

Builds an incident response runbook for a specific threat — detection indicators, containment, eradication, recovery, notification and roles. Use this per threat type; for the overall plan use the Incident Response Plan.

Severity Classification Matrix

Builds an incident severity classification matrix — SEV levels with criteria, response time, escalation and comms — for consistent triage, with examples. Use this to triage incidents; for the response steps use the Incident Response Plan.

Cloud Architecture

Cloud Architecture Review

Reviews your cloud architecture against the Well-Architected Framework pillars — a per-pillar assessment, critical risks, quick wins and a prioritised action list. Use this for a full review; for cost specifically use the Cloud Cost Optimization tool and for config hardening use the Security Hardening Checklist.

Cloud Cost Optimization

Recommends cloud cost optimisations (FinOps) — right-sizing, commitments, idle cleanup, storage tiering, autoscaling, spot and architecture — with estimated savings and effort. Use this to cut your bill; for an overall architecture review use the Well-Architected Assessment.

Well-Architected Assessment

Assesses your architecture against the Well-Architected pillars (Operational Excellence, Security, Reliability, Performance, Cost, Sustainability) with per-pillar scores, findings and priority actions. Use this for a full review; for cost specifically use the Cloud Cost Optimization tool.

Migration Plan Builder

Builds a migration plan — per-workload 6R strategy, phases, risks, cutover and rollback — for a cloud or platform migration. Use this to plan a migration; for a post-migration review use the Well-Architected Assessment.

Security Hardening Checklist

Builds a cloud security hardening checklist aligned to CIS benchmarks — IAM, network, encryption, logging/monitoring, storage and compute — prioritised by impact. Use this to harden config; for a full architecture review use the Well-Architected Assessment.

This is AI-assisted guidance. Verify with a qualified professional before any binding decision. Fees, authorities and processes vary by state and change over time — confirm with your state authority.