

Assurance Materials & Framework Status

DOCUMENT ID ATX-SOC-05	TITLE Assurance Materials & Framework Status
VERSION 1.0	CLASSIFICATION Public
OWNER Security Officer	APPROVED BY Chief Executive Officer
EFFECTIVE DATE 10 August 2026	NEXT REVIEW August 2027
STANDARDS MAPPING ISO/IEC 27001:2022 and SOC 2 Trust Services Criteria - Security and Availability (control references)	

1. Purpose

This document identifies the assurance materials available for customer review and states the status of the external frameworks referenced by Atlastix. The control scope covers **development, customisation, release, delivery and support of Atlas Automate, Atlastix Observability, Atlastix Device Intelligence, and product and custom software solutions**, together with corporate systems and customer data Atlastix receives across those activities (ATX-SOC-01).

Customer- and MSP-operated tenancies are outside the Atlastix control boundary. Responsibilities at that boundary are documented through shared-responsibility tables, deployment records and applicable agreements.

2. Current state

Atlastix maintains a management-approved Information Security Management System (ISMS) aligned to ISO/IEC 27001:2022, with its controls mapped to the SOC 2 Security and Availability criteria; both are used as control references. Independent certification and a SOC 2 examination are targets and are not yet held: the documents described here are management-prepared assurance materials that support a customer's own review, not a certificate or attestation.

The management-prepared ISMS corpus comprises:

CATEGORY	DOCUMENTS	COVERAGE
Governance (ATX-GOV-01 to ATX-GOV-12)	12	ISMS scope, information security policy, roles and responsibilities, document and record control, objectives and planning, training and awareness, communication planning, internal audit, management review, nonconformity and corrective action, performance measurement, legal/regulatory/contractual compliance register
Risk management (ATX-RSK-01 to ATX-RSK-04)	4	Risk assessment and treatment methodology, risk register, Statement of Applicability, risk treatment plan
Technical controls (ATX-TEC-01 to ATX-TEC-08)	8	Access control, authentication and password standard (including credential handling), cryptography and key management (including secrets management), logging and monitoring, network security, cloud security, vulnerability and patch management, endpoint security

CATEGORY	DOCUMENTS	COVERAGE
Engineering & data (ATX-ENG-01 to ATX-ENG-07)	7	Secure development, change management, asset management, asset register, data classification and handling, data retention and disposal, AI governance and responsible use
People & suppliers (ATX-PPL-01 to ATX-PPL-07)	7	Acceptable use, HR security, remote working and BYOD, physical security, supplier and third-party risk, data protection and privacy, supplier register
Resilience (ATX-RES-01 to ATX-RES-05)	5	Incident response, business continuity and disaster recovery, backup, threat intelligence, breach notification
SOC 2 & trust (ATX-SOC-01 to ATX-SOC-08)	8	System description, TSC control mapping, security whitepaper, vendor questionnaire self-assessment, this framework-status document, vulnerability disclosure policy, subprocessor and hosting register, security terms summary
Customer assurance (ATX-CUS-01 to ATX-CUS-02)	2	Management security position statement; Device Intelligence deployment data-flow and shared-responsibility annex
Total	53	

3. Customer review

Atlastix offers prospective and current customers the following review materials:

- 1. Documentation walkthrough.** A walkthrough of relevant ISMS policies, procedures and registers may be arranged under confidentiality, subject to legal, security, contractual and customer restrictions.
- 2. Completed questionnaire.** The public self-assessment (ATX-SOC-04), together with reasonable responses to customer-issued questionnaires.
- 3. Control discussion.** A management-led discussion with the Security Officer and authorised supporting records relevant to the assessment scope.
- 4. Contractual position.** Security, support, vulnerability response, incident notification, data handling and deletion terms are governed by the applicable customer agreement; ATX-SOC-08 is a non-binding topic summary.
- 5. Public documents.** The Security Whitepaper (ATX-SOC-03), Vendor Security Questionnaire - Self-Assessment (ATX-SOC-04), this Assurance Materials & Framework Status statement (ATX-SOC-05), Vulnerability Disclosure Policy (ATX-SOC-06), Subprocessor & Hosting Register (ATX-SOC-07) and Security Terms & Control Position (ATX-SOC-08), published without an NDA.
- 6. Supplier context.** Supplier location and assurance depend on the applicable service and configuration. ATX-SOC-07 identifies current supplier processing facts.

4. External assurance results

Any future SOC 2 report, ISO/IEC 27001 certificate or independent security-test summary will be described using its issued scope, date and qualifications and may be shared under applicable confidentiality and distribution terms.

Requests and status questions should be sent to support@atlastix.io.

5. Related documents

ATX-SOC-01 System Description; ATX-SOC-02 SOC 2 TSC Control Mapping; ATX-SOC-03 Atlastix Security Whitepaper; ATX-SOC-04 Vendor Security Questionnaire - Self-Assessment; ATX-SOC-06 Vulnerability Disclosure Policy; ATX-SOC-07 Subprocessor & Hosting Register; ATX-SOC-08 Security Terms & Control Position; ATX-GOV-01 ISMS Scope Statement.

Revision history

VERSION	DATE	CHANGE	APPROVED BY
1.0	10 Aug 2026	Initial release	Chief Executive Officer