

# SecureAIScore

Assess. Download. Improve.

## AI Security Assessment Report Example Organization

### SAMPLE REPORT

#### FICTIONAL ORGANIZATION DATA

Fictional assessment date: June 18, 2026

This document is a static fictional sample for product demonstration purposes only.

Confidentiality notice: This sample report contains fictional organization data and does not represent any real customer, environment, assessment response, or production identifier. Any resemblance to real entities is coincidental.

# Executive Overview

**Overall AI Security Score: 68/100**

**Maturity Level: Defined**

Example Organization demonstrates emerging governance discipline and measurable control coverage. Priority risks remain in incident readiness, model lifecycle controls, and third-party oversight. Focused remediation over the next two quarters can materially reduce operational and regulatory exposure.

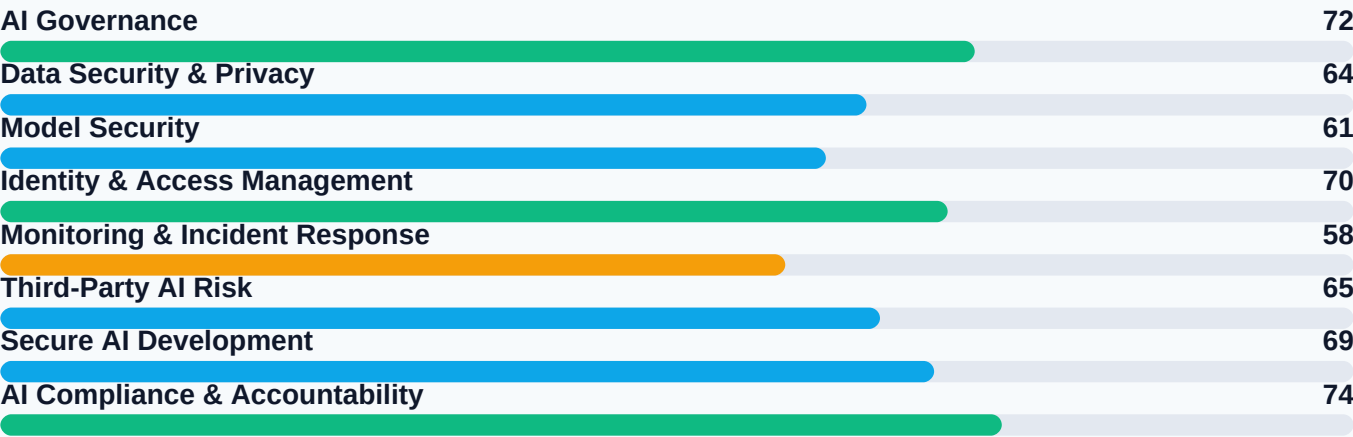
## Top Strengths

- 1. Executive awareness of AI risk and governance ownership
- 2. Early policy alignment with compliance obligations
- 3. Solid role-based access controls for core platforms

## Priority Improvement Areas

- 1. Build complete AI asset and model inventory coverage
- 2. Standardize AI incident response and escalation playbooks
- 3. Enforce model approval governance and logging consistency

Domain Scores



| Domain                         | Score | Interpretation  |
|--------------------------------|-------|-----------------|
| AI Governance                  | 72    | Stronger        |
| Data Security & Privacy        | 64    | Moderate        |
| Model Security                 | 61    | Moderate        |
| Identity & Access Management   | 70    | Stronger        |
| Monitoring & Incident Response | 58    | Needs attention |
| Third-Party AI Risk            | 65    | Moderate        |
| Secure AI Development          | 69    | Moderate        |
| AI Compliance & Accountability | 74    | Stronger        |

# Key Findings

## 1. Incomplete AI asset inventory (High)

Affected domain: AI Governance

Observation: Inventories do not consistently include prototypes, shadow models, and externally hosted AI services.

Business impact: Unknown assets increase exposure to unmanaged data flows and unreviewed model behavior.

Recommendation: Implement a unified AI asset registry with mandatory owner, data class, and lifecycle status fields.

## 2. Inconsistent access reviews (High)

Affected domain: Identity & Access Management

Observation: Periodic access certification is performed unevenly across AI tooling and service accounts.

Business impact: Over-privileged accounts and stale entitlements raise insider and misuse risk.

Recommendation: Enforce quarterly AI access recertification with automated revocation for exceptions.

## 3. Limited AI-specific incident playbooks (High)

Affected domain: Monitoring & Incident Response

Observation: Current response plans focus on traditional cyber events and do not define model misuse scenarios.

Business impact: Escalation delays during AI incidents increase operational disruption and regulatory risk.

Recommendation: Create AI incident playbooks for prompt abuse, model drift, data leakage, and output harm.

## Key Findings (Continued)

### 4. Third-party model risk gaps (Medium)

Affected domain: Third-Party AI Risk | Observation: Vendor due diligence lacks standardized scoring for model transparency and security attestations.

Business impact: Dependency risk can accumulate without clear contract and assurance controls.

Recommendation: Adopt a third-party AI risk questionnaire and minimum evidence standards before onboarding.

### 5. Insufficient prompt and output logging (Medium)

Affected domain: Data Security & Privacy | Observation: Prompt and output records are fragmented across teams and retention settings vary.

Business impact: Investigation quality and compliance reporting are weakened by incomplete traceability.

Recommendation: Centralize prompt/output telemetry with policy-based retention and integrity controls.

### 6. Fragmented model approval governance (Medium)

Affected domain: Model Security | Observation: Model promotion criteria and sign-off records are inconsistent between engineering squads.

Business impact: Uncontrolled releases may introduce biased, vulnerable, or non-compliant model behavior.

Recommendation: Establish a gated model approval board with required security and compliance checkpoints.

## Risk Register

| Risk ID | Risk                             | Likelihood | Impact | Rating   | Recommended treatment             |
|---------|----------------------------------|------------|--------|----------|-----------------------------------|
| R-01    | Untracked AI systems             | High       | High   | Critical | Asset registry and owner mapping  |
| R-02    | Privilege creep in AI tools      | Medium     | High   | High     | Quarterly access recertification  |
| R-03    | AI incident response delay       | Medium     | High   | High     | AI-specific playbooks and drills  |
| R-04    | Third-party model opacity        | Medium     | Medium | Medium   | Vendor risk scoring and controls  |
| R-05    | Insufficient telemetry retention | Medium     | Medium | Medium   | Centralized prompt/output logging |
| R-06    | Weak model approval controls     | Low        | High   | Medium   | Approval board and release gates  |

## Recommendations

### Immediate: 0-30 days

- Launch AI asset inventory remediation sprint and assign accountable owners.
- Approve mandatory AI access recertification workflow for privileged roles.
- Define minimum AI incident escalation matrix and on-call coverage.

### Near term: 31-90 days

- Standardize third-party model onboarding checks and evidence templates.
- Deploy centralized prompt/output logging with retention policy controls.
- Introduce baseline model risk assessment before production promotion.

### Medium term: 3-6 months

- Operationalize model approval governance board and documented criteria.
- Integrate AI control testing into internal audit and compliance reviews.
- Build role-specific AI risk training for security, engineering, and legal.

### Strategic: 6-12 months

- Automate policy-to-control mapping and continuous AI compliance tracking.
- Expand benchmark reporting across business units with target score thresholds.
- Embed AI risk KPIs into executive governance and quarterly planning cycles.

12-Month Roadmap

| Initiative                        | Priority | Target period | Owner role                 | Expected outcome                    |
|-----------------------------------|----------|---------------|----------------------------|-------------------------------------|
| AI asset registry completion      | High     | Q1            | Security Architecture Lead | Full asset visibility and ownership |
| AI access recertification program | High     | Q1-Q2         | IAM Lead                   | Reduced unauthorized access risk    |
| AI incident playbook rollout      | High     | Q2            | SOC Manager                | Faster containment and response     |
| Third-party AI risk framework     | Medium   | Q2-Q3         | Vendor Risk Manager        | Safer model procurement decisions   |
| Model approval governance board   | Medium   | Q3            | AI Governance Office       | Consistent release controls         |
| Continuous compliance dashboard   | Medium   | Q4            | GRC Director               | Improved audit readiness            |

Benchmark (Illustrative Sample Values)

Example Organization score: 68/100

Illustrative peer median: 62/100

Target maturity score: 78/100

Strongest domain: AI Compliance & Accountability (74)

Weakest domain: Monitoring & Incident Response (58)

Methodology

Scoring scale: 0-100 where higher values indicate stronger maturity and control effectiveness.

Maturity levels: Initial, Developing, Defined, Managed, Optimized.

Domain weighting: Balanced weighting across eight AI security domains with risk-adjusted prioritization.

Evidence basis: Questionnaire responses, documented controls, and workflow maturity indicators.

Sample limitation: This report is fully fictional and intended to illustrate structure and output only.

## Start Your Free Assessment

Assess your own AI security maturity in minutes and receive a tailored SecureAIScore report, prioritized roadmap, and actionable recommendations.

[secureaiscore.com/assessment](https://secureaiscore.com/assessment)

[secureaiscore.com/methodology](https://secureaiscore.com/methodology)

## Sample Disclaimer

SAMPLE REPORT - FICTIONAL ORGANIZATION DATA. This document contains no customer information, no production assessment responses, and no confidential identifiers. It is provided for demonstration and evaluation purposes only.