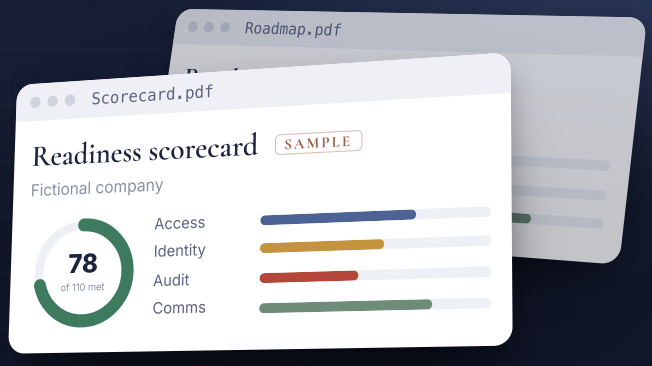
TheZara AI

SECURITY ASSESSMENTS · 2026

Know where you stand *before the assessor does.*



Readiness assessments for CMMC, FedRAMP, NIST, SOC 2, ISO 27001 and AI security. You leave with a scored gap analysis and a roadmap to close it.

Six assessments, one method

CMMC
Level 1 & 2 · NIST SP 800-171

Defense contractors handling FCI or CUI

Certified by a C3PAO

FedRAMP
Low & Moderate · NIST SP 800-53

Cloud providers selling to federal agencies

Assessed by a 3PAO

NIST
CSF 2.0 · 800-171 · 800-53

Any organization wanting a recognized baseline

Board and customer assurance

SOC 2
Type I & II · Trust Services Criteria

SaaS and service companies asked for a report

Audited by a CPA firm

ISO 27001
ISO/IEC 27001:2022 · Annex A

Companies selling internationally

Certified by a registrar

AI Security
NIST AI RMF · ISO/IEC 42001 · OWASP LLM

Teams using AI tools, copilots or agents

42001 certified by a registrar

Scope

IN THE INITIAL SCOPE

Assess the environment through interviews, configuration review and evidence. Identify the gaps, every control scored. Build a Plan of Action and Milestones (POA&M) where needed. Prepare you for the certification your contract or customer requires.

NOT IN THE INITIAL SCOPE

Applying the control fixes, quoted separately or handled by your team or MSP. The certification itself, issued by a C3PAO, 3PAO, CPA firm or registrar.

How it works

01 — Scope
Boundary set, fixed price agreed

02 — Assess
Examine, interview, test

03 — Score
Each control rated and risk-ranked

04 — Plan & readout
Roadmap, POA&M, leadership walkthrough

Jaclyn "Jax" Scott · Founder, TheZaraAI · Former Deputy CISO, Pearson

thezaraai.com/assessments · Jax@thezaraai.com

TheZara AI

Two packages, fixed price after scoping

PACKAGE 1

Assessment & Roadmap

One framework. Know your gaps and what to fix first.

50 TO 300 PEOPLE	$15,000 to $40,000
ENTERPRISE, 300+	$50,000 to $125,000

Typically 3 to 6 weeks (enterprise 6 to 12)

- Scoping and boundary definition
- Interviews, configuration and evidence review
- Scored gap analysis, control by control
- Risk-ranked findings in plain language
- Phased remediation roadmap
- Executive readout

PACKAGE 2 · MOST REQUESTED

Certification Readiness

For a contract or customer deadline.

50 TO 300 PEOPLE	$30,000 to $70,000
ENTERPRISE, 300+	$100,000 to $225,000

Typically 6 to 10 weeks (enterprise 10 to 16)

- ☐ Everything in Assessment & Roadmap, plus
- POA&M with owners and target dates
- SSP, policy and ISMS documentation gap review
- Evidence binder index mapped to each control
- Mock assessor interviews with control owners
- Crosswalk to one additional framework
- Readiness check 60 days after the readout

Where you land depends on headcount, locations, systems in scope and existing documentation. FedRAMP sits at the top of each range.

À la carte

CMMC Level 1 self-assessment
15 requirements, SPRS and affirmation support
from $4,000

POA&M development
Built from your existing findings
from $4,000

SSP or policy set
System Security Plan or core policies drafted
from $7,500

Framework crosswalk
Map one framework's controls to another
from $6,000

Mock assessment
Assessor-style interviews and evidence walk
from $6,500

Remediation validation
Re-check fixed controls before the audit
from $5,000

AI security & governance
NIST AI RMF and ISO/IEC 42001 review
from $10,000

Board briefing
Results presented to your board or owners
from $2,500

WHO DOES THE WORK

Jaclyn “Jax” Scott: U.S. Army Cyber and Electronic Warfare Special Operations Warrant Officer, former Deputy CISO and VP of Cybersecurity at Pearson, 20+ years in military and enterprise security. Nothing is subcontracted. TheZaraAI is an advisory practice, not a C3PAO, 3PAO, CPA firm or ISO registrar.

Prices are package prices set after a scoping call.

WHAT YOU RECEIVE

Documents you keep

Every engagement ends with a scorecard, a gap analysis, a remediation roadmap and, where needed, a POA&M, backed by objective-level working papers.

Assessment-Worksheet_AC.xlsx

Working paper: objective-level worksheet SAMPLE

CMMC AC.L2-3.1.1, assessed with NIST SP 800-171A methods · fictional company

OBJ.	DETERMINATION STATEMENT	METHOD	EVIDENCE REFERENCE	RESULT
[a]	Authorized users are identified	Examine, Interview	AD user export; HR roster	MET
[b]	Processes acting on behalf of users are identified	Examine	Service account register v1.2	NOT MET
[c]	Devices authorized to connect are identified	Examine, Test	Intune device list; NAC report	MET
[d]	Access is limited to authorized users	Test	Disabled-account login test	MET

Gap-Analysis.xlsx

Gap analysis SAMPLE

Every control, observed state, risk

REQ.	GAP	RISK
3.5.3	MFA on email only; VPN uses passwords	HIGH
3.3.1	Firewall logs kept 7 days; no central log	HIGH
3.11.2	Scans ad hoc, results not recorded	MED

POAM.xlsx

POA&M SAMPLE

Owners, milestones, target dates

ID	WEAKNESS	DUE
POA-04	3.1.10 Session lock not enforced	Jan 15
POA-07	3.13.11 Encryption not FIPS-validated	Feb 28
POA-09	3.8.4 CUI markings missing	Mar 31

The full package

Readiness scorecard
Results by domain, on one page for leadership

Assessment worksheet
Every objective, method, evidence and result

Gap analysis
Findings ranked by risk, in plain language

Remediation roadmap
What to fix first, phased by month

POA&M
Where the framework uses one

Executive readout
Walkthrough with your leadership

NEXT STEP

Book a fifteen-minute scoping call at thezaraai.com/assessments. Tell us the framework and the deadline; we confirm a fixed price before work begins.