ZeroTrusted.ai Academy

Training Program Catalog

Plans of Instruction, Course Descriptions, and Pricing — 2026 Edition 1.1

17 April 2026

13 Courses · Foundational through Executive Certification

Online, On-Site, and Private Dedicated Delivery Options

contact@zerotrusted.ai

1. Program Overview

The ZeroTrusted.ai Academy delivers practical, hands-on training across the full AI adoption lifecycle — from executive strategy through platform administration, from AI security fundamentals through federal certification. Every course is built around working outcomes: participants do not leave with a binder and a certificate alone, they leave with tools they can use, policies they can deploy, and frameworks they can apply on Monday morning.

1.1 Course Catalog at a Glance

Code	Course Title	Hours	Tier	Audience
EXEC-AI-401	Hands-on AI for Executives — Build Real Tools	4	Foundational	C-suite, VPs, Directors, Senior Leaders
AGENT-401	Building AI Agents to Get Massive Work Done	4	Foundational	Knowledge workers, analysts, managers, power users
AISEC-401	AI Security and Privacy	4	Foundational	Security engineers, IT leaders, compliance offi...
ZTA-ADMIN-801	ZeroTrusted.ai Administrator Training	8	Product	Platform administrators, security engineers, De...
ZTA-USER-401	ZeroTrusted.ai User Training	4	Product	End users, analysts, engineers who interact wit...
CIAO-801	Chief Information AI Officer (CIAO) Training Course	8	Executive Certification	Senior leaders stepping into or considering a C...
AICISO-801	AI CISO Training Course	8	Executive Certification	CISOs, deputy CISOs, senior security leaders
AICRO-801	AI Chief Risk Officer (AI CRO) Training Course	8	Executive Certification	CROs, chief compliance officers, senior risk an...
FEDISSO-1601	Federal ISSO / ISSM Training Course	16	Federal Certification	Federal ISSOs, ISSMs, AOs, and authorization su...
SOAR-801	AI SOAR In-Depth	8	Technical Deep-Dive	SOC analysts, SOAR engineers, detection enginee...
FW-HC-801	AI Firewall / HealthCheck In-Depth	8	Technical Deep-Dive	Security engineers, platform engineers, AI plat...
BOOTCAMP-1601	ZeroTrusted.ai Boot Camp — Tools and AI Security	16	Intensive	New security engineers, platform engineers, and...
AGENTCERT-401	AI Agent Testing and Certification Course	4	Specialist Certification	AI engineers, QA, red-teamers, AI application o...

1.2 Delivery Options

All courses are available in three delivery modes:

- Online public — scheduled public sessions. Per-seat pricing. Minimum 6 students to run; maximum 20 per session. Volume discounts available.
- Online private / dedicated — full session reserved for a single customer. Flat rate up to the online student cap; per-seat overage beyond cap.
- On-site private / dedicated — instructor(s) travel to customer facility. Flat rate up to on-site cap; per-seat overage beyond. Travel, lodging, and per diem billed hourly / at actual cost as other direct costs (ODCs).

All online courses may be split into 2-hour intervals across multiple days to accommodate operational schedules. On-site courses are delivered in contiguous sessions to minimize travel cost and maximize learning continuity.

1.3 Certification and Credentials

Courses at the product, technical deep-dive, and executive / federal certification tiers issue digital credentials (valid for two years; CPE or refresher required for renewal). Certificate-of-completion courses do not carry renewal requirements but are recognized across the ZeroTrusted.ai partner ecosystem.

1.4 Student Requirements — Universal

Unless a course specifies otherwise, every student must bring the following:

- A laptop capable of running a modern browser (Chrome, Edge, Safari, or Firefox)
- Administrative rights to install local tools where a course requires it

- An active subscription to at least one commercial AI service (ChatGPT Plus, Claude Pro, Gemini Advanced, or equivalent) for hands-on courses. Temporary access can be arranged on request.
- Reliable internet connectivity (minimum 10 Mbps, recommended 25 Mbps) for online courses
- Pre-class reading or preparation materials as listed per course

2. Plans of Instruction — Detailed Course POIs

Each course below follows a standardized Plan of Instruction format covering audience, prerequisites, learning objectives, module breakdown, hands-on exercises, materials, and student requirements.

2.1 Hands-on AI for Executives — Build Real Tools

Field	Detail
Course Code	EXEC-AI-401
Duration	4 hours
Tier	Foundational
Delivery	Online or on-site
Credential	Certificate of Completion
Target Audience	C-suite, VPs, Directors, Senior Leaders
Prerequisites	None. Laptop with internet browser required.
Per-Seat Price (online public)	$495
Private Online (flat rate)	$3,500 up to 15 students; $395/seat overage
Private On-Site (flat rate)	$5,500 up to 10 students + travel/ODCs; $395/seat overage

Course Description

A working session, not a lecture. Executives leave having built two to three production-ready AI tools they can use in their own workflows the next morning. Focus is on practical leverage: meeting summarization, briefing-document drafting, competitive analysis, decision-framework automation, and executive dashboards powered by AI. Participants learn what is real, what is hype, and where to push their organizations.

Learning Objectives

- Build 2-3 personal AI tools (briefing assistant, meeting-synthesis agent, strategic-analysis prompt library) during class
- Evaluate AI capabilities against business problems with a structured ROI framework
- Distinguish between chatbot automation, retrieval-augmented generation, and autonomous agents
- Identify where AI creates competitive advantage vs. where it creates organizational risk
- Articulate an AI governance posture appropriate to the executive role

Module Breakdown

Module 1 — The Executive AI Landscape (45 min)

- What AI actually does in 2026: capability map across reasoning, retrieval, generation, and action
- Vendor landscape: foundation model providers, orchestration platforms, and agent frameworks
- The three questions every executive should ask before any AI investment
- Hype filter: spotting real value vs. marketing theater

Module 2 — Hands-on Tool Building, Part 1 (75 min)

- Build a personal briefing assistant that summarizes reports, earnings calls, or industry news
- Construct a prompt library for recurring executive decisions
- Integrate with calendar and email to automate pre-meeting preparation
- Guardrails: what to keep human-in-the-loop

Break (15 min)

(Scheduled break — no instruction.)

Module 3 — Hands-on Tool Building, Part 2 (60 min)

- Build a competitive-intelligence agent that monitors public signals
- Create a strategic-analysis framework (SWOT, Porter, scenario planning) driven by AI
- Practical demonstration: boardroom-ready output in under 15 minutes

Module 4 — Governance, Risk, and What to Ask Your Team (45 min)

- Data-handling risk: what never to paste into a public LLM
- Setting AI policy without stifling innovation
- Budget and ROI framework for AI investments
- Q&A and individual coaching on each executive's top AI use case

Hands-On Deliverables

- Personal briefing assistant (working tool at end of class)
- Executive prompt library (10+ reusable prompts)

- Competitive monitoring agent

Materials Included

- Digital workbook with all exercises and reference materials
- Prompt library template (editable)
- Executive AI decision-framework one-pager
- 90-day post-class email coaching (5 check-ins)

Student Requirements

- Laptop with Chrome, Edge, or Safari browser
- Active AI subscription (ChatGPT Plus, Claude Pro, or Gemini Advanced) — instructor provides temporary access if needed
- Access to representative work materials for hands-on exercises (non-sensitive)

2.2 Building AI Agents to Get Massive Work Done

Field	Detail
Course Code	AGENT-401
Duration	4 hours
Tier	Foundational
Delivery	Online or on-site
Credential	Certificate of Completion
Target Audience	Knowledge workers, analysts, managers, power users
Prerequisites	Basic AI familiarity (prior chatbot use). Laptop required.
Per-Seat Price (online public)	$495
Private Online (flat rate)	$3,500 up to 15 students; $395/seat overage
Private On-Site (flat rate)	$5,500 up to 10 students + travel/ODCs; $395/seat overage

Course Description

A practical, build-everything workshop that takes participants from "I use ChatGPT sometimes" to "I have three agents running parts of my job." Covers agent design patterns, tool integration, multi-step reasoning, and operational patterns for agents that work while you sleep.

Learning Objectives

- Design and deploy a working multi-step AI agent by end of class
- Select appropriate agent frameworks for different use cases
- Integrate agents with calendar, email, documents, and third-party APIs
- Build safety and reliability into agent operations
- Scale from a single agent to a small team of cooperating agents

Module Breakdown

Module 1 — Agent Fundamentals (45 min)

- What makes something an agent vs. just an AI call
- Agent architecture: reasoning loops, tool use, memory, and planning
- When to use agents vs. when to use simpler automation
- Common agent patterns: ReAct, reflection, multi-agent collaboration

Module 2 — Building Your First Agent (75 min)

- Hands-on: build a research agent that monitors topics, drafts summaries, and files them in your workspace
- Connecting to real-world tools: calendar, Slack, email, Google Drive, SharePoint
- Prompt engineering for agent reliability
- Testing and debugging agent behavior

Break (15 min)

(Scheduled break — no instruction.)

Module 3 — Multi-Step and Multi-Agent Patterns (60 min)

- Build an agent that handles a complete workflow: intake → analysis → action → report
- Agent-to-agent coordination for complex tasks
- Error handling and human-in-the-loop checkpoints
- Memory and context management across sessions

Module 4 — Deployment, Monitoring, and Safety (45 min)

- Moving from sandbox to daily production use
- Monitoring agent behavior and catching failures early
- Data privacy and what agents should never touch
- Handing off to ZeroTrusted.ai for enterprise-grade governance

Hands-On Deliverables

- Working multi-step agent built during class

- Agent template library (5+ patterns)
- Integration cookbook for common tools

Materials Included

- Full digital workbook and code templates
- Agent design-pattern reference card
- 30-day access to instructor Slack channel for follow-up questions

Student Requirements

- Laptop with admin access to install local tools if desired
- Active AI subscription (ChatGPT Plus, Claude Pro, or similar)
- Optional: API access to preferred agent framework (OpenAI Assistants, Anthropic, LangChain, n8n, Make) — trial accounts available

2.3 AI Security and Privacy

Field	Detail
Course Code	AISEC-401
Duration	4 hours
Tier	Foundational
Delivery	Online or on-site
Credential	Certificate of Completion
Target Audience	Security engineers, IT leaders, compliance officers, privacy officers
Prerequisites	Basic security or IT background recommended.
Per-Seat Price (online public)	$495
Private Online (flat rate)	$3,500 up to 15 students; $395/seat overage
Private On-Site (flat rate)	$5,500 up to 10 students + travel/ODCs; $395/seat overage

Course Description

A focused introduction to the threat model unique to AI and LLM-enabled systems. Covers prompt injection, data exfiltration through models, shadow AI, model supply-chain risk, privacy-preserving AI techniques, and regulatory obligations under GDPR, HIPAA, and emerging AI-specific frameworks (EU AI Act, NIST AI RMF).

Learning Objectives

- Map the AI-specific threat landscape and articulate top risks for your organization
- Identify and mitigate prompt-injection, jailbreak, and model-misuse attack patterns
- Implement privacy-preserving techniques: redaction, tokenization, differential privacy, federated learning
- Evaluate vendor AI services against enterprise security requirements
- Build an AI acceptable-use policy and incident-response playbook

Module Breakdown

Module 1 — The AI Threat Model (45 min)

- AI-specific attack vectors: prompt injection, jailbreaks, data poisoning, model inversion
- OWASP Top 10 for LLM Applications
- Shadow AI: discovering and governing unsanctioned AI use
- Supply-chain risk in foundation models and model hubs

Module 2 — Data Protection in AI Workflows (60 min)

- Hands-on: data leakage via LLM conversations and RAG systems
- Redaction, tokenization, and prompt sanitization techniques
- Differential privacy and federated learning: when and why
- Data residency and cross-border AI processing under GDPR

Break (15 min)

(Scheduled break — no instruction.)

Module 3 — Attack Simulation and Defense (60 min)

- Hands-on: execute and defend against prompt-injection attacks
- Guardrails: input/output filtering, structured outputs, tool-use restrictions
- Red-team patterns for LLM applications
- Incident detection: signals that indicate AI misuse

Module 4 — Governance and Regulation (60 min)

- EU AI Act, NIST AI RMF, ISO/IEC 42001: what matters and when
- HIPAA, GLBA, FERPA implications for AI use
- Building an AI acceptable-use policy
- Incident-response playbook for AI-related events

Hands-On Deliverables

- Live prompt-injection attack and defense lab

- Data-redaction pipeline build
- Policy template customized for your org

Materials Included

- Full digital workbook
- AI security threat-model template
- Incident-response playbook template
- AI acceptable-use policy template (editable)

Student Requirements

- Laptop with internet access
- Active AI subscription for lab exercises
- Familiarity with basic security concepts (CIA triad, access controls)

2.4 ZeroTrusted.ai Administrator Training

Field	Detail
Course Code	ZTA-ADMIN-801
Duration	8 hours
Tier	Product
Delivery	Online or on-site
Credential	ZeroTrusted.ai Certified Administrator
Target Audience	Platform administrators, security engineers, DevOps
Prerequisites	Basic system administration experience. Familiarity with Kubernetes or cloud IAM recommended.
Per-Seat Price (online public)	$795
Private Online (flat rate)	$4,950 up to 15 students; $645/seat overage
Private On-Site (flat rate)	$7,500 up to 10 students + travel/ODCs; $645/seat overage

Course Description

Full-day deep dive into deploying, configuring, and operating the ZeroTrusted.ai platform. Covers architecture, installation, policy configuration, integration with identity providers and SIEM systems, monitoring, upgrade procedures, and troubleshooting. Required for personnel responsible for day-to-day platform operations.

Learning Objectives

- Install and configure ZeroTrusted.ai in private cloud or on-premise environments
- Configure policies for AI HealthCheck, Shadow AI Protection, and AI SOAR modules
- Integrate with enterprise identity (SAML, OIDC), SIEM (Splunk, QRadar, Sentinel), and ticketing systems
- Monitor platform health, investigate incidents, and tune detection rules
- Perform upgrades, backup/restore, and disaster recovery procedures

Module Breakdown

Module 1 — Architecture and Deployment (90 min)

- ZTA platform architecture, component map, and data flows
- Deployment options: SaaS, private cloud (AWS/Azure/GCP), on-premise
- Kubernetes installation walk-through and prerequisites
- Sizing and capacity planning

Module 2 — Initial Configuration (60 min)

- Bootstrapping: first-admin setup, certificates, network configuration
- Identity integration (SAML, OIDC, Active Directory)
- Role-based access control and admin delegation
- Connecting upstream LLM providers and internal models

Lunch (60 min)

(Scheduled break — no instruction.)

Module 3 — Policy and Detection Configuration (90 min)

- Policy architecture: global, group, and user-level policies
- Configuring AI HealthCheck rules and thresholds
- Shadow AI discovery and blocking policies
- AI SOAR playbook configuration and integration
- Hands-on: build and deploy a full policy set

Module 4 — Operations and Monitoring (75 min)

- Dashboard navigation and KPI review
- SIEM integration and log forwarding
- Alerting, escalation, and on-call workflows
- Performance monitoring and capacity management

Module 5 — Maintenance, Upgrades, and Troubleshooting (75 min)

- Upgrade procedures and rollback
- Backup, restore, and disaster recovery
- Common issues and diagnostic procedures
- Certification exam (30 min)

Hands-On Deliverables

- Full ZTA installation in lab environment
- Complete policy configuration
- SIEM integration exercise
- Troubleshooting scenario lab

Materials Included

- ZTA Handbook
- Configuration templates and runbooks
- Lab environment access for 30 days post-class
- ZeroTrusted.ai Certified Administrator credential (valid 2 years)

Student Requirements

- Laptop with SSH client, browser, and Kubernetes tooling (kubectl, helm)
- Administrative access to a test environment (provided if not available)
- Basic Linux command-line proficiency

2.5 ZeroTrusted.ai User Training

Field	Detail
Course Code	ZTA-USER-401
Duration	4 hours
Tier	Product
Delivery	Online or on-site
Credential	Certificate of Completion
Target Audience	End users, analysts, engineers who interact with AI systems governed by ZTA
Prerequisites	None.
Per-Seat Price (online public)	$445
Private Online (flat rate)	$2,950 up to 15 students; $345/seat overage
Private On-Site (flat rate)	$4,950 up to 10 students + travel/ODCs; $345/seat overage

Course Description

Practical training for end users of ZeroTrusted.ai-governed AI systems. Covers what the platform does, how it affects daily work, how to use ZTA-enabled AI assistants effectively, how to report issues, and how to stay productive within the guardrails.

Learning Objectives

- Understand what ZeroTrusted.ai does and why it matters for daily AI use
- Use ZTA-governed AI assistants confidently and effectively
- Recognize when ZTA is protecting you and when to request an exception
- Report suspected incidents and policy issues through proper channels
- Follow organizational AI acceptable-use guidelines

Module Breakdown

Module 1 — What ZeroTrusted.ai Does for You (30 min)

- Why the platform exists: data protection, compliance, and safe AI use
- What ZTA watches and what it doesn't
- Your responsibilities as a user

Module 2 — Using ZTA-Governed AI Effectively (90 min)

- Working with approved AI tools in your daily workflow
- Hands-on: common AI tasks within ZTA guardrails
- Understanding policy messages and what to do when blocked
- Requesting exceptions and the approval workflow

Break (15 min)

(Scheduled break — no instruction.)

Module 3 — Recognizing and Reporting Issues (45 min)

- Warning signs of compromised or misbehaving AI
- Data you should never paste into AI tools
- How to report a potential incident
- What happens after you report

Module 4 — Staying Current and Getting Help (30 min)

- Where to find up-to-date policy documentation
- Help-desk and escalation procedures
- AI literacy resources for continued learning
- Q&A

Hands-On Deliverables

- Guided tour of ZTA-governed AI workflow
- Exception-request walkthrough
- Incident-reporting drill

Materials Included

- User quick-reference card
- Acceptable-use policy summary
- Link library for ongoing AI literacy

Student Requirements

- Laptop with browser
- Organizational credentials for ZTA-governed systems

2.6 Chief Information AI Officer (CIAO) Training Course

Field	Detail
Course Code	CIAO-801
Duration	8 hours
Tier	Executive Certification
Delivery	Online or on-site
Credential	CIAO Certification (ZeroTrusted.ai Academy)
Target Audience	Senior leaders stepping into or considering a CIAO role
Prerequisites	Executive experience in IT, security, risk, or data leadership. 5+ years recommended.
Per-Seat Price (online public)	$1,995
Private Online (flat rate)	$9,500 up to 10 students; $1,495/seat overage
Private On-Site (flat rate)	$13,500 up to 8 students + travel/ODCs; $1,495/seat overage

Course Description

The CIAO is an emerging C-suite role combining AI strategy, governance, and operational accountability. This course prepares seasoned executives to own AI across the enterprise: strategy, portfolio, governance, risk, talent, vendor management, and board-level reporting.

Learning Objectives

- Articulate the CIAO mandate and how it differs from CIO, CISO, CDO, and CTO roles
- Build and defend an AI strategy at board level
- Design AI governance frameworks (NIST AI RMF, ISO/IEC 42001, EU AI Act)
- Manage the AI portfolio across build, buy, and partner options
- Establish KPIs and reporting cadences for AI investment and risk
- Navigate AI talent, vendor, and ethical considerations

Module Breakdown

Module 1 — The CIAO Mandate (60 min)

- Role definition and scope
- Reporting structures: to CEO, board, or peers
- Interactions with CIO, CISO, CDO, CRO, General Counsel
- Case studies from early CIAO appointments

Module 2 — AI Strategy at Enterprise Scale (90 min)

- Portfolio theory for AI: build, buy, partner, kill
- Aligning AI investment to business strategy
- Building a 3-year AI roadmap
- Case study: defending an AI strategy to the board

Lunch (60 min)

(Scheduled break — no instruction.)

Module 3 — Governance and Regulation (90 min)

- NIST AI RMF implementation
- ISO/IEC 42001 certification path
- EU AI Act compliance for global operations
- Building an AI Ethics Committee
- Risk register and tolerance setting

Module 4 — Operating the AI Portfolio (90 min)

- Vendor management: selecting and governing AI providers
- Model lifecycle management
- Cost and value tracking for AI investments
- Talent strategy and organizational design

Module 5 — Board-Level Communication and Certification (30 min)

- Board-ready reporting templates and cadences
- Crisis communication: AI incidents at the top
- Certification exam (60 questions)

Hands-On Deliverables

- Board-ready AI strategy deck (drafted in class)
- Personal AI governance framework
- Vendor evaluation scorecard

Materials Included

- CIAO Playbook
- Board-communication template library
- Governance framework templates (NIST, ISO 42001, EU AI Act)
- CIAO Certification credential (valid 2 years, CPE required)
- 90-day post-class executive coaching (3 sessions)

Student Requirements

- Laptop
- Pre-class reading: 4 assigned case studies (approximately 3 hours)
- Willingness to discuss own org challenges in peer setting

2.7 AI CISO Training Course

Field	Detail
Course Code	AICISO-801
Duration	8 hours
Tier	Executive Certification
Delivery	Online or on-site
Credential	AI CISO Certification (ZeroTrusted.ai Academy)
Target Audience	CISOs, deputy CISOs, senior security leaders
Prerequisites	CISO or deputy CISO role, or equivalent senior security experience. CISSP or equivalent preferred.
Per-Seat Price (online public)	$1,995
Private Online (flat rate)	$9,500 up to 10 students; $1,495/seat overage
Private On-Site (flat rate)	$13,500 up to 8 students + travel/ODCs; $1,495/seat overage

Course Description

Converts experienced CISOs into AI-fluent security leaders. Covers AI threat modeling, red-teaming LLM applications, securing the AI supply chain, governance under emerging regulation, and integrating AI security into existing security operations programs.

Learning Objectives

- Extend the security program to cover AI-specific threats and controls
- Red-team and defend LLM-enabled applications
- Secure the AI supply chain: data, models, frameworks, and inference
- Map AI controls to existing frameworks (NIST CSF, ISO 27001, SOC 2, FedRAMP)
- Build an AI security operations capability
- Communicate AI risk to the board and regulators

Module Breakdown

Module 1 — Extending the Security Program to AI (60 min)

- AI threat landscape beyond traditional cyber
- What changes and what stays the same
- OWASP Top 10 for LLM, MITRE ATLAS
- Building an AI security architecture reference

Module 2 — Red-Teaming LLM Applications (90 min)

- Hands-on: prompt injection, jailbreaks, data exfiltration
- Adversarial ML basics: model inversion, membership inference, poisoning
- Third-party model risk assessment
- Building internal AI red-team capability

Lunch (60 min)

(Scheduled break — no instruction.)

Module 3 — AI Supply Chain Security (75 min)

- Data provenance and integrity
- Model and framework vulnerabilities
- Hugging Face, model hub, and dependency risk
- Inference-layer security: prompts, outputs, tool use
- SBOM for AI (AI-BOM)

Module 4 — Governance and Regulation for Security Leaders (75 min)

- Mapping AI controls to NIST CSF, ISO 27001, SOC 2
- FedRAMP and DoD SRG implications for AI services
- EU AI Act security obligations
- Board and regulator reporting

Module 5 — AI Security Operations and Certification (60 min)

- SOC integration: detecting AI-specific incidents
- Runbook library for AI security incidents
- Budget and metrics for AI security programs
- Certification exam

Hands-On Deliverables

- Live red-team exercise against LLM application
- AI security architecture diagram for own org
- AI-BOM creation exercise
- Incident runbook drafting

Materials Included

- AI CISO Playbook
- Red-team methodology and scripts
- Control-mapping spreadsheets (NIST CSF, ISO 27001, SOC 2)
- Incident runbook templates
- AI CISO Certification credential (valid 2 years, CPE required)

Student Requirements

- Laptop with security tools (Burp Suite or equivalent)
- Pre-class: review organizational security architecture
- Strong security fundamentals

2.8 AI Chief Risk Officer (AI CRO) Training Course

Field	Detail
Course Code	AICRO-801
Duration	8 hours
Tier	Executive Certification
Delivery	Online or on-site
Credential	AI CRO Certification (ZeroTrusted.ai Academy)
Target Audience	CROs, chief compliance officers, senior risk and audit leaders
Prerequisites	Senior risk, compliance, audit, or GRC leadership role.
Per-Seat Price (online public)	$1,995
Private Online (flat rate)	$9,500 up to 10 students; $1,495/seat overage
Private On-Site (flat rate)	$13,500 up to 8 students + travel/ODCs; $1,495/seat overage

Course Description

Prepares senior risk leaders to own AI risk at the enterprise level. Covers AI-specific risk taxonomies, quantification techniques, third-party risk, regulatory exposure, model risk management, and integration with existing ERM programs.

Learning Objectives

- Extend enterprise risk management to cover AI-specific risks
- Quantify AI risk using frameworks appropriate to financial, operational, and reputational exposure
- Build third-party AI risk assessment programs
- Navigate model risk management (MRM) for AI/ML systems (SR 11-7, SS1/23 adaptations)
- Report AI risk to the board and regulators
- Design AI risk appetite statements and tolerance thresholds

Module Breakdown

Module 1 — AI Risk Taxonomy (60 min)

- Categories of AI risk: technical, operational, ethical, regulatory, reputational, systemic
- How AI risk differs from traditional IT and model risk
- Mapping to ERM categories
- Industry-specific lenses: financial services, healthcare, defense

Module 2 — Quantification and Appetite (90 min)

- Quantifying AI risk: loss-distribution, scenario analysis, stress testing
- AI risk appetite statements
- Key risk indicators (KRIs) specific to AI
- Integrating AI risk into enterprise risk reporting

Lunch (60 min)

(Scheduled break — no instruction.)

Module 3 — Model Risk Management for AI (90 min)

- SR 11-7 adaptations for AI/ML
- Model inventory, validation, and ongoing monitoring
- Challenger models and backtesting
- Explainability and interpretability for regulated use cases

Module 4 — Third-Party and Systemic AI Risk (75 min)

- Foundation model vendor risk
- Concentration risk: "everyone uses the same 3 models"
- AI supply-chain risk
- Contractual and SLA considerations

Module 5 — Regulation and Certification (45 min)

- EU AI Act risk tiers and obligations

- Sector-specific regulation (OCC, FDA, FCA, NYDFS)
- Board and regulator reporting templates
- Certification exam

Hands-On Deliverables

- Draft AI risk appetite statement for own org
- AI risk heat-map exercise
- Third-party assessment questionnaire build

Materials Included

- AI CRO Playbook
- Risk-quantification templates and worked examples
- Third-party AI assessment questionnaire library
- AI CRO Certification credential (valid 2 years, CPE required)

Student Requirements

- Laptop
- Familiarity with ERM frameworks (COSO, ISO 31000/42001)
- Pre-class reading: selected case studies

2.9 Federal ISSO / ISSM Training Course

Field	Detail
Course Code	FEDISSO-1601
Duration	16 hours (2 days)
Tier	Federal Certification
Delivery	Online (2 days) or on-site (2 days)
Credential	Federal AI ISSO/ISSM Certification (ZeroTrusted.ai Academy)
Target Audience	Federal ISSOs, ISSMs, AOs, and authorization support staff
Prerequisites	Active federal security clearance preferred but not required. Familiarity with RMF.
Per-Seat Price (online public)	$3,495
Private Online (flat rate)	$16,500 up to 12 students; $2,495/seat overage
Private On-Site (flat rate)	$22,500 up to 10 students + travel/ODCs; $2,495/seat overage

Course Description

Two-day intensive for federal Information System Security Officers and Managers responsible for AI-enabled systems. Covers AI-specific adaptations of the Risk Management Framework (RMF), FedRAMP and DoD SRG considerations for AI, ATO package preparation, continuous monitoring for AI systems, and incident response for AI-related events.

Learning Objectives

- Apply NIST SP 800-53 Rev. 5 controls to AI-enabled systems
- Prepare AI-specific additions to System Security Plans (SSPs)
- Navigate FedRAMP, DoD SRG (IL4/IL5/IL6), and CNSSI-1253 for AI services
- Build continuous monitoring programs for AI systems
- Respond to AI-related security incidents in federal environments
- Support Authorizing Officials in AI system authorization decisions

Module Breakdown

Day 1 — Module 1: RMF for AI Systems (90 min)

- RMF 6-step process refresher
- AI-specific control selection and tailoring
- Control overlays: NIST AI RMF crosswalk to 800-53
- CNSSI-1253 considerations for AI in NSS

Day 1 — Module 2: SSP Preparation for AI (90 min)

- AI-specific system description requirements
- Data flow diagrams for AI systems
- Documenting training data, model provenance, and inference pipelines
- Hands-on: SSP section drafting for AI workload

Day 1 — Lunch (60 min)

(Scheduled break — no instruction.)

Day 1 — Module 3: FedRAMP and DoD SRG for AI (90 min)

- FedRAMP Moderate and High for AI services
- DoD SRG IL4/IL5/IL6 and AI-specific considerations
- Boundary definition for AI-enabled systems
- Inheritance and shared controls for hosted AI platforms

Day 1 — Module 4: Assessment and Authorization (90 min)

- SAR preparation and AI-specific findings
- POA&M management for AI weaknesses
- AO briefing preparation and risk-based decisions
- Day 1 recap and homework

Day 2 — Module 5: Continuous Monitoring for AI (90 min)

- Model drift detection as a security control

- Data integrity monitoring
- Prompt injection and output anomaly detection
- Integrating AI telemetry into existing continuous monitoring

Day 2 — Module 6: Incident Response for Federal AI (90 min)

- US-CERT and component CIRT reporting for AI incidents
- Classification spillage involving AI
- Forensics for AI-related events
- Hands-on: incident response tabletop

Day 2 — Lunch (60 min)

(Scheduled break — no instruction.)

Day 2 — Module 7: ZeroTrusted.ai in Federal AI Systems (90 min)

- ZTA deployment patterns for IL4, IL5, IL6
- Control inheritance with ZTA
- ATO-supporting artifacts ZTA provides
- Case study: full ATO with ZTA in the boundary

Day 2 — Module 8: Capstone and Certification (90 min)

- Capstone exercise: full AI ATO package review
- Certification exam (100 questions)
- Post-class resources and community

Hands-On Deliverables

- SSP section drafting for AI workload
- SAR findings triage exercise
- AI incident tabletop
- Full capstone ATO package review

Materials Included

- Federal AI ISSO Playbook
- SSP templates with AI-specific language
- Control-mapping worksheets (800-53 ↔ NIST AI RMF)
- POA&M templates
- Incident-response playbooks for federal AI
- Federal AI ISSO Certification credential (valid 2 years, CPE required)
- Access to federal ISSO community of practice
- NOTE: May be tailored to specific Government or Department of War (DOW) Agency when artifacts are sent at least 2 weeks out.

Student Requirements

- Laptop
- Familiarity with RMF and NIST SP 800-53
- Pre-class: review at least one existing SSP
- Active or pending federal security clearance for classified portions (non-classified track available)

2.10 AI SOAR In-Depth

Field	Detail
Course Code	SOAR-801
Duration	8 hours
Tier	Technical Deep-Dive
Delivery	Online or on-site
Credential	ZTA AI SOAR Specialist Certification
Target Audience	SOC analysts, SOAR engineers, detection engineering teams
Prerequisites	SOC or security engineering experience. Familiarity with SOAR platforms.
Per-Seat Price (online public)	$1,295
Private Online (flat rate)	$6,950 up to 12 students; $995/seat overage
Private On-Site (flat rate)	$9,950 up to 10 students + travel/ODCs; $995/seat overage

Course Description

Full-day technical deep-dive into the AI SOAR module. Covers playbook design, integration with SOC tooling, AI-specific detection logic, automated response patterns, and measurement of SOAR effectiveness for AI incidents.

Learning Objectives

- Design and implement AI-specific SOAR playbooks
- Integrate AI SOAR with SIEM, EDR, XDR, and ticketing systems
- Build detection logic for AI-specific threats
- Automate response to common AI incidents
- Measure and tune SOAR effectiveness

Module Breakdown

Module 1 — AI SOAR Architecture (60 min)

- Component model and data flows
- Differences from traditional SOAR
- Integration patterns with existing SOC tooling

Module 2 — Playbook Design (90 min)

- Playbook patterns for AI incidents: prompt injection, data leak, shadow AI detection
- Hands-on: build three playbooks end-to-end
- Conditional logic and human-in-the-loop design

Lunch (60 min)

(Scheduled break — no instruction.)

Module 3 — Detection Engineering for AI (90 min)

- AI-specific detection signals
- Correlation across LLM telemetry, network, and identity
- Hands-on: write and tune detections

Module 4 — Response Automation (75 min)

- Auto-containment patterns
- User notification and coaching automation
- Ticket enrichment and case management integration
- Hands-on: full auto-response scenario

Module 5 — Measurement, Tuning, and Certification (45 min)

- SOAR metrics: MTTD, MTTR, automation rate, false-positive rate
- Tuning workflow
- Certification exam

Hands-On Deliverables

- Three complete playbook builds

- Detection engineering lab
- Full auto-response scenario
- Tuning exercise

Materials Included

- AI SOAR Engineer Handbook
- Lab environment access (30 days)
- ZTA AI SOAR Specialist credential (valid 2 years)

Student Requirements

- Laptop with SSH and browser
- SOC or detection engineering background
- Familiarity with at least one SIEM platform

2.11 AI Firewall / HealthCheck In-Depth

Field	Detail
Course Code	FW-HC-801
Duration	8 hours
Tier	Technical Deep-Dive
Delivery	Online or on-site
Credential	ZTA AI Firewall & HealthCheck Specialist Certification
Target Audience	Security engineers, platform engineers, AI platform owners
Prerequisites	Familiarity with network security or application security. ZTA Admin training recommended.
Per-Seat Price (online public)	$1,295
Private Online (flat rate)	$6,950 up to 12 students; $995/seat overage
Private On-Site (flat rate)	$9,950 up to 10 students + travel/ODCs; $995/seat overage

Course Description

Full-day deep dive into the AI Firewall and AI HealthCheck capabilities. Covers deep policy configuration, prompt/response inspection, model behavior monitoring, drift detection, compliance attestation, and integration with CI/CD pipelines for AI applications.

Learning Objectives

- Configure AI Firewall policies for prompt inspection, output filtering, and tool-use controls
- Deploy AI HealthCheck for continuous model and application monitoring
- Implement drift detection, bias monitoring, and compliance attestation
- Integrate with AI application CI/CD pipelines
- Tune detection for low false-positive rates

Module Breakdown

Module 1 — AI Firewall Architecture (60 min)

- Inline vs. out-of-band deployment
- Prompt and response inspection pipeline
- Tool-use and function-call governance
- Performance and latency considerations

Module 2 — Policy Configuration Deep Dive (90 min)

- Policy DSL and rule authoring
- Hands-on: build policies for PII, PHI, classified markings, secrets
- Output filtering: hallucination detection, toxicity, brand safety
- Tool-use restrictions and allow-lists

Lunch (60 min)

(Scheduled break — no instruction.)

Module 3 — AI HealthCheck Deployment (75 min)

- Continuous monitoring architecture
- Model drift detection and baselining
- Bias and fairness monitoring
- Compliance attestation generation

Module 4 — CI/CD Integration (75 min)

- Pre-deployment model evaluation
- Policy-as-code for AI applications
- Automated regression testing
- Hands-on: wire HealthCheck into sample pipeline

Module 5 — Tuning, Ops, and Certification (60 min)

- False-positive reduction workflow
- Operational runbook building

- Performance troubleshooting
- Certification exam

Hands-On Deliverables

- Complete policy set authoring
- HealthCheck deployment lab
- CI/CD integration exercise
- Tuning workshop

Materials Included

- AI Firewall & HealthCheck Engineer Handbook
- Policy template library
- Lab environment access (30 days)
- Specialist credential (valid 2 years)

Student Requirements

- Laptop with SSH, browser, and Git client
- Familiarity with network or application security
- Basic Python or similar scripting ability

2.12 ZeroTrusted.ai Boot Camp — Tools and AI Security

Field	Detail
Course Code	BOOTCAMP-1601
Duration	16 hours (2 days)
Tier	Intensive
Delivery	Online (2 days) or on-site (2 days)
Credential	ZeroTrusted.ai Boot Camp Certificate
Target Audience	New security engineers, platform engineers, and analysts joining AI-governed environments
Prerequisites	Basic security or IT background. Laptop required.
Per-Seat Price (online public)	$2,795
Private Online (flat rate)	$12,500 up to 12 students; $1,995/seat overage
Private On-Site (flat rate)	$17,500 up to 10 students + travel/ODCs; $1,995/seat overage

Course Description

Intensive two-day boot camp combining ZTA platform training with AI security fundamentals. Designed for new team members who need to be operational on the platform and fluent in AI security concepts within one week. Covers the essentials of user, admin, firewall, and SOAR functionality plus hands-on AI security exercises.

Learning Objectives

- Operate the ZeroTrusted.ai platform confidently as an administrator
- Understand and apply AI security fundamentals
- Build working AI security controls (policies, detections, playbooks)
- Respond to common AI security incidents
- Know where to go for deeper training in specific areas

Module Breakdown

Day 1 — Morning: ZTA Platform Essentials (4 hrs)

- Platform architecture and deployment basics
- Initial configuration and identity integration
- Hands-on: install and configure ZTA in lab

Day 1 — Lunch (60 min)

(Scheduled break — no instruction.)

Day 1 — Afternoon: Policy and Monitoring (4 hrs)

- Policy architecture and authoring
- AI HealthCheck and Shadow AI policies
- Monitoring, dashboards, and SIEM integration
- Hands-on: build and deploy policy set

Day 2 — Morning: AI Security Fundamentals (4 hrs)

- AI threat landscape and OWASP Top 10 for LLM
- Hands-on: prompt injection attack and defense
- Data protection in AI workflows
- Shadow AI discovery

Day 2 — Lunch (60 min)

(Scheduled break — no instruction.)

Day 2 — Afternoon: SOAR, Incident Response, Certification (4 hrs)

- AI SOAR playbook basics
- Incident-response workflow
- Hands-on: full incident scenario
- Boot Camp certification exam (60 questions)

Hands-On Deliverables

- Full ZTA lab install

- Policy authoring and deployment
- Prompt-injection lab
- Shadow AI discovery exercise
- Full incident response scenario

Materials Included

- ZTA Boot Camp Handbook
- Policy and playbook template libraries
- Lab environment access (60 days)
- Boot Camp certificate
- Recommended next-step learning path per role

Student Requirements

- Laptop with admin access, SSH, browser
- Basic Linux command-line proficiency
- Pre-class reading (approximately 2 hours)

2.13 AI Agent Testing and Certification Course

Field	Detail
Course Code	AGENTCERT-401
Duration	4 hours
Tier	Specialist Certification
Delivery	Online or on-site
Credential	ZeroTrusted.ai Certified Agent Tester
Target Audience	AI engineers, QA, red-teamers, AI application owners
Prerequisites	Familiarity with AI agents or LLM applications. Python or scripting experience helpful.
Per-Seat Price (online public)	$895
Private Online (flat rate)	$4,500 up to 12 students; $695/seat overage
Private On-Site (flat rate)	$6,500 up to 10 students + travel/ODCs; $695/seat overage

Course Description

Focused half-day training on how to test, evaluate, and certify AI agents before and during production deployment. Covers functional testing, safety testing, red-teaming, benchmark evaluation, and the ZeroTrusted.ai agent certification methodology.

Learning Objectives

- Design comprehensive test suites for AI agents
- Red-team agents against common failure modes
- Evaluate agent performance against benchmarks
- Apply the ZeroTrusted.ai agent certification methodology
- Document agents for production deployment

Module Breakdown

Module 1 — Agent Testing Fundamentals (45 min)

- What to test in an AI agent
- Functional vs. safety vs. performance testing
- Determinism, variance, and repeatability
- Benchmark selection

Module 2 — Red-Teaming Agents (75 min)

- Common agent failure modes
- Hands-on: red-team an agent against safety rubric
- Injection via tools, memory, and data sources
- Documenting findings

Break (15 min)

(Scheduled break — no instruction.)

Module 3 — The ZTA Certification Methodology (60 min)

- Certification levels and criteria
- Evidence collection
- Hands-on: run an agent through the full certification
- Ongoing monitoring post-certification

Module 4 — Documentation and Certification Exam (45 min)

- Production-ready agent documentation
- Handoff to operations
- Certification exam

Hands-On Deliverables

- Full red-team exercise
- Complete certification run against sample agent
- Documentation package build

Materials Included

- Agent Testing Handbook
- Red-team rubric and scripts
- Certification workflow templates
- ZTA Certified Agent Tester credential (valid 2 years)

Student Requirements

- Laptop
- Active AI API access (OpenAI, Anthropic, or similar)
- Python familiarity recommended

3. Pricing

3.1 Pricing Philosophy

ZeroTrusted.ai Academy pricing is structured around two delivery models: per-seat public courses for organizations sending individual students, and flat-rate private / dedicated sessions for organizations running an entire cohort together. Per-seat pricing is online-only. Private sessions can be delivered online or on-site.

All pricing is shown in US dollars and excludes applicable VAT, GST, or sales tax. International pricing and distributor treatment follow the same structure as the ZeroTrusted.ai platform — see the companion Global Pricing Description document.

3.2 Per-Seat Public Course Pricing (Online)

Scheduled public classes. Minimum 6 students to run a session; maximum 20 students per session. Volume discounts apply to single-organization purchases of multiple seats.

Course Code	Course Title	Hours	Per-Seat Price
EXEC-AI-401	Hands-on AI for Executives — Build Real Tools	4	$495
AGENT-401	Building AI Agents to Get Massive Work Done	4	$495
AISEC-401	AI Security and Privacy	4	$495
ZTA-ADMIN-801	ZeroTrusted.ai Administrator Training	8	$795
ZTA-USER-401	ZeroTrusted.ai User Training	4	$445
CIAO-801	Chief Information AI Officer (CIAO) Training Co...	8	$1,995
AICISO-801	AI CISO Training Course	8	$1,995
AICRO-801	AI Chief Risk Officer (AI CRO) Training Course	8	$1,995
FEDISSO-1601	Federal ISSO / ISSM Training Course	16	$3,495
SOAR-801	AI SOAR In-Depth	8	$1,295
FW-HC-801	AI Firewall / HealthCheck In-Depth	8	$1,295
BOOTCAMP-1601	ZeroTrusted.ai Boot Camp — Tools and AI Security	16	$2,795
AGENTCERT-401	AI Agent Testing and Certification Course	4	$895

Volume Discounts on Per-Seat Purchases

Seats Purchased	Discount	Notes
Standard	0%	Single-seat purchase, standard rate
10+ seats	10%	Applied to orders of 10+ seats across any combination of courses
25+ seats	20%	Applied to orders of 25+ seats across any combination of courses
50+ seats (contact sales)	30%	Custom program — dedicated cohort recommended

3.3 Private / Dedicated Session Pricing (Flat Rate)

Reserve a full session for your organization. Flat rate covers up to the stated student cap; per-seat overage pricing applies beyond the cap. On-site sessions add travel, lodging, and per diem as other direct costs (ODCs), billed at actual cost.

Online Private Sessions

Course Code	Course Title	Hours	Flat Rate	Max Students	Overage/Seat
EXEC-AI-401	Hands-on AI for Executives — Build Re...	4	$3,500	15	$395
AGENT-401	Building AI Agents to Get Massive Wor...	4	$3,500	15	$395
AISEC-401	AI Security and Privacy	4	$3,500	15	$395
ZTA-ADMIN-801	ZeroTrusted.ai Administrator Training	8	$4,950	15	$645
ZTA-USER-401	ZeroTrusted.ai User Training	4	$2,950	15	$345
CIAO-801	Chief Information AI Officer (CIAO) T...	8	$9,500	10	$1,495
AICISO-801	AI CISO Training Course	8	$9,500	10	$1,495
AICRO-801	AI Chief Risk Officer (AI CRO) Traini...	8	$9,500	10	$1,495
FEDISSO-1601	Federal ISSO / ISSM Training Course	16	$16,500	12	$2,495
SOAR-801	AI SOAR In-Depth	8	$6,950	12	$995
FW-HC-801	AI Firewall / HealthCheck In-Depth	8	$6,950	12	$995
BOOTCAMP-1601	ZeroTrusted.ai Boot Camp — Tools and ...	16	$12,500	12	$1,995
AGENTCERT-401	AI Agent Testing and Certification Co...	4	$4,500	12	$695

On-Site Private Sessions

Course Code	Course Title	Hours	Flat Rate	Max Students	Overage/Seat
EXEC-AI-401	Hands-on AI for Executives — Build Re...	4	$5,500	10	$395
AGENT-401	Building AI Agents to Get Massive Wor...	4	$5,500	10	$395

Course Code	Course Title	Hours	Flat Rate	Max Students	Overage/Seat
AISEC-401	AI Security and Privacy	4	$5,500	10	$395
ZTA-ADMIN-801	ZeroTrusted.ai Administrator Training	8	$7,500	10	$645
ZTA-USER-401	ZeroTrusted.ai User Training	4	$4,950	10	$345
CIAO-801	Chief Information AI Officer (CIAO) T...	8	$13,500	8	$1,495
AICISO-801	AI CISO Training Course	8	$13,500	8	$1,495
AICRO-801	AI Chief Risk Officer (AI CRO) Traini...	8	$13,500	8	$1,495
FEDISSO-1601	Federal ISSO / ISSM Training Course	16	$22,500	10	$2,495
SOAR-801	AI SOAR In-Depth	8	$9,950	10	$995
FW-HC-801	AI Firewall / HealthCheck In-Depth	8	$9,950	10	$995
BOOTCAMP-1601	ZeroTrusted.ai Boot Camp — Tools and ...	16	$17,500	10	$1,995
AGENTCERT-401	AI Agent Testing and Certification Co...	4	$6,500	10	$695

On-site flat rates do not include travel, lodging, or per diem. These are billed separately as ODCs. See Section 3.4.

3.4 Travel, ODCs, and Other Fees

Fee Type	Rate	Terms
Instructor travel time	$175/hour (portal-to-portal)	Billed from instructor departure to on-site arrival and return. Minimum 4 hours each way for continental US.
Airfare	Actual cost + 5% handling	Economy class for flights under 5 hours; business class for flights 5+ hours. GSA / government customers: per FTR.
Lodging	Actual cost, GSA rates for federal	Commercial rates for commercial customers, GSA per diem rates for federal customers.
Per diem (M&IE)	GSA rates	Standard GSA M&IE rate for on-site location.
Ground transportation	Actual cost + 5% handling	Rental car, rideshare, or taxi at instructor discretion.
Shipping (materials)	Actual cost	For physical training materials shipped in advance to on-site location.
Room rental	Per request	If customer cannot provide training space, ZTA arranges and invoices at actual cost + 10%.
Catering	Per request	If customer requests ZTA-arranged catering; actual cost + 10%.

All ODCs are invoiced monthly at actual cost with receipts. For federal customers, all travel conforms to the Federal Travel Regulation (FTR) and Joint Travel Regulations (JTR) as applicable.

3.5 Scheduling and Session Flexibility

- Online courses may be split into 2-hour intervals spread across multiple days. Scheduling must be agreed in advance; price does not change for split delivery.
- On-site courses are delivered as contiguous sessions to minimize travel expense. 16-hour courses are delivered as two consecutive days.
- Private sessions are scheduled within 30 days of booking subject to instructor availability. Expedited scheduling (under 10 business days) adds 15% to the flat rate.
- Cancellation: full refund 14+ days prior; 50% refund 7-13 days prior; no refund within 7 days. Rescheduling at no cost if requested 14+ days in advance.

3.6 Training Credits and Bundles

Organizations purchasing multiple courses or large cohort engagements may purchase training credits redeemable across the full course catalog. Credits are sold in blocks and provide additional discounts over the volume schedule:

Credit Block	List Value	Credit Price	Effective Discount	Expiration
25-seat equivalent	$22,375	$19,750	12%	12 months from purchase
50-seat equivalent	$44,750	$35,800	20%	12 months from purchase
100-seat equivalent	$89,500	$62,650	30%	18 months from purchase
250-seat enterprise pack	$223,750	$134,250	40%	24 months from purchase

Credits apply to per-seat pricing at current rates. Executive, federal, and intensive courses consume multiple credits per seat in proportion to their standard list price. Contact sales for exact credit consumption schedule.

3.7 Federal and Government Pricing

Federal customers purchasing through GSA, SEWP, or prime-contractor vehicles receive list pricing net of the applicable schedule markup. All travel conforms to FTR / JTR. Federal ISSO/ISSM Certification courses qualify for CPE credit toward common security certifications (CISSP, CAP, CGRC — subject to external accreditation bodies).

For DoD customers requiring delivery in classified or controlled environments, instructor cleared-facility rates and additional security-compliance fees apply. Contact contact@zerotrusted.ai for classified-delivery quotations.

4. Administrative Information

4.1 Booking and Payment

- Per-seat public courses: payment at registration via purchase order or credit card.
- Private sessions: 50% at booking, 50% 30 days before delivery or net-30 from invoice at delivery (commercial); net-30 from invoice (federal).
- Credit blocks: net-30 from invoice.

4.2 Cancellation and Rescheduling

- Per-seat public: transferable to another student at no cost; cancellation per Section 3.5 schedule.
- Private session: cancellation 14+ days prior, full refund; 7-13 days, 50%; under 7 days, no refund.
- ZTA-initiated cancellation (instructor illness, force majeure): full refund or reschedule at no cost.

4.3 Contact

- General inquiries: contact@zerotrusted.ai

All pricing and course content subject to change without notice. This catalog reflects 2026 pricing as of April 2026. Final pricing confirmed at quote or registration.