



ISSUED BY GAISB[™] • THE GLOBAL AI STANDARDS BODY

GAISB Certified AI Systems Security Architect[™]

Understand the whole picture of AI security — before you implement.

MAP THE RISK. BUILD THE DEFENSE. GOVERN THE USE.

REF: GAISB-SEC-ARCH / 2026 EDITION / VENDOR-NEUTRAL • EVERGREEN

01

Evergreen big-picture
credential

02

Builds a real AI Security
Blueprint

03

Publicly verifiable
credential

Organizations do not need more AI tools. They need to understand the risk *before they turn AI loose.*

AI is already inside most organizations — pasted into chatbots, wired into workflows, adopted team by team with no threat model behind it. Classical security guarded the doors against outsiders. This new intelligence works on the inside.

GAISB Certified AI Systems Security Architect™ trains professionals to see the whole board — every surface, every threat, every rule — and to carry a documented AI Security Blueprint into the implementation decision.



AI ADOPTED BLIND

- Shadow AI everywhere, unowned and unlogged
- Company data pasted into public chatbots
- No threat model for model, data, or agent
- Staff unprepared for deepfakes and voice clones
- No policy, no rules of the road

A CLEAR SECURITY PICTURE

- Exposure mapped across the organization
- Threats named, classified, and prioritized
- The human layer briefed and trained
- Data and IP exposure protected
- The rules understood before they bind

Security posture is evaluated against each organization's own baseline and context. GAISB makes no guarantee that any risk is eliminated; the credential develops judgment, not immunity.

From using AI to seeing *every way it can be attacked.*

The credential develops the whole map across nine modules. Every module ends in a guided lab that produces one layer of the learner's own AI Security Blueprint.

01 Why AI Breaks Classical Security	02 The Three Surfaces	03 The Attacker's Playbook
04 The Human Layer	05 Your Data, Your IP, Your Exposure	06 The Defender's Mindset
07 Using AI to Secure AI	08 The Rules of the Road	09 Capstone — The Blueprint Assembled

This is a strategic, evergreen credential — concepts and judgment, not tools or code. Nothing in it expires when the next model ships.

PROGRAM READINESS

Working familiarity with AI assistants such as Claude or ChatGPT; comfort discussing how the organization actually uses them.	No security background, coding qualification, or fixed number of years of experience is required.
GAISB AI Essentials™ or equivalent knowledge is recommended but not a mandatory prerequisite.	Access to a real organization — or an approved simulated case — for the AI Security Blueprint labs.

PRIMARY AUDIENCE

IT professionals who must advise, executives who must decide, and professionals who must work safely in an AI world.

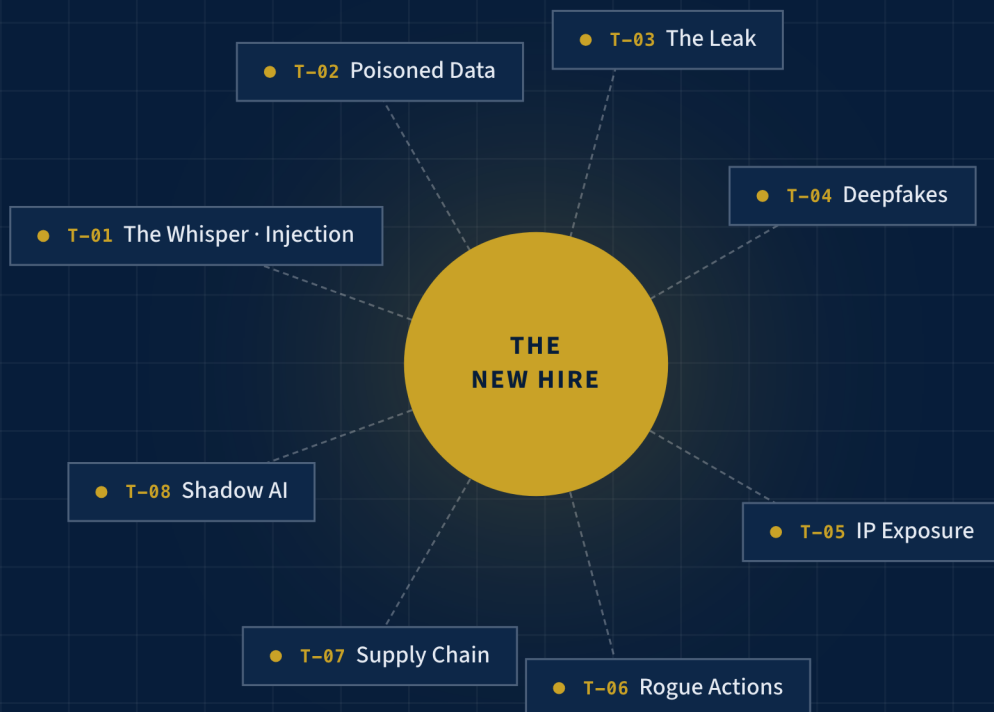
ALSO SUITED TO

Operations and transformation leaders, consultants, and business owners. These are fit indicators, not mandatory job titles.

Imagine AI as a brilliant new hire with genius knowledge and *zero judgment*.

It has read the whole internet, works at superhuman speed, has no memory of your rules unless you install them, and will do almost anything a confident voice tells it to. Classical security guarded the doors against outsiders. This genius already works on the inside. Everything confusing about AI security becomes obvious once you stop picturing a computer — and picture the person you just hired.

THE NEW HIRE · EIGHT WAYS IT GETS YOU IN TROUBLE



THE THREE SURFACES · EVERY AI CAN BE ATTACKED THROUGH

SURFACE / 01 Model The brain. What it believes, and who can talk it into anything.	SURFACE / 02 Data The memory. What it has read, and what it might repeat.	SURFACE / 03 Agent The hands. What it can touch, and what happens when it acts.
---	--	--

THE DURABLE QUESTIONS

What can it touch? Who can influence it? What happens when it gets it wrong? Tools change constantly; these surfaces and questions do not.

Map. Defend. Govern.

The AI Security Blueprint Method™: the whole method in three moves. Every lab in the program expands from these three words.

01 Map See where AI touches the organization — its surfaces, its threats, its blast radius.	02 Defend Apply durable principles and defensive AI to shrink the risk before it lands.	03 Govern Align to the rules, document the decisions, and keep the blueprint alive.
---	---	---

THE BLUEPRINT LAYERS · NINE GUIDED LABS

Each lab runs in Claude or ChatGPT — no tools, no code — and produces one layer.

01 AI Exposure Snapshot Where AI already touches your organization today.	02 Surface Map Every system decomposed into model, data, and agent.
03 Threat Profile The six attack classes, ranked for your context.	04 Human-Risk Briefing Deepfakes, voice clones, and phishing at scale — briefed plainly.
05 Data & IP Exposure Register Where prompts go; copyright, trade-secret, and privacy exposure.	06 Defense Principles One-Pager Least privilege, human-in-the-loop, kill switch, defense in depth.
07 AI Defender Use-Case Shortlist Where defensive AI earns its place: monitoring, detection, red-teaming.	08 Compliance Snapshot NIST AI RMF, EU AI Act, ISO 42001, OWASP — what binds you.
09 The AI Security Blueprint All layers assembled, plus the "Questions to Ask Before You Implement" checklist — the pre-implementation decision framework.	

The method is taught and assessed as professional practice. GAISB makes no guarantee that any specific risk is prevented; the blueprint is evaluated against each organization's own baseline.

THE PROGRAM

Learn the map. Build the blueprint. *Carry it to work.*

FULLY ONLINE · APPLIED · COHORT-SUPPORTED

PROGRAM DURATION

Typical completion: 3–6 weeks

CREDENTIAL LEVEL

Applied

COMMUNITY ACCESS

60 days · Prompt Atlas Club

WHAT THE PROGRAM INCLUDES

01 Self-guided curriculum All nine modules, at your pace	02 Live cohort sessions Guided, instructor-led learning
03 Guided AI lab sessions Nine labs in Claude or ChatGPT — no tools, no code	04 Assessment preparation Focused readiness for the knowledge check
05 60 days in Prompt Atlas Club Ongoing applied community access	06 The AI Security Blueprint A real deliverable you carry to work

COMPETENCY MAP

Threat mapping

Attack literacy

Human-layer defense

Data & IP protection

Defensive AI

AI governance

SELECTED GAISB PROGRAM FACULTY & STANDARDS LEADERSHIP

This program is delivered by credentialed, GAISB Council-appointed faculty and standards professionals.

“ You would never give a new hire the keys on day one. AI deserves the same interview. ”

— Kirwin M. Narine, Founding Chair & Chief Executive Officer, GAISB™



FOUNDING CHAIR & CEO
Kirwin M. Narine
GAISB™ · Former Microsoft Certified Trainer & Master Certified Novell Instructor



Brandon Basdeo
Director of Applied AI Standards & Frameworks



Dr. Winzy Adams
Director of Academic Courseware & Instructional Design

What a Certified AI Systems Security Architect can *demonstrate*.

The credential is defined by demonstrable capability, not tool coverage. Architects are not expected to master every platform. They are expected to see the whole board and prove it.

01 Map an organization's AI exposure.

02 Decompose any AI system into model, data, and agent.

03 Classify the six durable attack types.

04 Brief a team on AI-powered social engineering.

05 Audit data and IP exposure.

06 Apply the six defense principles.

07 Identify defensive-AI use cases.

08 Scope which AI regulations apply.

09 Assemble an organizational AI Security Blueprint.

10 Run the pre-implementation checklist.

“ *Capability is demonstrated by a blueprint that maps, defends, and governs an organization's AI — not by the number of tools a candidate can name.* ”

GAISB ASSESSMENT PRINCIPLE

The credential requires a completed *AI Security Blueprint*.

Every candidate assembles and submits one AI Security Blueprint, built layer by layer through the nine labs, meeting the published GAISB standard before the credential can be issued.



RECORDED BLUEPRINT WALKTHROUGH

The candidate records an 8–12-minute walkthrough explaining the exposure map, the threats prioritized, the defenses chosen, and the governance decisions behind them.

BLUEPRINT REQUIREMENTS

Blueprint layers	Nine
Review	Reviewed submission
Recorded walkthrough	8–12 min
Supporting artifacts	The nine layers

BLUEPRINT REVIEW AREAS

- | | |
|--------------------------|--------------------------|
| 01 Exposure Accuracy | 02 Threat Prioritization |
| 03 Human-Layer Clarity | 04 Data & IP Rigor |
| 05 Defensive-AI Judgment | 06 Governance Fit |
| 07 Presentation Quality | |

THE SUBMISSION PACKAGE

- AI Exposure Snapshot
- Threat Profile
- Data & IP Exposure Register
- Defender Use-Case Shortlist
- Assembled Blueprint + walkthrough
- Surface Map
- Human-Risk Briefing
- Defense Principles One-Pager
- Compliance Snapshot

CONTEXT & RESPONSIBILITY

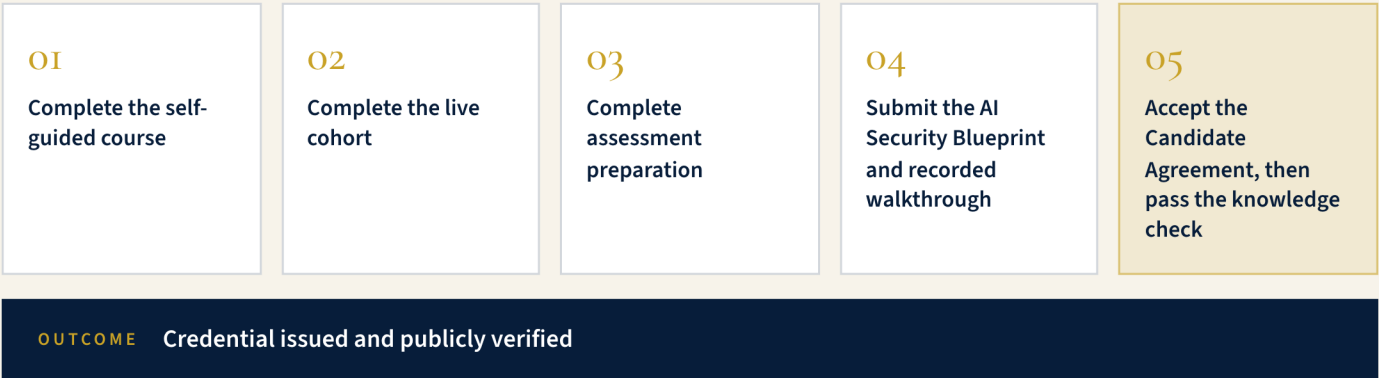
Candidates may use their own organization, employer, or an approved simulated case.

Candidates are responsible for obtaining appropriate authorization before using organizational information. Sensitive information must be removed, anonymized, or handled in accordance with the official guidance.

Submission alone is not sufficient. Blueprints that do not initially meet the required standard may be returned for revision in accordance with the published assessment policy.

Assessed through knowledge, application, and *judgment*.

ASSESSMENT FLOW



KNOWLEDGE CHECK Total questions [60] Duration [90 minutes] Format [Online, governed] Passing score [70%]	APPLIED ASSESSMENT <table><tr><td>AI Security Blueprint</td><td>One · Nine layers</td></tr><tr><td>Review</td><td>Reviewed submission</td></tr><tr><td>Recorded walkthrough</td><td>8–12 min</td></tr><tr><td>Judgment assessed</td><td>Yes</td></tr></table>	AI Security Blueprint	One · Nine layers	Review	Reviewed submission	Recorded walkthrough	8–12 min	Judgment assessed	Yes
AI Security Blueprint	One · Nine layers								
Review	Reviewed submission								
Recorded walkthrough	8–12 min								
Judgment assessed	Yes								
EXAMINATION VOUCHER USD \$395, purchased separately from program tuition. Valid for 12 months from issue; one attempt per voucher. A new voucher is required for each retake; a retake does not require repurchasing tuition.	CREDENTIAL RENEWAL Renewal every two years. Continuing professional education requirements apply to maintain an active credential.								

Assessment specifics shown in brackets are placeholders pending publication. Assessment is governed. GAISB does not guarantee assessment success, certification, or unlimited retakes. Separate assessment and retake fees apply.

WHAT YOU EARN

An applied credential designed for *public verification*.



ILLUSTRATIVE CREDENTIAL PREVIEW

GAISB AI Systems Security Architect™
APPLIED SECURITY CREDENTIAL

THIS CERTIFIES THAT

[Candidate Name]

Has satisfied the education, applied-blueprint, and assessment requirements established for the GAISB Certified AI Systems Security Architect™ credential.

Credential ID
[GAISB-YYYY-####]

Issued
[date]

Renews
[+2 years]



LinkedIn-ready digital badge
Add the credential to your professional profile.

PUBLIC REGISTRY RECORD

[registry.gaisb.org](#)ILLUSTRATIVE PREVIEW

CERTIFICATION	LEVEL
AI Systems Security Architect	Applied
STATUS	APPLIED BLUEPRINT
Active	Reviewed
ISSUED	VALID THROUGH
[date]	[+2 years]

Issued by GAISB™ Standards Council

REGISTRY-VERIFIED

ILLUSTRATIVE REGISTRY PREVIEW

- WHAT EMPLOYERS, CLIENTS AND PROFESSIONAL PARTNERS CAN VERIFY
- Credential title
 - Credential status
 - Renewal / expiry
 - Credential level
 - Issuance date
 - Public verification record

Where this credential *sits*.

GAISB Certified AI Systems Security Architect™ is the security specialization of the GAISB credential family — a sibling track to Governance, built on foundation and professional-core capability.



HOW THE CREDENTIAL IS APPLIED PROFESSIONALLY

Advise on AI adoption	Run AI security reviews	Brief boards and leadership
Set AI policy	Train the human layer	Keep the blueprint current

Professional application depends on individual effort, organization, and market circumstances. GAISB makes no promise of a specific fee, income, clients, employment, promotion, or business outcome.

Your path to the *GAISB Certified AI Systems Security Architect™* credential.

- 1 Complete the self-guided course
- 2 Complete the live cohort
- 3 Complete assessment preparation
- 4 Submit the AI Security Blueprint and walkthrough
- 5 Accept the Candidate Agreement, then pass the knowledge check

OUTCOME Receive and publicly verify the credential

TUITION

Program tuition

USD \$3,995

Examination voucher

Purchased separately · Valid 12 months · One attempt

USD \$395

TUITION INCLUDES

- Complete nine-module curriculum
- Guided AI lab sessions
- 60 days in Prompt Atlas Club
- Live cohort sessions
- Assessment preparation
- Blueprint submission review

Program tuition and the examination voucher are separate fees. May qualify for employer-sponsored professional development or reimbursement, subject to the employer's policies.

Enroll in GAISB Certified AI Systems Security Architect™

promptatlas.club

Request a Firm or Cohort

cohorts@gaisb.org



ENROLL · SECURITY
ARCHITECT



VERIFY A GAISB
CREDENTIAL

promptatlas.club · gaisb.org · registry.gaisb.org

Enrollment is open year-round; candidates receive immediate access to the self-guided curriculum and join the next available scheduled live cohort. All curriculum, cohort and lab sessions, assessment preparation, candidate support, blueprint submission and review, and the knowledge check are delivered online. Because access is granted immediately, program tuition is non-refundable after purchase except where required by applicable law; the knowledge-check voucher is sold separately under its own terms. Candidates unable to attend their intended cohort may transfer to a later cohort or use eligible session recordings, subject to the applicable program-access and transfer policies.

GAISB Certified AI Systems Security Architect™ is a private professional certification issued by GAISB™, a private professional standards organization. It is not an academic degree, occupational license, government-issued certification, employment guarantee, income guarantee or claim of ISO/IEC 17024 accreditation. Framework references (NIST AI RMF, EU AI Act, ISO/IEC 42001, OWASP) describe curriculum coverage and do not constitute endorsement by the referenced organizations. Current program terms, assessment fees, renewal requirements, access periods and assessment requirements are available through official GAISB channels.