SECURE AI WORKFORCE ENABLEMENT

Bring your workforce into the modern AI era. *Safely.*

With 20 years in business, ATOM helps organizations plan, implement, and govern AI adoption, from policy and training to engineering and ongoing monitoring, so teams can use modern AI productively and securely.

EXPERTISE ACROSS LEADING AI PLATFORMS

Claude	Anthropic's assistant, Claude Code, and Cowork, deployed with enterprise controls.
Grok	xAI's models, evaluated for data handling, safe use, and approved business tasks.
Gemini	Google's AI in Workspace and Google Cloud, configured to your data boundaries.
Microsoft Copilot Cowork	Agentic Microsoft 365 tasks, with permissions, governance, and credit cost planning.
Self-hosted & frontier models	Private, self-hosted, and frontier models for sensitive data and custom workloads.

FROM ROADMAP TO GOVERNANCE

What ATOM Delivers

AI Roadmap & Strategy

A prioritized plan for adopting AI, aligned with your business goals, data sensitivity, regulatory exposure, and the tools your teams need.

Engineering Implementation

Hands-on deployment and configuration of approved AI platforms, integrations, access controls, and data protections.

Regulatory Testing

Testing of AI use cases and configurations against applicable regulatory and contractual requirements before rollout.

Workforce AI Policies

Clear acceptable-use, data-handling, and approval policies that define how employees can use AI safely.

Training & Skills

Practical training that builds AI skills across the workforce, from safe everyday use to role-specific workflows.

Governance & Monitoring

Ongoing oversight of AI use, with monitoring, policy updates, and reviews as tools, regulations, and your organization evolve.

Schedule your free consultation.

Email **info@theatomgroup.com**

A SECURE APPROACH

Considerations Before Any AI Rollout

Data Access	What data each AI tool can reach, where it goes, and who can see it.
Safe Use	Approved tools and use cases that keep sensitive information protected.
Regulatory Exposure	How AI use intersects with privacy, industry, and contractual obligations.
Threats	AI-specific risks such as prompt injection, data leakage, and tool misuse.
Governance	Ownership, approvals, and oversight that keep AI use accountable over time.

PUTTING AI TO WORK

Enablement for Approved Use

Custom Engineering

Purpose-built AI solutions, agents, and automations designed around your workflows and data.

Business System Integrations

AI brought securely into existing financial, manufacturing, and operational tools.

AI in End-User Products

AI features integrated into the products your customers use, with security built in.

Skills & Tools

Skills, custom tools, and workflows that help teams get real value from approved platforms.

Application Registrations

Registering and configuring AI apps and integrations in your identity and cloud environments.

Cost-Effective Rollout

Partnering with your IT team on licensing, deployment, and integration choices that fit your budget.

TECHNICAL CONTROLS

Details in the technical overview

SSO & SCIM provisioning · **Role-based & conditional access** · **Data loss prevention** · **Retrieval & oversharing controls** · **Data residency & retention** · **MCP & connector governance** · **AI red teaming** · **Prompt injection testing** · **Audit logging** · **SIEM integration** · **Private model hosting** · **Secure API gateways**

FOR IT AND SECURITY TEAMS

Secure AI Architecture & Controls

Depending on your platforms and environment, ATOM's engineering work can include the following controls, configurations, and testing.

Identity & Access

- SSO and SCIM user provisioning for AI platforms
- Role-based and conditional access policies
- Application registrations with least-privilege permissions
- Admin console and tenant setting hardening

Data Protection

- Data loss prevention and sensitivity labeling
- Controls on what data AI can retrieve and index
- Oversharing review before AI goes live
- Data residency, retention, and training opt-out settings

Connectors, Agents & Integrations

- Governance of MCP servers, plugins, and connectors
- Agent permission scoping and human approval steps
- Secure API integration with business and product systems
- Secrets management for AI integrations

AI Security Testing

- AI red teaming and prompt injection testing
- Data leakage and jailbreak testing
- Evaluation of AI outputs for accuracy and safe behavior
- Testing mapped to regulatory and contractual requirements

Monitoring & Governance

- Audit logging and usage monitoring
- SIEM integration and alerting
- Usage and cost reporting, including credit-based billing
- Periodic governance reviews and policy updates

Self-Hosted & Private Models

- Private model hosting on-premises or in your cloud
- Network isolation and secure API gateways
- Model selection and evaluation for your workloads
- Hardening and patching of model infrastructure

RELATED ATOM SERVICES

Penetration Testing

AI red teaming and prompt injection testing, alongside full penetration testing of your environment.

Regulatory & Compliance Advisory

Licensed attorneys and specialists who map AI use to privacy, industry, and contractual obligations.

TYPICAL ENGAGEMENT DELIVERABLES

Scoped to your environment

- **AI risk assessment**
- **Architecture & data-flow review**
- **Configuration baselines**
- **Workforce AI policy set**
- **Security test reports**
- **Monitoring & governance runbook**

Questions From Your Technical Team?

Talk with ATOM's engineers about your platforms, architecture, and controls.

CONTACT
603-501-0003
info@theatomgroup.com
www.theatomgroup.com