CYBERSECURITY AUDIT & ASSESSMENT SERVICES

Know where you stand.
Know what to fix next.

A cybersecurity audit should give you more than a list of vulnerabilities. ATOM gives you a clear picture of your posture: meaningful gaps identified, risk prioritized, and practical recommendations, delivered remotely or onsite.

OUR APPROACH COMBINES FOUR DISCIPLINES

- **Technical evaluations**
- **Policy & documentation review**
- **Stakeholder interviews**
- **Penetration testing**

TECHNICAL + ADMINISTRATIVE

Comprehensive Audit & Gap Assessment

Cybersecurity Controls & Maturity

Baseline controls and organizational maturity, aligned with CIS standards, with gaps that could affect data confidentiality, integrity, or availability.

Policy & Administrative Controls

Review of policies, incident response plans, procedures, and administrative controls to identify governance gaps.

External Security & Firewall Review

Internet-facing infrastructure, access control lists, firewall and VPN configuration, and change-management practices.

Internal Vulnerability Assessment

Scanning of internal networks and applications for known vulnerabilities, with identified CVEs and CVSS severity.

Endpoint, Network, Cloud & Email

Endpoints, on-premises services, cloud environments, email systems, authentication practices, and security controls.

STAKEHOLDER INTERVIEWS

Behavior, Not Just Policy

We talk with the people who run your environment to capture institutional knowledge, then compare how work actually gets done with what policy says.

Schedule your free consultation.

Email info@theatomgroup.com

COMPLIANCE FRAMEWORKS

Our audits cover these standards and frameworks and more.

CMMC | CIS | NIST 800-53 | NIST 800-171 | FedRAMP | ISO 13485 | PCI | HIPAA | GDPR

FOR ORGANIZATIONS THAT BUILD OR MAINTAIN SOFTWARE

Application & Software Security

ATOM can extend the assessment into the application and the engineering processes that support it.

Application Security Assessment

Review of architecture, databases, source code repositories, dependencies, authentication and authorization, secrets management, CI/CD pipelines, environment segregation, and configuration, from development through production.

Engineering Process Review

Assessment of how software changes over time: SDLC controls, branching strategies, code and pull-request review, approval workflows, and testing practices, aligned with the NIST Secure Software Development Framework (SSDF).

FOR TECHNICAL TEAMS AND LEADERSHIP

Findings You Can Actually Use

Risk Register or POA&M
Structured findings and recommendations

→

Executive Summary
Immediate priorities and longer-term improvements

→

Practical Next Steps
A clear order for what to address first

Where remediation falls outside ATOM's scope, we provide specific recommendations for your existing MSP or IT provider, or identify trusted third-party resources. Where appropriate, we can also identify potential grant-funded services or scope remediation work ATOM can perform.

BEYOND INDIVIDUAL TECHNICAL FIXES

More Than an Audit

Cybersecurity Training

Customized training informed by current cybercrime and attack trends, with practical guidance for work and home. Typically a 90-minute interactive session, onsite or virtual.

Penetration Testing

Go beyond the audit: we test your defenses the way attackers do, with black, grey, and white box testing, red and purple teaming, and 180 days of retesting included.

Turn Findings Into a Plan

You don't need another report that sits on a shelf. ATOM helps you understand your posture, identify the risks that matter, and decide what to address first.

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