Cybersecurity Advisory Disclaimer

Last updated: June 25, 2026

Clear Cyber Advisory provides cybersecurity advisory, readiness review, documentation, and planning support for small and medium-sized businesses. Our services are designed to help organizations better understand and reduce business risks related to cyber insurance readiness, Shadow AI risk, and secure AI workflow automation.

Clear Cyber Advisory aims to provide practical, professional, and good-faith guidance based on the agreed scope, the information available, and the needs of the business.

This Disclaimer explains the limits of the information on this website and the limits of our advisory services.

Section 1: General Information Only

The information on this website is provided for general informational purposes only. It is not intended to be, and should not be relied on as, legal, insurance, financial, regulatory, compliance, accounting, or technical implementation advice.

Cybersecurity, privacy, insurance, technology, and regulatory requirements can vary by business, industry, contract, insurer, jurisdiction, and technical environment. You should consult appropriate legal, insurance, accounting, IT, cybersecurity, or other qualified professionals before making decisions that affect your business, systems, data, contracts, insurance coverage, compliance obligations, or security posture.

Section 2: Advisory Services

Clear Cyber Advisory provides practical advisory, review, documentation, planning, and risk-awareness support.

Our role is to help clients understand common risks, organize information, identify practical gaps, improve documentation, prioritize next steps, and know when to involve qualified specialists.

We do not sell insurance, act as an insurance broker, provide legal advice, provide accounting or tax advice, provide managed IT services, act as a managed security service provider, or monitor client networks 24/7.

We do not replace your IT provider, managed service provider, insurance broker, lawyer, accountant, auditor, regulator, implementation specialist, or internal management team.

Section 3: No Client Relationship From Website Use

Viewing this website, downloading materials, submitting a form, or contacting Clear Cyber Advisory does not create a client, advisory, consulting, fiduciary, or professional relationship.

A client relationship is created only when Clear Cyber Advisory and the client agree to a separate written engagement, proposal, statement of work, or service agreement.

Section 4: No Guarantee of Results

Our website content, reports, reviews, checklists, recommendations, and advisory services are intended to support better understanding, planning, documentation, prioritization, and decision-making.

Clear Cyber Advisory does not guarantee that our website content, reports, reviews, checklists, recommendations, or advisory services will prevent cyber incidents, data breaches, unauthorized access, fraud, business interruption, financial loss, system compromise, regulatory action, legal claims, or reputational harm.

Cybersecurity risk cannot be eliminated completely. Even well-managed organizations can experience security incidents, human error, vendor failure, software vulnerabilities, social engineering, or other unexpected events.

We also do not guarantee that a business will obtain cyber insurance, renew cyber insurance, receive lower premiums, satisfy insurer requirements, pass an audit, meet all legal or regulatory obligations, or satisfy every vendor, client, broker, insurer, regulator, underwriter, or third party.

Section 5: Cyber Insurance Readiness

Our cyber insurance readiness services are designed to help businesses better understand, organize, and prepare for common cybersecurity topics that may appear in insurance applications, renewals, questionnaires, evidence requests, or related discussions.

Insurance decisions are made by insurers, brokers, underwriters, and related parties. Clear Cyber Advisory does not make insurance decisions, provide insurance coverage, provide underwriting advice, interpret policy wording as legal advice, or guarantee any insurance outcome.

Clients are responsible for reviewing all insurance applications, answers, representations, policy documents, exclusions, warranties, conditions, and related communications with their broker, insurer, lawyer, or other qualified advisor before submission or reliance.

Section 6: Shadow AI Risk

Our Shadow AI risk services are designed to help businesses identify and reduce risks related to employee or business use of artificial intelligence tools, including risks involving confidential information, client data, vendor platforms, access controls, policies, approvals, and internal workflows.

AI tools and platforms may create risks related to data exposure, inaccurate outputs, hallucinations, intellectual property, privacy, security, compliance, vendor terms, and inappropriate reliance on automated outputs. Clear Cyber Advisory does not guarantee the accuracy, reliability, legality, security, or suitability of any AI tool, platform, vendor, output, or workflow.

Clients remain responsible for deciding which AI tools to use, what information may be entered into those tools, how outputs are reviewed, and how AI-related risks are managed within their organization.

Section 7: Secure AI Workflow Automation

Our secure AI workflow automation advisory services are designed to help businesses think through safer ways to improve selected workflows using AI, automation, documentation, access controls, approvals, and practical risk reduction.

Unless expressly agreed in a separate written agreement, Clear Cyber Advisory does not build, host, operate, maintain, monitor, or guarantee any automation system, software integration, AI model, third-party platform, or production workflow.

Clients are responsible for testing, approving, implementing, monitoring, maintaining, and securing any workflow, automation, integration, AI tool, or technical solution used in their business. Clients should ensure that any automation or AI-assisted process is reviewed by appropriate business, legal, technical, privacy, and security stakeholders before use with sensitive, confidential, regulated, or client information.

Section 8: Client Responsibility

Clients are responsible for final decisions they make based on our website content, advisory services, reports, checklists, recommendations, discussions, or other materials. Clear Cyber Advisory is responsible for providing advisory services in a professional, practical, and good-faith manner based on the agreed scope, the information available, and the limitations described in this Disclaimer and any applicable written agreement.

Clients are also responsible for implementing technical controls, maintaining systems, managing users, securing accounts, training staff, reviewing contracts, protecting data, selecting vendors, maintaining backups, testing security measures, and meeting applicable legal, regulatory, contractual, insurance, and business obligations.

Any recommendation or observation provided by Clear Cyber Advisory should be reviewed in the context of the client's specific business, systems, risk profile, industry, jurisdiction, budget, contracts, and obligations.

Section 9: No Audit, Certification, or Attestation

Clear Cyber Advisory provides practical advisory reviews, readiness support, documentation support, and action planning to help clients better understand gaps, organize information, and make informed decisions.

Unless specifically stated in a separate written agreement, Clear Cyber Advisory does not provide formal audits, certifications, attestations, penetration tests, vulnerability scans, compliance certifications, legal opinions, insurance opinions, or regulatory approvals.

Any review, scorecard, checklist, report, or readiness assessment we provide is intended to support business understanding and planning. It should not be treated as proof of compliance, proof of security, or a guarantee that controls are complete, effective, or sufficient for any specific third party.

Section 10: Third-Party Tools, Vendors, and Resources

Clear Cyber Advisory may refer to third-party tools, frameworks, vendors, platforms, insurers, brokers, IT providers, cybersecurity resources, AI tools, automation platforms, or other external materials.

These references are provided for convenience, education, or informational purposes only. They do not represent an endorsement or guarantee of the performance, security, availability, accuracy, compliance, or suitability of any third-party product, service, platform, vendor, or resource.

Clients are responsible for evaluating all third-party tools and providers before using them, including reviewing applicable terms, privacy practices, security controls, pricing, data handling, and contractual obligations.

Section 11: External Links

This website may contain links to third-party websites, tools, articles, resources, or platforms. Clear Cyber Advisory is not responsible for the content, accuracy, security, privacy practices, availability, or reliability of any third-party website or resource.

Accessing third-party links is at your own discretion and risk.

Section 12: Incident Response and Emergency Matters

Clear Cyber Advisory does not provide emergency cybersecurity response, 24/7 monitoring, live incident containment, law enforcement reporting, legal breach notification services, or emergency technical support unless expressly agreed in a separate written agreement.

If your business is experiencing an active cyber incident, suspected breach, ransomware event, account compromise, fraud, data loss, or urgent security issue, you should immediately contact your IT provider, cybersecurity incident response provider, insurer, broker, lawyer, and any other appropriate emergency or professional resources.

Section 13: Separate Written Agreements

Any paid services provided by Clear Cyber Advisory will be governed by a separate written proposal, statement of work, service agreement, or other written engagement terms.

If there is a conflict between this general website Disclaimer and a signed written agreement between Clear Cyber Advisory and a client, the signed written agreement will take precedence for that specific engagement.

Section 14: Changes to This Disclaimer

Clear Cyber Advisory may update this Disclaimer from time to time. The updated version will be posted on this website with a revised “Last updated” date. Continued use of this website after changes are posted means you accept the updated Disclaimer.

Section 15: Contact Information

Questions about this Disclaimer may be directed to:

Clear Cyber Advisory
Email: martin@clearcyberadvisory.com
Website: https://clearcyberadvisory.com