

CYBERSECURE 360™

Assess. Protect. Respond. Recover. Build Cyber Resilience.

EXECUTIVE SOLUTION OVERVIEW

CyberSecure 360™ is CISOG Technology Consults LLC's integrated cybersecurity advisory and transformation solution. It helps organizations understand their cyber risk, strengthen security controls, establish effective governance, improve resilience and create a measurable cybersecurity improvement roadmap.

ASSESS	PROTECT	RESPOND	RECOVER
Know your exposure	Reduce attack surface	Prepare for incidents	Build resilience

THE BUSINESS CHALLENGE

- Cyber threats continue to evolve while organizations face increasingly complex technology environments, cloud adoption, remote work, third-party dependencies and regulatory expectations.
- Many organizations know cybersecurity is important but lack an integrated view of risk, controls, governance, incident readiness and executive accountability.
- CyberSecure 360™ connects these areas into a practical, risk-based program designed around business priorities rather than technology alone.

WHAT CYBERSECURE 360™ DELIVERS

CAPABILITY	WHAT IT COVERS
Cybersecurity Strategy	Security strategy, objectives, priorities, investment roadmap and executive alignment.
Cyber Risk Management	Risk identification, analysis, treatment, risk register and executive risk reporting.
Security Governance	Roles, responsibilities, policies, committees, decision rights and accountability.
Security Architecture	Review of security architecture, technology controls and target-state improvements.
Identity & Access	IAM governance, privileged access, authentication and access-control improvement.
Vulnerability Management	Vulnerability identification, prioritization, remediation governance and metrics.
Incident Response	Incident-response planning, playbooks, tabletop exercises and readiness.
Security Monitoring	Security operations, logging, SIEM/SOC governance and detection capability advisory.
Data Protection	Data classification, protection, privacy-aligned security and resilience.
Third-Party Risk	Security due diligence and governance of vendors and technology partners.
Security Awareness	Role-based awareness, training and security culture improvement.
Resilience & Recovery	Business continuity, disaster recovery and cyber-resilience planning.

CYBERSECURE 360™ — SERVICE PACKAGES

1. Cybersecurity QuickScan™	5-10 business days
Rapid executive-level assessment answering: “How exposed are we?”	KEY OUTPUTS • Current-state security snapshot • Maturity score • Top cyber risks • Critical gaps • Executive risk dashboard • 90-day action plan
2. CyberSecure Assessment™	3-6 weeks
Comprehensive cybersecurity maturity, risk and control assessment.	KEY OUTPUTS • Stakeholder interviews • Policy and control review • Architecture review • Risk register • Maturity benchmarking • Gap analysis • Prioritized roadmap
3. CyberSecure Transformation™	3-9 months
Move from identified gaps to a measurable and governed cybersecurity program.	KEY OUTPUTS • Cybersecurity strategy • Governance framework • Policies and standards • Security controls • Risk management • Incident readiness • Security metrics • Transformation roadmap
4. CyberSecure Advisory™	Ongoing
Recurring cybersecurity advisory for organizations requiring continuous guidance and executive visibility.	KEY OUTPUTS • Monthly security advisory • Risk and roadmap reviews • Executive reporting • Security program oversight • Vendor/security reviews • Incident advisory • Policy governance • Leadership briefings

CYBERSECURITY LIFECYCLE

DISCOVER	ASSESS	PRIORITIZE	PROTECT	DETECT	RESPOND	RECOVER	IMPROVE
----------	--------	------------	---------	--------	---------	---------	---------

FRAMEWORK ALIGNMENT

CISOG can tailor CyberSecure 360™ to the client's regulatory, industry and risk environment. Depending on scope, alignment may include NIST Cybersecurity Framework, NIST SP 800-series guidance, CIS Controls, ISO/IEC 27001, COBIT and applicable industry or organizational requirements.

KEY DELIVERABLES

- Cybersecurity Strategy and Roadmap
- Cybersecurity Governance Framework
- Cyber Risk Register and Risk Treatment Plan
- Security Maturity Assessment
- Cybersecurity Gap Assessment
- Security Policies and Standards
- Security Control Catalogue
- Security Architecture Recommendations
- Incident Response and Recovery Framework
- Third-Party Cyber Risk Framework
- Security Metrics, KPIs and KRIs
- Executive Cybersecurity Dashboard

WHO CYBERSECURE 360™ IS FOR

CEOs & Boards: Need clear visibility into cyber risk, resilience and security investment priorities.

CIOs / CTOs: Need a structured cybersecurity strategy aligned with technology transformation.

CISOs: Need additional advisory capacity, program governance and transformation support.

COOs: Need cyber resilience integrated with business operations and continuity.

Risk & Compliance Leaders: Need measurable controls, evidence and risk reporting.

Mid-Market Organizations: Need mature cybersecurity capabilities without building every capability internally.

BUSINESS OUTCOMES

Risk Visibility	Understand the organization's most significant cybersecurity risks.
Risk Reduction	Prioritize investments and remediation based on business impact.
Resilience	Improve preparedness for cyber incidents and operational disruption.
Governance	Establish clear accountability and executive oversight.
Control Effectiveness	Strengthen and measure security controls.
Compliance Readiness	Improve alignment with relevant security and regulatory expectations.
Executive Confidence	Give leadership actionable metrics and a defensible security roadmap.

OPTIONAL SPECIALIST MODULES

- Cybersecurity Maturity Assessment™ — detailed maturity and control assessment.
- Incident Response Readiness™ — response plan, playbooks and tabletop exercise.
- Third-Party Cyber Risk Review™ — security due diligence and supplier risk assessment.
- Security Architecture Review™ — review of enterprise security architecture and target-state controls.
- Security Governance Accelerator™ — policies, governance model, committees and reporting.
- Executive Cyber Risk Briefing™ — board and leadership briefing on cyber risk and investment priorities.

WHY CISOG

CISOG Technology Consults LLC combines cybersecurity, GRC, IT governance, digital transformation and technology advisory capabilities. This enables CyberSecure 360™ to connect technical security decisions to enterprise risk, governance, business priorities and executive outcomes.

ENGAGEMENT MODEL

PHASE	ACTIVITY	PRIMARY OUTPUT
Discover	Business and technology context, stakeholder engagement	Cybersecurity baseline
Assess	Maturity, risk, controls and architecture assessment	Assessment and risk register
Prioritize	Risk-based remediation and investment planning	Prioritized roadmap

PHASE	ACTIVITY	PRIMARY OUTPUT
Transform	Implement governance, controls and operating capabilities	Improved security capability
Sustain	Metrics, advisory, monitoring and continuous improvement	Ongoing cyber resilience

READY TO STRENGTHEN YOUR CYBER RESILIENCE?

Schedule a CyberSecure 360™ consultation with CISOG Technology Consults LLC.

CISOG Technology Consults LLC | A Cisog Group company | CyberSecure 360™ | Datasheet