Security Simplified.

seisollc.com
(412) 206-6591
sales@seisollc.com

CyberSecure Strategy Blueprint

Simplify and accelerate your path to cybersecurity maturity that enables business imperatives and meets market demands.

Through a systematic planning methodology, we deliver a comprehensive, actionable roadmap to guide your security program from where you are now to where you need to be.

Our blueprint is a good fit for companies at all maturity levels, with lean teams navigating complex regulatory commitments and seeking structured, long-term guidance plus immediate action to align their security programs with business imperatives and market demands.

- **Compliance Readiness**: Be prepared for audits and maintain compliance with evolving standards.
- **Strategic Alignment**: Align security investments with business imperatives.
- **Vendor and Third-Party Risk Management**: Manage vendor risks and respond to security questionnaires confidently.
- **Security Assurance and Advantage**: Demonstrate effective controls and extend security capabilities and awareness with minimal disruption.

Our Process:

Document Review and Whiteboarding Sessions
We begin by reviewing your current documentation, then lead whiteboarding sessions and analytical exercises to explore your security requirements in-depth.

Risk Assessment and Control Selection
Aligned with global standards, we guide you through risk assessment planning and control selection, ensuring that your security measures are comprehensive and effective.

Blueprint Development for Implementation
Our team delivers a detailed strategy for deploying a security management system, including automated and streamlined processes to enhance efficiency.

What You Get:

Comprehensive Security Blueprint
A clear, actionable roadmap for establishing a robust cybersecurity framework, based on internationally recognized standards, including ISO 27001, SOC 2, CMMC, and NIST 800 series.

Tailored Risk and Compliance Strategy
We align your cybersecurity strategy with specific regulatory commitments and business imperatives, ensuring your program is audit-ready and built to address emerging regulations.

Enhanced Security Maturity and Efficiency
Our blueprint incorporates automation opportunities, allowing you to evolve from reactive cybersecurity to strategic, proactive management that reduces manual overhead and enhances security maturity.

Customer Results

Our customers are eliminating the complexities in the way of achieving their information security objectives — risk and vulnerability assessments, threat protection and regulatory compliance.

100% Certification Success

95% Customer Retention

Our unwavering commitment to customer satisfaction has enabled our customers to achieve their certifications without fail and turn security into advantage.

Rimsys

Achieved ISO 27001 and SOC 2 Audit Readiness Ahead of Expected Time.
This med-tech SaaS provider achieved audit-readiness for ISO 27001 and SOC 2 in less than 9-months to close a massive new customer deal.
Full case study

"Seiso guided us through dual audits with no nonconformities and we earned our ISO 27001 certification along with a SOC 2 attestation. This allowed us to close a significant deal with our biggest customer ever."
-- James Gianoutsos, Founder and CEO, Rimsys

JET ELECTRICAL TESTING

Strengthening Assurance and Incident Response with ISO 27001 Compliance
Using our 10 Domains framework to address compliance gaps, strengthen incident response, and build confidence for market growth.
Full case study

"Before Seiso, I was working with a big security c ompany for two years and getting nowhere. From the first call with Seiso, I learned more about the ISO process than I did after a year with the big consulting company. It was very easy to get started and they made me feel confident we'll get where we need to be. Thank God we were referred to Seiso."
—Al Mancini, IT Director, Jet Electrical Testing

TeleTracking

Cybersecurity Maturity for Business Growth
Developed, implemented, and maintained an information security management system that has withstood the test of evolving market requirements and compliance demand over time.
Full case study

""Seiso has been instrumental in transforming our cybersecurity posture, allowing us to confidently expand our services and meet rigorous industry standards. Their expertise and dedication have made them an invaluable partner in our growth journey. They are simply great to work with and I highly recommend them."
--- Brian Abercrombie, VP, IT and Information Security Officer, TeleTracking, Inc.

Seiso 10 Domains SM

Security Simplified.

Our approach is driven by a desire to simplify security. We follow a framework and tool agnostic method, the 10 Domains, that aims to swiftly evaluate and enhance your program, sidestepping the complexity and disruption often associated with traditional methodologies.

Governance

Creation of new governance documents or review and enhancement of those that already exist and bases them on a selected framework(s) such as ISO 27001, NIST, SOC 2, etc.

Risk Management

Risk management framework/methodology that is tailored to your Line(s) of Business (LoBs), industry/sector(s), and organizational risk profile and appetite.

Asset Management

Comprehensive identification, enumeration, and secure baseline configuration of organizational assets.

Identity & Access Management

Assessment of access management and enhancements needed to cover privileged access, cloud-based and on-premises access, and ongoing management.

Threat & Vulnerability Management

Comprehensive identification, assessment, and remediation of threats and vulnerabilities through expert-led simulations, analysis and targeted testing.

Situational Awareness & Information Sharing

Education and training programs to educate staff on actions they should take proactively and in response to threats.

Incident Response & Recovery

Assessment of current incident response policies and creation and implementation of an incident response plan/program.

Vendor Risk Management

Documentation and process optimization combined with controls and protections to to evaluate external vendor risk and respond to questionnaires more efficiently.

Workforce Management

Capabilities to achieve a security-aware culture that ensures personnel are highly competent, engaged, and accountable for fulfilling their responsibilities in maintaining a strong security posture.

Data Protection

Guidance and implementation for data protection program and comprehensive data catalog with updated controls.