

The SEISO 10 Domains

Key Benefits to Seiso's 10 Domains:

1. Streamline the assessment and development of a security program
2. Easily map to industry standard frameworks
3. Gain competitive advantage

Companies face the challenge of improving their security posture amidst increasing customer expectations for robust security practices. The plethora of frameworks like NIST, ISO 27x, SOC 2, CMMC can be overwhelming, leaving businesses unsure of where to begin or which to choose.

In 2017, Seiso's founders, driven by their experiences and the desire for a simpler approach, developed the Seiso 10 Domains. This framework-agnostic method aims to swiftly evaluate and enhance a company's security program maturity, sidestepping the complexity and disruption often associated with traditional methodologies.

The Seiso 10 Domains draw on best practices across standards, offering a streamlined, flexible approach to security program management. Organizations can choose any compatible practices, controls, or tools, making the Seiso Framework adaptable to various industries and regulatory environments, thus supporting business imperatives without the usual burdens.

1. **Governance:** Establishes rules for secure operations aligned with business needs.
2. **Risk Management:** Identifies, assesses, and mitigates unacceptable risks.
3. **Asset Management:** Tracks assets from creation to disposal.
4. **Identity & Access Management:** Manages user identities and access on a need-to-know basis.
5. **Threat & Vulnerability Management:** Identifies and mitigates security threats and vulnerabilities.
6. **Situational Awareness & Information Sharing:** Understands the security landscape and its impact.
7. **Incident Response & Recovery:** Ensures quick incident response and recovery with minimal disruption.
8. **Vendor Risk Management:** Assesses risks introduced by external vendors.
9. **Workforce Management:** Aligns workforce roles with security needs.
10. **Data Protection:** Identifies and protects organizational data.

The SEISO 10 Domains



- **People:** Skill and capability of personnel to execute security tasks.
- **Process:** Effectiveness of security processes in meeting stakeholder expectations.
- **Technology:** Infrastructure's support for security operations.

Why Seiso 10 Domains?

- Aligns with multiple frameworks including NIST CSF, ISO 27001 and SOC 2.
- Flexible, non-prescriptive controls suited to business needs.
- Simplifies security program development and review.
- Consolidates security into 10 functional areas to streamline assessing a security program.
- Uses clear language for broader understanding.
- Streamlines compliance with multiple frameworks into one method.

Seiso offers clients a competitive edge through streamlined security solutions, enhancing market access, deal speed, and modernization. Our approach simplifies security tasks and boosts competitive advantage with the Seiso 10 Domains for efficient security program execution.

Interested in streamlining your security? Contact us.