# External Information Security Officer (ISO)

**Leading Information Security Strategically – Without a Full-Time Internal Position**

iso-easy
ISO 27001

# Why an External Information Security Officer?

Information security is no longer an optional IT topic — it is a critical success factor for modern organizations. Customers, partners, regulators, and auditors expect structured security governance, clearly defined responsibilities, and an effective Information Security Management System (ISMS).

With our **External Information Security Officer (ISO) service**, we assume this responsibility for your organization — in a structured, continuous, and management-level aligned manner.

ISO 27001 requires clearly defined roles and responsibilities in the area of information security. The Information Security Officer (ISO) plays a central role in steering and maintaining the ISMS.

However, many small and medium-sized enterprises face similar challenges:
- No internal employee with sufficient security expertise
- Limited capacity for strategic security governance
- High personnel costs for a full-time position
- Risk of knowledge loss due to staff turnover
- Difficulty separating operational IT tasks from governance responsibilities

An external ISO provides a practical solution.
You gain access to experienced and independent expertise — without permanently allocating internal resources.

# The Role of the Information Security Officer

The Information Security Officer is not primarily a technical operator.
Rather, the role is strategic, supervisory, and governance-oriented. An effective ISO acts as:

- A strategic advisor to executive management
- The steering authority of the ISMS
- A coordinator between departments and IT
- The primary contact for auditors and external stakeholders
- The guardian of continuous improvement

The ISO ensures that information security is not treated as an isolated IT issue, but is structurally embedded throughout the organization.

iso-easy
ISO 27001

# Our Scope of Services as Your External ISO

Our service goes far beyond formally assigning a role. We actively assume the ISO function and manage it comprehensively.

## 1. Strategic Governance & Management Alignment

- Development and ongoing refinement of your information security strategy
- Definition of measurable security objectives and KPIs
- Regular alignment with executive management
- Integration of information security into business processes
- Establishment of clear decision-making and escalation structures

Information security becomes an integral part of corporate governance.

## 2. Establishment, Maintenance & Continuous Development of the ISMS

- Structuring and continuously improving your ISMS
- Ensuring compliance with ISO 27001 requirements
- Maintenance of the Statement of Applicability (SoA)
- Support for management reviews
- Integration of new business processes into the security framework

We ensure that your ISMS evolves alongside your organization — not as a static documentation system, but as a living management framework.

iso-easy
ISO 27001

# Our Scope of Services as Your External ISO

Our service goes far beyond formally assigning a role. We actively assume the ISO function and manage it comprehensively.

## 3. Risk Management & Threat Assessment

Effective information security is based on structured and ongoing risk management.
As your external ISO, we:
- Conduct and moderate regular risk assessments
- Identify and evaluate threats and vulnerabilities
- Assess potential business impact
- Prioritize mitigation measures
- Document and monitor residual risks
- Ensure traceability and transparency for audits

A professional risk management process protects not only sensitive information, but also business continuity, reputation, and stakeholder trust.

## 4. Policies, Controls & Documentation Management

ISO 27001 requires clear documentation and structured evidence. However, documentation must support operations — not overburden them. We support you with:
- Drafting and updating security policies
- Structuring procedures and control descriptions
- Reviewing documentation for audit readiness
- Maintaining structured, revision-safe records
- Ensuring alignment between policy and practice

We bring proven templates, methodologies, and best practices, and adapt them to your organization — ensuring clarity, practicality, and compliance.

iso-easy
ISO 27001

# Our Scope of Services as Your External ISO

Our service goes far beyond formally assigning a role. We actively assume the ISO function and manage it comprehensively.

## 5. Awareness, Training & Organizational Integration

An ISMS is only effective if it is understood and actively supported by employees. We help establish:

- Company-wide security awareness
- Executive briefings for management
- Clear role definitions (e.g., asset owners, system owners)
- Support for structured training programs
- Continuous awareness initiatives

Information security becomes part of your corporate culture — not just a documented requirement.

## 6. Audit Preparation & External Representation

A well-prepared audit reflects a well-managed ISMS.
As your external ISO, we:
- Prepare your organization for internal and external audits
- Support you throughout certification and surveillance audits
- Coordinate communication with certification bodies
- Represent your organization in discussions with auditors
- Support responses to customer security questionnaires
- Act as a professional point of contact for authorities and partners

You benefit from structured audit preparation, confident communication, and a significantly reduced risk of non-conformities.

iso-easy
ISO 27001

# Continuous Supervision Instead of Project-Based Support

The role of an Information Security Officer is not a one-time project.
It is an ongoing governance function. Our support model includes:

- Regular status meetings
- Risk review sessions
- Monitoring of implemented measures
- Documentation updates
- Strategic advisory sessions with management
- Ad-hoc support in case of security incidents

This ensures that your ISMS remains active, controlled, and continuously improved.

# Economic Advantages of an External ISO

Establishing an internal full-time ISO position typically involves:

- Significant annual personnel costs
- Ongoing training and certification expenses
- Limited availability during absence
- Risk of knowledge loss due to staff turnover

With our external ISO service, you receive:

- ✓ Predictable and transparent costs
- ✓ Immediate access to experienced security expertise
- ✓ Built-in substitution and continuity
- ✓ Cross-industry experience and best practices
- ✓ An independent and objective external perspective

This combination provides professional security governance
without long-term internal overhead.

**iso-easy**
ISO 27001

# Who Benefits from Our External ISO Service?

Our service is designed for organizations that want to establish professional, structured, and audit-compliant information security — without building an internal security department.

It is particularly suitable for:

- Small and medium-sized enterprises (SMEs)
- IT service providers and software companies
- Organizations preparing for ISO 27001 certification
- Companies facing increasing customer security requirements
- Businesses operating in regulated industries
- Organizations aiming to professionalize their governance structures

Whether you are at the beginning of your ISO 27001 journey or already certified, our external ISO service ensures structured leadership and sustainable development of your ISMS.

# An External ISO as a Strategic Competitive Advantage

A professionally managed ISMS does more than fulfill compliance requirements.

It:
- Strengthens trust with customers and partners
- Improves success rates in tenders and procurement processes
- Reduces operational and legal risks
- Enhances transparency in risk management
- Supports long-term organizational resilience

Information security becomes a strategic management discipline rather than a reactive IT function.

iso-easy
ISO 27001

# Working with iso-easy

iso-easy is part of Notivia GmbH, with more than 30 years of experience in digital solutions, IT security, compliance, and regulatory environments and customers like BMW, Allianz, Zeiss, SAMSUNG. Visit the website notivia.de.

We combine:
- Technical expertise
- Regulatory understanding
- Audit experience
- Pragmatic implementation
- Management-level communication

Our approach focuses on practical, business-oriented implementation — ensuring security without unnecessary bureaucracy.

# Your Next Step

If you would like to evaluate whether an external Information Security Officer is the right solution for your organization, we would be pleased to arrange a non-binding initial consultation.

Together, we will assess:
- Your current maturity level
- Regulatory and customer-driven requirements
- Organizational structure and responsibilities
- The optimal scope of ongoing support

Schedule your free initial consultation now.
Lead information security with clarity, structure, and confidence.
Partner with iso-easy for professional external ISO services.

Phone: +49 711 35 15 705
Email: feedback@iso-easy.de