iGUIDE

ISMS

Information Security Interested Parties

iNFOSECBASE

Contents

A Guide to Understanding the Needs and Expectations of Interested Parties

Introduction

ISO 27001 Clause 4.2 requires organisations to identify and understand the needs and expectations of interested parties that are relevant to the Information Security Management System (ISMS). This is a critical step in ensuring that the ISMS is aligned with both internal and external requirements, and it helps shape the scope, objectives and controls implemented within the ISMS.

Here's a step-by-step guide on how to meet the requirements of Clause 4.2:

What are Interested Parties?

Interested parties are individuals, groups or organisations that have a stake in, or are affected by, the organisation's information security. They can influence the ISMS or be impacted by its effectiveness.

Identify Interested Parties

The first step is to identify all the interested parties that have an impact on the ISMS or may influence its success; these could include:

Internal Interested Parties:

- **Employees**: all staff, including management and operational teams, who are involved in, or affected by, information security practices.
- **Owners/Shareholders**: individuals or groups with a vested interest in the success of the organisation.
- **IT and Information Security Teams**: departments or teams responsible for the management and security of information assets.
- **Management**: senior leadership that sets the strategic direction and policies of the ISMS.

External Interested Parties:

- **Customers/Clients**: organisations or individuals who expect their information to be protected when interacting with your business.
- **Suppliers and Contractors**: third-parties who provide services or products that could impact information security (e.g. cloud providers, outsourced IT services).
- **Regulators and Government Bodies**: authorities that enforce legal and regulatory requirements (e.g. data protection authorities for GDPR, financial regulators).
- **Partners and Business Alliances**: organisations with whom you share information or collaborate in business ventures.
- **Certification Bodies**: organisations that audit and certify your ISMS compliance with ISO 27001.

- **Competitors**: while not a direct stakeholder, competitors can influence information security if they create pressure to maintain a high security standard.

Determine Their Needs and Expectations

Once you have identified the relevant interested parties, the next step is to understand their needs and expectations. This involves recognising what these parties expect in terms of information security and compliance. Common needs and expectations include:

- **Compliance with legal and regulatory requirements**: interested parties, such as regulators or customers, may expect your organisation to comply with relevant laws, regulations and industry standards (e.g. GDPR, HIPAA, ISO 27001).
- **Confidentiality, integrity and availability**: many stakeholders will expect that their information is securely managed, protected from unauthorised access and is available when needed.
- **Incident response and breach notification**: customers, regulators and partners may expect timely reporting and handling of information security incidents.
- **Trust and reputational assurance**: maintaining a good reputation for secure information handling is often a key expectation, particularly from customers and shareholders.
- **Service continuity**: interested parties, such as customers and suppliers, may expect the organisation to have robust business continuity and disaster recovery plans in place.
- **Contractual obligations**: many customers, partners and suppliers will expect compliance with specific contractual information security terms.
- **Audit and oversight**: certification bodies and regulators may require periodic audits, reports or assessments to verify the organisation's compliance with information security controls.

Evaluate Which Needs and Expectations are Relevant to the ISMS

Not all the needs and expectations of interested parties will directly apply to the ISMS. You must evaluate which of these are relevant to your organisation's information security objectives and compliance obligations. Relevant needs and expectations typically include:

- **Legal and regulatory obligations**: laws and regulations that your organisation must comply with, such as data protection laws (GDPR, CCPA, etc.) and industry-specific regulations (HIPAA, PCI-DSS, etc.).
- **Contractual requirements**: security requirements defined in contracts with customers, suppliers or partners (e.g. service level agreements).
- **Organisational and industry standards**: compliance with internal policies, best practices and industry standards that influence your ISMS.

For each relevant need or expectation, document how it impacts the ISMS and how it will be addressed.

Power and Interest of Interested Parties

The influence of interested parties can vary depending on their power (ability to affect the organisation or its ISMS) and interest (level of concern about the organisation's information security), for example:

- **High Power, High Interest**: Regulators, key customers and board members require focused attention and frequent engagement.
- **High Power, Low Interest**: Senior executives may have significant influence but limited involvement, so concise and strategic updates are essential.
- **Low Power, High Interest**: Employees and some customers might actively engage with security processes but have less authority to enforce changes.
- **Low Power, Low Interest**: Parties such as the general public may have minimal impact but should still be considered if their interests align with the organisation's security objectives.

Understanding these dynamics helps prioritise engagement efforts and allocate resources effectively to meet stakeholder needs.

Benefits of Addressing Interested Parties' Needs

- Ensures compliance with applicable laws and regulations.
- Enhances trust and satisfaction among customers and partners.
- Reduces risks associated with external dependencies.
- Demonstrates a commitment to security, improving reputation and competitiveness.

By identifying and managing interested parties effectively, organisations can align their ISMS with business priorities, build strong relationships and ensure the ongoing success of their information security efforts.

Document and Communicate Findings

The findings related to the needs and expectations of interested parties should be documented as part of your ISMS. This documentation helps ensure transparency and demonstrates that the organisation understands and actively manages its obligations.

Common formats for documenting findings

- **Interested Parties Register**: a table or list that outlines each interested party, their relevant needs, expectations and how the ISMS addresses these.
- **Risk Assessment**: many of the needs and expectations of interested parties can be integrated into the risk assessment process, as they often highlight areas where risks must be mitigated.

Ensure that this information is shared with relevant stakeholders in the organisation, especially top management, to ensure alignment with the overall business strategy.

Review Regularly

The needs and expectations of interested parties can change over time due to new legal requirements, evolving technology or changes in stakeholder relationships. As part of the ISMS's continual improvement process (ISO 27001 Clause 10), it's essential

to review and update the list of interested parties and their expectations periodically.

- **Internal Review**: incorporate this into the management review process (Clause 9.3) to ensure it is reviewed regularly, alongside changes in risk or incidents.
- **Monitoring Changes**: stay informed about updates to laws, regulations and customer contracts and respond to changes as necessary.

Key Points for Compliance with Clause 4.2

- **Identify both internal and external interested parties** that affect or are affected by the ISMS.
- **Determine their needs and expectations**, especially those related to information security.
- **Evaluate which needs and expectations are relevant** to the ISMS and ensure they are addressed.
- **Document these findings** and communicate them to relevant stakeholders.
- **Review the needs and expectations** regularly to ensure ongoing compliance and relevance.

By understanding the needs and expectations of interested parties, your ISMS will be better aligned with both legal obligations and the strategic goals of the organisation, helping to protect information assets effectively.

Summary

ISO 27001 highlights the importance of identifying and addressing the needs of interested parties i.e. individuals or groups with a stake in the organisation's information security. These parties include internal stakeholders (e.g. employees, management), external stakeholders (e.g. customers, suppliers, regulators) and others (e.g. investors, community). Understanding the power and interest of these parties helps organisations prioritise their engagement, focusing on those with the highest influence or concern.

The process involves identifying interested parties, determining their expectations, prioritising their requirements and integrating them into the ISMS. Regular reviews ensure that the ISMS remains aligned with changing needs and regulatory requirements.

Effectively managing interested parties enhances compliance, builds trust, mitigates risks and ensures that the ISMS supports both security and business objectives.