Integral Management Systems

The role of an Information Steering Group within an IS Framework.

What is the purpose of an Information Security Steering Group?

A steering committee is an advisory group that makes directional decisions on various organizational projects. Its members directly support project managers working toward strategic company direction and achieving company goals and objectives.

The Information Security aspects of the overall IMS are managed through the input and oversight of the IS Steering Group (IS-SG) whose members are such that the company can make informed decisions about all its information security risks and investment decisions to mitigate those risks. And then further, a means to validate that the investments made are having the desired risk reduction impact.

The benefits of an Information Security Steering Group

Strengthening Cybersecurity Governance with ISO 27001:2022

To build trust among stakeholders and ensure that cybersecurity risks are effectively managed, executive management often look to implementing ISO standards such as ISO 27001 or as a minimum self-certification framework such as Cyber Essentials. In Europe the new regulatory requirements of NIS2 are now in effect and EU companies are expected to comply when it's transposed into laws within each country. As such, Cybersecurity governance is becoming a key aspect within most organizations.

Formal certification to ISO27001 requires not only a disciplined approach when defining and implementing the management system, but it requires a broad knowledge of systems, processes and existing controls and technical knowledge to ensure that the ISMS is effective within the business.

Do I Need a Steering Group if I'm a Micro Company?

When it comes to implementing an Information Security Management System (ISMS), the idea of forming a steering group might sound excessive—especially if you're a micro company with just a handful of staff. But regardless of company size, the core functions that a steering group performs are still highly relevant.

The primary purpose of a steering group is to separate cybersecurity governance and ISMS management activities from the day-to-day operational tasks of running the business. It ensures there's a dedicated focus on information security, rather than treating it as a background task.

For any organization—micro, small, or large—the role of a steering group typically evolves throughout the ISO 27001 journey. During the implementation phase, it helps coordinate tasks such as data gathering, documentation, publishing policies, and internal communication. After certification, the focus naturally shifts toward monitoring, reviewing performance, and driving continual improvement.

So, do micro companies need a steering group? Yes—but it doesn't have to be a formal committee. In a small setup, it could simply be one or two people taking on the responsibilities of coordinating ISMS efforts and ensuring progress isn't sidelined. The key is having a structured approach, however lean, to cover core areas like risk management, process development, and setting and reviewing objectives.

For larger businesses, the steering group becomes essential—not only to manage the complexity of implementation across departments but also to ensure ongoing involvement from leadership, IT, HR, operations, and other key areas.

In short, while the structure and scale of a steering group may differ, its purpose remains the same: to keep your ISMS focused, effective, and continuously improving.

Terms of Reference for a Steering Group

The IS Steering Group once established should be granted authority by the CEO or Senior Project Sponsor, typically a C-Level executive to provide the following:

- Provide Advice and Direction to the company on all matters relating to Information Security
- Set Project Timeline and Budgets associated with objectives, risk management and remedial actions.
- Monitor Information Security Incidents and actions taken.
- Evaluate and Monitor Risk activities.
- Review impacts or organizational change and the need to update the IS Policy framework.
- Define Project

Maximising the impact of the IS steering group.

A critical enabler of a successful ISO 27001 implementation is the formation of a dedicated steering group. This cross-functional team, typically composed of representatives from senior management, IT, legal, HR, and other key business areas, plays a vital role throughout the project.

Key Benefits of a Steering Group During ISO 27001 Implementation:

1. Clear Direction and Governance
The steering group ensures the project aligns with organisational objectives and provides strategic oversight. This helps keep the implementation on track, with clear priorities and defined milestones.

2. Executive Buy-in and Authority
With senior leadership involved, the project is more likely to receive the necessary resources and attention. Decisions can be made more swiftly, reducing delays caused by escalation or uncertainty.

3. Cross-Departmental Collaboration
Information security is not just an IT issue. A steering group ensures that perspectives from different business units are considered, enabling a more holistic and effective ISMS.

4. Risk-Aware Decision Making
The group can guide the organisation in identifying and prioritising risks based on business impact, ensuring the risk treatment plan is both practical and aligned with the company's risk appetite.

5. Faster Issue Resolution
When challenges arise—whether technical, procedural, or cultural—the steering group can quickly address them, drawing on the collective expertise of its members.

6. Sustained Momentum and Accountability
Regular meetings and progress updates help maintain momentum. Team members hold each other accountable, reducing the risk of project stagnation.

7. Stronger Culture of Security

Integral Management Systems

By involving leaders across the organisation, the steering group helps embed information security into the business culture from the top down.

Establishing a steering group not only facilitates a smoother implementation of ISO 27001, but also positions the organisation to sustain its information security practices long after certification. With clear oversight, shared responsibility, and strategic alignment, the steering group becomes a cornerstone of effective cybersecurity governance.

Written by

Jerry Lawrence
Lead Consultant
Integral Management Systems

Jerry is the owner/Lead consultant of Integral Management Systems who provide ISO 27001 & ISO 9001 Implementation, ISO Precertification and Internal audits. Jerry is a certified ISO 27001 Lead Implementer, ISO 27001 Lead Auditor and ISO 9001 Auditor. Jerry also has an extensive background in Software Development, Six Sigma and process improvement.