How to Implement Your ISMS in Notion

A practical guide based on the ICT Institute Notion ISMS templates for ISO 27001.

Why use Notion for your ISMS?

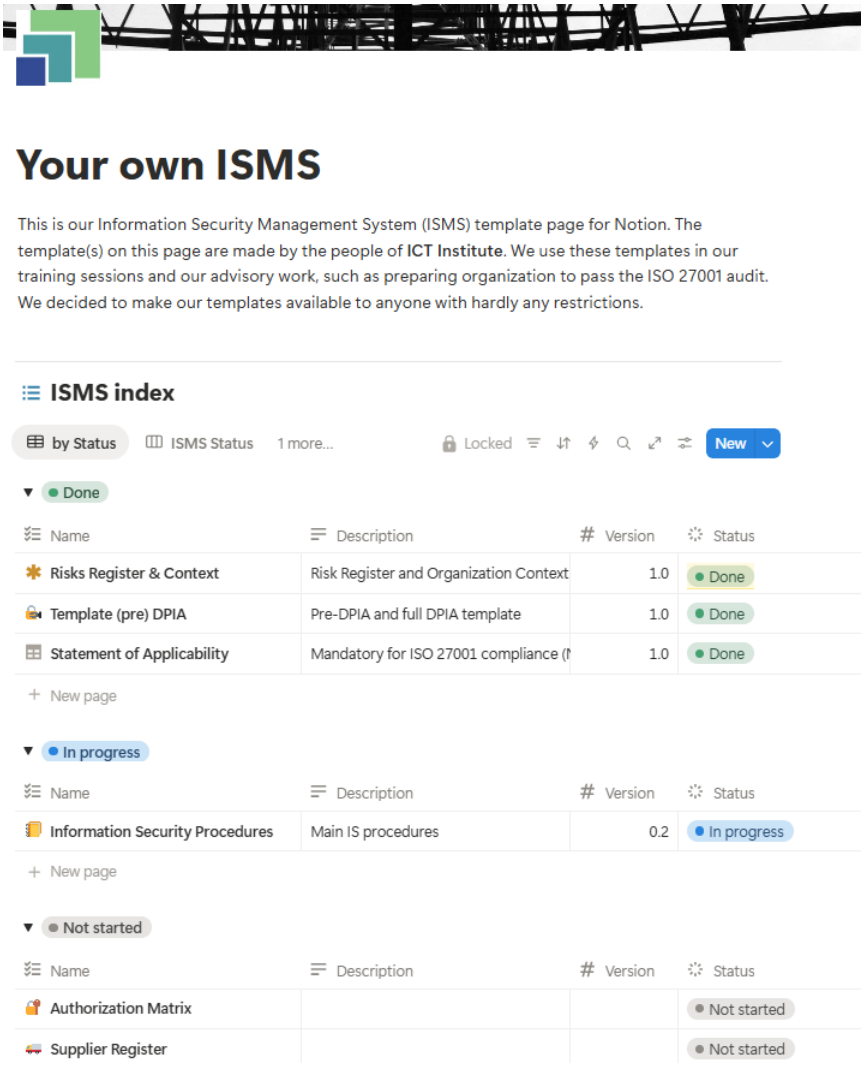
Notion is a modern collaboration platform that combines documents, databases, and integrations in a single workspace. These features align well with the concept of an Information Security Management System (ISMS): a structured set of policies, procedures, and records required by ISO 27001. Organizations already using Notion can leverage this familiarity to implement and maintain their ISMS more efficiently.

Pros
- Centralized documentation and clear structure
- Strong linking between ISMS components
- Full-text search across the workspace
- Real-time collaboration and version history

Cons
- Online-first dependency and limited offline use
- Performance impact in very large workspaces
- Loss of relations when exporting data
- Governance and cloud dependency considerations

Step 1 - Set up your ISMS homepage

The ISMS homepage acts as the central entry point for your management system. All policies, registers, and procedures are stored and accessed from here. You can think of it as an internal wiki or a structured SharePoint alternative. The ISMS Index provides an overview of all high-level ISMS components, grouped by status (Not started, In progress, Done). This allows you to immediately see what requires attention.



Your own ISMS

This is our Information Security Management System (ISMS) template page for Notion. The template(s) on this page are made by the people of **ICT Institute**. We use these templates in our training sessions and our advisory work, such as preparing organization to pass the ISO 27001 audit. We decided to make our templates available to anyone with hardly any restrictions.

ISMS index

by Status | ISMS Status | 1 more... | Locked | New

▼ Done

Name	Description	Version	Status
Risks Register & Context	Risk Register and Organization Context	1.0	Done
Template (pre) DPIA	Pre-DPIA and full DPIA template	1.0	Done
Statement of Applicability	Mandatory for ISO 27001 compliance (I	1.0	Done

+ New page

▼ In progress

Name	Description	Version	Status
Information Security Procedures	Main IS procedures	0.2	In progress

+ New page

▼ Not started

Name	Description	Version	Status
Authorization Matrix			Not started
Supplier Register			Not started

Step 2 - Follow the Harmonized/High-Level Structure (HLS)

The structure of the ISMS Index loosely follows the Harmonized/High-Level Structure of ISO 27001. This makes it easier to align your documentation with the standard and to navigate the ISMS during audits. Typical components include the Policies, Risk Register & Context, Statement of Applicability (SoA), procedures, and supporting registers.

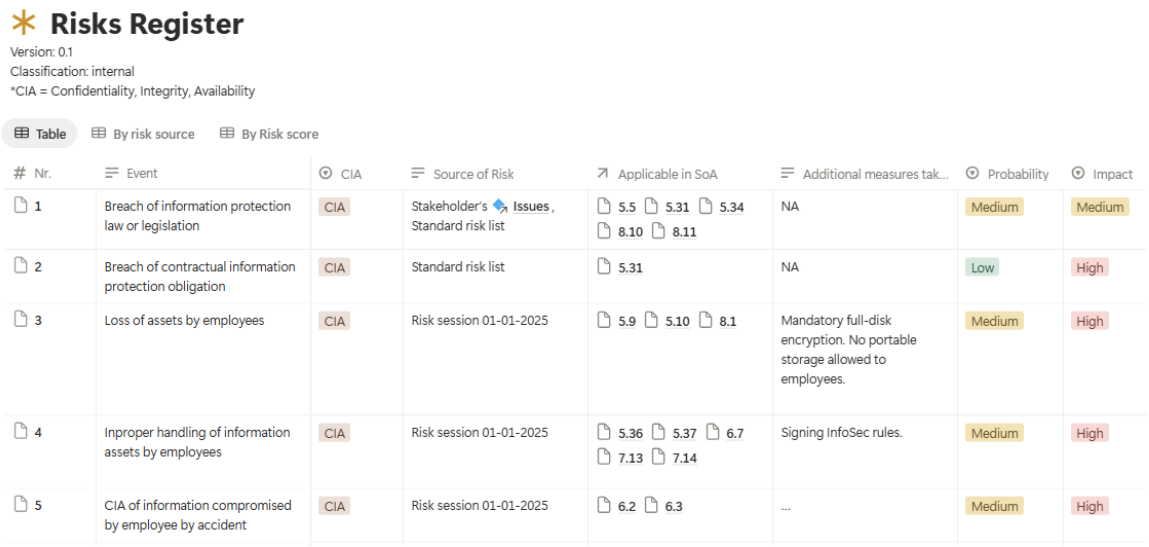
Read more:

- The Plan-Do-Check-Act (PDCA) cycle
- A summary of ISO2007: A summary of ISO 27001 requirements for information security

Step 3 – Starting point: Context & Identifying risks

As an example of a concrete implementation, Risk management is a mandatory ISO 27001 process and an ideal starting point. In the Notion template, we start from the Stakeholder analysis and company Issues. These serve as the context for identifying the relevant risks. The identified risks are then implemented as a Risk Register with self-contained pages, clear

explanations, ISO 27001 references, and linked databases. Each risk describes the event, CIA relevance, likelihood, impact, and calculated risk score. Acceptance thresholds and treatment decisions are automated using Notion formulas.



Risks Register

Version: 0.1
Classification: internal
*CIA = Confidentiality, Integrity, Availability

Table | By risk source | By Risk score

Nr.	Event	CIA	Source of Risk	Applicable in SoA	Additional measures tak...	Probability	Impact
1	Breach of information protection law or legislation	CIA	Stakeholder's Issues, Standard risk list	5.5 5.31 5.34 8.10 8.11	NA	Medium	Medium
2	Breach of contractual information protection obligation	CIA	Standard risk list	5.31	NA	Low	High
3	Loss of assets by employees	CIA	Risk session 01-01-2025	5.9 5.10 8.1	Mandatory full-disk encryption. No portable storage allowed to employees.	Medium	High
4	Inproper handling of information assets by employees	CIA	Risk session 01-01-2025	5.36 5.37 6.7 7.13 7.14	Signing InfoSec rules.	Medium	High
5	CIA of information compromised by employee by accident	CIA	Risk session 01-01-2025	6.2 6.3	...	Medium	High

A key strength of the template is the dynamic linking between the Risk Register and the Statement of Applicability. Controls selected in the risk treatment are automatically linked to the SoA, and vice versa. This ensures consistency and traceability across the ISMS without manual cross-referencing.

Read more:

- Our Notion risk register template with example context

Step 5 – Develop the following ISMS elements

Follow on the ISMS index to build your ISMS:

- Statement of applicability and the risk treatment
- Objectives, monitoring and measurement
- Plan an Internal audit program
- Set up Management reviews
- Begin the implementation of controls

Read more:

- We can support you in becoming ISO 27001 certified

Step 6 – Implement the annex controls

This is the part where you start documenting and implementing the Organizational, People, Physical and Technological controls of the ISO 27001 Annex, based on your Risk management and SoA. Each applicable control servers as a measure to control your risks in the four different

domains. Effective ISMS implementations focus less on 'having all controls' and more on embedding the relevant controls into everyday processes, roles, and decision-making. Governance controls set direction, people controls influence behavior, and technical controls enforce security in practice.

Use databases for registers (e.g. assets, suppliers, incidents, training), pages for policies and procedures, and relations to create bidirectional links between risks, controls, and evidence. Group controls by theme (such as governance, access management, suppliers, and incidents), assign clear owners, and use status and review fields to support continuous improvement. This approach keeps the ISMS auditable and maintainable.

Read more:

- ISO27002:2022 explained – Organizational controls
- ISO27002:2022 explained – People controls
- ISO27002:2022 explained – Physical controls
- ISO27002:2022 explained – Technological controls

Step 7 - Maintain and improve your ISMS

Notion supports continuous improvement through version history, collaboration, and integrations. You can document updates, assign risk owners, and link actions to yearly plans or procedures. Advanced integrations allow triggers such as creating meeting agenda items, tickets, or reminders when new risks are added.

Read more:

- Exploring Notion AI features for ISO 27001 and GDPR
- GDPR DPIA Template in Notion

Conclusion

Using Notion as the foundation for your ISMS can significantly reduce the effort required to implement and maintain ISO 27001 compliance. While Notion is not without limitations, it offers a flexible and accessible way to operationalize your ISMS when used with appropriate governance and risk awareness.

The ICT Institute templates provide a practical, ready-to-use starting point, especially for smaller organizations. Check out our website for the latest developments and services, and don't miss our YouTube channel for an accessible step-by-step video guidance for implementing the ISMS: https://www.youtube.com/@SieuwertExplains