DataGuard

GUIDE

ISO 27001 RISK MANAGEMENT

Central to any information security procedure in an organisation is its risk management process. Risk management involves two key elements: risk assessment (to identify any risks your organisation may face) and risk treatment (to ensure that comprehensive risk mitigation strategies are in place to handle them).

While it is regarded as the most crucial and challenging step in implementing the ISO 27001 standard in an organisation, understanding the 5 steps of risk management can help you manoeuvre the process more effectively.

STEP 1 - RISK IDENTIFICATION

To start identifying risks to your business, you need to assess your **information assets**, **internal and external threats** and any **vulnerabilities in your ISMS**. But before starting on your assessment, it is important to establish your risk assessment framework.

For your risk assessments to be auditable, objective and transparent, your process must be consistent, valid and comparable every time you do one. A risk assessment framework is a set of guidelines which ensures just that.

These guidelines must address:

1. The most important security criteria for your organisation
2. The scale of risk
3. Risk acceptance criteria
4. Methodology (risk assessment based on assets or scenarios)

When assessing risks for an asset-based risk assessment, consider the different asset types in your organisation including information and data, hardware and software, physical locations and storage, systems and services, people, organisations and intangibles. An asset database will further help you in conducting the assessment, where you can easily classify and assign responsibility to each asset.

Once the risks are identified, they should be allocated risk owners who are then given responsibility for the risk management process of the particular risks.

STEP 2 - RISK ANALYSIS

Assets may have several threats which can be exploited via multiple vulnerabilities in your system. It is important to **analyse and assess the likelihood of each combination of threat and vulnerability** along with their impact during the risk assessment. Outcomes of the analysis should also be reflected in the **Risk Assessment and Treatment Table.**

STEP 3 - RISK ASSESSMENT

Ranking risks based on their consequences and their likelihood would help your organisation deploy its resources effectively and can reduce redundancy. Through this, you can determine which hazards need to be prioritised and controlled immediately to prevent a possible security breach.

Overall Risk = Likelihood x Consequences

STEP 4 - RISK TREATMENT

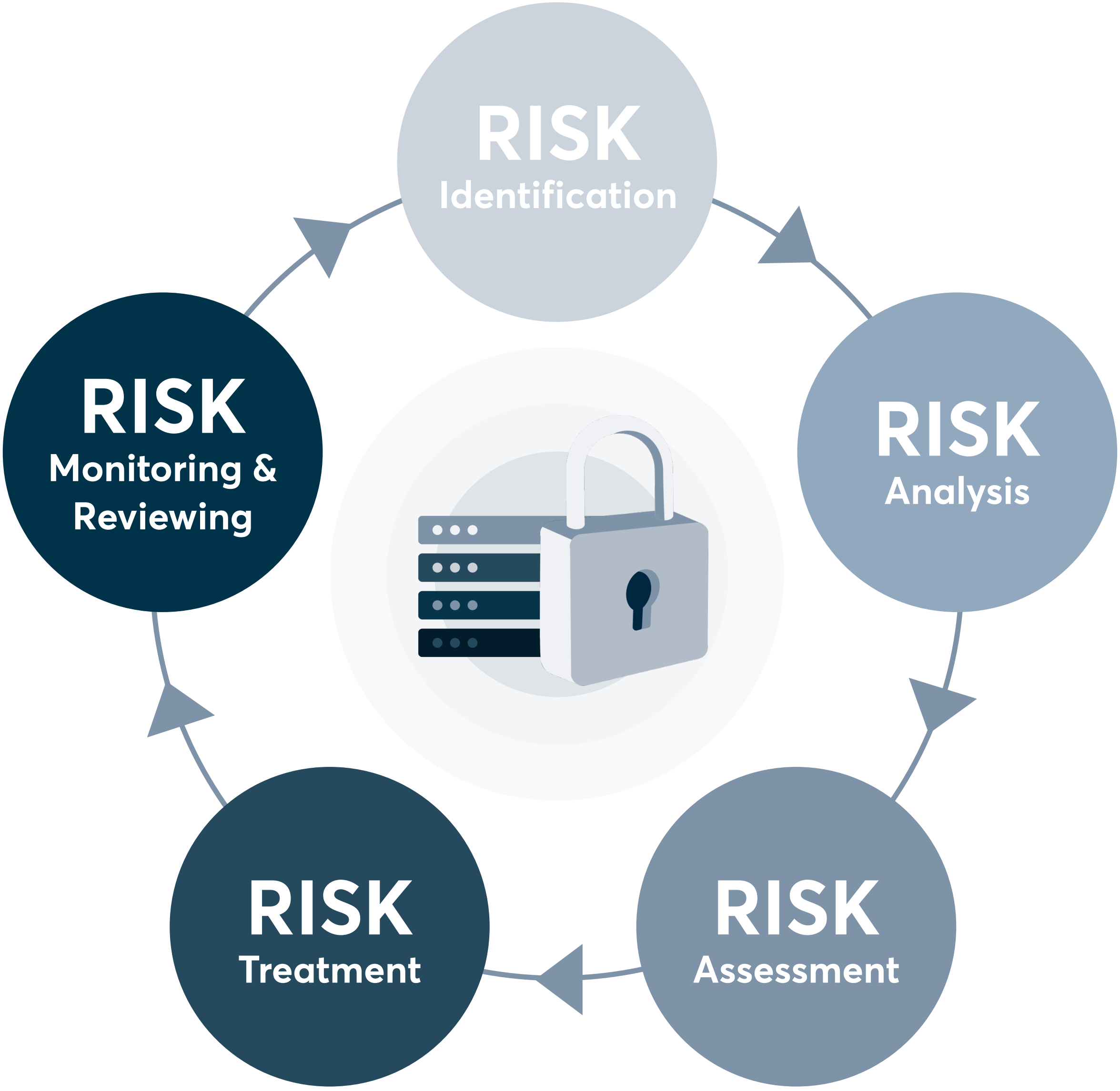
To start treating your risks, it is essential to create a Statement of Applicability (SoA). An SoA demonstrates your security posture by showing the controls you've chosen and the justification for their use, the controls you've implemented and how you've implemented them, and your justification for omitting any 27001 Annex A controls.

Next, it is time to formulate a Risk Treatment Plan (RTP). The RTP is an action plan which specifies the controls to be implemented and the responsible parties, the planned deadlines and the required resources. Risks are usually treated by transferring the risk to a third party, avoiding risks by divesting from the activity, reducing risk levels by employing mitigation strategies, or accepting the risk to internally control and tolerate it.

STEP 5 - RISK MONITORING

It is highly recommended to repeat risk assessments annually and monitor risks continuously. Involving your employees in the risk management process, management reviews and internal audits can help you stay on top of your changing ISMS and risks.

Understanding the steps involved in risk management can help you streamline your process and improve your cyber resilience. At the first glance, implementing the many steps of risk management can seem daunting. But with the right tools and some expert advice, you can ensure your organisation's risk management process is successful.



DataGuard is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalise Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.

Let's talk about your challenges and define first steps on your compliance journey:

Contact us

You might also like:

→ **8 Critical Steps to Successful Risk Assessment**

→ **Pitfalls To Avoid When Implementing ISO 27001**

→ **5 Steps to Successful ISO 27001 Internal Audit**

dataguard.co.uk contact@dataguard.com +44 20 3514 65 57

DataGuard