ISO 27001:2022
New controls and which Data Loss Prevention (DLP) measures are needed
1. What is the ISO 27001 standard and why do you need it?

2. What is new in the 2022 update?

3. Consequences for data security

4. Which DLP tools are needed

5. Conclusion
1. What is the ISO 27001 standard and why do you need it?

The ISO 27001 standard was created as an **international standard for information security** by the International Organization for Standardization ("ISO") in 2005. It was revised in 2013 and recently in 2022. ISO 27001 is supported by ISO 27002 - a document of guidelines to assist with your implementation of ISO 27001.

ISO 27001 is designed to support organisations in protecting their data via the creation of an **Information Security Management System** ("ISMS"). This should help organizations improve information asset security by establishing, implementing, maintaining, and continually improving their security standard. After the successful completion of an audit, organizations that meet the requirements can be certified by an accredited certification body.

The general goal of ISO 27001 is to protect against **three common data risk factors**:

- **Confidentiality**: ensuring that information is not available to unauthorized individuals and/or systems.
- **Integrity**: ensuring that only authorized people can modify information.
- **Availability**: the information must be accessible to authorized people whenever it is needed.
Why do you need an ISO 27001 certification?

In general, with an ISO 27001 certification, organizations assure that their data security controls reach an internationally-recognized level. However, there are more reasons to get certified:

- **Protection from security threats**
  An ISO 27001 certification will help you to avoid security threats - both on the level of external cyber criminal attacks, as well as internal data misuse caused by human error. As a result of ISO 27001, your organization is equipped with the tools to strengthen its people, processes, and technology.

- **Avoiding fines**
  Since ISO 27001 and the GDPR have a lot in common, you can avoid certain penalties connected to non-compliance by sticking to the ISO 27001 guidelines. And not only that: the framework is a good starting point for any regulation in data security. The GDPR, and data protection regulations from around the world, have a strong focus on risk-minimization through the identification and implementation of Technical and Organisational Measures (TOMs) - the ISO 27001 certification meets many of these requirements.

- **Reputation and trust**
  Being ISO 27001 certified is the ideal way to demonstrate to your stakeholders and clients that you take data security and protection seriously. Some organisations tend to only do business with certified companies.

- **Improvement of data security coordination**
  ISO 27001 enables you to create a system that ensures everyone maintains their focus on information security tasks, and within the system everyone knows their responsibilities.

- **No necessity of frequent audits**
  ISO 27001 is an international certification and globally accepted. Therefore, it reduces the need for repeated audits.

Borneo can help you with your **ISO 27001 certification** by covering the complete process: from pre-audit to implementation and certification, including all of the periodic reviews.

- We select and implement controls to address identified risks.
- Our team establish the applicability statement to specify which controls are to be implemented - or not - and why.
- We create the documentation and records required by the standard.
- Internal audit to review the required controls.
- Carry out the certification audit.
- Periodic reviews: Ongoing monitoring following certification to ensure recertification.

Get a free demo!

www.borneo.io
2. What is new in the 2022 update?

Whereas earlier ISO 27002 included 14 control domains, the new version only includes four categories: Organizational, People, Physical, and Technological.

The general number of controls has been decreased from 114 to 93. Even though there are fewer ones now, nothing has been deleted - they have just been merged and updated to better reflect the security landscape of 2022.

11 new controls have been introduced in the ISO 27001 2022 revision:

- A.5.7 Threat intelligence
- A.5.23 Information security for the use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding

Practical tip:

The fact that the controls have been put into four different sections instead of 14 is meant to simplify the implementation process. Different people inside your organisation are typically responsible for implementing different sets of controls. The practical advantage of classifying controls into four distinct groups is that it makes it easier for the implementation team to identify which internal organisation group is in charge of which particular set of controls.
3. Consequences for data security

The emphasis of the new version of ISO 27002 lies on data-centric security.

Organisations that have obtained the certification before, or that are considering to get it, need to update their approach to security accordingly. Even if you don't intend to obtain ISO 27001 certification, it's still wise to examine and implement the recommended controls because they represent industry best practice.

In light of this, three controls in the 2022 update particularly caught our attention:

**A.8.11 Data masking:** To limit the disclosure of sensitive information, this control mandates the use of access control and data masking. Since they are strictly regulated by privacy laws, this primarily refers to personal data, although it may also contain other types of sensitive data. In practice, techniques like anonymization and pseudonymization may help to enhance your data protection.

**A.8.12 Data leakage prevention:** Applying multiple data leakage protocols and solutions is required by this control in order to prevent the unauthorized disclosure of sensitive information and, in the event that it does happen, to quickly identify such instances. This applies to data on all devices, networks, and IT systems.

**A.8.16 Monitoring activities:** This control asks for constant system monitoring in order to spot unusual activity and, if necessary, initiate the proper incident response procedure. Your IT systems, networks, and apps are all monitored as part of this.

Complying with the ISO controls will protect your company against attacks that could be easily avoided. However, ISO 27001 certification alone does not mean a business can't be victim of targeted cybercrime.
With regulations like the GDPR or CCPA, your company is most likely already aware of what data masking is. In the ISO 27002 guideline, data masking is mentioned in combination with access control - to ensure that sensitive data isn’t compromised internally or externally. Techniques for data masking include pseudonymization, anonymization, encryption and obfuscation.

What tools do I need?

If you want to mask your sensitive data, you first need to know where it is located. In the cloud-first world this is often a challenge as sensitive data can be unstructured, making it even more difficult to locate.

For that reason, you should start with data mapping. Since manual data mapping is hard to do, we advise you to look for a solution that automates processes of data discovery and classification for you so you can mask the data afterwards easily.

As a first step, such solutions will need to understand which types of data you want to map with pre-tuned or custom-made infotypes. After that, the best-in-class solutions use machine learning to automate the process.

Our Borneo DLP integration, for example, offers real-time detection and redaction of sensitive data such as PII, HIPAA-protected health information, and regulated financial information in cloud collaboration tools like Slack, GDrive, Jira and more.

Aside from tool solutions, it is also recommendable to document your data masking guidelines and access rights in your Information Classification Policy, Access Control Policy and Secure Development Policy.
4. Which DLP tools are needed

A.8.12 Data leakage prevention

This control is about implementing measures and solutions to reduce the risk of inadvertent disclosure of sensitive data across systems, networks and devices. It also has the goal of helping companies to detect and remediate data leakage incidents as soon as possible - to avoid data breaches or thefts.

Which tools do I need?

Data loss prevention ("DLP") solutions are considered to be the most effective tool against data leakage. However, you should be careful when choosing the right solution for your business - not all solutions have the same benefits: some lack the functionality to extend into the cloud, others create numerous false positives which, in turn, generates more complexity and work into your data leakage efforts.

Newer solutions - like our Borneo integration - make use of automation and APIs to extend data leakage prevention to the cloud. That way, personal data is monitored as it travels through your infrastructure - including cloud-based applications. With this measure in place, the risk of data loss, theft or exposure is drastically reduced.

In the end, data leakage is not always an intended attack. Human error also plays a crucial role - an estimated number of 60 percent of data breaches were caused by employees unintentionally. Therefore, your implementation of DLP tools should also have the aim of raising awareness for cybersecurity topics and creating a culture where people actively try to handle data carefully.

Your DLP rules should be updated in the following documents: Information Classification Policy, Security Operating Procedures and Policy on Acceptable Use.
4. Which DLP tools are needed

A.8.16 Monitoring activities

This control is about detecting and reacting to irregular activity by pro-actively monitoring your applications, networks and systems. This way, you will know when an employee tries to log in at an odd time of night or when someone is attempting to download a suspicious amount of data.

Often this could indicate a hack attempt, though it could also be a simple human error made by your employees that has the end result of compromising data.

Which tools do I need?

Monitoring user behavior for specific signs of data misuse is often done by User and Entity Behavior Analytics (UEBA). However, if these tools don't have automatic remediation powers they can cost your IT teams and employees hours of work-time and stress.

Consequently, you should find a DLP solution that can be used for real-time monitoring and auto-remediation of sensitive data. Our Borneo DLP integration gives employees the chance to self-remediate any leak and is, therefore, not blocking any workflows.

Using cloud DLP like Borneo is an essential step to implement a security approach where employees are educated but still empowered when it comes to handling sensitive data.

That also means you should communicate to your employees the expectations you hold regarding their behavior towards data security.
5. Conclusion

If your company decides to protect itself from security threats, avoid fines and at the same time demonstrate to stakeholders that they take data security seriously, there is no way around ISO 27001 and its updates.

In order to comply you have to take action and our Borneo DLP integration supports you in doing exactly that - locate and identify data, ensure that it is not compromised or disclosed across systems, networks and devices and monitor in real-time who is sharing what with whom to react to anomalous activity.

WHAT’S NEW?

• Control reduction from 114 to 93
• 4 categories: Organisational, People, Physical, Technological

DATA MASKING

Make sure that sensitive data is neither internally nor externally (by cybercriminals) compromised with the help of DLP tools.

DATA LEAKAGE PREVENTION

Reduce the risk of disclosure of sensitive data across devices, networks and systems by putting adequate DLP tools in place.

MONITORING ACTIVITIES

Monitor your Cloud data in real-time so you can detect anomalous activity and remediate it with Borneo’s DLP integration.
How can we help you?

**IDENTIFY ALL YOUR SENSITIVE DATA**
Identify all the personal data that your company manages

**UNDERSTAND RISKS IN REAL TIME**
Identify and analyse threats and weaknesses in your processes and what needs to be done to reduce the risk

**REMEDIATE & ACT WHEN NEEDED**
Report necessary security measures, helping to enforce policies while creating tasks for the department’s responsible in your company to mitigate the risk

**MONITOR & STAY UP TO DATE**
Ongoing risk control, monitoring and alerts that indicate necessary changes, updates and tasks

Contact us for a free demo.