Protecting Product IP

How ISO 27001:2022 practices safeguard your intellectual property

Compliance

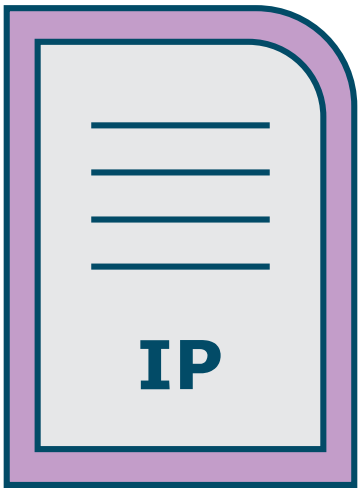
99x.io

Contents

Since 2004 , 99x has taken over 150 digital products to market with zero intellectual property disputes

In the demanding and competitive world of software product development, protecting your intellectual property (IP) is paramount. As a company that specializes in software product development and outsources developers to Scandinavian customers, safeguarding our IP and that of our clients is a top priority. **ISO 27001:2022**, the latest version of the international standard for information security management systems (ISMS), offers a comprehensive framework for achieving this. This paper explores how ISO 27001:2022 helps protect your product IP and outlines the benefits of implementing this standard in our business operations.

What exactly is product IP?

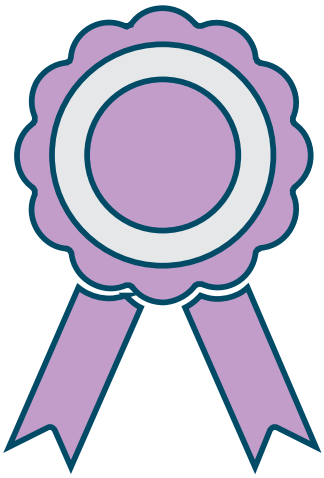


Product Intellectual Property refers to the unique creations, innovations, and proprietary information developed by a company that provide a competitive advantage in the marketplace. It encompasses various forms of intangible assets that are legally protected to ensure the company can exclusively benefit from its inventions and creative works.

Product IP encompasses a wide range of intangible assets that are crucial for a company's growth, profitability, and competitive positioning. Effective protection and management of product IP are essential for sustaining innovation and business success.

The ISO 27001:2022 framework

ISO 27001:2022 is an internationally recognized standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS. It provides a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. The standard is designed to help organizations manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.



Why does your product IP matter?

In the software development industry, IP represents a significant portion of a company's value. It includes source code, algorithms, proprietary processes, and other critical assets. For companies that outsource developers, the risk of IP theft or leakage can be particularly high, making robust security measures essential. ISO 27001:2022 offers a structured approach to identifying and mitigating these risks, ensuring that IP remains protected at all stages of the development lifecycle.

Challenges software companies face in protecting product IP

Global piracy and counterfeiting: One of the biggest challenges for software companies is preventing piracy and the unauthorized distribution of their products. Even with security measures, software can be cracked, reverse-engineered, or illegally copied in countries with weak IP enforcement laws.

Balancing open source usage: Many software products integrate open-source components, and ensuring compliance with open-source licenses is critical. If mismanaged, this could expose proprietary code to the public, jeopardizing the IP.

Employee turnover and insider threats: Employees with access to proprietary code or trade secrets pose a risk if they leave the company and share information with competitors. Insider threats, whether accidental or malicious, are one of the top concerns in IP protection.

Managing third-party relationships: Software companies often collaborate with external contractors, vendors, or partners. These third parties may have access to sensitive IP, making it essential to enforce strict access controls and confidentiality agreements.

Cloud and SaaS Security: With the rise of cloud-based services and SaaS platforms, companies face challenges in securing their IP. Ensuring that cloud providers and shared environments maintain strong security measures is critical to protect sensitive data from exposure or breaches.

Reverse Engineering: Competitors or hackers can reverse-engineer software products to discover proprietary algorithms or code. This is particularly challenging for software companies, as reverse engineering is difficult to prevent completely, and legal protection often comes after the damage is done.

Overview of 99x's ISO 27001:2022 practices

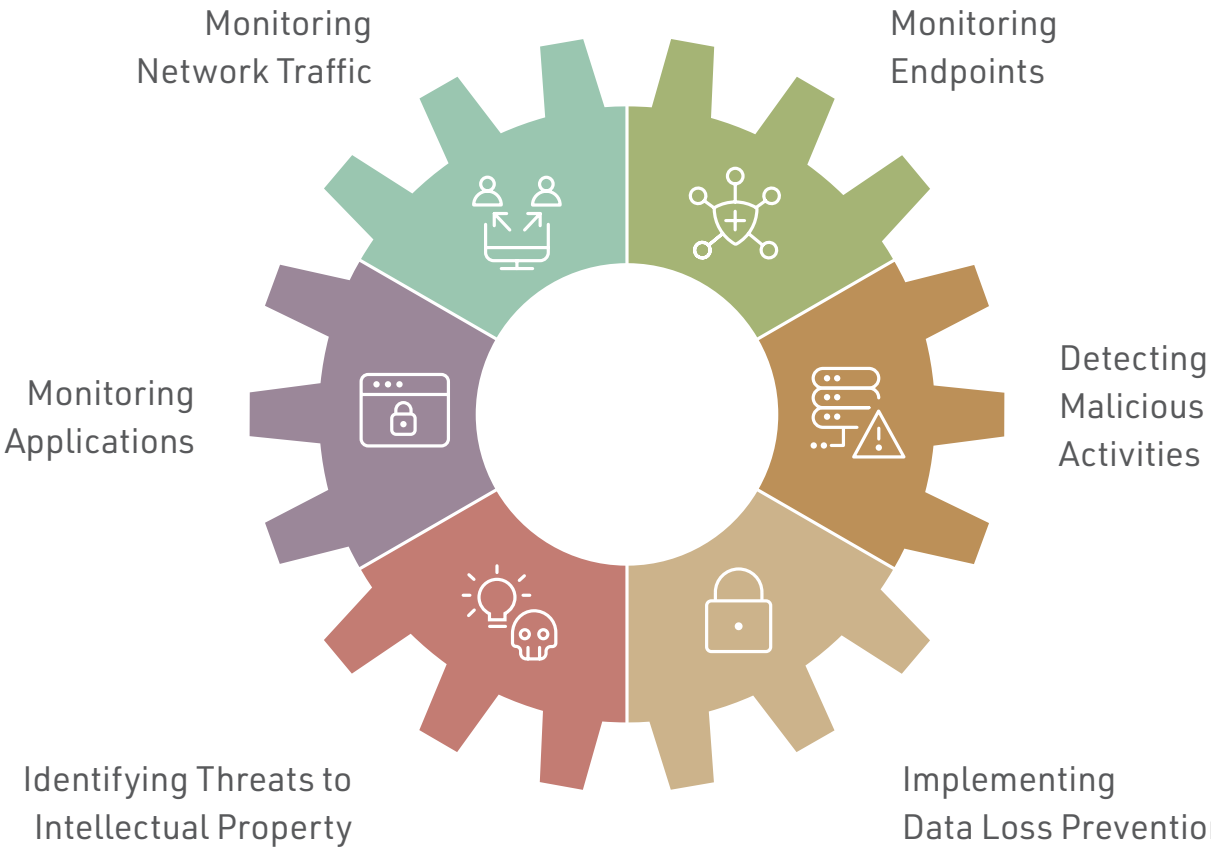
Let's look at examples of ISO 27001:2022 practices at 99x which protect your product IP. These include areas such as contracting, risk management, managing access control and physical security and conducting internal / external audits.

Strategic direction	• ISMS policy and ISMS • Security strategy
Tactical initiatives	• Security controls • Risk management
Operational practices	• Communication strategies • Internal and external audits • Training and awareness

Security Operation Centre (SOC)

Security operation centers continuously monitor network traffic, endpoints, and applications for signs of malicious activity or breaches. This helps in identifying potential threats to product IP early, allowing for swift action to mitigate risks. Apart from that, DLP (Data Loss Prevention) system strategies to monitor and control the movement of sensitive data. This prevents accidental or malicious data leaks that could compromise product IP.

Key Functions of a Security Operations Center

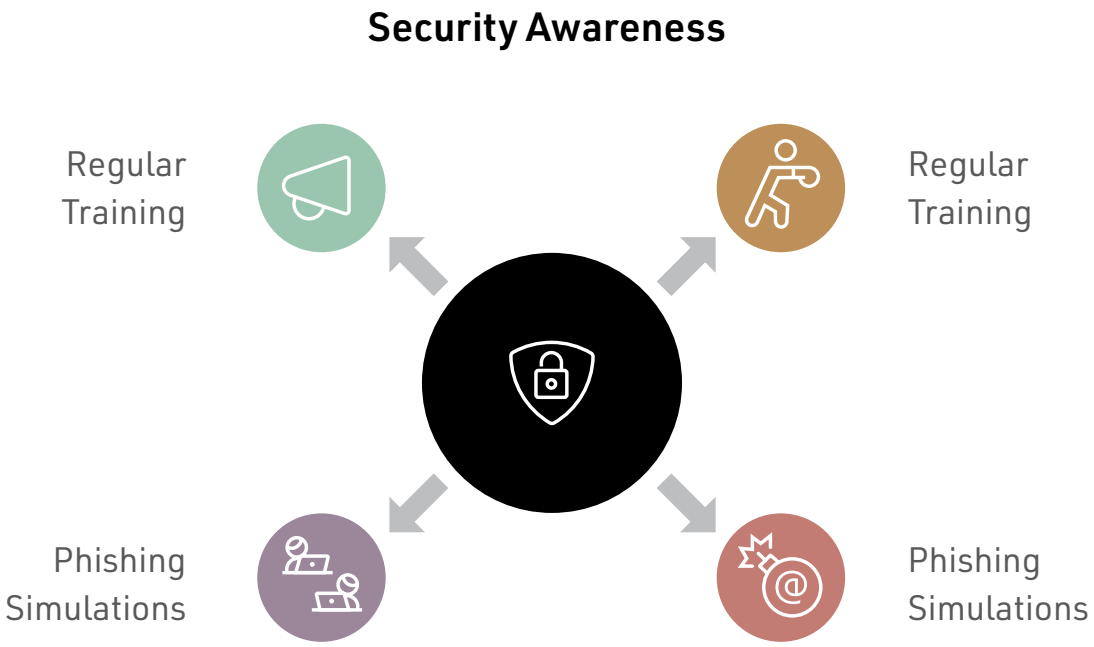


Internal and external audits

The ISO 27001 audit process is essential for ensuring that an organization's Information Security Management System (ISMS) aligns with international standards. Internal audits are conducted every six months by an internal audit committee, which includes privacy and security specialists. The primary purpose of these audits is to evaluate the effectiveness of the ISMS, identify non-conformities, and ensure that security controls are functioning properly. Through thorough reviews of policies, procedures, and controls, as well as interviews and evidence collection, the internal audit helps the organization pinpoint areas for improvement before an external audit takes place. Findings are documented, and corrective actions are implemented to foster continuous improvement.

External audits, also conducted every six months, are performed by a third-party audit firm to provide an independent assessment of the ISMS. These audits are crucial for verifying that the organization meets ISO 27001 requirements and for maintaining certification. During the external audit, auditors review documentation, interview staff, and test controls to confirm their effectiveness. The audit concludes with a report that highlights any non-conformities, which the organization must address to maintain compliance and certification.

Key components of our security awareness program



1. Regular training sessions

We conduct mandatory security awareness training for all employees. These sessions cover essential topics such as:

- Phishing
- Password management
- Data protection
- Incident reporting

To ensure relevance, these training sessions are updated regularly to address emerging threats and evolving best practices.

2. Phishing simulations

To reinforce the training received, we regularly conduct phishing simulations. These simulated attacks serve as practical exercises for employees, helping them to:
Identify malicious emails
Understand the importance of vigilance in their daily work

3. Interactive workshops

Our hands-on workshops simulate real-world scenarios, allowing employees to practice identifying and responding to security incidents in a controlled environment. These workshops are tailored to different roles within the organization, ensuring that the content is relevant and engaging for all participants.

4. Awareness campaigns

In addition to formal training, we provide ongoing education through various channels, including:

- Newsletters
- Webinars
- Security bulletins

By implementing these strategies, we are committed to fostering a culture of security awareness that empowers our employees to take an active role in protecting our organization's information assets.

Conclusion

ISO 27001:2022 is an essential standard for organizations seeking to protect their product IP from a wide range of threats. By implementing a robust ISMS, organizations can ensure that their IP is safeguarded against unauthorized access, theft, and misuse. Whether through secure development practices, third-party management, or continuous improvement, ISO 27001:2022 provides a comprehensive framework for maintaining the confidentiality, integrity, and availability of product IP. In an era where IP is often the key differentiator in the market, ISO 27001:2022 is not just a compliance requirement—it is a strategic imperative for long-term success.