Understanding Penetration Testing in the Context of ISO 27001 Security Certification

Zanda, a leading practice management software for allied health practitioners, is proud to have achieved the ISO 27001 Security Certification. This underscores our commitment to providing clients with the highest level of security and data protection. A critical part of obtaining this certification was the regular completion of a Penetration Test. This document aims to provide an in-depth understanding of Penetration Testing as a fundamental component of ISO 27001 certification.

What is penetration testing?

Penetration Testing, often referred to as "Pen Testing" or "ethical hacking", is a proactive and authorised method of evaluating the security of IT infrastructure by attempting to safely exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations, or end-user behaviour. Penetration testing is designed as a deliberate attempt to mimic the actions of a hacker to uncover potential points of entry and identify weaknesses that could be exploited.

Who conducts a penetration test?

An external specialist information security firm conducts an official pen test according to the scope.

Penetration testing and ISO 27001

ISO 27001 is an internationally recognised standard that sets out the specification for an Information Security Management System (ISMS). This system preserves *information confidentiality, integrity, and availability* by applying risk management processes and providing assurance to interested parties.

Penetration testing is a critical component of the risk management process under ISO 27001. It helps to identify vulnerabilities and quantify the risk they pose to an organisation's information security. The results of a penetration test provide valuable data points that feed into the overall ISMS, guiding the implementation of appropriate security controls and measures.

The penetration testing process

The penetration testing process typically consists of five stages:

1. **Planning and Reconnaissance:** This initial stage involves defining the scope and goals of the test and gathering intelligence to understand the system and its potential vulnerabilities.
2. **Scanning:** In this stage, the pen tester interacts with the target system to understand how it will respond to various intrusion attempts.
3. **Gaining Access:** The pen tester exploits the identified vulnerabilities to understand how much damage they can cause.
4. **Maintaining Access:** This stage aims to see if the vulnerability can achieve a persistent presence in the exploited system—mimicking what an attacker might do.
5. **Analysis and Reporting:** The final stage involves compiling a detailed report, including the specific vulnerabilities discovered, the data that was exposed, and recommendations for mitigation strategies.

Benefits of penetration testing

Without performing regular, certified Penetration Testing, businesses might believe their data to be secure, but it is never certain until expert vulnerability hackers attempt to gain access.

Penetration testing provides several benefits, such as:

- **Identifying Vulnerabilities:** Penetration testing uncovers system weaknesses that attackers can exploit.
- **Quantifying Risk:** It helps to quantify the risk posed by specific vulnerabilities, guiding the prioritisation of remediation efforts.
- **Supporting Compliance:** Regular penetration testing is required to maintain ISO 27001 certification, among other regulatory standards.
- **Maintaining Trust:** Demonstrating a commitment to security via penetration testing helps to build trust with clients, stakeholders, and regulatory bodies.

Obtaining results

Obtaining and maintaining the ISO 27001 certification involves demonstrating a robust and effective Information Security Management System (ISMS). A key component of this process is managing and mitigating various risks often identified through penetration testing. The level of these risks - high, medium, or low - plays a significant role in the certification process.

- **High-Risk Vulnerabilities:** High-risk vulnerabilities are security weaknesses that, if exploited, could lead to significant damage. This could include severe data breaches, extensive system damage, or significant interruptions to business operations. If left unaddressed, these vulnerabilities could indicate a failure in the organisation's ISMS, a serious barrier to achieving or maintaining ISO 27001 certification.

- **Medium to Low-Risk Vulnerabilities:** Medium to low-risk vulnerabilities represent potential security weaknesses less likely to lead to severe damage or disruption. However, they could still be exploited in a way that harms the organisation, particularly if multiple vulnerabilities are exploited together.

  These vulnerabilities, while less severe, still require attention. Identifying these issues demonstrates the thoroughness of our testing procedures, and addressing them shows our commitment to continuous improvement - both key aspects of ISO 27001.

In summary

As a recent recipient of the ISO 27001 Security Certification, Zanda conducts rigorous security measures, including penetration testing, to maintain our clients' highest level of data protection. It provides a practical way to test against threats, comply with essential standards, and build client trust.

By understanding the nature of penetration testing, stakeholders can better appreciate the efforts taken by Zanda to ensure data integrity and security and comprehend the importance of these actions in the broader context of information security management. Zanda remains committed to maintaining these high standards, providing its clients with the utmost confidence in their data's safety.

Zanda's Penetration Test Confirmation

Zanda is pleased to confirm the successful completion of a comprehensive penetration test. The latest test was performed by **Cacilian, a CREST Pentest certified Security Services organisation**, and was last completed on **December 27, 2022**.

Penetration test scope

The objective of our penetration test was to identify design and implementation weaknesses in our applications that an attacker could potentially exploit. A comprehensive suite of vulnerability checks was performed to evaluate the application's overall security, verify the effectiveness of existing controls, and identify any areas requiring improvement.

Penetration test results

The findings from our recent test were:

- **No High-Risk Vulnerabilities:** Testing found zero high-risk vulnerabilities. This is a significant achievement, suggesting that our stringent security measures protect against serious threats that could significantly impact data integrity.

These results suggest that our web-based application is secure. The absence of any high vulnerabilities demonstrates the effectiveness of our security controls in protecting against significant threats.

Confirmation

This test is confirmed by:

Paul Adler
Chief Technology Officer (CTO), Zanda

Zanda's ethos has always been to ensure the highest level of data security for our clients, and this recent Penetration Test underscores our commitment to maintaining robust information security controls.