# ZERO-TRUST ARCHITECTURE AND ISO 27001:2022

OCTOBER EDITION
EXPERT PUBLICATION

## INTEGRATING ZERO TRUST ARCHITECTURE & ISO 27001:2022 FOR A ROBUST ROBUST DATA SECURITY

In today's digital landscape, data security is paramount, and organizations are continually seeking innovative approaches to fortify their cybersecurity measures. Two prominent strategies, Zero-Trust Architecture (ZTA) and ISO 27001:2022, offer a robust foundation for safeguarding sensitive information. This article delves into the synergies between Zero-Trust Architecture and ISO 27001:2022, highlighting how these methodologies converge to create a formidable defence against evolving cybersecurity threats.

*"The Zero Trust framework requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data."*

**JOY CHIVILE ADHIAMBO**
SENIOR CONSULTANT
INFORMATION SECURITY & DATA PROTECTION

Zero Trust places its emphasis on safeguarding resources at a detailed level, utilizing technologies such as multi-factor authentication, identity and access management, and encryption. It enacts access controls based on the principle of least privilege, thereby reducing unauthorized access, and mitigating potential harm resulting from security breaches. Through ongoing monitoring and immediate responses to threats, Zero Trust aids organizations in proactively addressing the ever-evolving landscape of cybersecurity risks.

ISO 27001, a globally acknowledged standard for the management of information security, offers a methodical framework for overseeing the protection of sensitive data from loss of confidentiality, integrity, or availability. It guarantees security through a set of controls that encompass individuals, procedures, and IT systems. Notable components of ISO 27001 that correspond with the principles of the Zero Trust Security Model involve risk assessment, access control, and the pursuit of ongoing enhancements. The risk assessment procedure is consistent with the Zero Trust tenet of "never trust, always verify," aiding in the recognition and mitigation of potential threats. Some of the ISO27001:2022 Annex A Controls that can be implemented to attain Zero Trust are:

## *Clause A.5.15 Access Control*

The Zero-Trust Architecture approach mandates verification for all entities, regardless of their device or location. This ensures that authorized access is granted while effectively preventing unauthorized access to information and interconnected networks.

## *Clause A.5.18 Access Rights*

The Zero Trust architecture necessitates ongoing monitoring and verification to ensure that both users and their devices possess the appropriate privileges and attributes. It also mandates the enforcement of policies that take into account the risk associated with both the user and the device, in addition to compliance and other prerequisites that must be considered before authorizing a transaction. Furthermore, it requires organizations to have comprehensive knowledge of all their service and privileged accounts and the ability to establish controls regarding the connections they make and where they connect. A single validation at a single point in time is insufficient, as both threats and user attributes are susceptible to change.

## Clause A.6.7. Remote working

Implementing a zero-trust approach to endpoint security has emerged as one of the most effective strategies for ensuring the long-term security of adaptable or hybrid workforces, which encompass remote work scenarios. Organizations that adopted Zero Trust Architecture (ZTA) during the 2020 Pandemic successfully enabled their employees to access resources from their homes without disruptions or typical security challenges that typically arise during significant workforce transitions.

## Clause A.8.1 End Point Devices

This strategy commences with the fundamental premise that each endpoint requires ongoing security, not just at the initial sign-on, but also as the employee interacts with applications and services. Zero Trust also requires consideration of encryption of data, securing email, and verifying the hygiene of assets and endpoints before they connect to applications.

## Clause A.8.3 Information Access Restriction and 8.5. Secure Authentication

The Zero Trust approach involves verifying a user's identity and granting access based on the principle of least privilege. Zero Trust Architecture (ZTA) employs various measures to enhance security and minimize risks associated with connecting users to applications and data. Initially, it scrutinizes every connection request by ascertaining the user's identity, their intentions, and their destination. This falls under the realm of identity and access management, where technologies such as multi-factor authentication (MFA) play a crucial role in safeguarding against credential theft. Subsequently, the system assesses the risk associated with the request, for instance, whether the requester is seeking access to resources beyond their job role. In place are mechanisms to automatically reduce the risk of these requests, with the possibility of blocking overly risky users.

# Conclusion

Integrating the Zero Trust Security Model with ISO 27001 has yielded valuable knowledge and experience. A significant takeaway is the vital need for a comprehensive perspective that combines Zero Trust principles with ISO 27001 controls, creating a well-rounded cybersecurity strategy. This synchronization not only bolsters the security posture but also efficiently minimizes information security risks. Additionally, continuous monitoring and evaluation emerge as a crucial element, aligning seamlessly with ISO 27001's focus on continual improvement.

BY
JOY CHIVILE ADHIAMBO
SENIOR CONSULTANT

SENTINEL AFRICA CONSULTING LTD
RISK MANAGEMENT CONSULTANCY FIRM

Sentinel Africa

Your Advisor of Choice

www.sentinelafricaconsulting.com

FOLLOW US : **SENTINEL AFRICA CONSULTING**