Avecto

ISO 27001

In this short article we examine the roles least privilege and application control have to play in ISO/IEC 27001 compliance.

Introduction

ISO 27001 is an information security standard that defines how an IT system should be planned, implemented, monitored, reviewed, and improved.

It was first published in October 2005 by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), and updated in 2013.

As ISO standards are widely recognized across a variety of business management disciplines - such as health and safety, and IT service management - complying with ISO/IEC 27001 protects against security breaches and can be used as a marketing tool to provide a clear message that IT security is taken seriously.

As a management standard, ISO/IEC 27001 doesn't define any technical controls, but ISO/IEC 27002 contains a list of controls, some or all of which may need to be adhered to depending on the outcome of a risk assessment as required by ISO 27001. Organizations cannot be ISO/IEC 27002 certified because it is not a management standard.

Risk assessment and treatment

Before looking at the controls in ISO/IEC 27002 in more detail, it's worth considering the most complex part of ISO/IEC 27001: security risk assessment and treatment. A security risk assessment involves identifying an organization's assets, and then determining the threats and vulnerabilities that the assets are potentially exposed to. The risk level can be calculated by ascertaining the likelihood that an asset could be compromised by any of the identified threats or vulnerabilities.

Once the risk level of each asset has been established, there are several options for how the risks can be treated. One or more security controls listed in ISO/IEC 27002 could be applied, the risk could be transferred to an insurance company, avoided by modifying business practices, or accepted if the cost of mitigating the risk is higher than the resulting damage after a security breach.

A Statement of Applicability (SoA) then provides an overview of the organization's security profile and acts as the main guide during an audit. It outlines all the implemented security controls, including a justification of why they have been selected and how they've been realized.

Annex A security access controls

The security controls in ISO/IEC 27002 are referenced in Annex A of ISO/IEC 27001. The requirement for an access control policy is outlined in ISO/IEC 27002, and requires that asset owners establish access control rules, access rights, and restrictions for different user roles according to the risks determined in the information security risk assessment.

What follows is a brief summary of the user and privileged access management controls, which are some of the most detailed in any existing security standard. And while an organization might determine that as part of the security risk assessment not all of the recommended access control policies are necessary, most of them are essential for organizations with an interest in establishing basic security best practices. Additionally, it's worth noting the controls apply equally to servers and end-user devices.

User access management

To prevent unauthorized access, each user should be assigned a unique ID so they can be held accountable for their actions, i.e. no shared user accounts, including domain admins, unless there is a documented business case.

Avecto

Management of privileged access rights

The need to restrict the use of privileged access rights using a formal authorization process is detailed in Control 9.2.3. Furthermore, admin rights should be allocated on a need-to-use basis – sometimes referred to as Just-Enough Administration (JEA) – and on an event-by-event basis, or in other words Just-In-Time Administration (JIT). And most importantly, access rights should be granted to users 'based on the minimum requirement for their functional roles'.

A comprehensive log of access rights should be kept, and if privileged access rights are granted, a policy should exist to determine when and if those rights must be revoked. If privileged rights are granted on a long-term basis, they should be reviewed periodically to ensure they are still required and match the employee's current duties and responsibilities.

Privileged utility programs

ISO/IEC 27002 Control 9.4.4 directly references utilities used by IT staff for systems administration, and that these utilities should be segregated from line-of-business applications, and authentication and authorization provided separately. It is also suggested that use of administrative utilities should be logged.

Malware prevention

Antimalware solutions and implementation of information security awareness training are widely accepted best practices, but ISO/IEC 27002 goes further by recommending system access and Change Management controls as a malware prevention strategy.

Also, guidance is provided on prohibiting the use of unauthorized software and the implementation of controls to prevent users from installing and running software not approved by the organization, primarily to reduce the attack surface by ensuring software doesn't introduce vulnerabilities that could lead to data loss or degradation of system integrity.

Privilege management solutions

Meeting the technical objectives set out in ISO/IEC 27002 requires the removal of administrative privileges from end users. But relying on the application control and privilege management features in Windows means users will be more secure but restricted in how they can use legacy applications and operating system features.

Least privilege security

Third-party Privileged Elevation and Delegation Management solutions can be used to define exactly which processes users can elevate, helping to keep IT systems secure but at the same time providing the flexibility required to carry out their duties. Defendpoint can be used to assign as many or as few privileges to processes and applications as required, while leaving users with restricted access tokens. This is unlike the limited privilege management features provided by Windows User Account Control (UAC).

Additionally, a challenge/response mechanism allows users to request process elevation even when a policy hasn't been defined by IT, which is especially important for remote workers.

Application control

Flexible application control policies can be applied to all supported Windows SKUs so that whitelists of approved applications can quickly be created and enforced. Defendpoint allows customization of end-user messages and provides multilingual support, providing a better user experience.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.