How UEM Central helps to Comply with ISO 27001?

ManageEngine
IT Management, Simplified

UEM Central can make your organization to comply with the ISO 27001:2013 controls. A.6.2.1 to support security measures adopted to manage risks introduced by Mobile Devices. A.8.1.1, A.8.1.2, A.8.1.3 and A.8.3.1controls help organizations to manage assets and keep the IT updated with the latest information and generate evidence. UEM Central also fulfills the controls A12.5.1 and 12.6.2 that ensures the installation of software on operational systems.

Additionally, UEM Central complements Annexure A12.6.1 control helps organization to prevent systems from any technical vulnerability by providing up-to- date patches for applications installed in the systems

Requirement Number	Requirement Description	How UEM Central fulfills the requirement
A.6.2.1 - Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	UEM Central help enterprises perform mobile device management to configure and secure their mobile devices using profile management. It let's to configure profile settings to create and impose Policies and Restrictions to let user access work related data. UEM Central helps in providing selective access to corporate accounts like Email, Wi-Fi, VPN and device grouping based on department, location. Also, helps in building parameters to create a passcode and configure the passcode settings.
A.8.1.1 - Inventory of assets	Control Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	UEM Central's Web- based Inventory Management helps to identify computer, devices and software assets inside the organizations and also provides out-of-the-box network inventory reports to get the required details in a very few clicks.

		These reports help to get a quicker view of the network inventory details. The ability to export the reports into PDF or CSV formats helps to integrate with third-party reporting engines or print it out for future reference.
A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	UEM Central inventory management lets IT admin to maintain details of the computers with information such as device owner, search tag, email-id, etc.
A. 8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	UEM Central provides out-of-the-box reports to view the software and hardware details of the network. These reports help to get a quicker view of the network inventory details. The ability to export the reports into PDF or CSV formats helps to integrate with third-party reporting engines or print it out for future reference.
A.8.3.1 Management of Removal Media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	UEM Central's Secure USB feature would help IT admin limit the scope of USB device usage. It enables to centrally control the usage of various USB devices in the network by blocking or disabling the USB devices to prevent unauthorized download and upload activities through these local computer devices. The restriction can be set both at the computer level and at the user level, providing more levels of security.

A.12.4.1 Event Logging	Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly.	UEM Central enables role-based administration, and logs every action performed by all the users along with date and time. The logs will be maintained for a specified number of days which can be configured. UEM Central enables administrator to review the changes done by all the users. The view can also be filtered user-wise and module-wise for easier analysis.
A.12.5.1 Installation of software on operational Systems	Procedures shall be implemented to control the installation of software on operational systems.	UEM Central enables to distribute, install, update and uninstall software applications automatically to users or computers as per the requirement. UEM Central provides Software repositories, which enables to store software packages. These packages can either be for MSI-based software applications or EXE-based software applications. Also, UEM Central lets to uninstall the applications, if those applications are no longer needed for the user.

A12.6.1 Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	UEM Central keeps updated about the vulnerabilities in applications and detects the missing patches/hotfix. IT admins can deploy the patches or perform automatic patch installation, which ensures that systems are secured. Also, UEM Central reports on system vulnerabilities, Patches, OS, etc. and provides an update of the patch deployment status.
A12.6.2 - Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	UEM Central helps to fully-automate the detection and removal of prohibited software by blacklisting the applications. It let's IT team to configure and receive notification through email whenever blacklisted software is identified. Both Admin users and end users can receive these alerts. Also, IT personnel can generate the prohibited software report to find the computers in company network using such applications at any given point of time.