Unitrends Compliance Manager

FREQUENTLY ASKED QUESTIONS

Unitrends Compliance Manager is like having a compliance assistant in a box. This automated tool coordinates the collection of manually inputted information from various stakeholders, runs automated data scans across the computer network, collects and collates information and then produces mandatory reporting required for both GDPR and HIPAA. Using Unitrends Compliance Manager makes meeting industry regulations and preparing for audits as effortless and hassle-free as possible.

What documents does Unitrends Compliance Manager provide for GDPR?

Unitrends Compliance Manager provides the scans and documentation required to pass a GDPR audit.

GENERAL DATA PROTECTION REGULATION

PRIMARY GDPR DOCUMENTS INCLUDE:

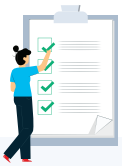
Unitrends Compliance Manager for GDPR Checklist
The GDPR Auditor Checklist gives you a high-level overview of how well the organization complies with the GDPR. The checklist details specific compliance items, their status and helpful references. Use the checklist to quickly identify potential issues that need to be remediated in order to achieve compliance.

ISO 27001-2013 Auditor Checklist
The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organization complies with ISO 27001-2013. The checklist details specific compliance items, their status and helpful references. Use the checklist to quickly identify potential issues to be remediated in order to achieve compliance.

EU GDPR Policies and Procedures
One of the first requirements is to have a set of policies and procedures that can be used to implement Personal Data security and compliance with GDPR. Some organizations don't have a set of data protection policies – or at least one that conforms to GDPR. The tool provides an "out of the box" version of policies and procedures for GDPR for use by those organizations.

ISO 27001 Policies and Procedures
Guidance suggests that compliance with ISO 27001 can be used to demonstrate technical compliance with the information security aspects of GDPR. The tool provides an "out of the box" version of policies and procedures for ISO 27001 for use by your organization. These work in tandem with our GDPR P&P.

Risk Treatment Plan
Based on the findings in the GDPR Compliance Assessment, the organization must create a Risk Treatment Plan with tasks required to minimize, avoid or respond to risks. Beyond gathering information, Unitrends Compliance Manager for GDPR provides a risk-scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are solved. The Risk Treatment plan defines the strategies and tactics the organization will use to address its risks.



SUPPORTING GDPR DOCUMENTS INCLUDE:

External Port Use Worksheet
This worksheet allows you to document business justifications for all the allowed external ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.

User Access Review Worksheet
The User Access Worksheet is used to augment the user data that was collected during the internal network scans.

Asset Inventory Worksheet
The Asset Inventory Worksheet is used to augment the asset data that was collected during the internal network scans. Details include the asset owner, acceptable use, environment, backup agent status, as well as device and sensitive information classification. Sensitive Information Classification is used to determine the risk to the organization in the event of a security incident where the asset's information is compromised.

GDPR Compliance Questionnaire
The GDPR Compliance Questionnaire will collect information about the network and environment that cannot be discovered through automated scans. This includes information about the Data Protection Officer, principles relating to the processing of personal data, privacy policies and third-party information processors.

ISO 27001 Compliance Questionnaire
This questionnaire will collect information required to demonstrate ISO 27001 compliance that cannot be discovered through automated scans.

Data Protection Impact Assessment
The Data Protection Impact Assessment (DPIA) is the foundation for the entire GDPR compliance and IT security program. The DPIA identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of Personal Data at rest and/or during its transmission.

GDPR Evidence of Compliance
Compiles compliance information from both automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the Auditor Checklists with real data.

Site Walkthrough Checklist
Assess the physical security and the workplace environment as it relates to information security. It is best done on-site since it requires identifying risk that may currently exist in your environment outside the computer network itself.

Personal Data Scan System Selection Worksheet
The Personal Data Scan System Selection Worksheet allows you to specify which systems are scanned for personal data (PD) during the assessment. A comprehensive scan should be performed annually to help identify and document all potential locations for personal data, as defined by GDPR.

Personal Data Validation Worksheet
During the Personal Data (PD) scan, suspected PD may be detected in files stored on the network and in stand-alone computers. The Personal Data Validation Worksheet report presents a record of which computer files containing actual instances of PD were verified by a participant in the GDPR assessment process.

External Vulnerability Scan Detail by Issue
Detailed report showing security holes and warnings and informational items, including CVSS scores, as scanned from outside the target.

Internal Vulnerability Scan Detail by Issue
Detailed report showing security holes and warnings and informational items, including CVSS scores, as scanned from inside the target network. Closing internal vulnerabilities helps prevent external attackers and internal users from exploiting weaknesses typically protected by external firewalls.

What documents does Unitrends Compliance Manager provide for HIPAA?

Unitrends Compliance Manager provides the scans and documentation required to pass a HIPAA audit.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

PRIMARY HIPAA DOCUMENTS INCLUDE:

HIPAA Security Rule Auditor Checklist
The HIPAA Security Rule Auditor Checklist gives you a high-level overview of how well the organization complies with the HIPAA provisions. The checklist details specific compliance items, their status and helpful references.

HIPAA Policies and Procedures
One of the first requirements is to have a set of policies and procedures used to implement ePHI data security and compliance with HIPAA. Some organizations don't have a set of data protection policies – or at least one that conforms to HIPAA provisions. The tool provides an "out of the box" version of policies and procedures for HIPAA for use by those organizations.

HIPAA Evidence of Compliance
Compiles compliance information from both automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the HIPAA Security Rule Auditor Checklist with real data.

HIPAA Management Plan
Based on the findings in the HIPAA Compliance Assessment, the organization must create a HIPAA Management Plan with tasks required to minimize, avoid or respond to risks. Beyond gathering information, Unitrends Compliance Manager for HIPAA provides a risk-scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources, and ensure that issues identified are issues solved.

HIPAA Risk Analysis
The HIPAA Risk Analysis is the foundation for the entire HIPAA compliance and IT security. The HIPAA Risk Analysis identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of ePHI at rest and/or during its transmission.

SUPPORTING HIPAA DOCUMENTS INCLUDE:

External Port Use Worksheet
This worksheet allows you to document business justifications for all the allowed external ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.

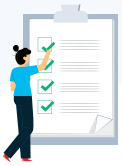
User Identification Worksheet
The User Identification Worksheet is used to augment the user data that was collected during the internal network scan.

Computer Identification Worksheet
The Computer Identification Worksheet is used to augment the asset data that was collected during the internal network scan. Details include the Device Name, Device Type, IP Address, Operating System, System Description, as well as device and sensitive information classification. The ePHI Access Classification is used to determine the risk to the organization in the event of a security incident where the asset's information is compromised.

HIPAA Policies and Procedures Verification Worksheet
The HIPAA Policy and Procedures Verification Worksheet will collect information about the network and environment that cannot be discovered through automated scans. This includes information principles relating to the processing of ePHI, including sanctions, incident response and Business Associates of the Covered Entity.

HIPAA On-Site Survey
Assess the physical security and the workplace environment as it relates to information security. This worksheet includes information about the information security. It is best done on-site since it requires identifying risk that may currently exist in the client's environment outside the computer network itself.

ePHI Scan System Selection Worksheet
Understanding where you have ePHI Data is an important component of HIPAA compliance.



ADDITIONAL SUPPORTING HIPAA DOCUMENTS REGARDING PERSONAL DATA INCLUDE:

The Personal Data Scan System Selection Worksheet allows you to specify which systems are scanned for ePHI during the assessment process. A comprehensive scan should be performed annually to help identify and document all potential locations for personal data, as defined by HIPAA.

ePHI Validation Worksheet
During the ePHI scan, suspected ePHI may be detected in files stored on the network and in stand-alone computers. The ePHI Validation Worksheet report presents a record of which computer files containing actual instances of ePHI were verified by a participant in the HIPAA assessment process.

External Vulnerability Scan Detail by Issue
Detailed report showing security holes and warnings and informational items, including CVSS scores, as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

Drive Encryption Worksheet
Encryption is such an effective tool used to protect data that if an encrypted device is lost then it does not have to be reported as a data breach. The Disk Encryption Report identifies each drive and volume across the network, whether it is fixed or removable, and if encryption is active.

Network Share Identification Worksheet
The Network Share Identification Worksheet takes the list of network shares gathered by the Data Collection process and lets you identify those that store or access ePHI.

HIPAA Compliance PowerPoint
Use the generated PowerPoint presentation as the basis for conducting a meeting to present your findings from the Unitrends Compliance Manager assessment. General summary information along with the risk and issue score are presented along with specific recommendations and next steps.

Security Exceptions Worksheet
It allows you to document explanations on suspect items. Your explanation can include why various discovered items are not true issues and indicate possible false issues. Additionally, you can explain why a certain compliance requirement should not apply to you – or an alternative way through which you have met the requirement.

READY TO MAKE COMPLIANCE AS EFFORTLESS AND HASSLE-FREE AS POSSIBLE?
LEARN HOW

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY

PART # DS-1127-ENG-B