WHITE PAPER

Top 7 Audit-Prep Reports

Pre-Audit Report Checklist

solarwinds

Executive Summary

Whether your audit process is driven by GDPR, PCI DSS, HIPAA, or SOX (or all four), detailed reporting is a critical success factor for compliance. Knowing and reporting on data access is essential for regulatory compliance. Unfortunately, analyzing Active Directory® permissions isn't straightforward, and often IT team members are not in a position to determine if access is appropriate.

Typically, data owners, rather than the IT team, are in the best position to determine who should have access to data—yet the responsibility still lands on the IT team. SolarWinds® **Access Rights Manager (ARM)** helps bridge this gap by securely delegating rights management directly to data owners, and delivering reports that expose data risks and help support audits.

Pre-Audit Report Checklist

Even though it's a good idea to prepare for your next audit, it's not always easy to know exactly where to focus before auditors arrive or what questions they will ask when they do. We've developed a list of the top seven reports to run before your next audit or assessment. By tackling the most common findings threatening regulatory compliance before the audit, your audits can be easier, faster, and much less painful.

1 USER AND GROUP ACCESS

Knowing where a particular user or group member has access is a good first step to determining whether that access is appropriate.

Why it's important

Listings of all access rights (e.g., read-only, write, etc.) to file server directories for user accounts and group members provide essential documentation to auditors that you're effectively implementing a secure account management process. For example, the EU General Data Protection Regulation (GDPR) Article 5, Principles for the Processing of Personal Data, mandates, "protection from unauthorized access and undesired loss, destruction, or damage, through the appropriate technical and organizational means." Whether your auditor is assessing GDPR, HIPAA, or PCI DSS compliance, reviewing user and group access is likely a key introductory practice.

Common Challenges

While these listings can provide answers to the question of who has access to what, it's unclear whether this access is appropriate—unless you're already familiar with the data. For example, without the context of operational chain of command, we may not know if a specific user should have access to these files and folders.

How to overcome this with ARM

Since data owners are the experts on data and its relevance, ARM allows you to connect Active Directory users with the attribute "Manager" to specific file server resources. By running the "where do a manager's employees have access?" report, you'll be able to show your auditor how you continuously validate whether user access is appropriate.

2 OVERPRIVILEGED ACCOUNTS (OR EXCESSIVE ACCESS)

The principle of least privilege is a sacrosanct rule in cybersecurity. Auditors may indeed ask for proof you're enforcing this principle—and information on how you're flagging any violations.

Why it's important

Monitoring and restricting privileged account access is a common requirement for many regulatory standards, as well as a best practice for protecting data. Additionally, using an account with escalated privileges unnecessarily can easily lead to costly mistakes that could expose your organization to risk.

Common Challenges

"Everyone" accounts (e.g., authenticated users, domain users) can increase the risks associated with unauthorized access, yet these types of accounts cannot be automatically removed from Active Directory.

How to overcome this with ARM

After generating a report on all access rights for the "Everyone" account, scan the report for sensitive directories and remove the access rights for "Authenticated Users." You can also identify globally accessible directories in order to resolve additional data risks.

3 RISKY GROUP CONFIGURATIONS (EMPTY OR RECURSIVE GROUPS)

Groups that exist in Active Directory without any members complicate administration and can prolong audits. Nested or recursive group membership configurations may also add to confusion and complexity.

Why it's important

Over time, Active Directory group membership configurations can drift into a complicated and nonsensical mess, prolonging audits and increasing risk. Cleaning these risky group configurations before the audit can help streamline the compliance process.

Common Challenges

Some groups may become empty of members. Others may have members in multiple groups, in nested or recursive ways that can result in excessive rights and increased risks (of failing your audit or leaking data). Without visibility into these risky group configurations, these complications tend to increase over time, increasing the risk of data leakage.

How to overcome this with ARM

The Risk Assessment dashboard identifies groups in recursion, so you can proactively mitigate these risks and streamline group membership configurations. Tip: The deeper your group structure, the more likely you are to encounter circular nested group structures. ARM makes it easy to monitor the number of nested group levels—and keep them manageable.

4 INACTIVE AND TEMPORARY ACCOUNTS

Accounts that haven’t been used or have exceeded their expiration dates are ripe for removal before your next audit.

Why it's important

Inactive accounts are a key weapon used by attackers to steal and manipulate data under cover of an authorized user. Temporary accounts, if left in place after they’re necessary, can easily remain inactive, exposing your organization to risk and complicating your audits and assessments. In fact, PCI DSS 8.1.4 requires temporary or inactive accounts be removed or disabled within 90 days.

Common Challenges

The presence of inactive accounts is often caused by a failure in operational process or interdepartmental communication (e.g., temporary account expires without anyone noticing). Unfortunately, these procedural failures increase risk and require quick IT identification to resolve them.

How to overcome this with ARM

After viewing the Inactive Account report, you can choose to delete the account and its access rights across AD, or you can “soft” delete the account by deactivating it (e.g., putting it into a group with strict limitations).

5 INSECURE ACCOUNT CONFIGURATIONS

Accounts with passwords that never expire or other risky configurations violate security policy and increase risk.

Why it's important

Insecure account configurations like passwords that never expire leave your organization exposed to insider threats and unauthorized access. Plus, accounts with weak or never-expiring passwords violate a number of regulatory requirements. For example, HIPAA administrative safeguard §164.308(a)(5) establishes "procedures for creating, changing, and safeguarding passwords," while PCI DSS requirement 2 includes a 90-day password reset among other password configuration specifications. Even though GDPR doesn't specify password requirements, it does state the need to implement "appropriate safeguards."

Common Challenges

Lack of standardization during Active Directory account creation often results in insecure account configurations that could endanger your compliance status. Without insight into account configurations, these hidden risks could quickly escalate.

How to overcome this with ARM

ARM automatically scans your domain for user accounts with never-expiring passwords, so you can resolve these issues proactively. Our role-specific templates help you establish standardized, safe configurations for all Active Directory accounts.

5 PERMISSIONS DIFFERENCES MONITORING

Tracking and verifying administrative changes to user permissions and access is a critical part of your security and compliance program.

Why it's important

Poorly managed administrative privilege contributes to insider threat. Whether it’s an unnecessary escalation of privilege or simply an operational error, monitoring permission changes is essential for incident response and compliance. For example, GDPR Article 5, paragraph 2 states that “data processing organizations must account for the exact access and permissions history of each directory.”

Common Challenges

It’s difficult to retroactively review access rights configuration changes in Active Directory—or know what all the consequences of a permissions change may be for a particular user account across Active Directory resources. In the rapid pace of onboarding users, it’s easy to make mistakes, and difficult to catch them before they impact security and compliance.

How to overcome this with ARM

The "Permission Differences" report compares the access rights on your file server at two different points in time and shows you how the access rights context has changed. Showing auditors granular details on administrative activity helps demonstrate compliance with user access control requirements. Specifically, PCI DSS Requirement 7.2 is focused on access control, as is HIPAA § 164.312(a)(1), which is the first of the technical safeguards in the standard. The same is true of GDPR, with Article 5 outlining the need for personal data to be secured from unauthorized access and loss.

7 HISTORICAL ACTIVE DIRECTORY STRUCTURES

Capturing time snapshots of Active Directory user access is a critical part of investigating data breaches. These reports can also demonstrate your effective incident response process to auditors.

Why it's important

After a data breach or other security exposure, reviewing historical Active Directory structures is a good security compliance best practice. It provides the detail you need to pinpoint the source of the attack, as well as the specific credentials used (or abused) for the attack.

Common Challenges

Auditors, as well as incident responders, understand the value of a reliable audit trail. Unfortunately, Active Directory doesn't make it easy. Building a clear timeline using native Active Directory features is not straightforward and can impede security and compliance programs.

How to overcome this with ARM

By capturing who had access (and who didn't have access) during the time of a security incident, ARM provides the critical audit trail evidence needed for investigations. Easily accessible historical scans provide instant visibility into Active Directory access rights the moment a breach occurs.

Access Rights Manager: How It Works

SolarWinds **Access Rights Manager (ARM)** is an affordable and easy-to-use software solution designed to help IT and security administrators quickly analyze user authorizations and access permission to systems, data, and files. Granular insight into user access helps protect organizations from the risks of failed audits as well as stolen data.

ARM is focused around five central disciplines to help you streamline access rights management. This framework helps you prepare for audits by finding and fixing risks quickly with detailed, custom, on-demand reporting.

PERMISSION ANALYSIS

Displays a comprehensive overview of the access rights situation to resources in your organization.

DOCUMENTATION & REPORTING

Records any access rights activity in our logbook and creates audit-ready reports.

SECURITY MONITORING

Monitors security- relevant actions in Active Directory and on your file servers.

ROLE & PROCESS OPTIMIZATION

Shortens your access rights management process and involves only the most important actors.

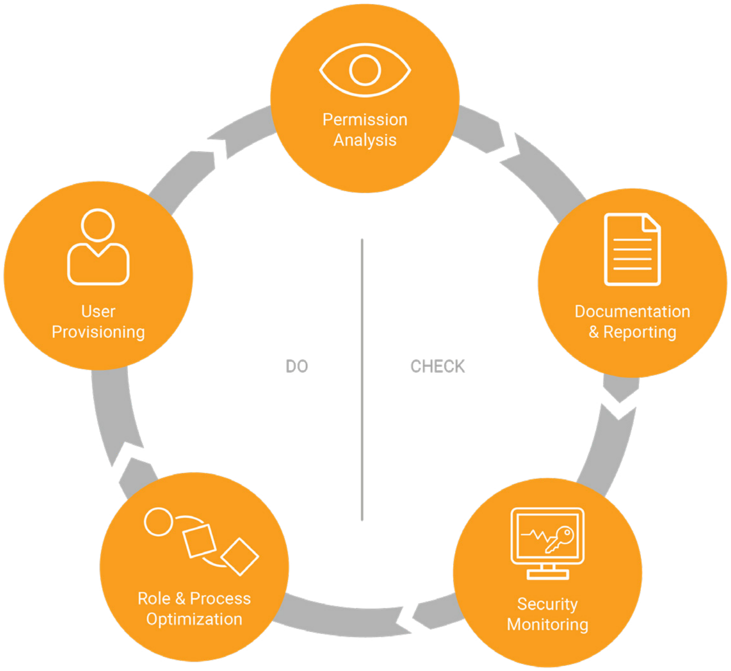


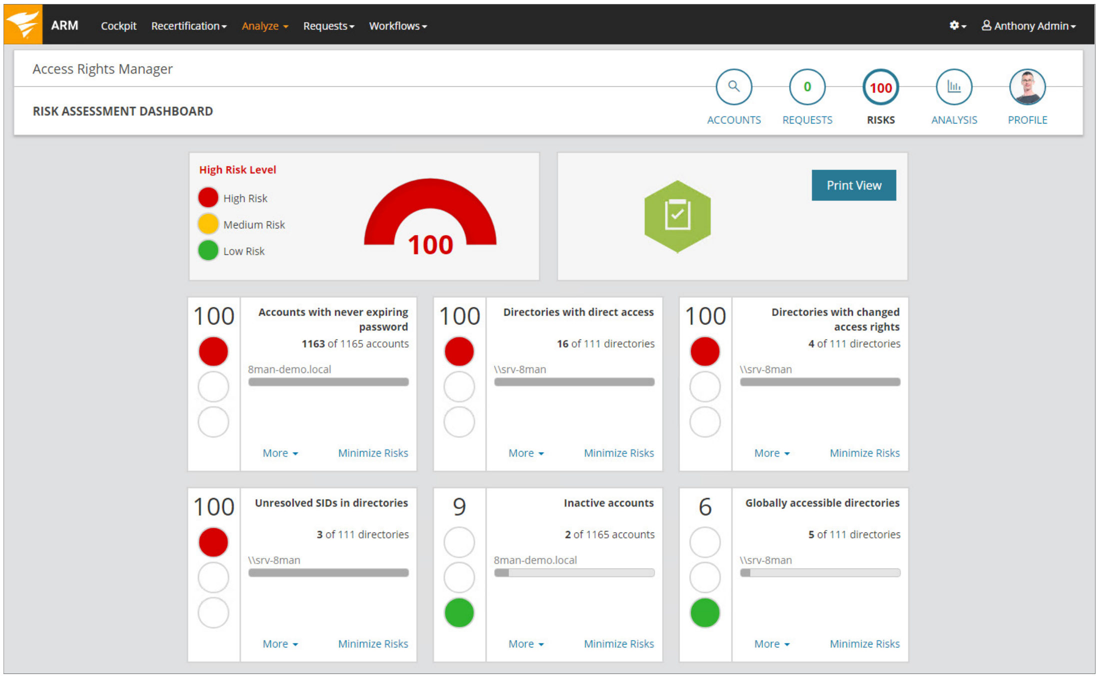
Figure 1: Five Central Disciplines of Access Rights Manager

USER PROVISIONING

Sets rules for the creation of new user accounts, provisioning of rights, and editing of account details.

Next Steps

To find out how ARM can help you prepare for your next audit or risk assessment, simply download a free **30-day trial** or **give us a call**, and one of our specialists will arrange a personalized demo.



TRY IT FREE

30 days, full version

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

This document is provided for informational purposes only. Information and views expressed in this document may change and/or may not be applicable to you. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.