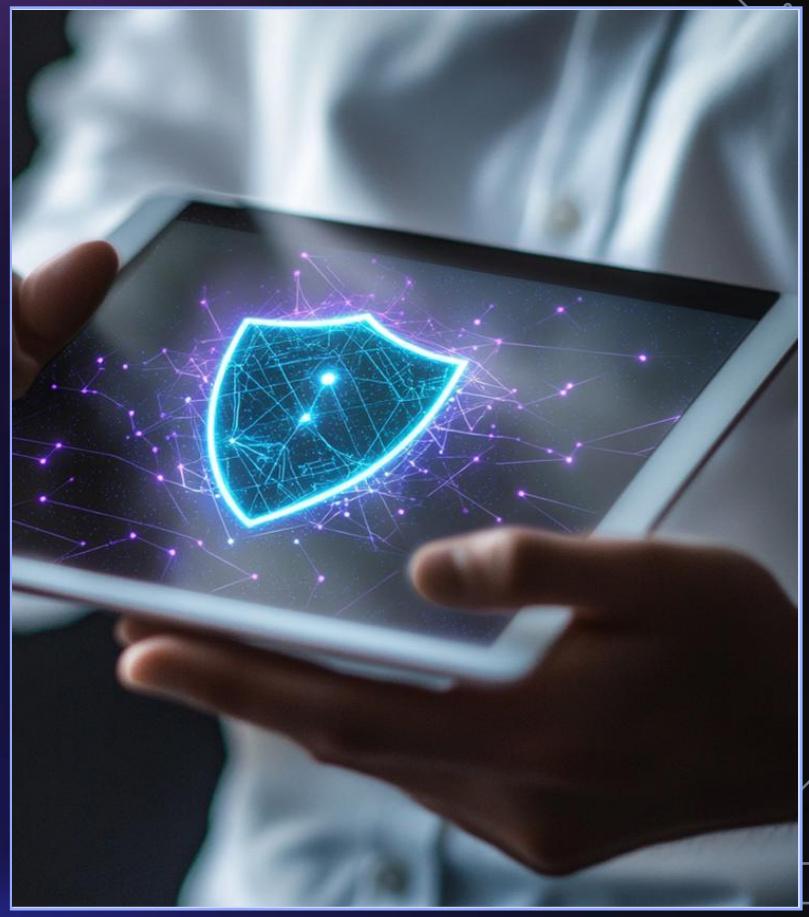
Microsoft Purview

Auditing

01

Setting Up Microsoft Purview Audit



Importance of Audit Solutions

Role in Compliance

Audit solutions play a critical role in ensuring adherence to legal and regulatory standards. They provide organizations with a systematic way to monitor and report on compliance efforts, thereby minimizing risks of penalties and reputational damage.

Enhancing Security

By implementing robust audit solutions, organizations can enhance their overall security posture. These solutions help identify vulnerabilities, monitor access controls, and detect unauthorized activities, contributing to a stronger defense against data breaches.

Prerequisites for Access

Required Licenses

To utilize Microsoft Purview Audit, users must ensure they possess the necessary licenses, which typically include Microsoft 365 Compliance or equivalent subscriptions, to access audit functionalities.

User Permissions

Proper user permissions are essential for accessing audit features. Users need to be assigned roles such as Compliance Administrator or Audit Logs Reader to effectively manage and review audit settings.

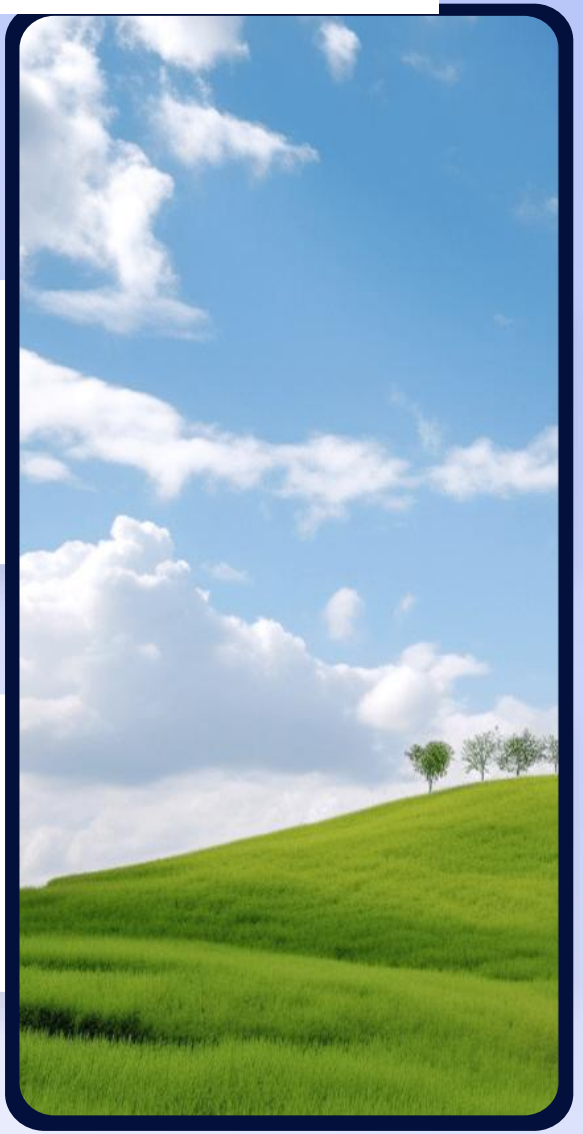
Configuring Audit Settings

Accessing the Audit Dashboard

The Audit Dashboard serves as the central interface for monitoring activities. Users can access this dashboard via the Microsoft Purview portal, where they can view recent audit logs and settings.

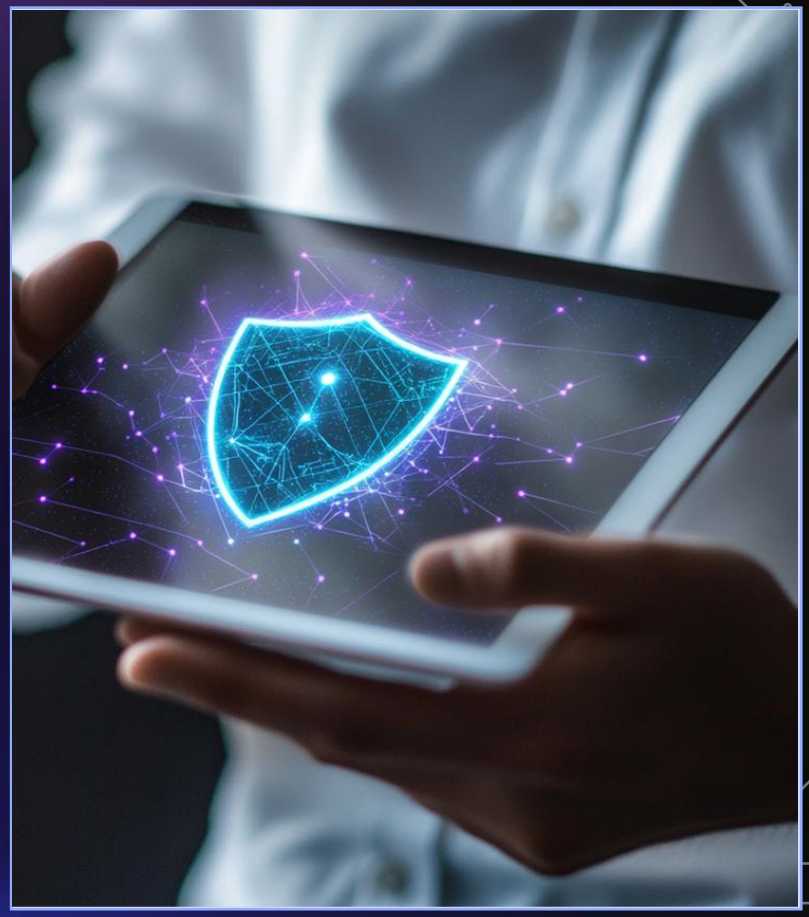
Customizing Audit Log Retention

Organizations can customize the retention period for audit logs based on compliance needs. Configurations can be made to retain logs from a minimum of 90 days to several years, depending on regulatory requirements.



02

Accessing Audit Logs



Navigating the Audit Logs Interface

Overview of the Interface

The audit logs interface provides a centralized view of all logged activities, allowing users to monitor actions effectively and identify potential issues within the system.

Key Components of the Logs

This section details the essential elements such as timestamps, user identifiers, and action descriptions, which collectively facilitate a comprehensive understanding of logged events.

Filtering Audit Log Data

Setting Date Range

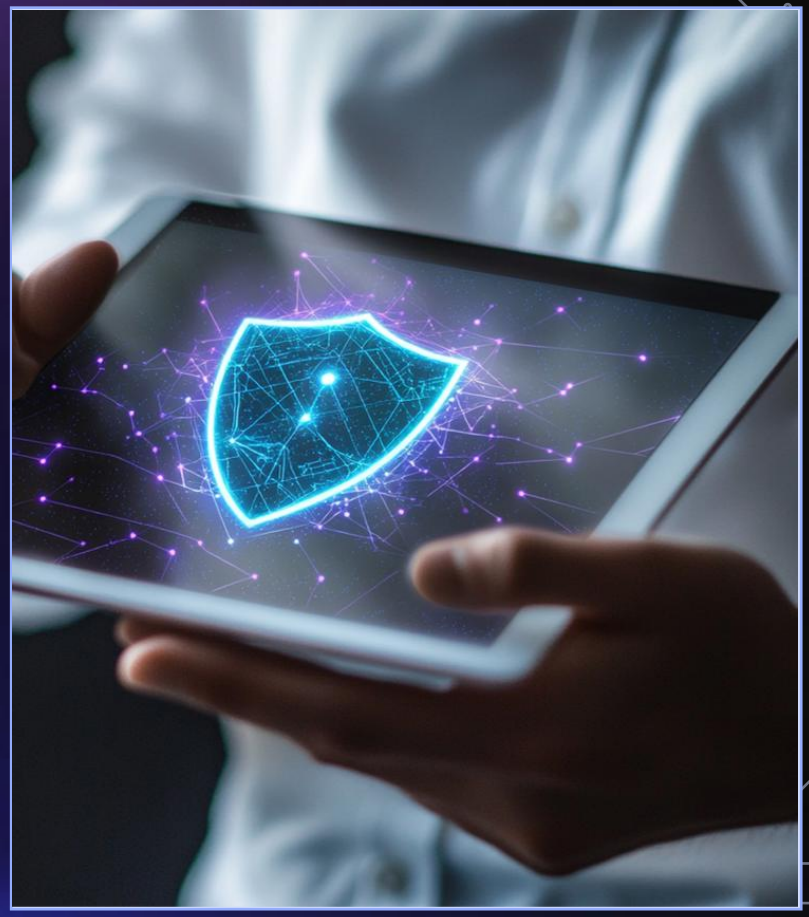
Users can specify a date range to narrow down the logs to a particular timeframe, enhancing the efficiency of data retrieval and analysis.

Applying User Filters

This feature allows users to filter logs based on specific users, ensuring that relevant activities of individuals are easily accessible for review and compliance purposes.

03

Analyzing Audit Data



Defining Audit Policies

Policy Creation Guidelines

Establish clear guidelines for creating audit policies, ensuring they align with organizational objectives and compliance requirements, while also considering scalability and maintenance.

Policy Types in Purview

Explore various types of audit policies available in Purview, including access audits, activity logs, and compliance checks, highlighting their specific use cases and importance.

Selecting Audit Events

Common Audit Events

Identify and describe the most frequently audited events, such as user logins, data access, and modifications, emphasizing their significance in maintaining security and compliance.

Custom Event Selection

Discuss the process of selecting custom audit events tailored to specific organizational needs, allowing for a more focused approach to monitoring and compliance.

Understanding Log Entries

Types of Activities Logged

Audit logs encompass various activities, including user access, modifications to data, and system events, providing a comprehensive overview of interactions within the system.

Importance of Each Entry

Each log entry serves a crucial purpose in security and compliance, aiding in identifying unauthorized actions, tracking user behavior, and ensuring accountability within the system.

Exporting Audit Logs

Export Formats Available

Audit logs can be exported in several formats, such as CSV, JSON, and XML, each offering different advantages for analysis and compatibility with various systems.

01

Steps for Exporting Data

The process for exporting audit logs involves selecting the desired logs, choosing the preferred format, and executing the export function, ensuring the data is captured accurately and efficiently.

02

Updating Audit Policies

Policy Modification Procedures

“Care and feeding” is required to ensure policies reflect current regulatory requirements and organizational objectives.

Version Control Practices

Leverage auditing to also track updates to compliance policies and configurations. What about the compliance landscape changes over time, how does it change, and what are the implications?

Deleting Audit Logs

Compliance Considerations

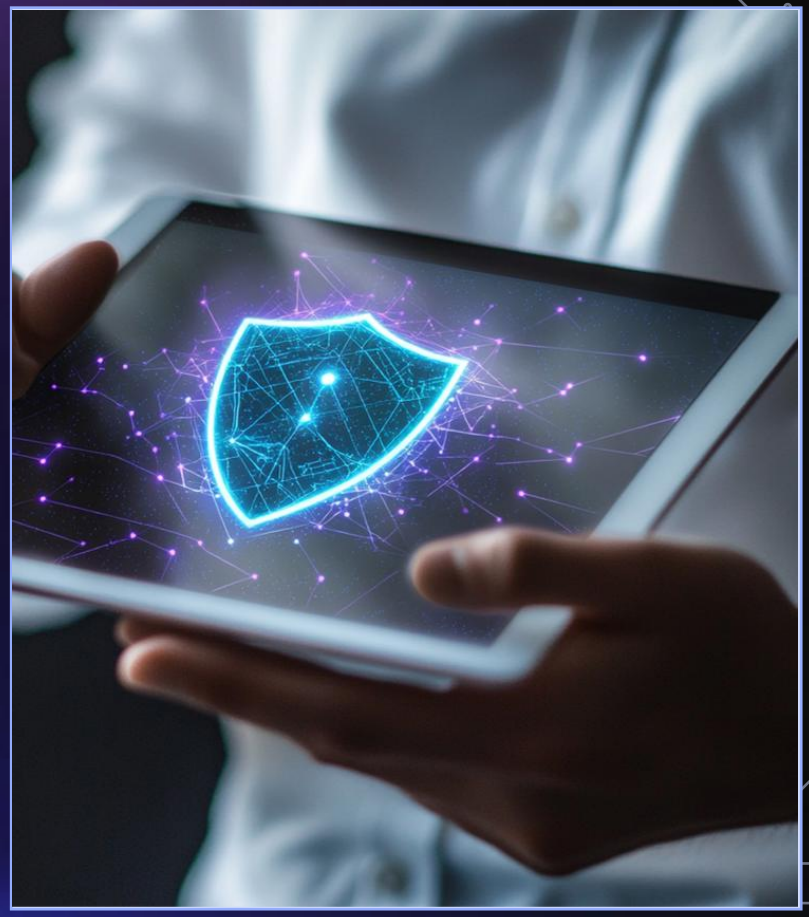
Like other types of data, understanding the legal and regulatory considerations related to the management and deletion of audit logs can be critical.

Steps to Archive Logs

Retention policies can be created specifically for audit data and audit logs.

04

Advanced vs. Standard Audits in Purview



Standard Audits - Definition and Scope

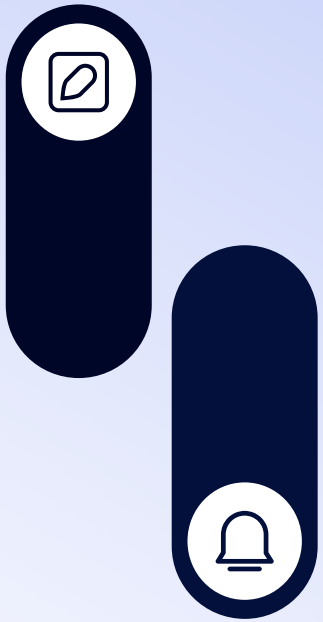
The standard audit framework outlines the procedures and guidelines necessary for conducting effective audits, ensuring compliance with regulatory requirements and best practices.

Key components of standard audits include planning, execution, reporting, and follow-up, which collectively facilitate a thorough evaluation of an organization's financial and operational processes.

Benefits of Standard Audits

Simplicity and Accessibility

Standard audits provide a clear and straightforward approach, making it easier for organizations to understand audit processes and requirements without overwhelming complexity.



Resource Efficiency

By utilizing a standard audit approach, organizations can optimize resource allocation, reduce unnecessary expenses, and streamline operations while maintaining compliance and accountability.

Advanced Audits - Definition and Characteristics

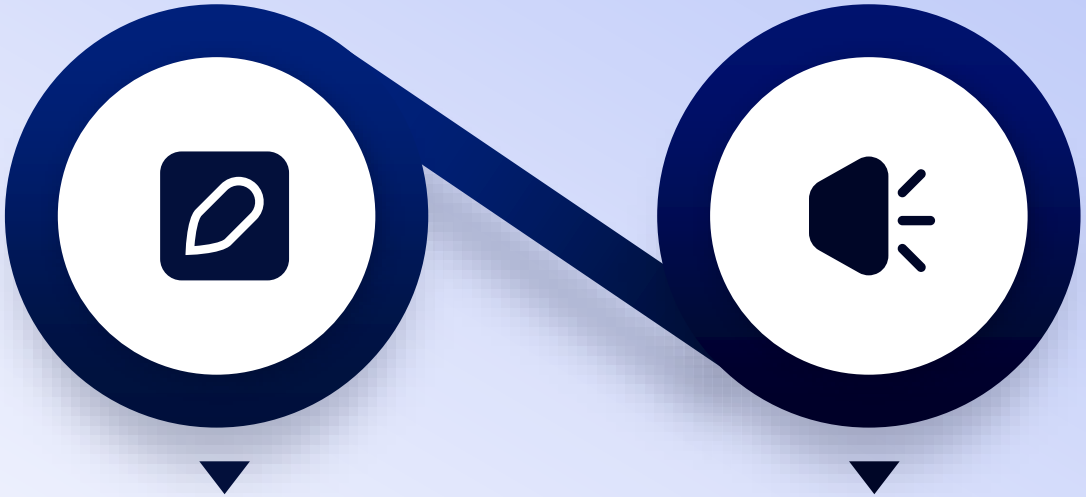
In-Depth Analysis

An advanced audit encompasses a thorough examination of systems and processes, focusing on both qualitative and quantitative metrics to ensure compliance and efficiency.

Customization Options

Advanced audits can be tailored to specific organizational needs, allowing for flexible methodologies that address unique challenges and objectives in various operational contexts.

Benefits of Advanced Audits



Comprehensive Insights

These audits provide a holistic view of organizational performance, revealing critical insights that can inform strategic decision- making and improve overall effectiveness.

Enhanced Security Features

Implementing advanced audits bolsters security measures, identifying vulnerabilities and ensuring adherence to regulatory standards, thus protecting sensitive data and maintaining trust.

Depth of Analysis

01

Data Granularity

The degree of detail included in audit data, with advanced audits analyzing minute transactions while standard audits focus on broader categories, impacting insights and decision-making.

02

Reporting Capabilities

Advanced audits often feature sophisticated reporting tools that provide visualizations and comprehensive insights, while standard audits typically offer simpler, more traditional reports.

Use Cases

01

Situations Favoring Standard Audits

Ideal for organizations with straightforward operations or compliance requirements, standard audits provide sufficient oversight without necessitating extensive resources or complexities.

02

Scenarios for Advanced Audits

Recommended for organizations with intricate structures or high- risk environments, advanced audits deliver deeper insights and risk management, ensuring thorough assessment and enhanced accountability.

Comparative Analysis of Tools

Standard Audit Tools

Standard audit tools offer fundamental features for tracking user activity and compliance. They are typically user-friendly and suitable for organizations with basic auditing needs, ensuring ease of implementation.

Advanced Audit Tools

Advanced audit tools provide deeper insights and analytics for comprehensive auditing capabilities. These tools support complex compliance requirements and offer detailed reporting functions, tailored for larger organizations or those with stringent regulatory mandates.

Choosing the Right Audit Type

Factors to Consider

When selecting an audit type, evaluate the organization's specific needs, regulatory requirements, potential risks, and the scope of the audit to ensure comprehensive coverage and effectiveness.

01

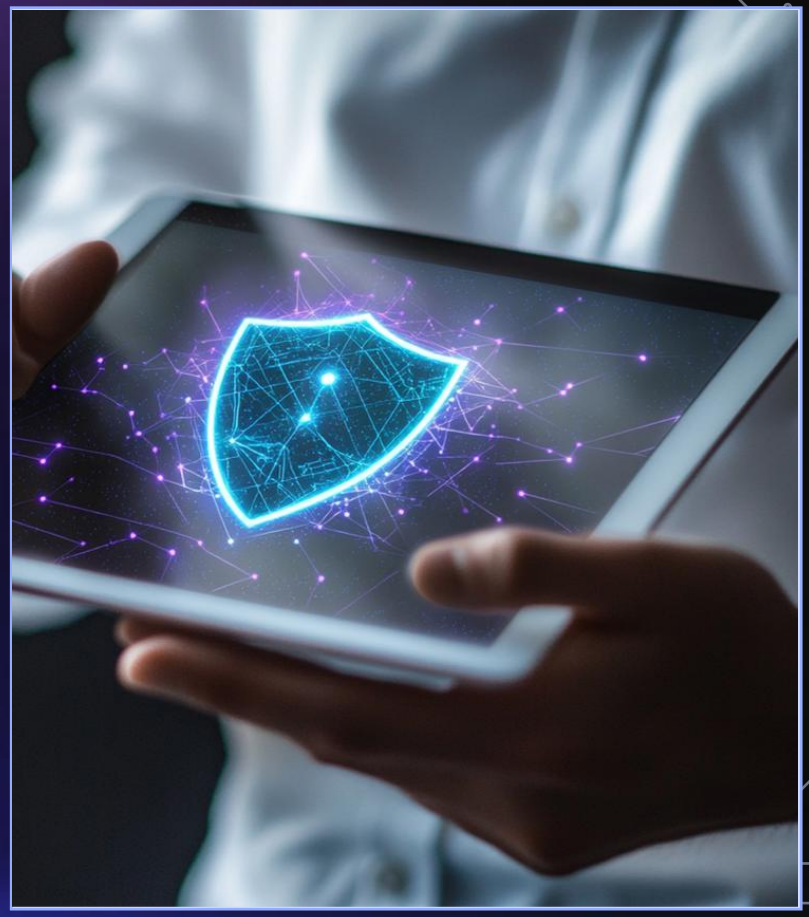
Stakeholder Input

Engaging stakeholders early in the audit process is crucial. Their insights can shape the audit's focus and ensure that the objectives align with organizational goals and stakeholder expectations.

02

05

Utilizing Audit Insights



Accessing Audit Reports

Report Types Available

Various types of audit reports are available, including compliance reports, security reports, and performance reports, each tailored to meet specific organizational needs and standards.

01

Report Customization Options

Users can customize audit reports by selecting specific data points, date ranges, and formats to ensure that the information presented aligns with individual requirements or compliance mandates.

02

Interpreting Audit Logs

Key Metrics to Consider

When analyzing audit logs, key metrics such as user access patterns, error rates, and system performance indicators should be evaluated for a comprehensive understanding of activity.

Understanding Log Data Structure

Understanding the structure of log data is essential; it typically includes timestamps, user IDs, action types, and resource identifiers, facilitating effective analysis and reporting.

Identifying Trends and Patterns

01 Recognizing Anomalies

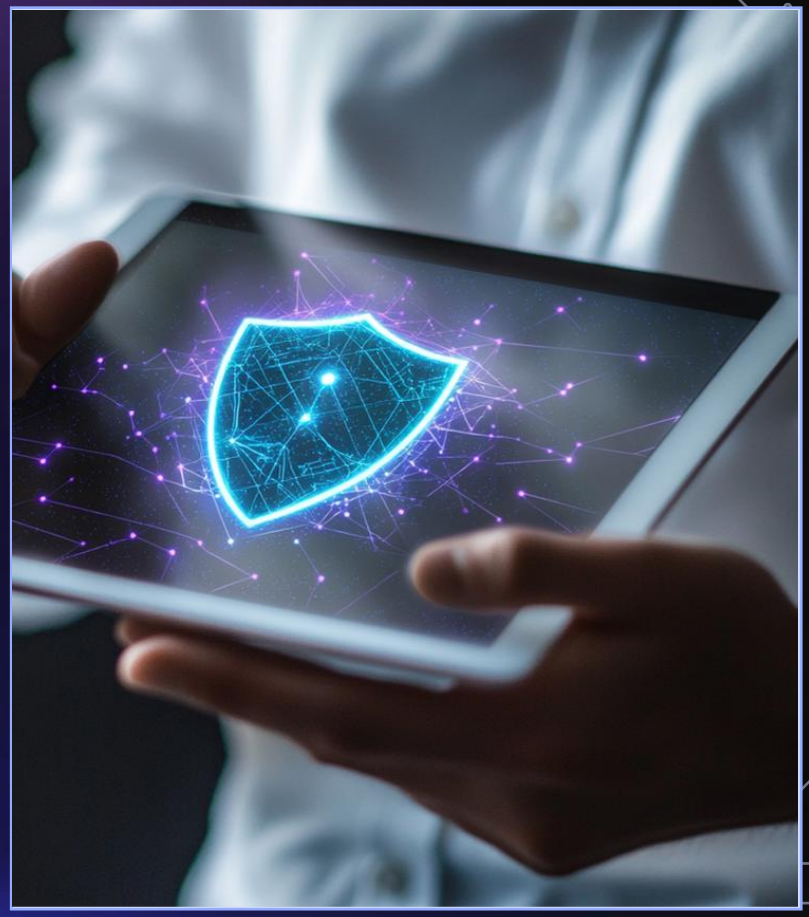
Identifying anomalies involves detecting irregularities or deviations from established norms during audits, which can signify underlying issues that require attention and remediation.

02 Reporting Findings

Effective reporting of audit findings ensures that all stakeholders are informed of critical issues and trends. Clear communication facilitates timely decision-making and strategic planning based on data insights.

06

Troubleshooting Common Issues



Access Issues

Resolving Permission Errors

To resolve permission errors, ensure that the user has the necessary rights to access the resource. Check user roles and permissions within the system settings.

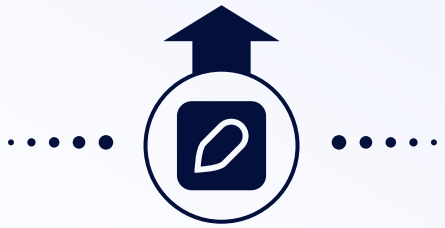
Troubleshooting Log Visibility

Log visibility issues may stem from configuration settings. Verify the logging level is appropriately set, allowing access to logs for troubleshooting and monitoring purposes.

Data Integrity Concerns

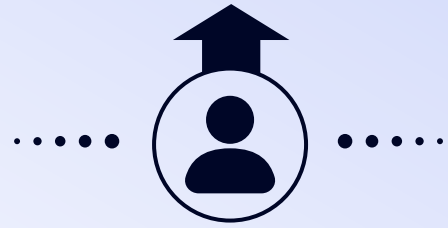
Addressing Incomplete Logs

Incomplete logs can lead to misinterpretation of events. Regularly audit log entries to identify gaps and implement measures for comprehensive data capture.



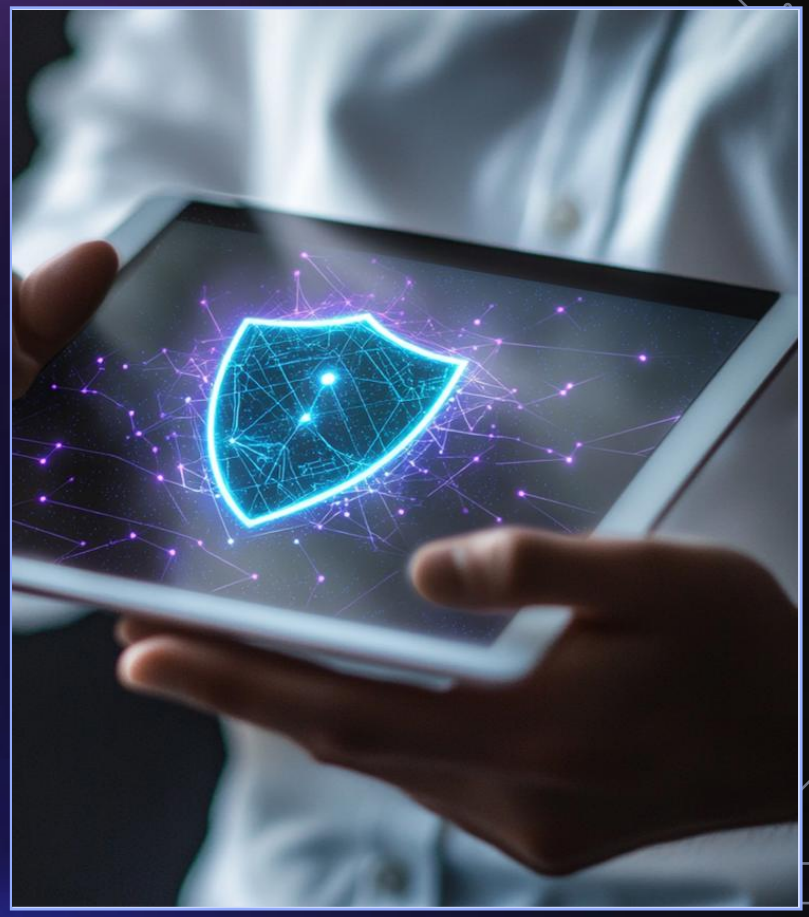
Ensuring Accurate Log Representation

Accurate log representation is critical for effective analysis. Validate log formatting and content to ensure that they accurately reflect system activity and events.



07

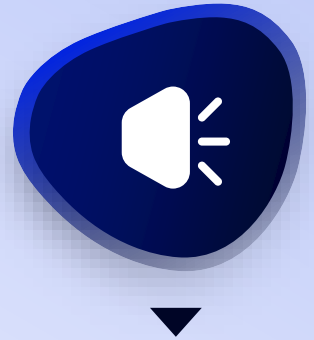
Best Practices for Auditing



Regular Review of Audit Logs

Establishing a Review Schedule

Creating a systematic review schedule ensures timely analysis of audit logs, facilitating prompt identification of anomalies and compliance with regulatory requirements.



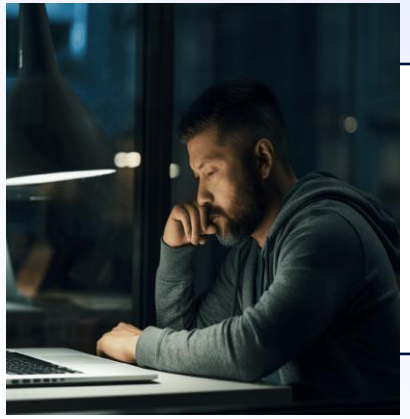
Involving Key Stakeholders

Engaging relevant stakeholders in the review process enhances accountability and ensures that varied perspectives are considered, promoting a comprehensive understanding of audit findings.

Training Users on Audit Processes

Conducting Workshops

Workshops can be employed to equip users with the necessary skills and knowledge regarding audit processes, fostering a culture of compliance and proactive engagement with auditing practices.



Providing Resource Materials

Distributing resource materials, such as guides and manuals, supports continuous learning and serves as a reference for users, ensuring they have access to critical information on audit processes.

Thanks