

ITdesign AudIT Berechtigungsreporter

Version 1.1

Wien, September 2011



TAKE IT EASY

Konzeption und Inhalt: ITdesign

Nutzung durch Dritte nur mit schriftlicher Genehmigung von ITdesign

Inhaltsverzeichnis

1	MANAGEMENT SUMMARY	3
2	ITDESIGN AUDIT - FUNKTIONSBESCHREIBUNG ALLGEMEIN	5
2.1	VORTEILE VON AUDIT	5
2.2	NUTZEN FÜR DEN KUNDEN	6
3	LEISTUNGSBESCHREIBUNG DES AUDIT-STANDARDPAKETS	7
3.1	IMPLEMENTIERUNG	7
3.1.1	Erstellung eines Umsetzungsplans	7
3.1.2	Umsetzung.....	8
3.1.3	Dokumentation.....	8
3.1.4	Know How Transfer	8
3.1.5	Abnahme	9
4	AUDIT WARTUNGSVERTRAG	10
5	ABGRENZUNG UND VORAUSSETZUNGEN	11
5.1	ABGRENZUNG.....	11
5.2	VORAUSSETZUNGEN	11
5.2.1	AudIT Server	11
5.2.2	Datenbank Server.....	12
5.3	TECHNISCHE VORGABEN.....	12

1 Management Summary

Der Berechtigungsreporter **AudIT** ist die Lösung für unternehmensweite Transparenz in Bezug auf Berechtigungen.

Die Highlights der Lösung sind:

- Sie sind in kürzester Zeit berichtsfähig für Revision und Wirtschaftsprüfung
- Sie optimieren die Sicherheit Ihrer Informationen und Prozesse, indem **AudIT** die Zusammenhänge zwischen Anwendern, Organisation und Berechtigungen darstellt und Sie dadurch potentielle Verstöße gegen Richtlinien erkennen können
- **AudIT** automatisiert die Erfassung der Zugriffsberechtigungen und visualisiert das Ergebnis übersichtlich und einheitlich.
- **AudIT** integriert Ihre gesamte IT Landschaft mit allen Verzeichnissen, Datenbanken und Anwendungen der unterschiedlichsten Hersteller.
- **AudIT** präsentiert alle Informationen zu den aktuellen Zugriffsberechtigungen auf einen Blick. Die Darstellung der compliancerelevanten Daten ist übersichtlich und aussagekräftig. Sie ermöglicht es jedem Verantwortlichen, etwaigen eingeschränkten Bestätigungsvermerken zuvorzukommen.

Anwendungsverantwortliche aus den Fachabteilungen, Administratoren in der EDV und der Helpdesk können jederzeit die Berechtigungen über Webbrowser einsehen.

AudIT deckt den Bereich „Control Self Assessment“ des vorgeschriebenen Risikomanagement-Systems und stellt die notwendigen Tasks für die zuständigen Personen zur Aktualisierung der Berechtigungen dar. Damit wird das geforderte Minimalitätsprinzip im Rahmen eines wiederkehrenden Prozesses gewährleistet.

Die Berechtigungsdaten werden aus den Zielsystemen regelmäßig exportiert und in die Datenbank des **AudIT** Servers importiert. Dabei werden die Daten überprüft und etwaige Fehler in Log-Tabellen geschrieben, welche über das Intranet abgefragt werden können.

Beispiele für Zielsysteme:

- MS Active Directory
- Novell eDirectory
- LDAP Verzeichnis
- SAP
- iSeries / DB2
- MS SQL Server
- Oracle
- MS Exchange Mailboxes/Public Folder
- Filesysteme (NTFS, Novell)
- File Shares

AudIT ist der logische erste Schritt und schafft die notwendigen Voraussetzungen für die erfolgreiche Einführung eines umfassenden IDM- (Identitätsmanagement) Systems. Wenn Anbindung, Datenkonsistenz und Berichtsfähigkeit durch **AudIT** erreicht sind, können die Themen Anwenderlebenszyklus, Provisioning mit Rollen und Genehmigungen jederzeit mit einem marktführenden IDM Werkzeug, wie z.B. Novell Identity Manager oder Quest Active-Entry hinzugefügt werden. **AudIT** unterstützt hierbei zusätzlich bei der Konzeption des Rollensystems.

In der vorliegenden Produktbeschreibung werden zunächst die Funktionen von **AudIT** im Allgemeinen beschrieben; anschließend wird die konkrete Ausprägung des **AudIT**-Standardpaketes angeboten.

2 ITdesign AudIT - Funktionsbeschreibung allgemein

AudIT stellt in seinem vollen Funktionsumfang die vergebenen Berechtigungen unternehmensweit und einheitlich dar, wie es mit den einzelnen Administrationstools der Anwendungen nicht möglich ist:

- Automatische Sammlung aller Berechtigungsdaten quer durch das ganze Unternehmen
 - Berechtigungsdaten aus Verzeichnisdiensten, Datenbanken, Dateiablagen bzw. -freigaben, Web-Anwendungen, ERP, CRM, HR, Warenwirtschaft, etc., egal von welchen Herstellern (Microsoft, Oracle, SAP, IBM, OpenSource, usw.)
 - Personen- und Organisationsdaten aus Personalsystem, Organisationsmanagement und/oder Verzeichnissen
 - Protokollierung und Ablage historischer Daten
- Zentrale Konsolidierung und Verlinkung von Anwendern mit Benutzerkonten und Berechtigungen im organisatorischen Kontext
- Fehler-Reports zeigen Inkonsistenzen und Aktualisierungsbedarf
- Übersichtliche Darstellung und Navigationsmöglichkeit
- Bestätigungsfunktion für Vorgesetzte
- Rollenbasiertes internes Rechtesystem (an das Unternehmensverzeichnis gekoppelt)

2.1 Vorteile von AudIT

AudIT ist speziell für österreichische Mittelstandsunternehmen entwickelt worden: kostengünstig und rasch können die geforderten Berichte generiert werden. Durch die eingesetzte Architektur werden die Zielsysteme integriert, ohne Software darauf installieren zu müssen. Selbst ausgefallene Systeme lassen sich einfach und flexibel einbinden.

Langwierige organisatorische Vorarbeiten sind dafür nicht notwendig: **AudIT** kommt vorkonfiguriert und paketiert mit Professional Services, sodass ein Reporting über die wichtigsten Infrastruktursysteme in wenigen Tagen hergestellt werden kann.

Die Investition in **AudIT** rechnet sich alleine über die Zeitersparnis bei der Berichtserstellung innerhalb kürzester Zeit (meist innerhalb eines Quartals) und ist zusätzlich eine wertvolle Hilfe bei der Analyse der Berechtigungen.

Die Vorteile im Überblick:

- Rasche Integration und Berichtsfähigkeit
- Geringe Anschaffungskosten und Betriebsaufwendungen
- Erfüllung der Vorschriften und Ableitung von Datenbereinigungsaktivitäten
- Erfordert keine zusätzliche Software (Agents) an den Zielsystemen

2.2 Nutzen für den Kunden

Für den Kunden ergibt sich mit **AudIT** folgender Nutzen:

- **Höhere IT-Sicherheit:** Transparenz und umfassenden Überblick über die Berechtigungen im Unternehmen schaffen
- **Risikominimierung:** Berechtigungsaltlasten, welche durch Personalrotation entstehen, werden durch die mit **AudIT** ermöglichte Kontrolle vermieden.
- **Reduzierung der Verwaltungsaufgaben**
- **Interne Kostenverrechnung:** Durch die mit **AudIT** ermöglichte Kontrolle durch die Fachbereiche können Personen, die die Abteilung gewechselt haben, gefunden werden
- **Compliance:** Gewährleistung der Zuordnung von Ressourcen zu berechtigten Personen (Steuerprüfung, Revisionssicherheit)
- Aufzeigen von isolierten Richtlinien und ineffizienten Vorgehensweisen (Business Governance)
- Grundlagen schaffen für ein umfassendes Identity Management in Ihrem Unternehmen.
- Validierung und Automatisierung von Business Governance Themen.

3 Leistungsbeschreibung des AudIT-Standardpakets

Lange Projektlaufzeiten und ausufernde Kosten kennzeichnen oft – trotz langer Vorlaufzeit für die Definition der Gesamtlösung – die Implementierungen derartiger Funktionalitäten. Um dem Risiko einer Kostenexplosion zu begegnen und eine sehr kurze Durchlaufzeit sicherzustellen, hat ITdesign ein Paket entworfen, mit dem es möglich ist, diese Gefahren auszuschalten.

Finden Sie nachfolgend die Beschreibung des Pakets, dessen Abgrenzung und den Ablauf der Implementierung.

Folgende Leistungen werden im Rahmen dieses Angebots für ein standardisiertes **AudIT** -Paket erfüllt:

- Customizing des Berechtigungsexports
- Einrichten der periodischen Export-Jobs
- Know How Transfer
- Dokumentation
- Testbetrieb
- Produktivsetzung
- Wartungsvertrag

3.1 Implementierung

Um rasch Funktionen aus dem Berechtigungsreporter nutzen zu können (quick wins) - und aus den Erfahrungen ähnlicher - Projekte empfiehlt ITdesign folgende Vorgangsweise:

3.1.1 Erstellung eines Umsetzungsplans

Ein Tag Workshop (Kick Off) zur Definition:

- Zielsysteme
- Zuständigkeiten
- Attributmapping
- Matching-Kriterien
- Festlegen der Personal- und Organisationsquelle

Weiters dient dieses Meeting auch dazu, dass alle Beteiligten die Ziele und die Rahmenbedingungen kennen lernen.

Die im Kick Off Meeting besprochenen Themen werden in Abstimmung mit den Mitarbeitern des Kunden in einem Protokoll festgehalten. Dieser Umsetzungsplan wird vom Kunden innerhalb einer Woche nach Vorlage überprüft, bei Akzeptanz abgenommen und gilt als beidseitig verbindliche Basis für die weitere Abwicklung des Projekts und als Basis für die Abnahme.

3.1.2 Umsetzung

Den Dienstleistungsaufwand für die folgenden Tätigkeiten/Funktionalitäten bieten wir jeweils als Pauschalleistung unter dem Punkt Preisgestaltung / Verrechnung mit folgenden Vorgaben an:

- Aufwendungen für eventuelle Adaptierungen und Konfigurationsänderungen der Zielsysteme, um den Erhalt von Berechtigungsdaten zu ermöglichen, erfolgen durch den Kunden (z.B.: Einrichten von Security-Einstellungen und Zugriffsberechtigungen, ...)

Inhalte:

- Installation **AudIT** Server
- Anbindung der definierten Zielsysteme
 - Einrichten der Export Jobs
 - Einrichten der Matching Kriterien
 - Einrichten der Attributsmappings

3.1.3 Dokumentation

Die Dokumentation wird von ITdesign für die gesamte, im Zuge der Installation geschaffene Landschaft erstellt. In der Dokumentation wird die Konfiguration der **AudIT** Implementierung detailliert beschrieben.

Die Dokumentation wird besonders für die folgenden Aufgaben benötigt:

1. Grundlage für den Know How Transfer Der Tatsache, dass – wie die Erfahrung zeigt – die Erstellung von Dokumentationen oftmals vernachlässigt wird, versucht ITdesign dadurch entgegenzuwirken, dass der weitere Verlauf des Projektes die Dokumentation voraussetzt. Das ist mit ein Grund, warum die Dokumentation als Grundlage für den Know How Transfer Workshop dient.
2. Einbindung zusätzlicher Systeme Werden zusätzliche Systeme eingebunden, wird dies in der vorhandenen Dokumentation festgehalten.
3. Nachschlagewerk für die EDV Betreuer und neue EDV-Mitarbeiter Die EDV-Betreuer, die anhand der Dokumentation eingewiesen werden, haben ein Nachschlagewerk über ihre Systemumgebung jederzeit zur Verfügung.

Nach Abschluss des Projektes erfolgt die Wartung der Dokumentation durch Mitarbeiter des Kunden.

3.1.4 Know How Transfer

Prinzipiell ist der Know How Transfer permanent während der Installation vorgesehen. Am Ende der Installation ist ein Workshop – mit einem halben Arbeitstag limitiert – geplant.

Der vom Kunden gewünschte Umfang des Know How Transfers hängt erfahrungsgemäß stark davon ab, wie intensiv die Einbindung der verantwortlichen Personen während der Installation möglich war.

Die Wissensweitergabe erfolgt anhand praktischer Beispiele an bis zu drei vom Kunden definierte Mitarbeiter. Als Grundlage dienen dabei der Umsetzungsplan, die durchzuführenden Abnahmetests und die Projektdokumentation.

Nach dem Know How Transfer sollten die Administratoren des Kunden in der Lage sein, weitere Systeme eigenständig einzubinden.

3.1.5 Abnahme

Die im Umsetzungsplan definierten Abnahmekriterien werden gemeinsam besprochen, überprüft und die Ergebnisse in einem Protokoll festgehalten.

Das Projekt gilt als abgenommen, wenn bei der Abnahme keine gravierenden Mängel erkannt wurden.

4 AudIT Wartungsvertrag

Bei Abschluss eines Wartungsvertrages für den Berechtigungsreporter erwirbt der Kunde das Recht auf folgende Leistungen:

- **Periodische Information über aktuelle Versionen und Entwicklungen**
Durch Newsletter wird der Kunde über neue Funktionen und Lösungen von **AudIT** informiert.
- **Nutzung der aktuellen Version**
Der Kunde erhält das Recht, die jeweils aktuellste Version von **AudIT** einzusetzen.
- **Installation der aktuellen Version**
Installation der jeweils aktuellste Version von **AudIT**, sofern die Installation remote erfolgen kann. Adaptierungen vor Ort bzw. Konfigurationsänderungen sind im Wartungsvertrag nicht enthalten und werden gesondert in Rechnung gestellt.
Nicht enthalten sind Installationen und Updates von Komponenten, die nicht direkt am unter Vertrag befindlichen **AudIT** Server installiert sind, wie z.B.: vorhandene Agents oder Scripts an den Zielsystemen.

Die Aufwendungen für diese Updates, Adaptierungen vor Ort, wie auch von Konfigurationsänderungen, welche durch neue Funktionen bedingt sind (z.B. Anpassungen von Zielsystemen, Anpassungen der bestehenden Export-, Importroutinen, Einbindung zusätzlicher Zielsysteme) können pauschal oder nach Aufwand gelöst werden und sind **nicht** im Wartungsvertrag enthalten.
- **Zugriff auf Hotline**
Der Kunde hat innerhalb der ITdesign Bürozeiten kostenfreien Zugriff auf die ITdesign **AudIT** Hotline (0800 - 99 88 44 oder audit@itdesign.at) und erhält durch Spezialisten umgehend telefonische Unterstützung bei auftretenden Problemen seiner **AudIT** Lösung. Im Wartungsvertrag sind keine Aufwände für Änderungen am System inkludiert. Diese Änderungen werden in Form von Consulting angeboten.
- **20% Rabatt auf alle Neuentwicklungen**
Der Kunde erhält alle von ITdesign im Laufe der Zeit neu entwickelten Module um 20% vergünstigt.

5 Abgrenzung und Voraussetzungen

5.1 Abgrenzung

Im Rahmen des **AudIT** -Standardpakets ist die Einbindung der nachfolgend aufgelisteten Systeme vorgesehen:

- Ein Unternehmensverzeichnis (Single Domain)inkl.
 - Konten
 - Gruppen
 - File Shares
- Ein Mailsystem inkl. Verteiler
- Zwei Datenbank- / Web-Applikationen
 - Einbindung der Usertabelle
 - Einbindung der Berechtigungstabelle mit bis zu max. 10 Berechtigungsstufen
- Eine Quelle für Personal- und Organisationsdaten (z.B. SAP HR oder das Unternehmensverzeichnis)
 - Bereitstellung über .csv Dateien
- Für die Installation von **AudIT** werden Lizenzen für MS Windows Server und MS SQL Server vorausgesetzt.

5.2 Voraussetzungen

5.2.1 AudIT Server

ITdesign geht davon aus, daß die benötigte Hardware, erforderlichen Lizenzen und Installationskits für den Betrieb und Installation des **AudIT** Servers (incl Datenbanklizenzen) vom Kunden zur Verfügung gestellt wird.

Der Audit Server kann auch in einer virtualisierten Umgebung betrieben werden.

Betriebssystemvoraussetzung:

- mind. Microsoft Windows 2003 SP1
- IIS 7.0
- .net 3.5 SP1

Vom Kunden sind zu definieren:

- Accountnamen und Passwörter der Service Accounts für die periodischen Export-Jobs
- Passwort für den „Administrator“ des **AudIT** Servers
- IP Adresse für den **AudIT** Server
- Subnet Mask
- Default Gateway
- 2 DNS Server
- Full Qualified Domain Name

5.2.2 Datenbank Server

IT design geht davon aus, das die **AudIT** Datenbank auf einem bestehenden, vom Kunden zur Verfügung gestellten, MS SQL Datenbank Server läuft. Der Datenbankserver kann auch auf dem AudIT Server laufen (MS SQL Express Edition)

Datenbankvoraussetzung:

- MS-SQL Server ab 2005 oder MS SQL Express Edition ab 2005
- Datenbankgröße 4GB

5.3 Technische Vorgaben

Installationsvorgaben

Der Spezialist von ITdesign benötigt für die Installation:

- Die Erlaubnis, sich mit dem mitgebrachten Notebook ins Firmennetzwerk des Kunden zu verbinden
- Ein Netzkabel und eine IP Adresse
- Der Notebook von ITdesign muss eine Zugriffsberechtigung ins Internet bekommen (http und https)

Vorgaben für die Zielsysteme des Kunden

Die technische Umsetzung der Integration von Zielsystemen setzt einen oder mehrere der hier angeführten Punkte voraus:

- Die Endsysteme sind in der Lage, Daten an den **AudIT** Server zu übermitteln (z.B. csv Files)
- Die gewünschten Daten lassen sich aus dem entsprechenden Zielsystem auslesen