Anforderungsspezifikation <Webbasiertes Reporting von Userberechtigungen für Windows Active Directory - WRAD>

Projektteam 2/3
Dario Furigo
Philipp Köfer
Nicola Michaelis
Beat Schärz

v0.7
21.11.2018

Berner Fachhochschule
Departement für Technik und Informatik

Inhaltsverzeichnis

1 Versionskontrolle

Version	Datum	Beschreibung	Autor
0.1	28.09.2018	Dokument erstellt	N.M.
0.2	06.10.2018	Dokument erweitert (Kapitel 7.1 und 7.2)	B.S.
0.3	07.10.2018	Dokument erweitert (Kapitel 6)	D.F.
0.4	07.10.2018	Dokument erweitert (Kapitel 7.3 und 7.4)	N.M.
0.5	09.10.2018	Dokument reviewed und korrigiert	D.F.
0.6	14.10.2018	Dokument erweitert (Kapitel 8)	N.M.
0.7	14.11.2018	Dokument überarbeitet	D.F.

2 Zweck des Dokuments

Dieses Dokument beschreibt die Ziele und Anforderungen für das Projekt „Webbasiertes Reporting von Userberechtigungen für Windows Active Directory

3 Vision

Das Reportingtool ist eine webbasierte Lösung, welches Audits über ein Active Directory vereinfacht. Die Lösung ist sowohl für Systemadministratoren als auch für Manager und Auditoren nützlich. Mit den Reports werden einerseits klassische Probleme wie z.B. verwaiste Accounts ersichtlich, andererseits ist aber auch ein IST/SOLL Vergleich der Berechtigungen möglich. Weiter kann dem Tool auch eine „History“ eines Users entnommen werden, welche aufzeigt wie sich dieser User über die Zeit entwickelt hat.

4 Stakeholder

Stakeholder	Beschreibung
Auditor	Der Auditor hat eine Read-Only Sicht auf die Applikation. Für ihn ist das Reporting relevant und er meldet Verstösse des IST/SOLL Zustandes.
Systemadministrator	Der Systemadministrator hat eine Read-Only Sicht auf die Applikation. Für ihn ist das Dashboard relevant.
Application Owner	Betreibt die Applikation und hat vollen Zugriff auf das System.
Autorisierungsstelle	Prüft den SOLL Zustand und meldet Verstösse beim SOLL Zustand. Dies wird nicht mit er Applikation realisiert.
Abteilungsleitung	Erfasst den SOLL Zustand und kann diesen gegen den IST Zustand abgleichen.
Auftraggeber (Christof Jungo)	Experte für das Projekt.
Projektteam	Entwickler des Projekts.

5 Projektziele

5.1 Alle Stakeholder

Es ist das Ziel ein Webservice anzubieten, welcher den IST- und SOLL-Zustand eines Active Directorys aufzeigt und verschiedene Reports generiert.
Zudem soll die Applikation dem User ein übersichtliches Dashboard zur Verfügung stellen.

5.2 Auditor

Der Auditor ist dafür zuständig, dass Normen und Gesetzgebung eingehalten werden.
Er kann einen Report generieren lassen, welcher ihm ermöglicht den Zustand des Active Directorys zu bewerten.

5.3 Systemadministrator

Der Systemadministrator hat zusätzlich zum Dashboard die gleiche Sicht wie der Auditor. Er sieht so tagesaktuell Abweichung zwischen dem IST- und SOLL-Zustand seiner Objekte im Active Directory.

5.4 Application Owner

Der Application Owner hat Zugriff auf alle Einstellungen des Systems. Auf dem Dashboard müssen relevante Statusinformationen zum System ersichtlich sein. Der Application Owner stellt jederzeit die Verfügbarkeit der Applikation sicher und passt diese bei Bedarf an.

5.5 Autorisierungsstelle

Die Autorisierungsstelle prüft den SOLL Zustand und kann Reports ausführen.
Dieser Stakeholder wird nicht direkt in die Applikation integriert.

5.6 Abteilungsleitung

Die Abteilungsleitung bearbeitet den SOLL-Zustand.
Auf dem Dashboard ist primär der IST/SOLL-Vergleich ersichtlich.

5.7 Auftraggeber

Die Applikation soll ohne negative Einwirkung auf das vorgegebene System installiert werden können.

5.8 Projektteam

Ist verantwortlich für die Durchführung des Projektes und das Erreichen der gesteckten Projektziele.

6 Systemabgrenzung

6.1 Prozessumfeld

Die Applikation unterstützt die folgenden Geschäftsprozesse:
- Eintritt eines neuen Mitarbeiters und dessen Rechteverwaltung
- Austritt eines Mitarbeiters
- Mutation/Übertritt eines Mitarbeiters
- Korrektur von nichtautorisierten Berechtigungen durch den IST- und SOLL-Vergleich

Das Grundsätzliche Prozedere eines Eintrittes ist wie folgt:
Die HR-Abteilung stösst den Eintritt eines neuen Mitarbeiters an. Anschliessend wird die zuständige Abteilungsleitung des neuen Mitarbeiters das Rollenprofil bzw. die Berechtigungen festlegen (SOLL Profil). Diese Rollen und Berechtigungen werden der Autorisierungsstelle vorgelegt, welche diese prüft und freigibt. Die Autorisierungsstelle gibt anschliessend das Go für die Umsetzung an die Systemadministratoren des Active Directory als SOLL Profil oder meldet der Abteilungsleitung, dass zu viele Rollen/Berechtigungen gegenüber dem SOLL vorhanden sind. Die Systemadministratoren informieren nach der erfolgreichen Umsetzung die zuständige Abteilungsleitung bzw. dem neuen Benutzer, dass dies geschehen ist.
Die Systemadministratoren bearbeiten somit den IST-Zustand direkt im Active Directory, welcher anschliessend ausgelesen wird.

Bei einem Austritt informiert die HR-Abteilung direkt die Systemadministrator, welchen diesen User sperren und parallel dazu wird derselbe Prozess durchlaufen, um den SOLL-Zustand zu bereinigen und den User aus dem Active Directory anschliessend zu löschen.

Ein Übertritt oder eine Mutation läuft wie ein Eintritt ab, nur muss dabei die vorherige Abteilungsleitung, wie auch die neue Abteilungsleitung informiert und das SOLL angepasst werden.

Eine Korrektur von nichtautorisierten Berechtigungen bzw. einen Fehler im SOLL/IST Vergleich meldet der Auditor der Abteilungsleitung und der Autorisierungsstelle, um gegebenfalls das SOLL oder das Active Directory zu korrigieren.

Diese Prozesse unterscheiden sich natürlich von Firma zu Firma und es werden teilweise Stakeholder zusammengefasst. Autorisierungsstelle und Auditor oder Autorisierungsstelle und Abteilungsleitung können ein und dieselbe Person sein.

Der Prozess mit Ressourcen wie Sitzungszimmer, Service Accounts und Mailaccounts, welche oftmals in einem Audit als inaktiv auftauchen, ist nicht im Scope und wird direkt bei der Autorisierungsstelle abgehandelt, welche diese Accounts rausfiltern kann.
Weiterhin ist der Prüfungsmechanismus der Autorisierungsstelle nicht Bestandteil der Applikation.

Damit nach der Installation der Applikation der SOLL-Zustand einfach abgebildet werden kann, ist es für den Application Owner möglich ein CSV mit dem SOLL-Zustand nach vorgegebenem Format hochzuladen.
Alle Aktionen, die am SOLL verändert werden oder Filter, die gesetzt werden, werden protokolliert und sind nachvollziehbar vorhanden.

6.2 Systemumfeld

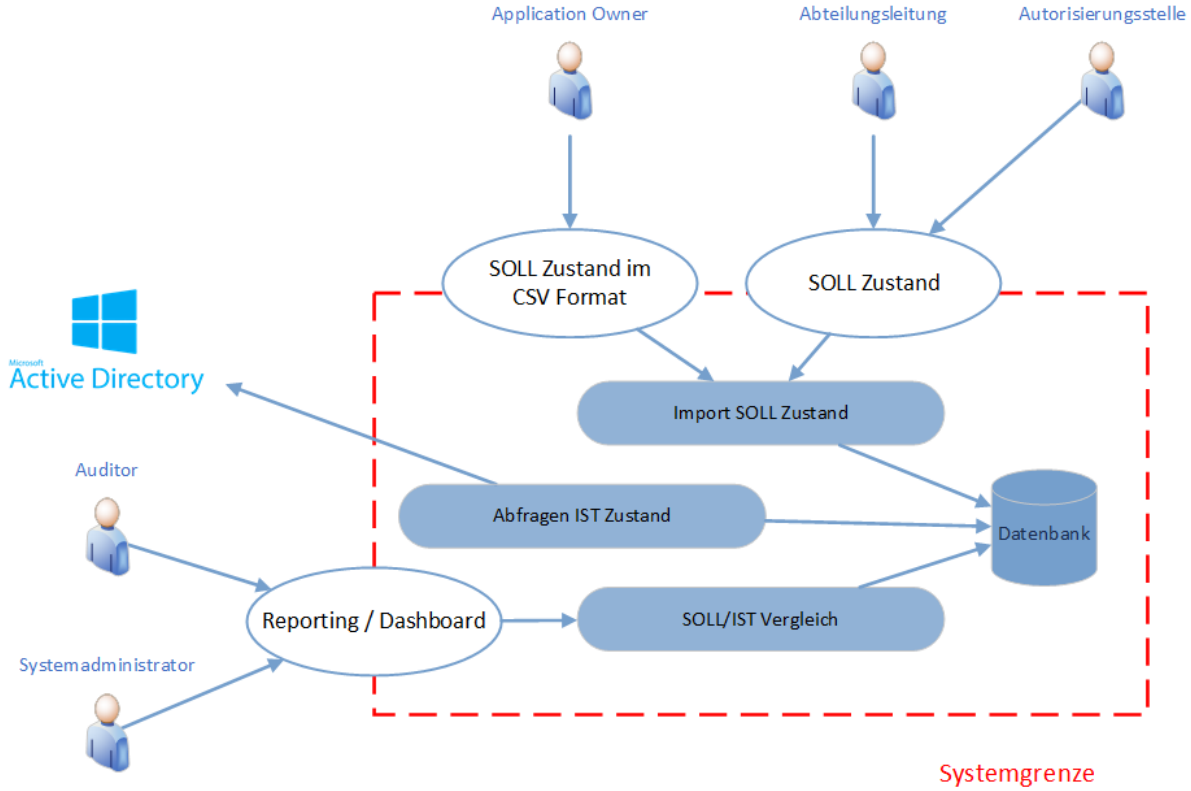

ABBILDUNG 1: ZEIGT DAS SYSTEMUMFELD DER APPLIKATION

Die Applikation holt den IST Zustand aus dem bestehenden Active Directory und der SOLL Zustand wird vom Application Owner bei der Installation bzw. von der Abteilungsleitung im täglichen Betrieb geliefert. Diese Zustände werden in der Datenbank gespeichert. Die Speicherung des IST Zustandes erfolgt historisch und ist somit jederzeit nachvollziehbar.
Der Auditor und der Systemadministrator greifen per Dashboard auf die Webapplikation zu und können bei Bedarf Reports generieren.
Die Autorisierungsstelle greift nur prüfend auf das SOLL zu. Dies wird jedoch nicht als Funktion realisiert, sondern muss im Prozess der Firma abgehandelt werden.

7 Anforderungen

7.1 Quellen und Vorgehen

Folgende Quellen werden bei der Ermittlung der Anforderungen verwendet:

Quelle	Beschreibung
Initialer Projektbeschrieb	Der initiale Projektbeschrieb liefert eine grobe Übersicht über die Funktionalität des zu erstellenden Tools.
Interview mit Auftraggeber	Der Auftraggeber Christof Jungo liefert detaillierte Anforderungen an das Tool und schränkt so den Projektbeschrieb weiter ein.
Projektteam	Da das Projekt nicht durch einen konkreten Anwender in Auftrag gegeben wurde, kann kein Interview mit einem Enduser durchgeführt werden. Stattdessen liefert das Projektteam selber Inputs und Ideen zu möglichen Anwendungsfällen.
Auftraggeber & Projektteam	Bei einem Brainstorming im ersten Meeting lieferten sowohl der Auftraggeber als auch das Projektteam Inputs, welche festgehalten wurden und so eine erste konkrete Richtung aufzeigten.

7.2 Funktionale Anforderungen

ID	Status	Prio	Beschreibung
F1			Allgemeiner User des Systems
F1.1	Freigegeben	O P2	Als User des Systems will ich, dass das Interface mehrere Sprachen unterstützt.

ID	Status	Prio	Beschreibung
F2			Auditor
F2.1	Freigegeben	M	Als Auditor will ich fertige Reports zur Verfügung haben, welche ich nur noch ausführen muss, sodass ich nicht nach den Informationen suchen muss.
F2.2	Freigegeben	M	Als Auditor will ich ein Vergleich des SOLL- und IST-Zustands machen können, sodass ich falsche Berechtigungen erkenne.
F2.3	Freigegeben	M	Als Auditor will ich eine Liste von deaktivierten Usern abrufen können.
F2.4	Freigegeben	M	Als Auditor will ich eine Liste von inaktiven Usern abrufen können, sodass ich sehe welche sich lange nicht mehr eingeloggt haben.
F2.5	Freigegeben	M	Als Auditor will ich einen Report im PDF-Format erstellen können.
F2.6	Freigegeben	M	Als Auditor will ich Zugriff auf eine History eines Users, sodass ermittelt werden kann, wann dieser eingetreten ist, verändert wurde etc.

ID	Status	Prio	Beschreibung
F3			Systemadministrator
F3.1	Freigegeben	M	Als Systemadministrator will ich auf dem Dashboard schnell für mich relevante Informationen wie die Zeit der letzten Statusabfrage sehen, sodass ich nicht danach suchen muss.
F3.2	Freigegeben	M	Als Systemadministrator will ich dieselben Möglichkeiten haben wie ein Auditor.
F3.3	Freigegeben	O P1	Als Systemadministrator will ich ein Paket haben um das Tool zu installieren, sodass dies nicht von Hand gemacht werden muss.

ID	Status	Prio	Beschreibung
F4			Application Owner
F4.1	Freigegeben	M	Als Application Owner will ich vollen Zugriff auf alle Funktionen des Systems, sodass ich die Applikation pflegen kann.
F4.2	Freigegeben	M	Als Application Owner will ich Zugriff auf ein Log, welches alle Aktionen der Anwender der Applikation loggt, so dass ich diese nachvollziehen kann.
F4.3	Freigegeben	O P3	Als Application Owner will ich die Möglichkeit haben, gefundene Diskrepanzen zwischen IST- und SOLL-Zustand direkt ins AD *remediaten* zu können, sodass dies nicht von Hand gemacht werden muss.
F4.4	Freigegeben	O P1	Als Application Owner will ich einen SOLL-Zustand in einem CSV importieren können.
F4.5	Freigegeben	O P2	Als Application Owner will ich einen SOLL-Zustand in ein CSV exportieren können.

7.3 Qualitätsanforderungen

ID	Status	Prio	Beschreibung
Q1			Sicherheit, Performance
Q1.1	Freigegeben	M	Alle von der Applikation verwendeten User und Passwörter müssen verschlüsselt gespeichert werden.
Q1.2	Freigegeben	M	Die Applikation darf keine Änderungen an der AD vornehmen.
Q1.3	Freigegeben	M	Die Applikation kann verschiedenen Benutzern verschiedene Rollen zuteilen.
Q1.4	Freigegeben	M	Ein Benutzer kann mehrere Rollen besitzen.
Q1.5	Freigegeben	M	Die Applikation kann Nested-AD-Gruppen bis zu 10 Stufen zurückverfolgen.
Q1.6	Freigegeben	M	Die Applikation läuft mit den Mindestanforderungen eines Windows Server 2016 und MariaDB.
Q1.7	Freigegeben	M	Alle Wartezeiten der Applikation werden angezeigt (Z.B. beim Laden des IST-SOLL-Vergleiches wird eine Sanduhr angezeigt o.ä.)
Q1.8	Freigegeben	M	Als User des Systems will ich, dass das Interface intuitiv bedienbar ist, sodass ich das Tool ohne Schulung verstehe.
Q1.9	Freigegeben	M	Als User des Systems will ich, dass das Interface performant ist, sodass ich nie auf einen Task warten muss oder dies deutlich sichtbar ist.

ID	Status	Prio	Beschreibung
Q2			Zuverlässigkeit, Benutzbarkeit
Q2.1	Freigegeben	M	Die Applikation hat eine Ausfallsicherheit von 95% pro Jahr zur Uptime des darunterliegenden Servers.
Q2.2	Freigegeben	M	Zur Verwendung der Applikation wird keine Schulung benötigt.
Q2.3	Freigegeben	M	Im Installationsordner der Applikation befindet sich eine Anleitung.
Q2.4	Freigegeben	M	Die Applikation kann via den gängigen Webbrowser angesteuert werden.

ID	Status	Prio	Beschreibung
Q3			Änderbarkeit (Wartbarkeit), Übertragbarkeit (Installation)
Q3.1	Freigegeben	M	Die Applikation ist in Powershell geschrieben.
Q3.2	Freigegeben	M	Der Code der Applikation ist kommentiert.
Q3.3	Freigegeben	M	Die Struktur der Applikation ist klar definiert.
Q3.4	Freigegeben	M	Die Installation der Applikation kann von jedem IT Systemtechniker ausgeführt werden.
Q3.5	Freigegeben	M	Zur Installation werden eine Anleitung und ein Script erstellt.

7.4 Mockups

7.4.1 Auditor

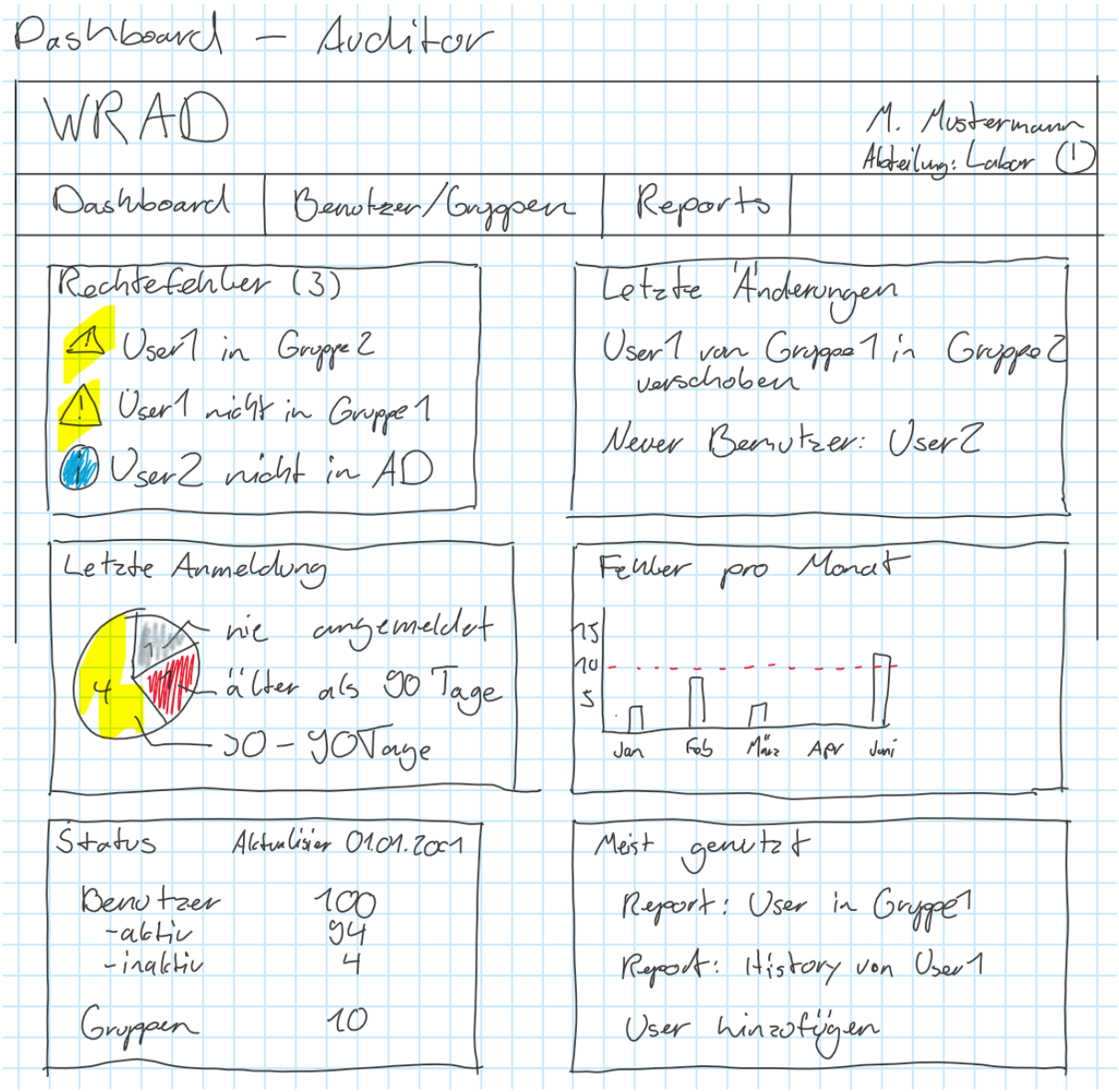

ABBILDUNG 2: MOCKUP «GUI AUDITOR»

7.4.2 Systemadministrator

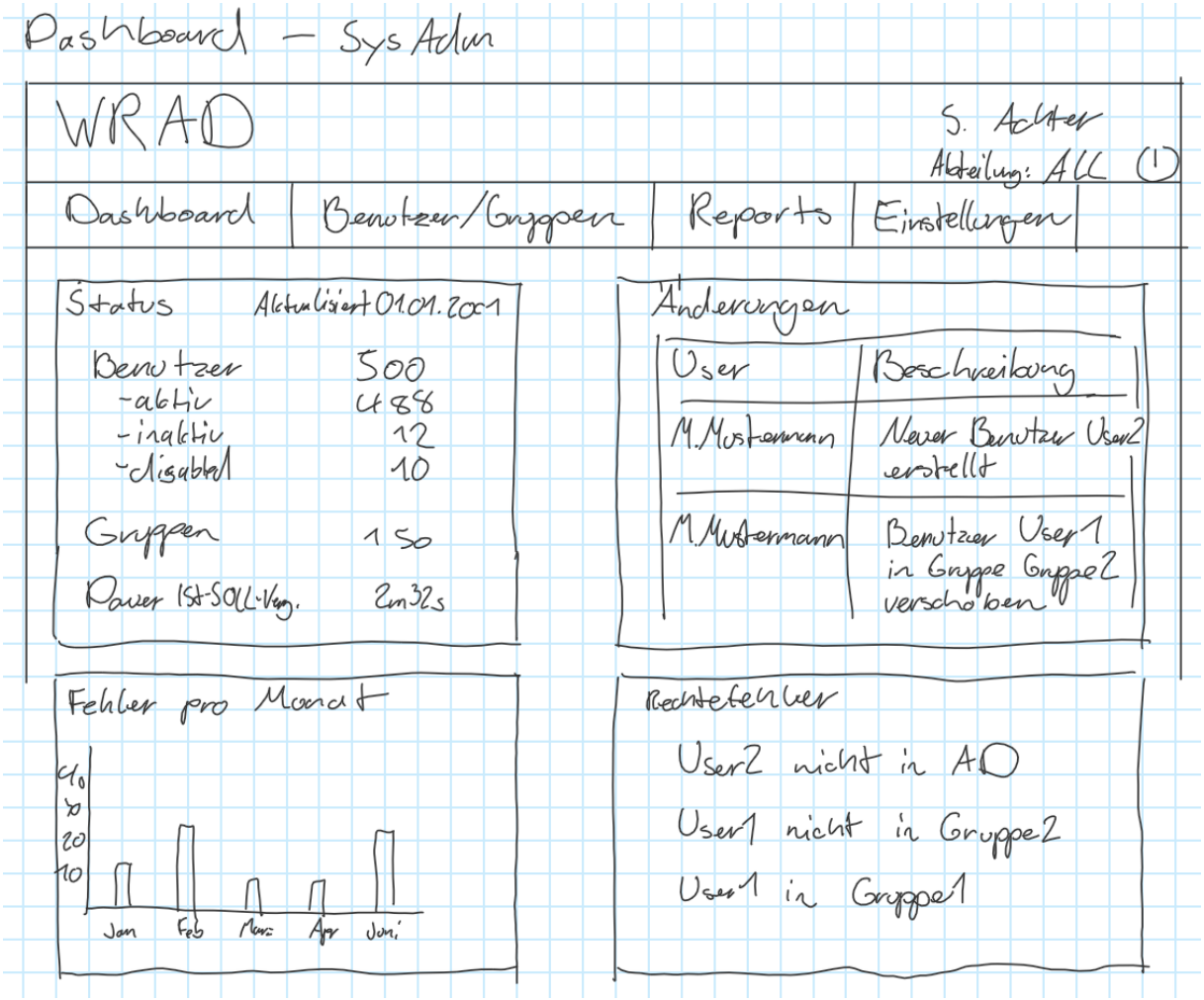

ABBILDUNG 3: MOCKUP «GUI SYSTEMADMINISTRATOR»

7.4.3 Application Owner

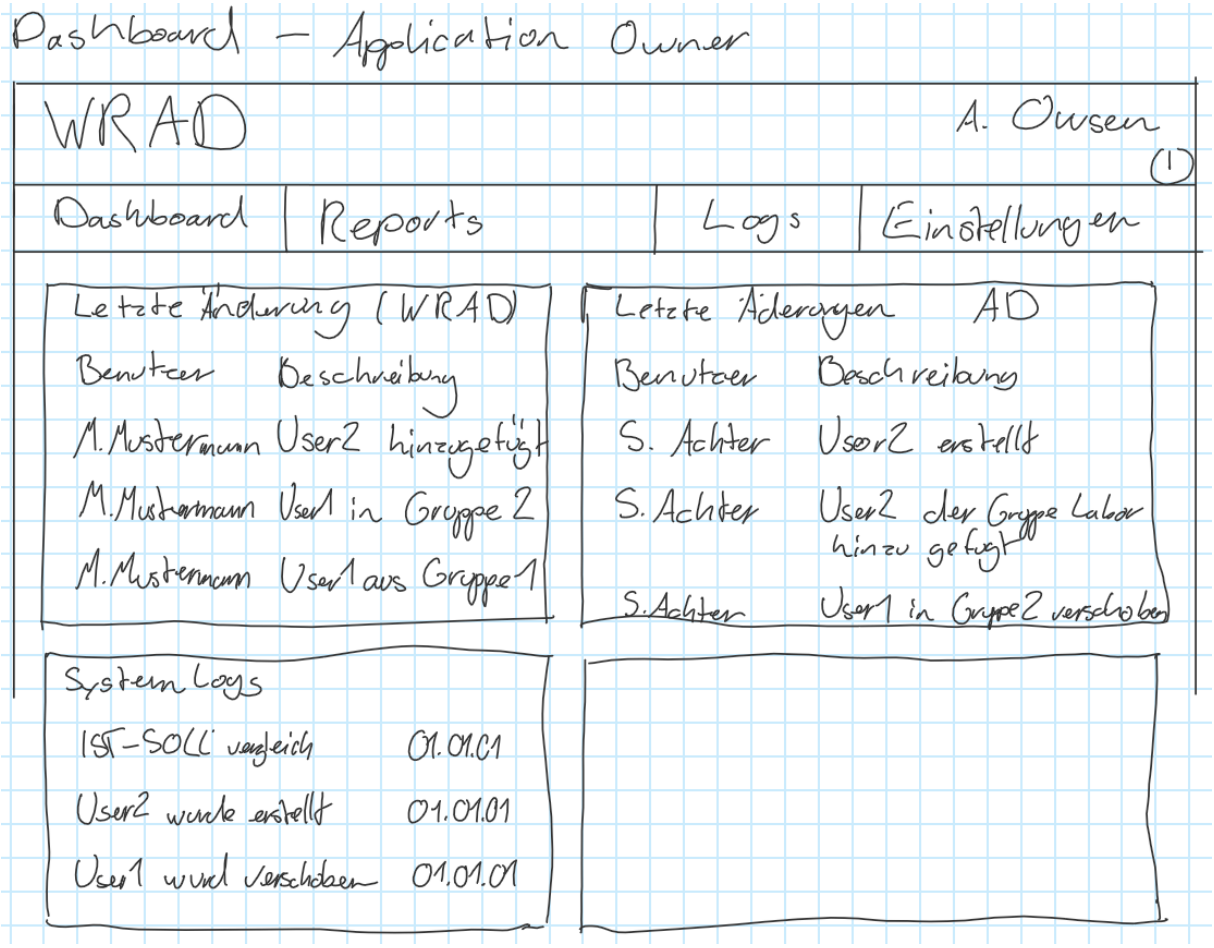

ABBILDUNG 4: MOCKUP «GUI APPLICATION OWNER»

7.4.4 Abteilungsleitung

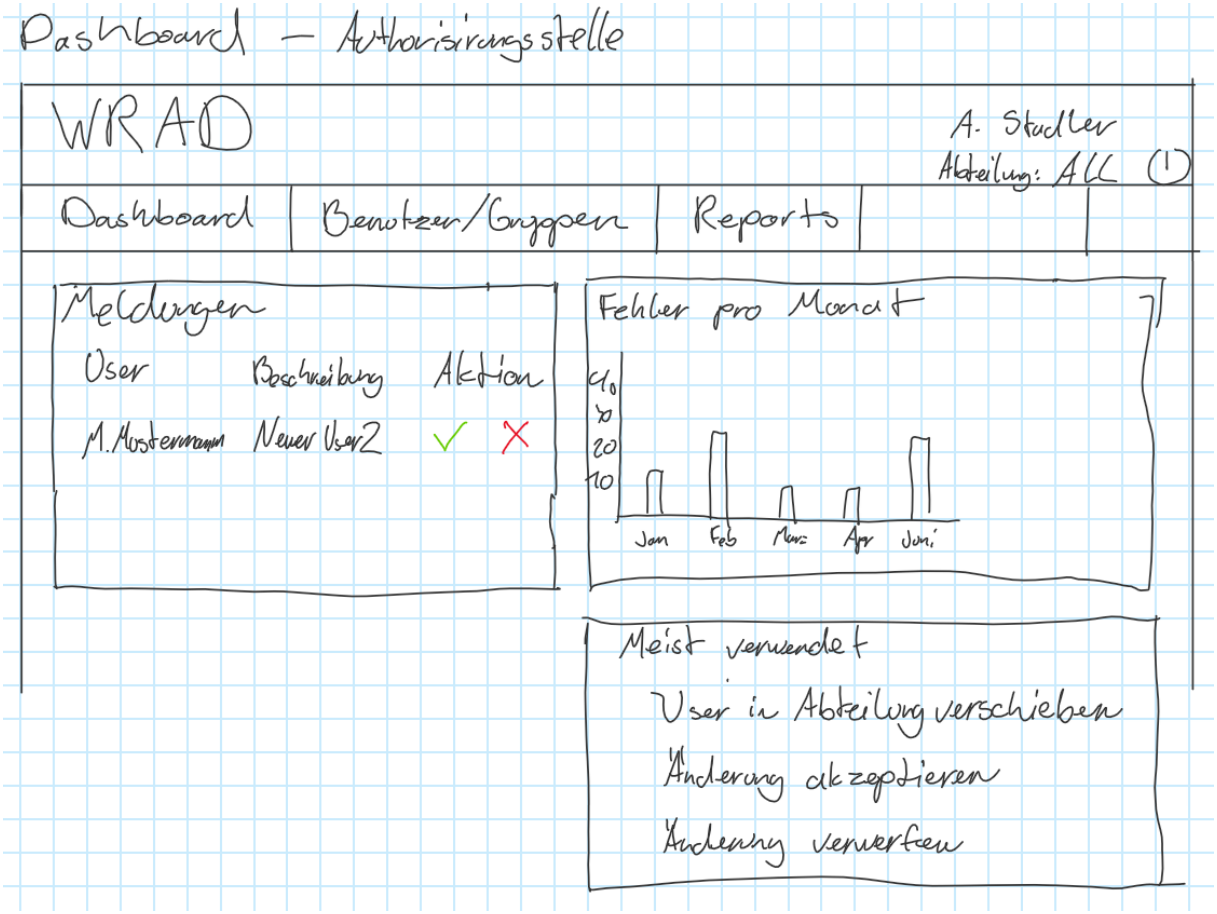

ABBILDUNG 5: MOCKUP «GUI ABTEILUNGSLEITUNG»

7.5 Randbedingungen

ID	Status	Prio	Beschreibung
R1			Randbedingungen
R1.1	Freigegeben	M	Das Projekt wird Agil geführt.
R1.2	Freigegeben	M	Das Projekt muss die definierten Meilensteine zeitgemäss erreichen
R1.3	Freigegeben	M	Das Projekt muss im geplanten Aufwand fertiggestellt werden.
R1.4	Freigegeben	M	Der vom Team geschriebenen Code wird OpenSource lizenziert.
R1.5	Freigegeben	M	Die Applikation läuft auf den Windows Server Versionen 2012R2 und 2016
R1.6	Freigegeben	M	Die Applikation läuft als Web-Service im internen Netzwerk

7.6 Datenmodell

7.6.1 Berechtigungen

Der Zugriff auf die verschiedenen Funktionen des Systems wird über folgende Rollen erfolgen.

ID	Name	Beschreibung
R01	Reports – Reports anzeigen	Darf die zugeordneten Reports anzeigen/ausdrucken.
R02	Benutzer – Benutzer erfassen	Darf einen User in WRAD erfassen.
R03	Benutzer – Benutzer bearbeiten	Darf einen User in WRAD bearbeiten.
R04	Benutzer – Benutzer entfernen	Darf einen User aus WRAD entfernen.
R05	Benutzer – Benutzer History anzeigen	Darf die History eines Benutzers des WRADs einsehen
R06	Benutzer – Benutzer anzeigen	Darf verschiedene Kategorien von WRAD Usern einsehen
R07	Gruppe – Gruppe erfassen	Darf eine Gruppe in WRAD erfassen.
R08	Gruppe – Gruppe bearbeiten	Darf eine Gruppe in WRAD bearbeiten.
R09	Gruppe – Gruppe entfernen	Darf eine Gruppe aus WRAD entfernen.
R10	Gruppe – Gruppen History anzeigen	Darf die History einer WRAD Gruppen einsehen.
R11	Gruppe – Gruppe anzeigen	Darf verschiedene Kategorien von WRAD Gruppen einsehen
R12	Rechtefehler anzeigen	Darf den IST/SOLL-Vergleich einsehen und wie viele Fehler es im Moment gibt anzeigen.
R13	Log anzeigen	Darf den vom System generierten Log einsehen.
R14	WRAD Einstellungen bearbeiten	Darf die Einstellungen des Systems bearbeiten.
R15	CSV exportieren/importieren	Darf die Basis der AD als CSV (IST-Zustand) importieren oder der Stand des WRAD (SOLL-Zustand) exportieren.

7.6.2 Rollenmatrix

Benutzer / Berechtigung	Abteilungsleiter	Auditor	System Administrator	Application Owner
R01	X	X	X	X
R02	X			X
R03	X			X
R04	X			X
R05	X	X	X	X
R06	X	X	X	X
R07	X			X
R08	X			X
R09	X			X
R10	X	X	X	X
R11	X	X	X	X
R12	X	X	X	X
R13				X
R14				X
R15				X

8 Glossar

Begriff	Beschreibung
AD	Active Directory
CSV	Das Dateiformat CSV steht für Comma-Separated Values und beschreibt den Aufbau einer Textdatei zur Speicherung von Daten.
HR	Human Resources
MariaDB	MariaDB ist eine relationale Datenbank.
Remediate	«Ein Defizit oder ein Problem korrigieren oder verbessern» / «Ein gewünschter Zustand abbilden».
Verwaiste Accounts	Accounts gelten als verwaist, wenn diese über einen Zeitraum nicht mehr gebraucht werden.

9 Literaturverzeichnis

10 Abbildungsverzeichnis