VAES - Testprotokoll & Automatisierungsplan

Version: 1.0 **Stand:** 2026-02-11 **Projekt:** Vereins-Arbeitsstunden-Erfassungssystem (VAES) v1.3 **Autor:** QA-Team / Software Tester **Zielgruppe:** Manueller Tester, Test-Manager, Entwicklungsteam

---

Inhaltsverzeichnis

---

1. Einleitung & Zielsetzung

1.1 Zweck

Dieses Testprotokoll definiert eine strukturierte Vorgehensweise zur vollstaendigen funktionalen Pruefung der VAES-Anwendung. Es deckt alle Rollen, Workflows, Sicherheitsmechanismen und Geschaeftsregeln ab.

1.2 Teststrategie

Ebene	Methode	Werkzeug	Abdeckung
Unit-Tests	Automatisiert	PHPUnit	Modelle, Services, Helper
Controller-Tests	Automatisiert (geplant)	PHPUnit + HTTP-Mocks	Alle Endpunkte
API-Tests	Automatisiert (geplant)	cURL / Guzzle Scripts	Alle POST-Aktionen
UI-Tests	Manuell + teilautomatisiert	Browser + Selenium (geplant)	Alle Seiten
Sicherheitstests	Manuell + automatisiert	Browser DevTools + Scripts	CSRF, XSS, SQLi
E-Mail-Tests	Manuell	Mailhog / echtes SMTP	Alle Trigger

1.3 Bestehende automatisierte Abdeckung

Bereich	Tests	Status
Modelle (User, WorkEntry, Role, Category)	47	Vorhanden
Services (Auth, Workflow, RateLimit, Settings)	77	Vorhanden
Helper (Security, View, Version)	65	Vorhanden
Integration (Auth-Flow, Workflow-Lifecycle)	23	Vorhanden
Controller (HTTP-Ebene)	**0**	**Luecke**
Repositories (Datenbank)	**0**	**Luecke**
Middleware (Auth, Role, CSRF)	**0**	**Luecke**
Services (Email, PDF, CSV, Import, TOTP)	**0**	**Luecke**

Gesamt automatisiert: 212 Tests **Manuelle Testszenarien:** 100+ (dokumentiert in `tests/MANUAL_TESTS.md`)

---

2. Testumgebung & Voraussetzungen

2.1 Testumgebung

Eigenschaft	Wert
Server	Lokaler PHP-Entwicklungsserver oder Strato Staging
PHP-Version	8.x
Datenbank	MySQL 8.4 (Testdatenbank mit Seed-Daten)
Browser	Chrome (aktuell), Firefox (aktuell)
E-Mail	Mailhog (lokal) oder echtes SMTP (Staging)

2.2 Test-Accounts

ID	Rolle	E-Mail	Mitgliedsnr.	Passwort
T1	Administrator	admin@test.de	ADMIN001	Test123!
T2	Pruefer 1	pruefer1@test.de	M001	Test123!
T3	Pruefer 2	pruefer2@test.de	M002	Test123!
T4	Mitglied	mitglied@test.de	M003	Test123!
T5	Erfasser	erfasser@test.de	M004	Test123!
T6	Auditor	auditor@test.de	M005	Test123!

2.3 Vorbereitung vor Testdurchfuehrung

1. Datenbank zuruecksetzen: `scripts/database/create_database.sql` ausfuehren
2. Test-Accounts anlegen (oder via Seed-Daten)
3. SMTP konfigurieren (Mailhog oder echter Mailserver)
4. Alle 2FA-Setups fuer Test-Accounts durchfuehren
5. Mindestens 5 Kategorien aktiv
6. Soll-Stunden-Feature aktiviert

---

3. Testmatrix: Rollen und Berechtigungen

3.1 Funktionsmatrix

Funktion	Mitglied	Erfasser	Pruefer	Auditor	Admin
Login / 2FA	X	X	X	X	X
Dashboard	X	X	X	X	X
Eigene Eintraege sehen	X	X	X	-	X
Eintrag erstellen (eigene)	X	X	X	-	X
Eintrag erstellen (fuer Andere)	-	X	X	-	X
Eintrag bearbeiten (Entwurf)	X	X	X	-	X
Eintrag einreichen	X	X	X	-	X
Eintrag zurueckziehen	X	X	X	-	X
Eintrag stornieren	X	X	X	-	X
Eintrag reaktivieren	X	X	X	-	X
Dialog-Nachricht schreiben	X	X	X	-	X
Berichte eigene Stunden	X	X	X	-	X
Pruef-Funktionen:					
Pruef-Liste sehen	-	-	X	-	X
Antrag freigeben (fremde)	-	-	X	-	X
Antrag ablehnen (fremde)	-	-	X	-	X
Rueckfrage stellen	-	-	X	-	X
Korrektur nach Freigabe	-	-	X	-	X
Berichte alle Mitglieder	-	-	X	-	X
Admin-Funktionen:					
Benutzerverwaltung	-	-	-	-	X
Kategorieverwaltung	-	-	-	-	X
Soll-Stunden-Verwaltung	-	-	-	-	X
Systemeinstellungen	-	-	-	-	X
CSV-Import	-	-	-	-	X
Audit:					
Audit-Trail einsehen	-	-	-	X	X
Geloeschte Eintraege sehen	-	-	-	X	X
PDF-/CSV-Export	X	X	X	-	X

3.2 Kritische Zugriffsverbote (MUSS getestet werden)

Aktion	Gesperrt fuer	Test-ID
Eigenen Antrag freigeben	Pruefer, Admin	SELF-01..05
Admin-Bereich oeffnen	Mitglied, Erfasser, Auditor	ACC-01..03
Pruef-Liste oeffnen	Mitglied, Erfasser	ACC-04..05
Audit-Log oeffnen	Mitglied, Erfasser, Pruefer	ACC-06..08
Fremde Eintraege bearbeiten	Alle (ausser via Korrektur)	ACC-09

---

4. Testprotokoll Rolle: Mitglied

Test-Account: T4 (mitglied@test.de / M003)

4.1 Anmeldung & Navigation

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
M-AUTH-01	Login als Mitglied	1. `/login` oeffnen 2. mitglied@test.de / Test123! eingeben 3. 2FA-Code eingeben	Dashboard wird angezeigt, Begruessung "Willkommen" sichtbar	[ ]	
M-AUTH-02	Navigation pruefen	1. Navbar inspizieren	Sichtbar: Dashboard, Arbeitsstunden, Berichte. NICHT sichtbar: Verwaltung, Pruefung, Audit	[ ]	
M-AUTH-03	Breadcrumbs pruefen	1. Auf Arbeitsstunden klicken 2. Breadcrumb pruefen	Breadcrumb zeigt "Dashboard > Arbeitsstunden"	[ ]	
M-AUTH-04	Logout	1. "Abmelden" klicken	Weiterleitung zu Login-Seite, Session beendet	[ ]	

4.2 Dashboard

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
M-DASH-01	Dashboard-Inhalt	1. Dashboard aufrufen	Eigene Statistiken: Anzahl Eintraege, Stunden, Status-Verteilung	[ ]	
M-DASH-02	Soll-/Ist-Vergleich	1. Dashboard pruefen	Soll-Stunden und Ist-Stunden werden angezeigt (wenn aktiviert)	[ ]	
M-DASH-03	Ungelesene Dialoge	1. Navbar pruefen	Badge mit Anzahl ungelesener Dialoge (falls vorhanden)	[ ]	
M-DASH-04	Dialog-Polling	1. Dashboard offen lassen 2. In anderem Browser als Pruefer Rueckfrage stellen 3. 60 Sekunden warten	Badge-Zaehler aktualisiert sich, Dashboard laedt neu	[ ]	

4.3 Arbeitsstunden-Erfassung

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
M-ENT-01	Eintrag erstellen	1. `/entries/create` aufrufen 2. Datum, Stunden (4.5), Kategorie waehlen 3. "Speichern"	Eintrag als Entwurf gespeichert, Antragsnummer zugewiesen (Format YYYY-NNNNN)	[ ]	
M-ENT-02	Pflichtfelder pruefen	1. Formular leer absenden	Validierungsfehler fuer Datum, Stunden, Kategorie	[ ]	
M-ENT-03	Eintrag bearbeiten	1. Entwurf oeffnen 2. Stunden aendern 3. "Speichern"	Aenderungen gespeichert, Audit-Eintrag erstellt	[ ]	
M-ENT-04	Eintrag anzeigen	1. Eintrag in Liste anklicken	Detailansicht mit allen Feldern, Breadcrumb "Dashboard > Arbeitsstunden > Eintrag YYYY-NNNNN"	[ ]	
M-ENT-05	Eintrag loeschen (Soft-Delete)	1. Entwurf oeffnen 2. "Loeschen" klicken 3. Bestaetigen	Eintrag nicht mehr in Liste, aber nicht physisch geloescht	[ ]	
M-ENT-06	Eintrag einreichen	1. Entwurf oeffnen 2. "Einreichen" klicken	Status wechselt zu "Eingereicht", E-Mail an Pruefer gesendet	[ ]	
M-ENT-07	Eingereichten Eintrag nicht editierbar	1. Eingereichten Eintrag oeffnen	Kein "Bearbeiten"-Button, keine Editiermoeglichkeit	[ ]	
M-ENT-08	Eintrag zurueckziehen	1. Eingereichten Eintrag oeffnen 2. "Zurueckziehen"	Status wechselt zurueck zu "Entwurf"	[ ]	
M-ENT-09	Eintrag stornieren	1. Eingereichten Eintrag oeffnen 2. "Stornieren"	Status wechselt zu "Storniert"	[ ]	
M-ENT-10	Stornierten Eintrag reaktivieren	1. Stornierten Eintrag oeffnen 2. "Reaktivieren"	Status wechselt zurueck zu "Entwurf"	[ ]	
M-ENT-11	Freigegebenen Eintrag pruefen	1. Freigegebenen Eintrag oeffnen	Nur Ansicht, keine Aktionen moeglich (Endstatus)	[ ]	
M-ENT-12	Abgelehnten Eintrag pruefen	1. Abgelehnten Eintrag oeffnen	Nur Ansicht, Ablehnungsgrund sichtbar, keine Aktionen	[ ]	

4.4 Dialog-System

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
M-DLG-01	Auf Rueckfrage antworten	1. Eintrag "In Klaerung" oeffnen 2. Antwort eingeben 3. "Nachricht senden"	Antwort gespeichert, Frage als beantwortet markiert	[ ]	
M-DLG-02	Dialog-Verlauf sichtbar	1. Eintrag mit Dialog oeffnen	Gesamter Dialog chronologisch sichtbar, Fragen/Antworten unterscheidbar	[ ]	
M-DLG-03	Keine Loesch-Option	1. Dialog-Nachrichten pruefen	Kein Loeschen-/Bearbeiten-Button fuer Nachrichten (Revisionssicherheit)	[ ]	
M-DLG-04	Ungelesen-Badge	1. Neue Rueckfrage erhalten (anderer Browser) 2. Navbar pruefen	Ungelesen-Badge zeigt aktuelle Anzahl	[ ]	
M-DLG-05	Gelesen-Status	1. Eintrag mit ungelesener Nachricht oeffnen 2. Navbar pruefen	Badge-Zaehler reduziert sich	[ ]	

4.5 Berichte

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
M-REP-01	Eigene Berichte	1. `/reports` aufrufen	Nur eigene Eintraege sichtbar, Zusammenfassung der Stunden	[ ]	
M-REP-02	Filter nach Zeitraum	1. Datum-Filter setzen	Nur Eintraege im gewaehlten Zeitraum	[ ]	
M-REP-03	Filter nach Status	1. Status-Filter setzen	Nur Eintraege mit gewaehltem Status	[ ]	
M-REP-04	PDF-Export	1. "PDF exportieren" klicken	PDF-Download mit korrekten Daten	[ ]	
M-REP-05	CSV-Export	1. "CSV exportieren" klicken	CSV-Download, in Excel oeffenbar (UTF-8-BOM)	[ ]	

4.6 Zugriffsbeschraenkungen

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
M-ACC-01	Admin-Bereich gesperrt	1. URL `/admin/users` direkt aufrufen	Weiterleitung zu Dashboard, Fehlermeldung "Keine Berechtigung"	[ ]	
M-ACC-02	Pruef-Liste gesperrt	1. URL `/review` direkt aufrufen	Weiterleitung zu Dashboard, Fehlermeldung	[ ]	
M-ACC-03	Audit-Log gesperrt	1. URL `/audit` direkt aufrufen	Weiterleitung zu Dashboard, Fehlermeldung	[ ]	
M-ACC-04	Fremden Eintrag aufrufen	1. URL `/entries/{fremde-id}` direkt aufrufen	Fehlermeldung oder Zugriffsverweigerung	[ ]	

---

5. Testprotokoll Rolle: Erfasser

Test-Account: T5 (erfasser@test.de / M004)

5.1 Erfasser-spezifische Funktionen

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
E-ENT-01	Eintrag fuer anderes Mitglied erstellen	1. `/entries/create` aufrufen 2. Mitglied-Auswahl sichtbar? 3. Anderes Mitglied waehlen 4. Daten eingeben, speichern	Eintrag erstellt mit user_id des gewaehlten Mitglieds, created_by_user_id = Erfasser	[ ]	
E-ENT-02	Mitglied-Auswahl vorhanden	1. Erstell-Formular pruefen	Dropdown/Auswahl fuer Mitglied ist vorhanden	[ ]	
E-ENT-03	Eigenen Eintrag erstellen	1. Eigenen Eintrag erstellen	Funktioniert wie bei Rolle Mitglied	[ ]	
E-ENT-04	Fremdeintrag einreichen	1. Fuer anderes Mitglied erstellten Eintrag einreichen	Status wechselt zu "Eingereicht", E-Mail an Pruefer	[ ]	

5.2 Zugriffsbeschraenkungen

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
E-ACC-01	Pruef-Liste gesperrt	1. URL `/review` direkt aufrufen	Weiterleitung zu Dashboard	[ ]	
E-ACC-02	Admin-Bereich gesperrt	1. URL `/admin/users` direkt aufrufen	Weiterleitung zu Dashboard	[ ]	
E-ACC-03	Kann nicht freigeben	1. URL `/entries/{id}/approve` per POST aufrufen (curl)	Fehlermeldung oder 403	[ ]	

6. Testprotokoll Rolle: Pruefer

Test-Account: T2 (pruefer1@test.de / M001)

6.1 Pruef-Workflow

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
P-REV-01	Pruef-Liste anzeigen	1. `/review` aufrufen	Liste aller eingereichten/in-Klaerung-Eintraege anderer Mitglieder	[ ]	
P-REV-02	Eintrag aus Pruef-Liste oeffnen	1. Eintrag anklicken	Detailansicht mit Breadcrumb "Dashboard > Pruefung > Eintrag YYYY-NNNNN"	[ ]	
P-REV-03	Eintrag freigeben	1. Eingereichten Antrag eines anderen Mitglieds oeffnen 2. "Freigeben" klicken	Status "Freigegeben", E-Mail an Mitglied	[ ]	
P-REV-04	Eintrag ablehnen mit Begruendung	1. Eintrag oeffnen 2. Ablehnungsgrund eingeben 3. "Ablehnen"	Status "Abgelehnt", Grund gespeichert, E-Mail an Mitglied	[ ]	
P-REV-05	Ablehnung ohne Begruendung	1. Eintrag oeffnen 2. "Ablehnen" ohne Text	Fehlermeldung: Begruendung ist Pflicht	[ ]	
P-REV-06	Rueckfrage stellen	1. Eintrag oeffnen 2. Rueckfrage-Text eingeben 3. "Rueckfrage"	Status "In Klaerung", Dialog-Nachricht erstellt, E-Mail an Mitglied	[ ]	
P-REV-07	Eintrag nach Klaerung freigeben	1. Eintrag "In Klaerung" mit beantworteter Frage oeffnen 2. "Freigeben"	Status "Freigegeben"	[ ]	
P-REV-08	Zurueck zur Ueberarbeitung	1. Eintrag oeffnen 2. "Zurueck zur Ueberarbeitung"	Status wechselt, Dialog bleibt erhalten	[ ]	

6.2 Korrektur nach Freigabe

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
P-KORR-01	Stunden korrigieren	1. Freigegebenen Antrag eines Anderen oeffnen 2. Neue Stundenzahl eingeben 3. Begruendung eingeben 4. "Korrektur speichern"	Stunden geaendert, is_corrected=true, Original-Stunden gespeichert, E-Mail	[ ]	
P-KORR-02	Korrektur ohne Begruendung	1. Korrektur ohne Text versuchen	Fehlermeldung: Begruendung Pflicht	[ ]	
P-KORR-03	Korrektur-Anzeige	1. Korrigierten Eintrag oeffnen	Original-Stunden und neue Stunden sichtbar, Korrektur-Vermerk	[ ]	

6.3 Selbstgenehmigung (KRITISCH)

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
P-SELF-01	Eigenen Antrag freigeben	1. Eigenen Antrag einreichen 2. "Freigeben" versuchen	BLOCKIERT: "Eigene Antraege koennen nicht selbst genehmigt werden."	[ ]	
P-SELF-02	Eigenen Antrag ablehnen	1. Eigenen Antrag einreichen 2. "Ablehnen" versuchen	BLOCKIERT	[ ]	
P-SELF-03	Eigene Rueckfrage	1. Eigenen Antrag einreichen 2. "Rueckfrage" versuchen	BLOCKIERT	[ ]	
P-SELF-04	Eigenen Fremdeintrag pruefen	1. Als Pruefer+Erfasser Eintrag fuer anderes Mitglied erstellen 2. Selbst pruefen	BLOCKIERT: "Von Ihnen erstellte Antraege koennen nicht von Ihnen selbst geprueft werden."	[ ]	

6.4 Zugriffsbeschraenkungen

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
P-ACC-01	Admin-Bereich gesperrt	1. `/admin/users` direkt aufrufen	Weiterleitung zu Dashboard	[ ]	
P-ACC-02	Berichte aller Mitglieder	1. `/reports` aufrufen	Kann Berichte fuer alle Mitglieder filtern	[ ]	

---

7. Testprotokoll Rolle: Auditor

Test-Account: T6 (auditor@test.de / M005)

7.1 Audit-Trail

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
A-AUD-01	Audit-Log anzeigen	1. `/audit` aufrufen	Chronologische Liste aller System-Aktionen	[ ]	
A-AUD-02	Filter nach Benutzer	1. Benutzer-Filter setzen	Nur Aktionen des gewaehlten Benutzers	[ ]	
A-AUD-03	Filter nach Aktion	1. Aktions-Filter (create, update, delete, login, status_change, etc.)	Nur Eintraege der gewaehlten Aktion	[ ]	
A-AUD-04	Filter nach Zeitraum	1. Datums-Filter setzen	Nur Eintraege im gewaehlten Zeitraum	[ ]	
A-AUD-05	Detail-Ansicht	1. Audit-Eintrag anklicken	Alte/neue Werte (JSON), IP-Adresse, User-Agent, Beschreibung, Metadaten sichtbar	[ ]	
A-AUD-06	Geloeschte Eintraege sichtbar	1. Audit-Log nach "delete"-Aktionen filtern	Soft-Delete-Eintraege sind sichtbar mit Zeitstempel	[ ]	
A-AUD-07	Breadcrumbs korrekt	1. Audit-Detail oeffnen	Breadcrumb zeigt "Dashboard > Audit-Trail > Details"	[ ]	

7.2 Nur-Lese-Zugriff

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
A-RO-01	Keine Aenderungsmoeglichkeiten	1. Alle Audit-Seiten durchgehen	Keine Buttons fuer Erstellen, Bearbeiten, Loeschen	[ ]	
A-RO-02	Admin-Bereich gesperrt	1. `/admin/users` direkt aufrufen	Weiterleitung zu Dashboard	[ ]	
A-RO-03	Pruef-Liste gesperrt	1. `/review` direkt aufrufen	Weiterleitung zu Dashboard	[ ]	
A-RO-04	Arbeitsstunden gesperrt	1. `/entries` direkt aufrufen	Abhaengig von Rollenkombination - wenn nur Auditor, kein Zugriff auf eigene Eintraege	[ ]	

8. Testprotokoll Rolle: Administrator

Test-Account: T1 (admin@test.de / ADMIN001)

8.1 Benutzerverwaltung

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
ADM-USR-01	Benutzer-Liste	1. `/admin/users` aufrufen	Liste aller Benutzer mit Rollen, Status	[ ]	
ADM-USR-02	Benutzer suchen	1. Suchfeld nutzen	Filterung nach Name/E-Mail/Mitgliedsnummer	[ ]	
ADM-USR-03	Benutzer nach Rolle filtern	1. Rollen-Filter nutzen	Nur Benutzer mit gewaehlter Rolle	[ ]	
ADM-USR-04	Benutzer anlegen	1. "Neuer Benutzer" klicken 2. Pflichtfelder ausfuellen 3. Speichern	Benutzer erstellt, Einladungs-E-Mail gesendet	[ ]	
ADM-USR-05	Benutzer-Detail	1. Benutzer anklicken	Detailseite mit allen Informationen, Breadcrumb korrekt	[ ]	
ADM-USR-06	Rollen zuweisen	1. Benutzer-Detail oeffnen 2. Rolle hinzufuegen 3. Speichern	Rolle zugewiesen, Audit-Log-Eintrag	[ ]	
ADM-USR-07	Rolle entziehen	1. Benutzer-Detail oeffnen 2. Rolle entfernen 3. Speichern	Rolle entzogen, Audit-Log-Eintrag	[ ]	
ADM-USR-08	Benutzer deaktivieren	1. "Deaktivieren" klicken	Benutzer kann sich nicht mehr einloggen	[ ]	
ADM-USR-09	Benutzer reaktivieren	1. Deaktivierten Benutzer oeffnen 2. "Aktivieren"	Benutzer kann sich wieder einloggen	[ ]	
ADM-USR-10	Einladung erneut senden	1. "Erneut einladen" klicken	Neue Einladungs-E-Mail gesendet mit neuem Token	[ ]	

8.2 CSV-Import

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
ADM-IMP-01	Gueltige CSV importieren	1. `/admin/users/import` 2. CSV mit Pflichtfeldern hochladen	Benutzer erstellt, Einladungen gesendet, Ergebnis-Seite	[ ]	
ADM-IMP-02	CSV ohne Pflichtfelder	1. CSV ohne `mitgliedsnummer` hochladen	Fehlermeldung: Pflichtfeld fehlt	[ ]	
ADM-IMP-03	CSV mit ungueltiger E-Mail	1. CSV mit "nicht-gueltig" als E-Mail	Zeile als Fehler gemeldet, andere Zeilen verarbeitet	[ ]	
ADM-IMP-04	CSV-Update bestehender Mitglieder	1. CSV mit vorhandenen Mitgliedsnummern	Stammdaten aktualisiert (kein Duplikat), Audit-Eintrag	[ ]	
ADM-IMP-05	Semikolon-Delimiter	1. Excel-CSV mit ";" statt ","	Automatische Erkennung, Import funktioniert	[ ]	
ADM-IMP-06	Import-Ergebnis pruefen	1. Nach Import Ergebnis-Seite	Anzahl erstellt, aktualisiert, Fehler; Details pro Zeile	[ ]	

8.3 Kategorieverwaltung

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
ADM-CAT-01	Kategorien anzeigen	1. `/admin/categories` aufrufen	Alle Kategorien mit Sortierung, Status	[ ]	
ADM-CAT-02	Kategorie erstellen	1. Name und Beschreibung eingeben 2. "Erstellen"	Neue Kategorie aktiv, am Ende der Liste	[ ]	
ADM-CAT-03	Kategorie bearbeiten	1. Kategorie-Name aendern 2. Speichern	Name geaendert, Audit-Eintrag	[ ]	
ADM-CAT-04	Kategorie deaktivieren	1. "Deaktivieren" klicken	Kategorie nicht mehr in Erfassungsformular waehlbar	[ ]	
ADM-CAT-05	Deaktivierte Kategorie bei alten Eintraegen	1. Eintrag mit deaktivierter Kategorie oeffnen	Kategorie-Name weiterhin sichtbar	[ ]	
ADM-CAT-06	Kategorie-Reihenfolge aendern	1. Drag-and-Drop oder Reihenfolge aendern	Neue Sortierung gespeichert	[ ]	
ADM-CAT-07	Kategorie reaktivieren	1. Deaktivierte Kategorie aktivieren	Kategorie wieder im Formular waehlbar	[ ]	

8.4 Soll-Stunden-Verwaltung

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
ADM-TGT-01	Uebersicht	1. `/admin/targets` aufrufen	Alle Mitglieder mit Soll-Stunden fuer aktuelles Jahr	[ ]	
ADM-TGT-02	Individuelles Soll setzen	1. Mitglied waehlen 2. Soll-Stunden eingeben 3. Speichern	Individueller Wert gespeichert	[ ]	
ADM-TGT-03	Mitglied befreien	1. "Befreit" ankreuzen 2. Speichern	Kein Soll angezeigt fuer dieses Mitglied	[ ]	
ADM-TGT-04	Massen-Update	1. Bulk-Update mit Standard-Wert	Alle nicht-individuellen Soll-Werte aktualisiert	[ ]	
ADM-TGT-05	Breadcrumbs korrekt	1. Mitglied-Soll bearbeiten	"Dashboard > Verwaltung > Soll-Stunden > [Name]"	[ ]	

8.5 Systemeinstellungen

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
ADM-SET-01	Einstellungen anzeigen	1. `/admin/settings` aufrufen	Alle konfigurierbaren Einstellungen gruppiert	[ ]	
ADM-SET-02	Einstellung aendern	1. Wert aendern 2. Speichern	Neuer Wert gespeichert, Audit-Log-Eintrag mit altem/neuem Wert	[ ]	
ADM-SET-03	Soll-Stunden deaktivieren	1. target_hours_enabled auf false 2. Dashboard als Mitglied	Keine Soll-/Ist-Anzeige auf Dashboard	[ ]	
ADM-SET-04	Test-E-Mail senden	1. "Test-E-Mail senden" klicken	E-Mail wird empfangen, Bestaetigung angezeigt	[ ]	
ADM-SET-05	Feld-Konfiguration: hidden	1. Feld "Projekt" auf "hidden" setzen 2. Erfassungsformular pruefen	Feld nicht sichtbar	[ ]	
ADM-SET-06	Feld-Konfiguration: required	1. Feld "Beschreibung" auf "required" 2. Formular ohne Beschreibung absenden	Server-Validierungsfehler	[ ]	

8.6 Admin als Pruefer

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
ADM-REV-01	Pruef-Liste sichtbar	1. `/review` aufrufen	Admin hat Zugriff auf Pruef-Funktionen	[ ]	
ADM-REV-02	Selbstgenehmigung blockiert	1. Eigenen Antrag freigeben versuchen	BLOCKIERT - auch fuer Admin!	[ ]	
ADM-REV-03	Audit-Trail via Admin-Pfad	1. `/admin/audit` aufrufen	Breadcrumb: "Dashboard > Verwaltung > Audit-Trail"	[ ]	

9. Querschnittstests (Rollenuebergreifend)

9.1 Authentifizierung & 2FA

ID	Testfall	Rollen	Schritte	Erwartetes Ergebnis	OK	Bemerkung
Q-AUTH-01	TOTP-2FA-Setup	Alle	1. 2FA-Setup aufrufen 2. TOTP waehlen 3. QR-Code scannen 4. Code bestaetigen	TOTP aktiviert, zukuenftiger Login erfordert TOTP	[ ]	
Q-AUTH-02	E-Mail-2FA-Setup	Alle	1. 2FA-Setup aufrufen 2. E-Mail waehlen	E-Mail-2FA aktiviert, Code wird per E-Mail gesendet	[ ]	
Q-AUTH-03	Falsches Passwort (5x)	Alle	1. 5x falsches Passwort eingeben	Account gesperrt fuer 15 Minuten	[ ]	
Q-AUTH-04	Passwort-Reset	Alle	1. "Passwort vergessen" 2. E-Mail eingeben 3. Link in E-Mail klicken 4. Neues Passwort setzen	Passwort geaendert, alle Sessions beendet	[ ]	
Q-AUTH-05	Session-Timeout	Alle	1. Einloggen 2. 30+ Min warten 3. Seite laden	Weiterleitung zu Login	[ ]	
Q-AUTH-06	2FA-Code falsch (5x)	Alle	1. Login erfolgreich 2. 5x falschen 2FA-Code eingeben	Zurueck zum Login, Fehlermeldung	[ ]	
Q-AUTH-07	Einladungslink verwenden	Neuer User	1. Admin erstellt Benutzer 2. E-Mail mit Link empfangen 3. Passwort setzen	Passwort gespeichert, Login moeglich	[ ]	
Q-AUTH-08	Einladungslink abgelaufen	Neuer User	1. Link nach Ablauf (Standard 7 Tage) verwenden	"Ungueltiger oder abgelaufener Einladungslink"	[ ]	

9.2 Vollstaendiger Workflow-Durchlauf (End-to-End)

ID	Testfall	Beteiligte	Schritte	Erwartetes Ergebnis	OK	Bemerkung
Q-WF-01	Happy Path: Erstellen bis Freigabe	Mitglied + Pruefer	1. Mitglied erstellt Eintrag 2. Mitglied reicht ein 3. Pruefer genehmigt	Status: Entwurf → Eingereicht → Freigegeben, E-Mails bei jedem Schritt	[ ]	
Q-WF-02	Klaerungsweg	Mitglied + Pruefer	1. Mitglied reicht ein 2. Pruefer stellt Rueckfrage 3. Mitglied antwortet 4. Pruefer genehmigt	Entwurf → Eingereicht → In Klaerung → Freigegeben	[ ]	
Q-WF-03	Ablehnungsweg	Mitglied + Pruefer	1. Mitglied reicht ein 2. Pruefer lehnt ab	Eingereicht → Abgelehnt, Begruendung sichtbar	[ ]	
Q-WF-04	Stornierung und Neueinreichung	Mitglied + Pruefer	1. Mitglied reicht ein 2. Mitglied storniert 3. Mitglied reaktiviert 4. Mitglied reicht erneut ein 5. Pruefer genehmigt	Kompletter Zyklus, Dialog bleibt erhalten	[ ]	
Q-WF-05	Erfasser-Workflow	Erfasser + Pruefer	1. Erfasser erstellt fuer Mitglied 2. Eintrag einreichen 3. Anderer Pruefer genehmigt	Korrekte user_id und created_by_user_id	[ ]	
Q-WF-06	Korrektur nach Freigabe	Pruefer	1. Freigegebenen Antrag korrigieren	Original-Stunden gespeichert, neue Stunden aktiv, E-Mail	[ ]	

9.3 E-Mail-Benachrichtigungen

ID	Testfall	Trigger	Empfaenger	Inhalt pruefen	OK	Bemerkung
Q-MAIL-01	Einreichung	Mitglied reicht ein	Alle Pruefer	Antragsnummer, Link zum Antrag	[ ]	
Q-MAIL-02	Freigabe	Pruefer genehmigt	Mitglied	Freigabe-Bestaetigung	[ ]	
Q-MAIL-03	Ablehnung	Pruefer lehnt ab	Mitglied	Ablehnungsgrund	[ ]	
Q-MAIL-04	Rueckfrage	Pruefer stellt Frage	Mitglied	Rueckfrage-Text	[ ]	
Q-MAIL-05	Korrektur	Pruefer korrigiert	Mitglied	Alte/neue Stunden, Begruendung	[ ]	
Q-MAIL-06	Einladung	Admin erstellt User	Neuer User	Setup-Link, Ablaufdatum	[ ]	
Q-MAIL-07	Passwort-Reset	User fordert Reset an	User	Reset-Link, 24h Gueltigkeit	[ ]	
Q-MAIL-08	E-Mail-Fehler	SMTP deaktiviert	-	Workflow gelingt trotzdem, Fehler wird geloggt	[ ]	

10. Sicherheitstests

10.1 CSRF-Schutz

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
SEC-CSRF-01	CSRF-Token vorhanden	1. Formular-HTML inspizieren	Hidden-Field `csrf_token` in allen POST-Formularen	[ ]	
SEC-CSRF-02	POST ohne CSRF-Token	1. cURL-Request ohne Token an POST-Endpunkt	HTTP 403 Forbidden	[ ]	
SEC-CSRF-03	POST mit falschem Token	1. Token-Wert im HTML aendern 2. Formular absenden	HTTP 403 Forbidden	[ ]	
SEC-CSRF-04	AJAX CSRF-Header	1. JavaScript-Fetch pruefen	X-CSRF-Token Header wird gesendet	[ ]	

10.2 XSS-Schutz

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
SEC-XSS-01	Script-Tag in Beschreibung	1. Eintrag mit `<script>alert('XSS')</script>` erstellen	Text wird escaped angezeigt, kein Alert	[ ]	
SEC-XSS-02	Script in Dialog-Nachricht	1. Dialog-Nachricht mit `<img onerror=alert(1) src=x>`	HTML wird escaped, kein Script ausgefuehrt	[ ]	
SEC-XSS-03	Script in Benutzername	1. Admin erstellt User mit `<script>` im Namen	Name wird korrekt escaped in allen Views	[ ]	
SEC-XSS-04	Script in Kategoriename	1. Admin erstellt Kategorie mit HTML im Namen	Name wird escaped	[ ]	

10.3 SQL-Injection

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
SEC-SQL-01	Login mit SQL-Injection	1. E-Mail: `' OR 1=1 --` eingeben	Fehlermeldung "Unbekannte E-Mail", kein Zugriff	[ ]	
SEC-SQL-02	Suchfeld mit SQL	1. Benutzersuche mit `'; DROP TABLE users; --`	Kein SQL-Fehler, normale Suche	[ ]	
SEC-SQL-03	URL-Parameter	1. `/entries/1 OR 1=1` aufrufen	Fehler 404 oder Validierungsfehler, keine Datenfreigabe	[ ]	

10.4 Zugriffskontrolle

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
SEC-AC-01	Unautorisierte Seite	1. Ohne Login `/entries` aufrufen	Weiterleitung zu `/login`	[ ]	
SEC-AC-02	Session-Manipulation	1. Session-Cookie manuell aendern	Weiterleitung zu `/login`	[ ]	
SEC-AC-03	Horizontale Eskalation	1. Als Mitglied A Eintrag von Mitglied B aufrufen	Zugriff verweigert	[ ]	
SEC-AC-04	Vertikale Eskalation	1. Als Mitglied Admin-URL aufrufen	Weiterleitung zu Dashboard	[ ]	
SEC-AC-05	Deaktivierter Benutzer	1. Admin deaktiviert Benutzer 2. Benutzer versucht Login	Login verweigert	[ ]	

10.5 Sicherheits-Header

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
SEC-HDR-01	Content-Security-Policy	1. Response-Header pruefen	CSP-Header vorhanden	[ ]	
SEC-HDR-02	X-Frame-Options	1. Response-Header pruefen	`SAMEORIGIN` gesetzt	[ ]	
SEC-HDR-03	Cookie-Flags	1. Cookies inspizieren	HttpOnly, Secure, SameSite=Lax	[ ]	
SEC-HDR-04	X-Content-Type-Options	1. Response-Header pruefen	`nosniff` gesetzt	[ ]	

11. Negativtests & Grenzwerte

11.1 Eingabe-Grenzwerte

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
NEG-01	Stunden = 0	1. Eintrag mit 0 Stunden erstellen	Validierungsfehler: Mindestwert	[ ]	
NEG-02	Stunden negativ	1. Eintrag mit -5 Stunden	Validierungsfehler	[ ]	
NEG-03	Stunden extrem hoch	1. Eintrag mit 999 Stunden	Validierungsfehler oder Obergrenze	[ ]	
NEG-04	Datum in der Zukunft	1. Eintrag mit morgen als Datum	Abhaengig von Validierung: Fehler oder Warnung	[ ]	
NEG-05	Datum sehr weit zurueck	1. Eintrag mit Datum 01.01.2000	Abhaengig von Validierung	[ ]	
NEG-06	Leere Pflichtfelder via DevTools	1. HTML-required entfernen 2. Leer absenden	Server-seitige Validierung greift	[ ]	
NEG-07	Ueberlange Texte	1. 10.000 Zeichen in Beschreibung	Wird gespeichert oder Laengenbegrenzung greift	[ ]	
NEG-08	Sonderzeichen in allen Feldern	1. Unicode, Umlaute, Emojis eingeben	Korrekt gespeichert und angezeigt	[ ]	
NEG-09	Passwort < 8 Zeichen	1. Passwort "Abc1" setzen	Validierungsfehler: Mindestens 8 Zeichen	[ ]	
NEG-10	Passwort ohne Grossbuchstabe	1. Passwort "abcd1234"	Validierungsfehler	[ ]	
NEG-11	Passwort ohne Zahl	1. Passwort "Abcdefgh"	Validierungsfehler	[ ]	
NEG-12	Doppelte Mitgliedsnummer bei Import	1. CSV mit zweimal gleicher Mitgliedsnummer	Duplikat erkannt, Update statt Neu	[ ]	

11.2 Concurrent Access

ID	Testfall	Schritte	Erwartetes Ergebnis	OK	Bemerkung
NEG-CC-01	Gleichzeitige Bearbeitung	1. Tab A: Eintrag bearbeiten 2. Tab B: gleichen Eintrag bearbeiten 3. Tab A speichern 4. Tab B speichern	Optimistic Locking: Tab B erhaelt Fehler	[ ]	
NEG-CC-02	Gleichzeitiger Login	1. Browser A: einloggen 2. Browser B: einloggen	Beide Sessions funktionieren	[ ]	
NEG-CC-03	Status-Rennbedingung	1. Pruefer A und Pruefer B oeffnen gleichen Antrag 2. Beide genehmigen gleichzeitig	Nur einer erfolgreich, anderer erhaelt Fehler	[ ]	

12. Regressionstests nach Aenderungen

12.1 Regressions-Checkliste (nach jedem Deployment)

Diese Kurzfassung der wichtigsten Tests soll nach jedem Deployment ausgefuehrt werden:

#	Bereich	Pruefung	OK	Bemerkung
1	Login	Einloggen mit 2FA funktioniert	[ ]	
2	Dashboard	Dashboard laedt korrekt, Statistiken sichtbar	[ ]	
3	Erfassung	Neuen Eintrag erstellen (Entwurf)	[ ]	
4	Einreichen	Eintrag einreichen, E-Mail pruefen	[ ]	
5	Freigabe	Als Pruefer fremden Antrag freigeben	[ ]	
6	Selbstgenehmigung	Eigenen Antrag freigeben → blockiert	[ ]	
7	Dialog	Rueckfrage stellen und beantworten	[ ]	
8	Berichte	PDF-Export herunterladen	[ ]	
9	Admin	Benutzer-Liste anzeigen	[ ]	
10	Audit	Audit-Trail anzeigen	[ ]	
11	Navigation	Breadcrumbs auf allen Seiten korrekt	[ ]	
12	Sicherheit	CSRF-Token in Formularen vorhanden	[ ]	

12.2 Regressionsmatrix: Feature vs. betroffene Bereiche

Aenderung an...	Betrifft Tests
AuthController / AuthService	Q-AUTH-*, SEC-AC-*, Login-Regression
WorkEntryController	M-ENT-*, P-REV-*, Q-WF-*
WorkflowService	P-SELF-*, Q-WF-*, P-REV-*, P-KORR-*
EmailService	Q-MAIL-*
UserController / ImportService	ADM-USR-*, ADM-IMP-*
CategoryController	ADM-CAT-*
TargetHoursController	ADM-TGT-*
Middleware (Auth/Role/CSRF)	SEC-*, M-ACC-*, E-ACC-*, P-ACC-*, A-RO-*
Views / CSS / JS	Visuelle Pruefung aller betroffenen Seiten
Datenbank-Schema	Alle Tests, vollstaendiger Regressionstest

---

13. Automatisierungsplan

13.1 Uebersicht: Aktueller Stand vs. Ziel

```
 Aktuell:    212 automatisierte Tests (Models, Services, Helpers, Integration)
Ziel:       ~450+ automatisierte Tests
Reduktion:  ~70% der manuellen Tests automatisierbar
```

13.2 Phasen-Plan

Phase 1: Controller-Tests (Prioritaet HOCH)

Ziel: Alle HTTP-Endpunkte automatisiert testen **Geschaetzter Umfang:** 80-100 neue Tests
Verzeichnis: `tests/Unit/Controllers/`

Ansatz: PHPUnit mit gemocktem PSR-7 Request/Response

```
 // Beispiel: AuthControllerTest.php
class AuthControllerTest extends TestCase
{
    public function test_login_page_returns_200(): void
    {
        $request = $this->createRequest('GET', '/login');
        $response = $this->app->handle($request);
        $this->assertEquals(200, $response->getStatusCode());
    }

    public function test_login_post_with_valid_credentials_redirects_to_2fa(): void
    {
        $request = $this->createRequest('POST', '/login', [
            'email' => 'mitglied@test.de',
            'password' => 'Test123!',
            'csrf_token' => $this->csrfToken,
        ]);
        $response = $this->app->handle($request);
        $this->assertEquals(302, $response->getStatusCode());
        $this->assertStringContains('/2fa', $response->getHeaderLine('Location'));
    }
}
```

Test-Dateien zu erstellen:

Datei	Endpunkte	Testfaelle
`AuthControllerTest.php`	10 Routes (Login, 2FA, Reset, Setup)	~25 Tests
`WorkEntryControllerTest.php`	14 Routes (CRUD, Workflow-Aktionen)	~30 Tests
`DashboardControllerTest.php`	2 Routes (Index, Unread Count)	~5 Tests
`ReportControllerTest.php`	3 Routes (Index, PDF, CSV)	~8 Tests
`UserControllerTest.php`	10 Routes (CRUD, Roles, Import)	~15 Tests
`CategoryControllerTest.php`	7 Routes (CRUD, Reorder)	~10 Tests
`AdminControllerTest.php`	3 Routes (Settings)	~5 Tests
`AuditControllerTest.php`	2 Routes (Index, Show)	~5 Tests
`TargetHoursControllerTest.php`	4 Routes (Index, Edit, Bulk)	~7 Tests

Was getestet wird: - HTTP-Statuscodes (200, 302, 403, 404) - Redirect-Ziele bei unautorisierten Zugriffen - CSRF-Validierung auf allen POST-Endpunkten - Korrekte View-Daten im Response - Flash-Messages bei Erfolg/Fehler

---

Phase 2: Middleware-Tests (Prioritaet HOCH)

Ziel: Auth, Role und CSRF Middleware isoliert testen **Geschaetzter Umfang:** 25-30 neue Tests **Verzeichnis:** `tests/Unit/Middleware/`

```
 // Beispiel: RoleMiddlewareTest.php
class RoleMiddlewareTest extends TestCase
{
    public function test_mitglied_cannot_access_admin_routes(): void
    {
        $middleware = new RoleMiddleware(['administrator']);
        $request = $this->createAuthenticatedRequest($this->mitgliedUser);
        $response = $middleware->process($request, $this->handler);
        $this->assertEquals(302, $response->getStatusCode());
    }

    public function test_admin_can_access_admin_routes(): void
    {
        $middleware = new RoleMiddleware(['administrator']);
        $request = $this->createAuthenticatedRequest($this->adminUser);
        $response = $middleware->process($request, $this->handler);
        $this->assertEquals(200, $response->getStatusCode());
    }
}
```

Test-Dateien:

Datei	Testfaelle
`AuthMiddlewareTest.php`	~10 Tests (Session-Check, 2FA-Erzwingung, Timeout)
`RoleMiddlewareTest.php`	~12 Tests (Jede Rolle gegen jede Route-Gruppe)
`CsrfMiddlewareTest.php`	~8 Tests (Token-Validierung, Header, Body, Fehler)

Phase 3: Fehlende Service-Tests (Prioritaet MITTEL)

Ziel: Kritische Services ohne Tests abdecken **Geschaetzter Umfang:** 50-60 neue Tests
Verzeichnis: `tests/Unit/Services/`

Datei	Was wird getestet	Testfaelle
`EmailServiceTest.php`	E-Mail-Zusammensetzung, Template-Rendering, Fehlerbehandlung	~12 Tests
`TotpServiceTest.php`	TOTP-Generierung, Verifizierung, QR-Code-URI	~8 Tests
`CsvExportServiceTest.php`	CSV-Formatierung, UTF-8-BOM, Spalten, Sonderzeichen	~8 Tests
`PdfServiceTest.php`	PDF-Generierung, Seitenstruktur, Daten-Integration	~6 Tests
`ReportServiceTest.php`	Berechtigungsfilter, Aggregation, Datumsfilter	~10 Tests
`ImportServiceTest.php`	CSV-Parsing, Validierung, Delimiter-Erkennung, Fehlersammlung	~12 Tests
`AuditServiceTest.php`	Log-Erstellung, Kontext-Setzung, Metadaten	~6 Tests
`TargetHoursServiceTest.php`	Soll-Berechnung, Befreiung, Jahreswechsel	~6 Tests

Phase 4: Repository-Integrationstests (Prioritaet MITTEL)

Ziel: Datenbank-Interaktionen mit Test-Datenbank pruefen **Geschaetzter Umfang:** 40-50 neue Tests **Verzeichnis:** `tests/Integration/Database/`

Voraussetzung: Test-Datenbank `vaes_test` mit Schema aber ohne Produktivdaten

```
 // Beispiel: WorkEntryRepositoryTest.php
class WorkEntryRepositoryTest extends DatabaseTestCase
{
    protected function setUp(): void
    {
        parent::setUp();
        $this->seedTestData();
    }

    public function test_soft_deleted_entries_not_in_default_query(): void
    {
        $this->repo->softDelete($this->testEntryId);
        $entries = $this->repo->findByUserId($this->testUserId);
        $this->assertEmpty(array_filter($entries, fn($e) => $e->getId() === $this->testEntryId));
    }

    public function test_optimistic_locking_prevents_stale_update(): void
    {
        // Alte Version laden
        $entry = $this->repo->findById($this->testEntryId);
        // Parallel-Update simulieren
        $this->repo->updateStatus($this->testEntryId, 'eingereicht', 1, $entry->getVersion());
        // Erneuter Update mit alter Version
        $this->expectException(StaleDataException::class);
        $this->repo->updateStatus($this->testEntryId, 'freigegeben', 2, $entry->getVersion());
    }

    protected function tearDown(): void
    {
        $this->cleanupTestData();
        parent::tearDown();
    }
}
```

Benoetigte Infrastruktur: - `DatabaseTestCase` Basisklasse mit DB-Verbindung und Transaktions-Rollback - Seed-Skript fuer minimale Testdaten - phpunit.xml Erweiterung um DB-Konfiguration

Test-Dateien:

Datei	Was wird getestet	Testfaelle
`UserRepositoryTest.php`	CRUD, Suche, Soft-Delete, Rollen	~8 Tests
`WorkEntryRepositoryTest.php`	CRUD, Status-Update, Soft-Delete, Version-Lock	~10 Tests
`CategoryRepositoryTest.php`	CRUD, Sortierung, Soft-Delete	~6 Tests
`DialogRepositoryTest.php`	Erstellen, Abfragen, Unveraenderbarkeit	~5 Tests
`AuditRepositoryTest.php`	Erstellen, Filtern, Unveraenderbarkeit	~6 Tests
`SessionRepositoryTest.php`	Token-Verwaltung, Ablauf, Bereinigung	~5 Tests
`SettingsRepositoryTest.php`	Get/Set, Typen	~4 Tests
`YearlyTargetRepositoryTest.php`	CRUD, Befreiung	~4 Tests

Phase 5: API-/Smoke-Testskript (Prioritaet MITTEL)

Ziel: Schneller End-to-End-Check aller Endpunkte via cURL **Datei:** `scripts/test_api.sh` (oder `scripts/test_api.php`)

```
 #!/usr/bin/env php
<?php
/**
 * VAES API Smoke Test Script
 * Prueft alle Endpunkte auf Erreichbarkeit und korrekte HTTP-Statuscodes.
 *
 * Verwendung: php scripts/test_api.php [base-url]
 * Beispiel:   php scripts/test_api.php http://localhost:8000
 */

$baseUrl = $argv[1] ?? 'http://localhost:8000';

// 1. Session aufbauen (Login)
$ch = curl_init();
// ... Login-Flow simulieren ...

// 2. Alle Endpunkte pruefen
$tests = [
    // Public Routes
    ['GET', '/login', 200, null, 'Login-Seite'],
    ['GET', '/forgot-password', 200, null, 'Passwort-vergessen-Seite'],

    // Authenticated Routes (nach Login)
    ['GET', '/', 200, 'mitglied', 'Dashboard'],
    ['GET', '/entries', 200, 'mitglied', 'Eintragsliste'],
    ['GET', '/entries/create', 200, 'mitglied', 'Eintrag-Erstellen'],
    ['GET', '/reports', 200, 'mitglied', 'Berichte'],

    // Zugriffsbeschraenkungen
    ['GET', '/review', 302, 'mitglied', 'Pruef-Liste als Mitglied → Redirect'],
    ['GET', '/admin/users', 302, 'mitglied', 'Admin als Mitglied → Redirect'],
    ['GET', '/audit', 302, 'mitglied', 'Audit als Mitglied → Redirect'],

    // Admin Routes
    ['GET', '/admin/users', 200, 'admin', 'Benutzerverwaltung'],
    ['GET', '/admin/categories', 200, 'admin', 'Kategorien'],
    ['GET', '/admin/settings', 200, 'admin', 'Einstellungen'],
    ['GET', '/admin/audit', 200, 'admin', 'Audit-Trail (Admin)'],
    ['GET', '/admin/targets', 200, 'admin', 'Soll-Stunden'],

    // Reviewer Routes
    ['GET', '/review', 200, 'pruefer', 'Pruef-Liste'],

    // Auditor Routes
    ['GET', '/audit', 200, 'auditor', 'Audit-Trail (Auditor)'],
];

// 3. Ergebnisse ausgeben
foreach ($tests as [$method, $path, $expectedStatus, $role, $description]) {
    $actualStatus = executeRequest($method, $baseUrl . $path, $role);
    $ok = $actualStatus === $expectedStatus;
    echo ($ok ? 'PASS' : 'FAIL') . " [{$method}] {$path} → {$actualStatus} (erwartet: {$expectedS
}
```

Vorteile: - Schneller Smoke-Test nach Deployment (~30 Sekunden) - Prueft alle Routen auf Erreichbarkeit - Prueft Zugriffsbeschraenkungen pro Rolle - Kann in CI/CD integriert werden

Phase 6: Browser-Automatisierung (Prioritaet NIEDRIG)

Ziel: UI-Tests fuer kritische Workflows **Werkzeug:** Selenium WebDriver oder Playwright (PHP-Binding) **Verzeichnis:** `tests/Browser/`

Hinweis: Auf Strato Shared Hosting nicht ausfuehrbar. Nur lokal oder in CI/CD.

Kandidaten fuer Browser-Tests:

Workflow	Warum Browser-Test noetig
2FA-Setup mit QR-Code	QR-Code-Rendering, JavaScript-Interaktion
Passwort-Staerke-Anzeige	JavaScript-basiert, Client-seitige Validierung
Auto-Submit bei 6-stelligem Code	JavaScript: Auto-Submit nach 6 Ziffern
Flash-Message-Auto-Dismiss	5-Sekunden-Timer, Bootstrap-Animation
Dialog-Polling (60s)	AJAX-Polling, Badge-Update, Auto-Reload
Kategorie-Drag-and-Drop	JavaScript Drag-and-Drop-Sortierung
Responsive Layout	Bootstrap Breakpoints pruefen

Alternative ohne Browser-Tests: Viele dieser Interaktionen koennen manuell mit der Regressions-Checkliste (Abschnitt 12.1) abgedeckt werden. Die Automatisierung lohnt sich erst bei haeufigen Releases.

13.3 Infrastruktur-Anforderungen

Phase	Benoetigt	Aufwand
Phase 1 (Controller)	Slim App Test-Bootstrap, PSR-7 Factory	Einmalig TestCase-Basisklasse erstellen
Phase 2 (Middleware)	PSR-7 Mock-Requests	Gering, nutzt bestehende Patterns
Phase 3 (Services)	PHPMailer Mock, TCPDF Mock	Pro Service individuell
Phase 4 (Repositories)	MySQL Test-DB, Transactions	DatabaseTestCase Basisklasse, Test-DB Setup
Phase 5 (API-Script)	cURL, laufender Server	Geringer Aufwand, hoher Nutzen
Phase 6 (Browser)	Selenium/Playwright, ChromeDriver	Hoher initialer Aufwand

13.4 Empfohlene Reihenfolge

```
 Sofort:     Phase 5 (API-Smoke-Script)        → schneller ROI, geringer Aufwand
Kurzfristig: Phase 1 (Controller-Tests)         → groesste Luecke schliessen
Kurzfristig: Phase 2 (Middleware-Tests)          → Sicherheits-kritisch
Mittelfristig: Phase 3 (Service-Tests)           → Business-Logik absichern
Mittelfristig: Phase 4 (Repository-Tests)        → Datenbank-Integritaet
Langfristig: Phase 6 (Browser-Tests)            → nur bei haeufigen Releases
```

13.5 CI/CD-Integration

Fuer eine zukuenftige CI/CD-Pipeline (z.B. GitHub Actions):

```
 # .github/workflows/tests.yml
name: VAES Tests
on: [push, pull_request]
jobs:
  unit-tests:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - uses: shivammathur/setup-php@v2
        with:
          php-version: '8.2'
          extensions: pdo_mysql, mbstring
      - run: cd src && composer install --no-progress
      - run: cd src && vendor/bin/phpunit --testsuite Unit

  integration-tests:
    runs-on: ubuntu-latest
    services:
      mysql:
        image: mysql:8.4
        env:
          MYSQL_ROOT_PASSWORD: test
          MYSQL_DATABASE: vaes_test
        ports: ['3306:3306']
    steps:
      - uses: actions/checkout@v4
      - uses: shivammathur/setup-php@v2
        with:
          php-version: '8.2'
      - run: mysql -h 127.0.0.1 -u root -ptest vaes_test < scripts/database/create_database.sql
      - run: cd src && composer install --no-progress
      - run: cd src && vendor/bin/phpunit --testsuite Integration

  smoke-test:
    runs-on: ubuntu-latest
    needs: [unit-tests]
    steps:
      - uses: actions/checkout@v4
      - run: cd src/public && php -S localhost:8000 &
      - run: sleep 3 && php scripts/test_api.php http://localhost:8000
```

13.6 Erwartete Endabdeckung nach allen Phasen

Bereich	Aktuell	Nach Automatisierung
Modelle	47 Tests	47 Tests (unveraendert)
Services	77 Tests	~135 Tests (+58)
Helper	65 Tests	65 Tests (unveraendert)
Controller	0 Tests	~110 Tests (+110)
Middleware	0 Tests	~30 Tests (+30)
Repositories	0 Tests	~48 Tests (+48)
Integration	23 Tests	~23 Tests (unveraendert)
API-Smoke	0 Tests	~35 Tests (+35)
Gesamt	**212 Tests**	**~493 Tests**

Manuelle Tests die NICHT automatisierbar sind: - E-Mail-Zustellung pruefen (echter SMTP) - QR-Code mit Authenticator-App scannen - PDF visuell pruefen (Layout, Schrift) - Responsive Design auf echten Geraeten - Performance unter realer Last - Deployment auf Strato Shared Hosting

14. Anhang: Testprotokoll-Vorlage

14.1 Kopfzeile fuer Testdurchfuehrung

```
┌──────────────────────────────────────────────────────┐
│ VAES Testprotokoll                                   │
│                                                      │
│ Tester:       _____________________________________  │
│ Datum:        _____________________________________  │
│ Version:      _____________________________________  │
│ Umgebung:     [ ] Lokal  [ ] Staging  [ ] Produktion │
│ Browser:      _____________________________________  │
│                                                      │
│ Getestete Rollen:                                    │
│ [ ] Mitglied   [ ] Erfasser   [ ] Pruefer            │
│ [ ] Auditor    [ ] Administrator                     │
│                                                      │
│ Ergebnis:                                            │
│ Bestanden: ___  Fehlgeschlagen: ___  Uebersprungen: ___ │
│                                                      │
│ Unterschrift: _____________________________________  │
└──────────────────────────────────────────────────────┘
```

14.2 Fehlerbericht-Vorlage

```
┌─────────────────────────────────────────────────────────┐
│ FEHLERBERICHT                                           │
│                                                         │
│ Test-ID:       _____________________________________    │
│ Schweregrad:   [ ] Kritisch  [ ] Hoch  [ ] Mittel  [ ] Niedrig │
│ Datum:         _____________________________________    │
│ Tester:        _____________________________________    │
│                                                         │
│ Beschreibung:                                           │
│ _____________________________________________________   │
│ _____________________________________________________   │
│                                                         │
│ Schritte zur Reproduktion:                              │
│ 1. _____________________________________________________ │
│ 2. _____________________________________________________ │
│ 3. _____________________________________________________ │
│                                                         │
│ Erwartetes Ergebnis:                                    │
│ _____________________________________________________   │
│                                                         │
│ Tatsaechliches Ergebnis:                                │
│ _____________________________________________________   │
│                                                         │
│ Screenshots/Logs:                                       │
│ _____________________________________________________   │
│                                                         │
│ Zugewiesen an: _____________________________________    │
│ Status:        [ ] Offen  [ ] In Bearbeitung  [ ] Geloest │
└─────────────────────────────────────────────────────────┘
```

14.3 Zusammenfassung der Test-IDs

Praefix	Bereich	Anzahl
M-AUTH	Mitglied: Authentifizierung	4
M-DASH	Mitglied: Dashboard	4
M-ENT	Mitglied: Arbeitsstunden	12
M-DLG	Mitglied: Dialog	5
M-REP	Mitglied: Berichte	5
M-ACC	Mitglied: Zugriffsbeschraenkungen	4
E-ENT	Erfasser: Eintraege	4
E-ACC	Erfasser: Zugriffsbeschraenkungen	3
P-REV	Pruefer: Pruef-Workflow	8
P-KORR	Pruefer: Korrektur	3
P-SELF	Pruefer: Selbstgenehmigung	4
P-ACC	Pruefer: Zugriffsbeschraenkungen	2
A-AUD	Auditor: Audit-Trail	7
A-RO	Auditor: Nur-Lese-Zugriff	4
ADM-USR	Admin: Benutzerverwaltung	10
ADM-IMP	Admin: CSV-Import	6
ADM-CAT	Admin: Kategorien	7
ADM-TGT	Admin: Soll-Stunden	5
ADM-SET	Admin: Einstellungen	6
ADM-REV	Admin: Pruef-Funktionen	3
Q-AUTH	Querschnitt: Authentifizierung	8
Q-WF	Querschnitt: End-to-End-Workflow	6
Q-MAIL	Querschnitt: E-Mail	8
SEC-CSRF	Sicherheit: CSRF	4
SEC-XSS	Sicherheit: XSS	4
SEC-SQL	Sicherheit: SQL-Injection	3
SEC-AC	Sicherheit: Zugriffskontrolle	5
SEC-HDR	Sicherheit: Header	4
NEG	Negativtests / Grenzwerte	12
NEG-CC	Concurrent Access	3
Gesamt		**~167 manuelle Testfaelle**

Erstellt: 2026-02-11 | VAES v1.3 | QA-Team