Compliance-Nachweise

Übersicht

Dieses Kapitel dokumentiert die Compliance-Nachweise für verschiedene Sicherheitsstandards und Regularien.

ISO 27001:2022

Statement of Applicability (SoA)

Die folgende Tabelle zeigt die Anwendbarkeit und Implementierung der ISO 27001:2022 Annex A Controls:

Control	Anwendbar	Implementiert	Evidenz
A.5.15	Ja	Ja	`application/permission/auditable.go` - RBAC-System
A.5.16	Ja	Ja	`application/user/usecases.go` - User Lifecycle
A.5.17	Ja	Ja	`application/user/password.go:111` - Argon2id
A.8.2	Ja	Ja	`application/flow/evt_repository_assigned.go:27`
A.8.3	Ja	Ja	`application/permission/auditable.go` - Audit()
A.8.5	Ja	Ja	`application/user/uc_authenticates_by_password.go:42`
A.8.9	Ja	Ja	`application/security.go` - Master Key Management
A.8.12	Ja	Ja	`application/management_mail.go:126` - User Enumeration
A.8.13	Ja	Ja	`application/backup/usecases.go` - Encrypted Backups
A.8.16	Ja	Ja	`application/evs/` - Event Store Audit Trail
A.8.24	Ja	Ja	`pkg/blob/crypto/crypto.go` - AES-GCM-256
A.8.25	Ja	Ja	20 Security Notes im Quellcode dokumentiert

Audit-Evidenz-Katalog

A.5.17 - Authentifizierungsinformationen

Evidenz-Typ: Quellcode

Datei: `application/user/password.go`

Zeilen: 111-113

```
// OWASP-konforme Passwort-Speicherung
// https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html
func argon2idMin(password string, salt []byte) []byte {
    return argon2.IDKey([]byte(password), salt, 2, 19*1024, 1, 32)
}
```

Nachweis: Argon2id mit OWASP-Minimalparametern implementiert.

A.8.5 - Sichere Authentifizierung

Evidenz-Typ: Quellcode

Datei: application/user/uc_authenticates_by_password.go

Zeilen: 42-47

```
if !usr.EMailVerified {
    // security note: intentionally it is not safe to let the user login
    return std.None[User](), std.NewLocalizedError("Login nicht möglich",
        "Das Konto muss zuerst bestätigt werden").WithError(EMailNotVerifiedErr)
}
```

Nachweis: E-Mail-Verifikation ist Voraussetzung für Login.

A.8.24 - Verwendung von Kryptographie

Evidenz-Typ: Quellcode

Datei: pkg/blob/crypto/crypto.go

Zeilen: 34-56

```
// 256-bit AES-GCM with random nonce
func encrypt(plaintext []byte, key *[32]byte) (ciphertext []byte, err error) {
    block, err := aes.NewCipher(key[:])
    gcm, err := cipher.NewGCM(block)
    nonce := make([]byte, gcm.NonceSize())
    io.ReadFull(rand.Reader, nonce)
    return gcm.Seal(nonce, nonce, plaintext, nil), nil
}
```

Nachweis: AES-GCM-256 mit Random Nonce implementiert.

SOC 2 Type II

Trust Service Criteria Mapping

Kriterium	Beschreibung	Implementierung	Evidenz
Security (Common Criteria)			
CC6.1	Logische Zugangssicherheit	RBAC mit Permission-System	`application/permission/`
CC6.2	Zugangsbeschränkungen	Permission-Audit vor jeder Aktion	`subject.Audit()`
CC6.3	Registrierung und Autorisierung	User Management mit E-Mail-Verifikation	`application/user/`
CC6.6	Verschlüsselung	AES-GCM-256 für sensible Daten	`pkg/blob/crypto/`
CC6.7	Zugang zu Systemen	Session-basierte Authentifizierung	`application/session/`
Availability			
CC7.1	System-Überwachung	Event Bus Logging	`application/evs/`
CC7.2	Vorfallsreaktion	Audit Trail für Forensik	Event Store
Processing Integrity			
CC8.1	Input-Validierung	Password-Stärke, E-Mail-Format	`application/user/password.go`
Confidentiality			
CC9.1	Vertrauliche Informationen	Encrypted Blob Storage	`pkg/blob/crypto/`
CC9.2	Entsorgung	Backup mit verschlüsselten Stores	`application/backup/`

DSGVO/GDPR Compliance

Artikel-Mapping

Artikel	Anforderung	Implementierung
Art. 5 (1) f	Integrität und Vertraulichkeit	AES-GCM-256 Verschlüsselung, TLS, Argon2id
Art. 25	Privacy by Design	E-Mail-Verifikation Pflicht, Verschlüsselung Standard
Art. 32 (1) a	Pseudonymisierung und Verschlüsselung	Master Key Verschlüsselung für sensible Stores

Artikel	Anforderung	Implementierung
Art. 32 (1) b	Vertraulichkeit, Integrität	RBAC, Permission-Audit, AES-GCM Authentication Tag
Art. 32 (1) c	Belastbarkeit	Session-Recovery, Backup-Restore
Art. 32 (1) d	Überprüfungsverfahren	Audit Trail, Structured Logging
Art. 33	Meldung von Verletzungen	Siehe Incident Response Plan
Art. 34	Benachrichtigung Betroffener	Siehe Incident Response Plan

Consent-Verwaltung

Das Framework unterstützt DSGVO-konforme Einwilligungsverwaltung:

```
// example/cmd/tutorial-62-dataimporter/main.go:61-80
usrSettings.Consents = []user.ConsentOption{
    {
        ID:       consent.DataProtectionProvision,
        Register: user.ConsentText{
            Label: "Ja, ich habe die [Datenschutzbestimmungen](/page/datenschutz)
gelesen und akzeptiert."
        },
        Required: true,
    },
    {
        ID: consent.Newsletter,
        Register: user.ConsentText{
            Label: "Ja, ich melde mich zum Newsletter an.",
            SupportingText: "Ein Widerspruch ist jederzeit möglich.",
        },
    },
}
```

Evidenz:

- Pflicht-Consent für Datenschutzbestimmungen
- Optionaler Newsletter-Consent
- Widerrufsmöglichkeit dokumentiert

BSI IT-Grundschutz

Baustein-Mapping

Baustein	Anforderung	Implementierung
APP.3.1	Webanwendungen und Webservices	Input Validation, XSS-Schutz via VueJS

Baustein	Anforderung	Implementierung
APP.3.2	Webserver	chi Router mit Middleware, Structured Logging
CON.1	Kryptokonzept	AES-GCM-256, Argon2id, TLS
CON.3	Datensicherungskonzept	Backup-System mit Verschlüsselung
OPS.1.1.2	Ordnungsgemäße IT-Administration	RBAC, Audit Trail, Bootstrap-Admin mit Zeitlimit
OPS.1.2.5	Fernwartung	SSO via NLS, Session-basierte Authentifizierung
DER.1	Detektion von sicherheitsrelevanten Ereignissen	Event Bus, Structured Logging, Audit-UI

Penetrationstest-Historie

Template für Pentest-Berichte

Feld	Beschreibung
Testzeitraum	[Datum von - bis]
Tester	[Name/Firma]
Scope	Nago Framework Application Layer
Methodik	OWASP Testing Guide, STRIDE
Findings	[Anzahl Kritisch/Hoch/Mittel/Niedrig]
Status	[Offen/In Bearbeitung/Geschlossen]

Finding-Template

Feld	Wert
ID	[PT-YYYY-NNN]
Titel	[Kurzbeschreibung]
Schweregrad	[Kritisch/Hoch/Mittel/Niedrig]
CVSS Score	[0.0-10.0]
Betroffene Komponente	[Pfad/Datei]
Beschreibung	[Detaillierte Beschreibung]
Reproduktion	[Schritte zur Reproduktion]
Empfehlung	[Behebungsempfehlung]
Status	[Offen/In Bearbeitung/Geschlossen]

Feld	Wert
Behebungsdatum	[Datum oder N/A]

Vulnerability Disclosure Policy

Meldeverfahren

Sicherheitslücken können gemeldet werden an:

- E-Mail: security@worldiety.de
- PGP-Key: [Key-ID verfügbar auf Anfrage]

Reaktionszeiten

Schweregrad	Ziel-Reaktionszeit
Kritisch	24 Stunden
Hoch	72 Stunden
Mittel	7 Tage
Niedrig	30 Tage

Veröffentlichungspolitik

- Coordinated Disclosure nach 90 Tagen
- Benachrichtigung betroffener Kunden vor Veröffentlichung
- Security Advisory mit CVE-ID (falls zutreffend)

Security Notes Index

Die folgenden Security Notes sind im Quellcode dokumentiert:

Nr.	Datei:Zeile	Beschreibung
1	`flow/evt_repository_assigned.go:27`	Privilege Escalation Schutz
2	`session/ui/login.go:145`	User Enumeration Schutz bei Login
3	`management_mail.go:126`	User Enumeration Schutz bei Password-Reset
4	`management_mail.go:131`	Neue Security Codes bei Reset
5	`management_mail.go:169`	User Enumeration Schutz bei Verification

Nr.	Datei:Zeile	Beschreibung
6	`management_mail.go:174`	Neue Verification Codes
7	`user/password.go:49`	Keine Sleep-Verzögerung wegen Argon2id
8	`user/password.go:52`	Trade-off bei schwachen Passwörtern
9	`dataimport/ui/page_select_parser.go:72`	Staging-ID nicht via Query
10	`usercircle/ui/view_users.go:32`	Circle-Admin UI-Schutz
11	`usercircle/ui/page_my_circle_groups.go:30`	Circle-Definition Berechtigung
12	`usercircle/ui/page_my_circle_roles.go:30`	Circle-Definition Berechtigung
13	`usercircle/ui/page_my_circle_licenses.go:30`	Circle-Definition Berechtigung
14	`usercircle/ui/page_my_circle_groups_users.go:26`	Circle-Definition Sichtbarkeit
15	`usercircle/ui/page_my_circle_roles_users.go:26`	Circle-Definition Sichtbarkeit
16	`usercircle/ui/page_my_circle_licenses_users.go:31`	Circle-Definition Sichtbarkeit
17	`usercircle/ui/page_my_circle_licenses_users.go:48`	Circle-Definition Zuweisung
18	`usercircle/ui/page_my_circle_licenses_users.go:56`	Circle-Definition Entzug
19	`drive/uc_read_drives.go:38`	Drive User-ID Zugriff
20	`secret/usecases.go:59`	Credentials Type-Safety