

Dominik Auer

FIDELA

Cyber-Hygiene für KMUs unter NIS2 – Erfahrungen beim Aufbau eines pragmatischen Managementsystems für KMUs und warum KI sowie Open Source den Unterschied machen könnten



Hygiene Manual

For Small Children and Starter-Parents



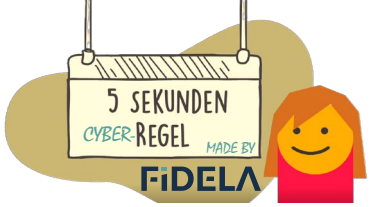
Cyber Hygiene Manual

For Small Businesses and Start-Ups



Cyber Hygiene Management System

For Small Businesses and Start-Ups



ÜBER MICH

Dominik Auer

- Absolvent der USTP
  - Masterarbeit zu Cyber Hygiene für kleine Unternehmen
- Mitgründer der FIDELA GmbH
  - Informationssicherheit für KMUs
    ISMS | ISO/IEC 27001 Auditor
    NIS Auditor | Lieferkettensicherheit

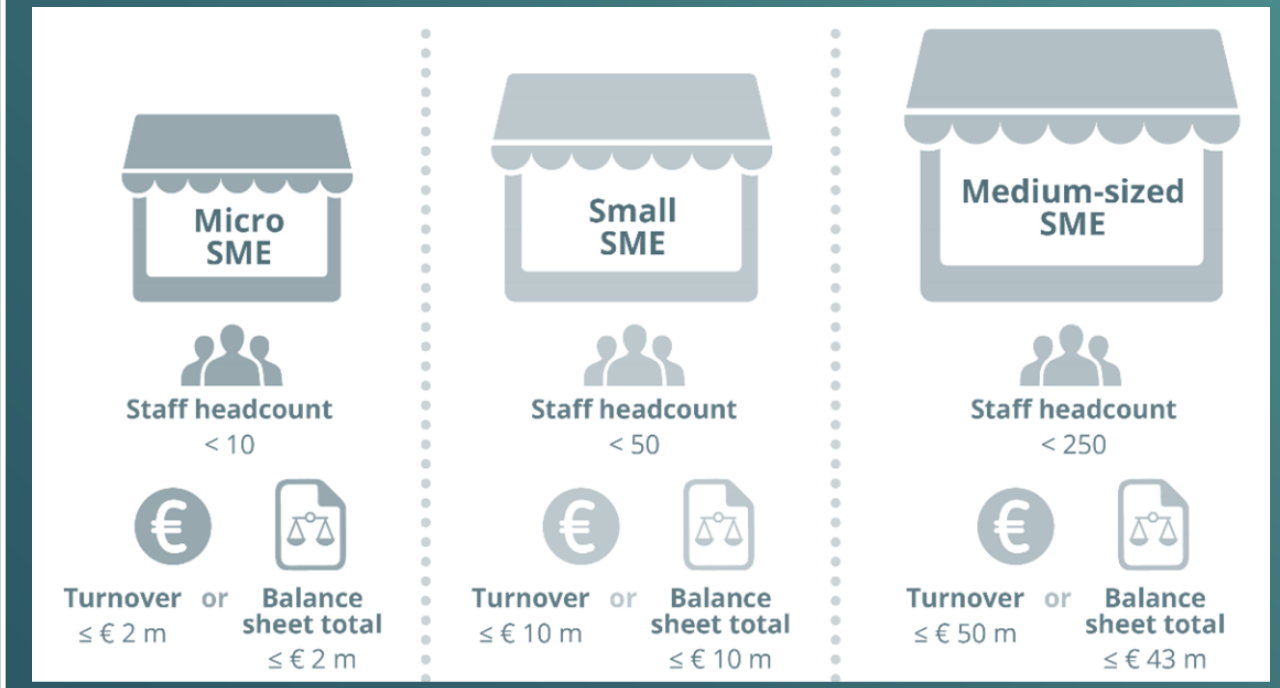


Kontakt: dominik@fidela.at

FiDELA

University of Applied Sciences St. Pölten

Ausgangslage und Motivation



KMU-Größenklassen laut EU-Definition

Lieferkette

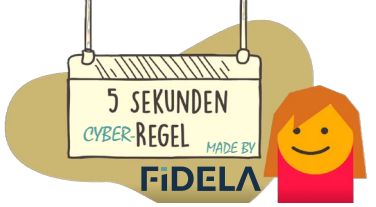
NIS2 trifft auch kleine Zulieferer indirekt

Bedrohungslage

Konflikte werden auch im Cyberraum ausgetragen

? % sind KMU

? % davon haben weniger als 10 Mitarbeitende



AKT I.

AKT III.

AKT II.

Forschungsfrage und Vorgehen

„Wie kann ein modular aufgebautes und an die spezifischen Bedürfnisse kleiner Unternehmen angepasstes Rahmenwerk zur Umsetzung der Risikomanagementmaßnahmen gemäß Artikel 21 der NIS2-Richtlinie gestaltet werden, um grundlegende Cyber-Hygiene-Maßnahmen nachhaltig im Unternehmen zu etablieren?“



AKT I.

AKT III.

AKT II.

Forschungsfrage und Vorgehen

„Wie kann ein modular aufgebautes und an die spezifischen Bedürfnisse kleiner Unternehmen angepasstes Rahmenwerk zur Umsetzung der Risikomanagementmaßnahmen gemäß Artikel 21 der NIS2-Richtlinie gestaltet werden, um grundlegende Cyber-Hygiene-Maßnahmen nachhaltig im Unternehmen zu etablieren?“

Akt I.:

- KMU-Herausforderungen
- Defizite von Leitfäden
- Design Prinzipien

AKT I.

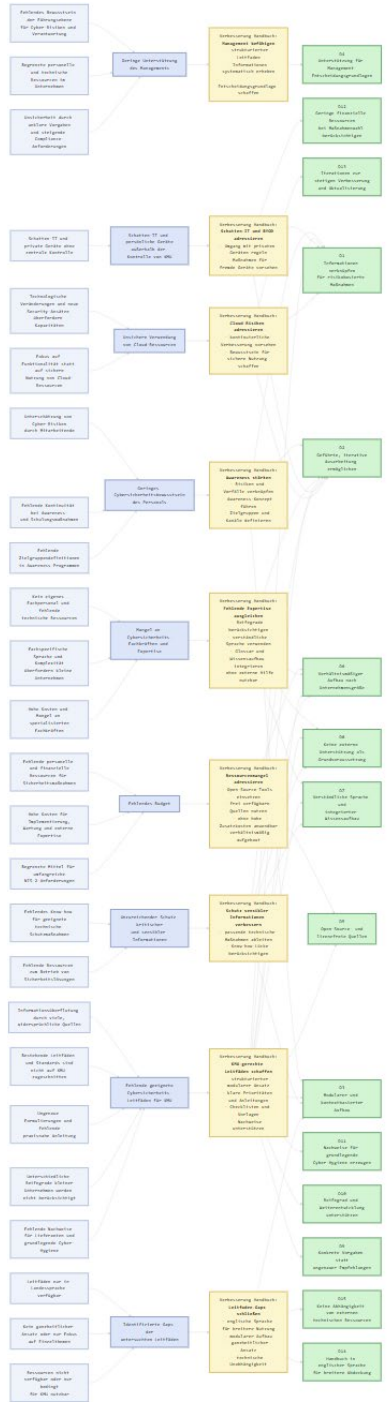
ANALYSE

8 KMU-Herausford d Defizite ergeben 15 Design

Analyse

Literatur & Leitfäden

zu KMU, NIS2 und Cyber-Hygiene



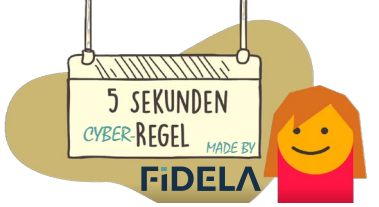
Defizite in bestehenden Leitf

zu spezifisch · Landesprac · ohne Rücksicht auf den R ät

Abgeleitet

15

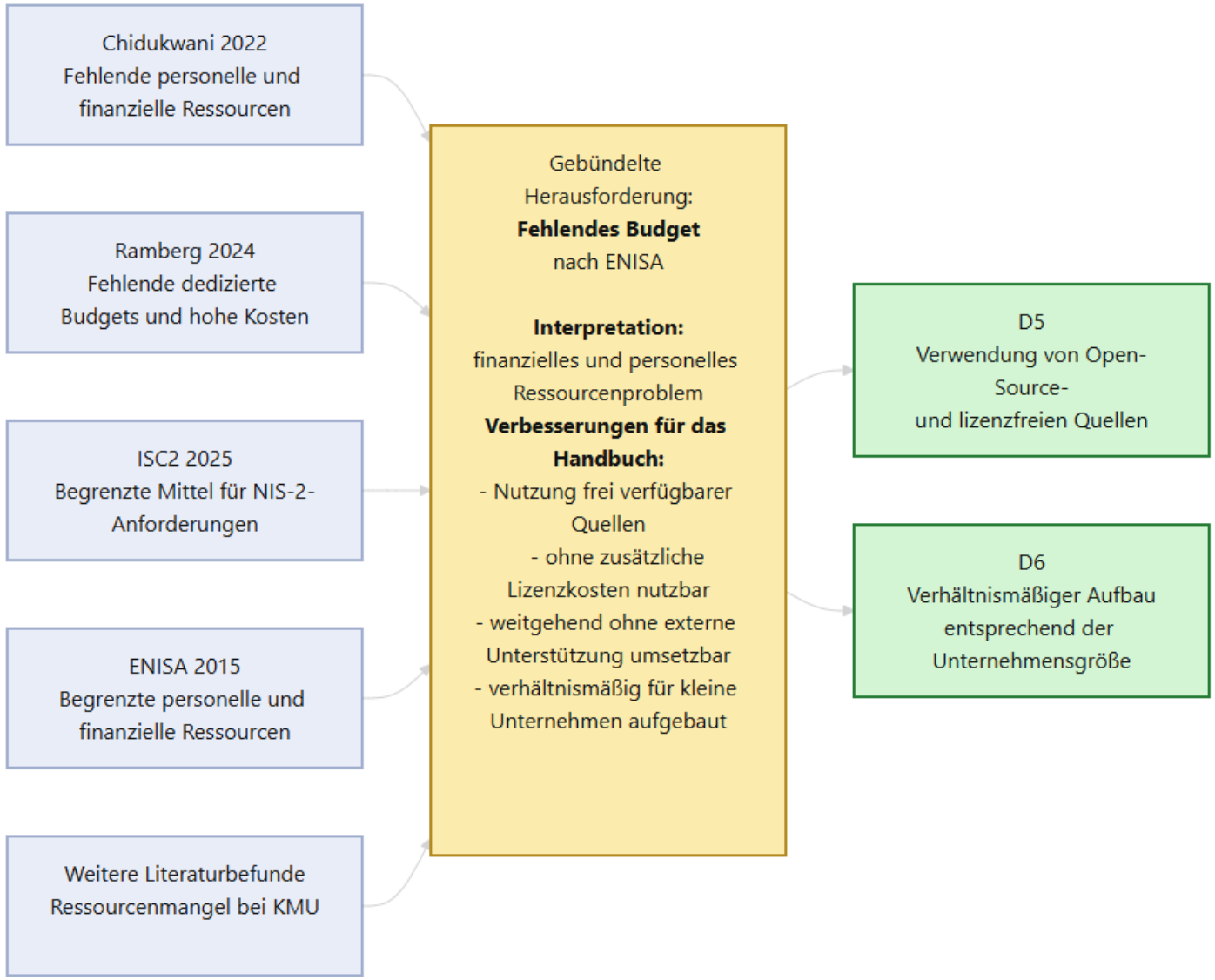
Design-Prinzipien für das CHMS/Handbuch



AKT I.

ANALYSE

Von Herausforderungen zu Design-Prinzipien





AKT I.

AKT III.

AKT II.

Forschungsfrage und Vorgehen

„Wie kann ein modular aufgebautes und an die spezifischen Bedürfnisse kleiner Unternehmen angepasstes Rahmenwerk zur Umsetzung der Risikomanagementmaßnahmen gemäß Artikel 21 der NIS2-Richtlinie gestaltet werden, um grundlegende Cyber-Hygiene-Maßnahmen nachhaltig im Unternehmen zu etablieren?“

Akt II.:

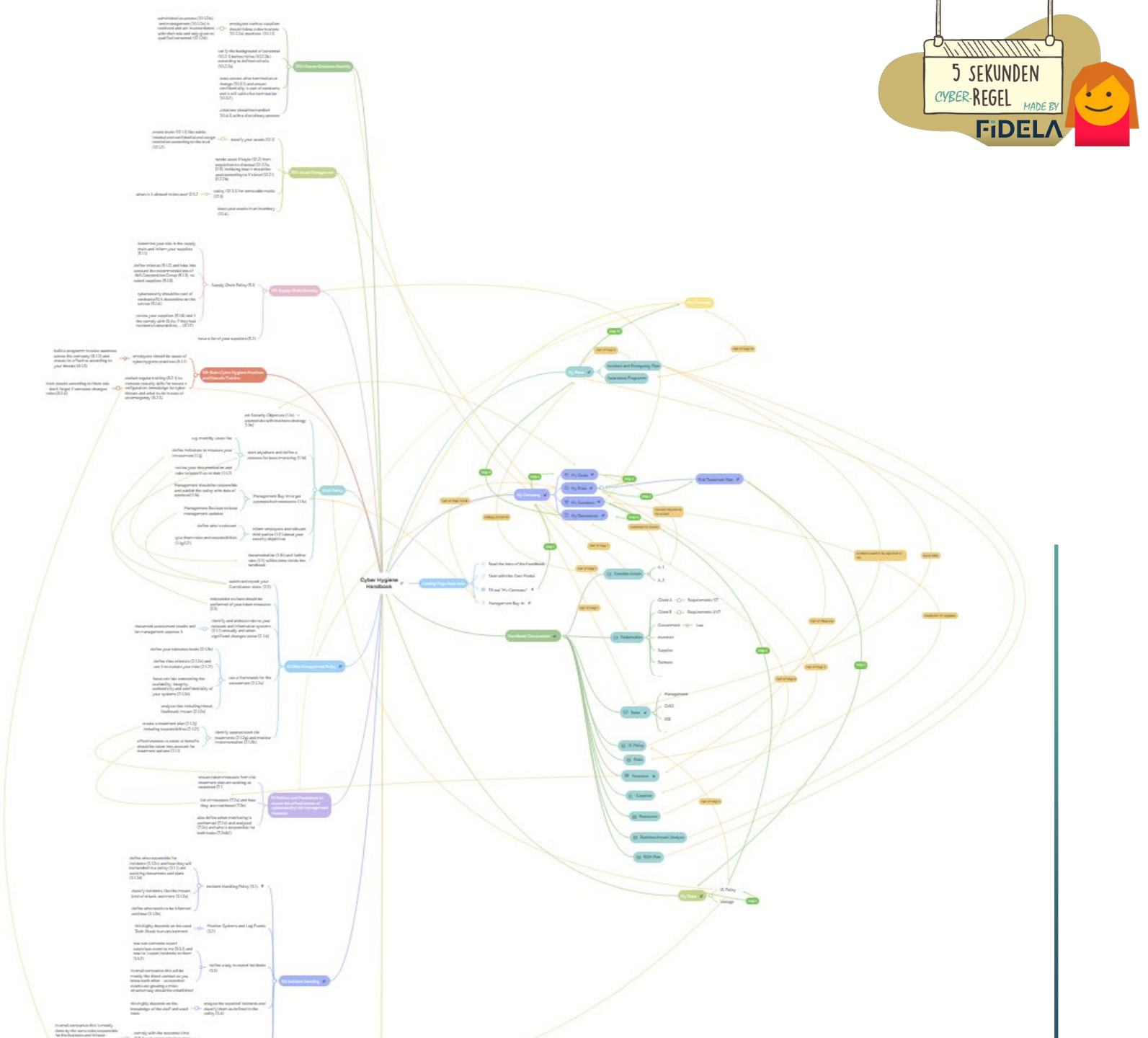
- Cyber Hygiene Management System bzw. Handbuch

AKT II.

HANDBUCH

Prototyp

Eigenschafte
Seiten
Worte/Zeic
Querverwe
Aufgaben
Fachbegrif
Referenzer
„Nächste S

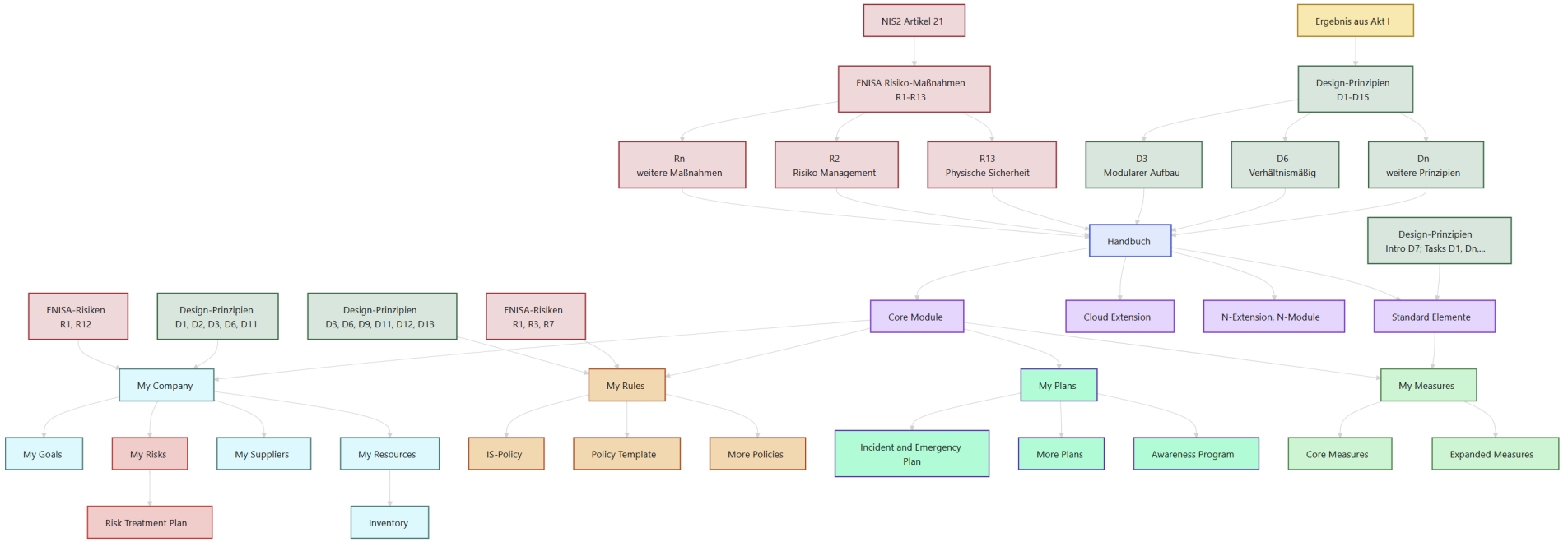


5 SEKUNDEN CYBER-REGEL MADE BY FIDELA

AKT II.

HANDBUCH

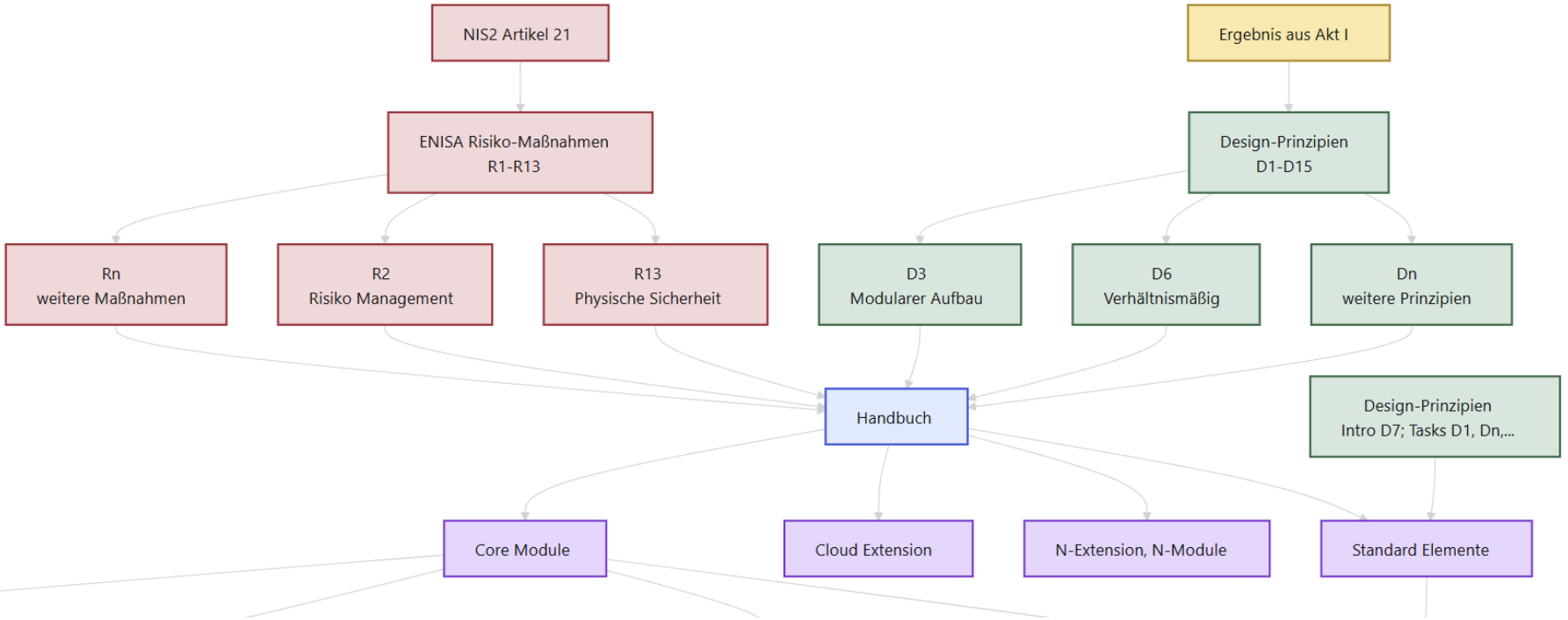
Ausgangslage und Aufbau



AKT II.

HANDBUCH

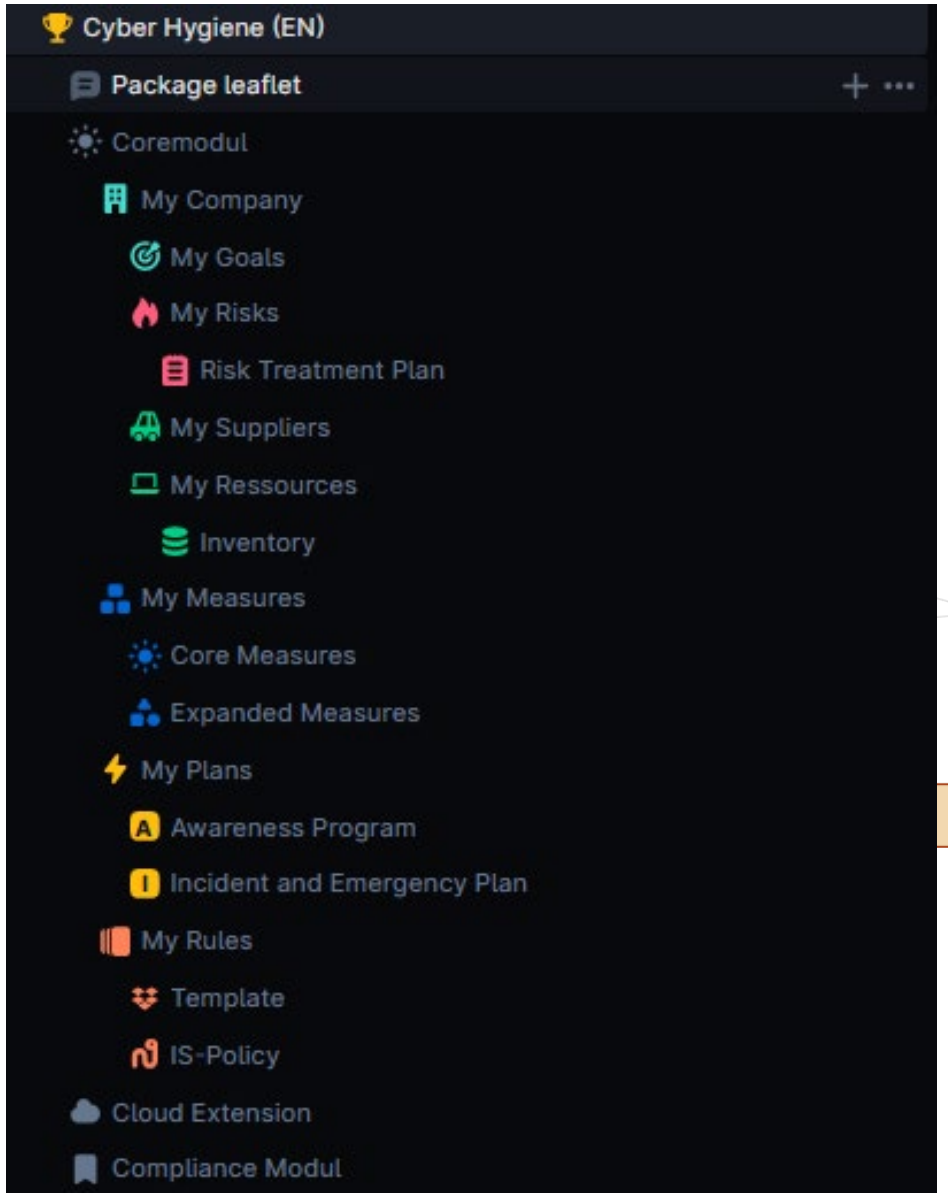
Ausgangslage und Aufbau

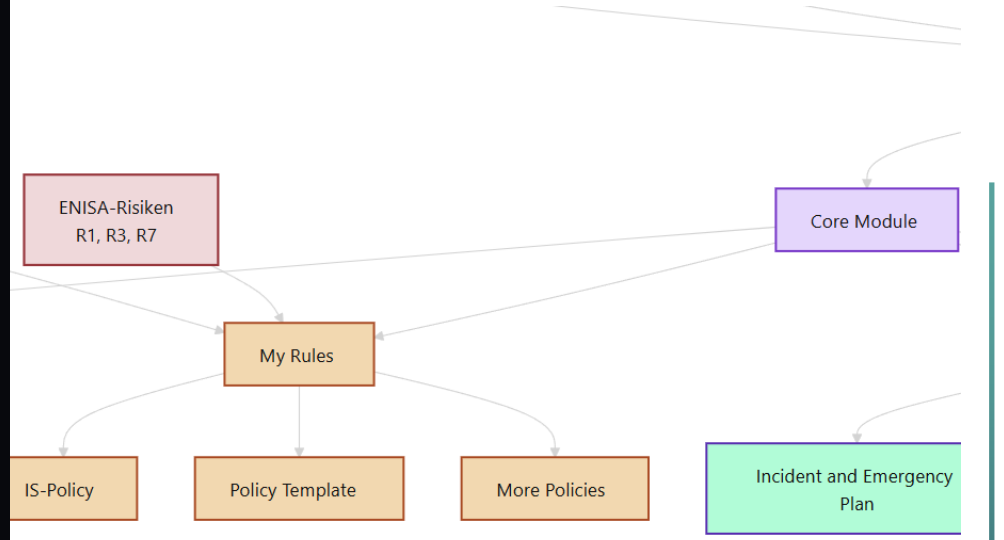


AKT II.

HANDBUCH

Seitenüberblick und Elemente





AKT II.

HANDBUCH

Seitenüberblick und Elemente

🚀 Overview of Measures

It's time to consolidate an **overview of existing and planned measures** and identify potential gaps.

💬 Terms

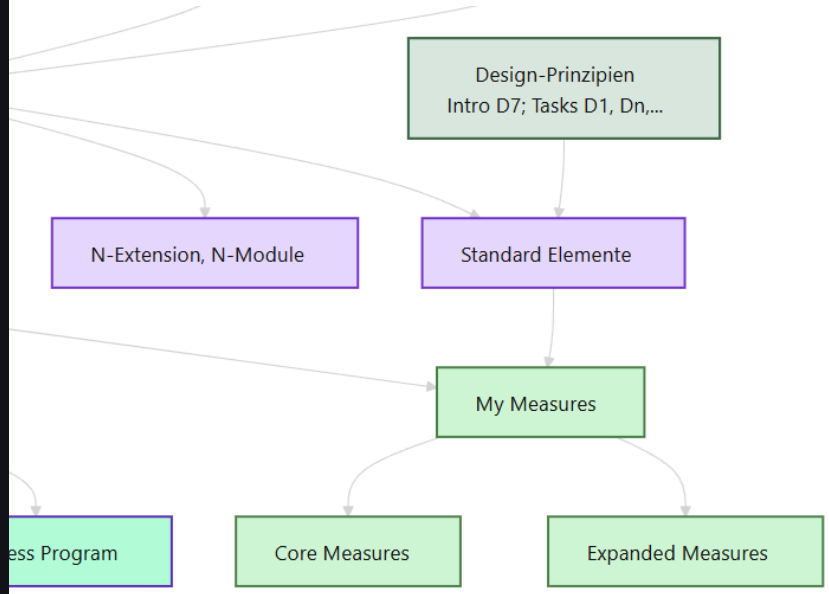
Term	Explanation
Statement of Applicability (SoA)	Document showing which security controls are implemented, planned, or intentionally excluded. Important for audits and compliance evidence.
Key Performance Indicator (KPI)	Measurable value assessing the effectiveness of a measure. Examples: patch compliance rate (% of critical patches within 30 days), average incident response time, employee training participation rate.
Effectiveness Assessment	Systematic review of whether a measure achieves its intended goal. ENISA recommends regular assessments via self-assessment, audits, penetration testing, or benchmarking.
Compliance Monitoring	Ongoing monitoring of compliance with security policies and regulatory requirements to detect deviations and corrective actions.
Risk Assessment	Systematic evaluation of cyber risks, identifying threats, vulnerabilities, and potential impact; forms the basis for prioritized measure planning.
KVP	Continuous improvement process for ongoing enhancement of security posture and operational effectiveness.

📚 References

- ISO/IEC 27001:2022 – 9.1 Monitoring, measurement, analysis, and evaluation
- ENISA Technical Implementation Guidance – Chapter 7: "Policies and Procedures to Assess the Effectiveness of Cybersecurity Risk-Management Measures"

⏭️ Next Step

Further modules or context-specific extensions can now be implemented. Prioritization is generally based on the risk assessment and the 🗄 Risk Treatment Plan





AKT I.

AKT III.

AKT II.

Forschungsfrage und Vorgehen

„Wie kann ein modular aufgebautes und an die spezifischen Bedürfnisse kleiner Unternehmen angepasstes Rahmenwerk zur Umsetzung der Risikomanagementmaßnahmen gemäß Artikel 21 der NIS2-Richtlinie gestaltet werden, um grundlegende Cyber-Hygiene-Maßnahmen nachhaltig im Unternehmen zu etablieren?“

Akt III.:

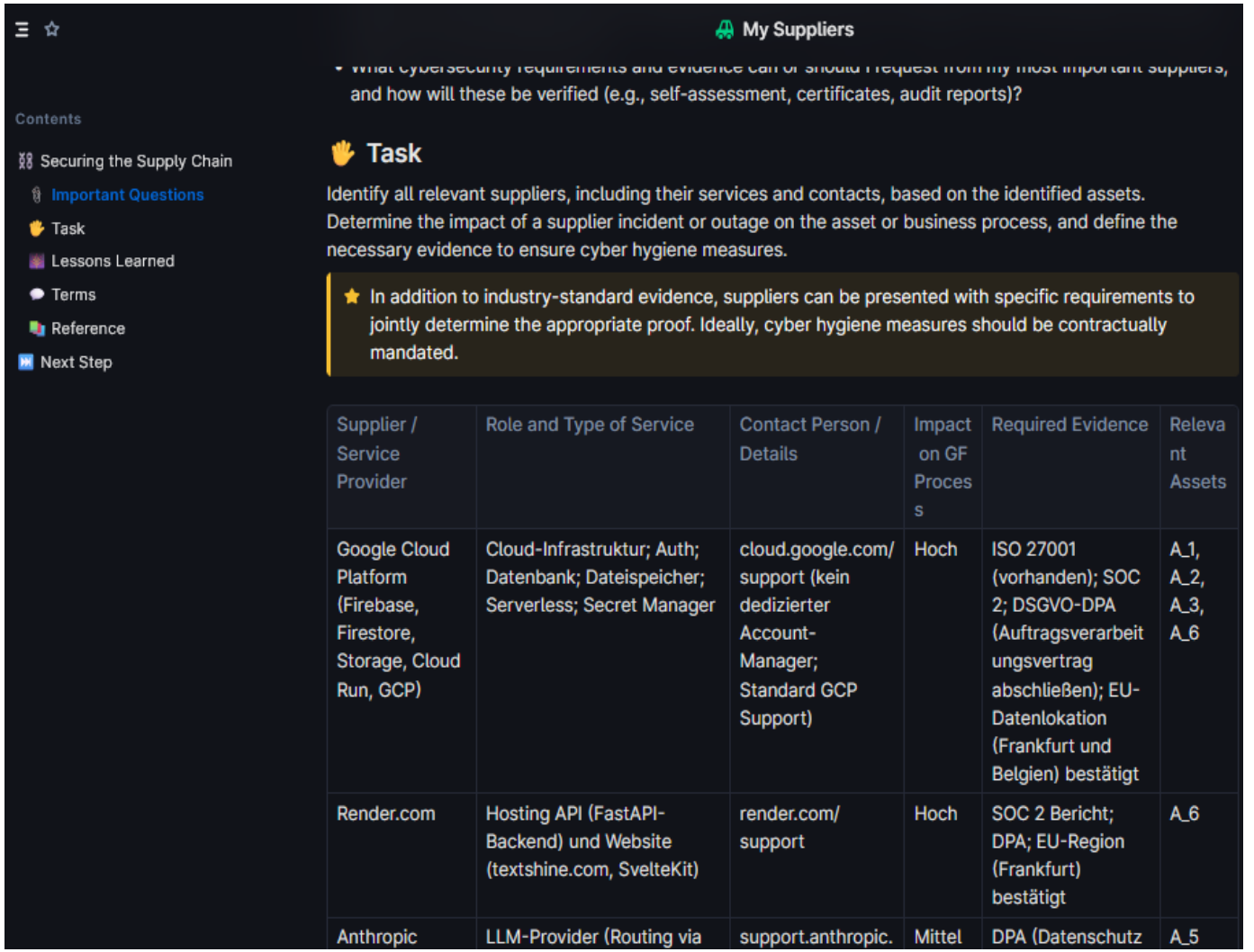
- von Anwender getestet
- von Experten bewertet

AKT III.

TESTEN

Validierung durch Anwender und Experten

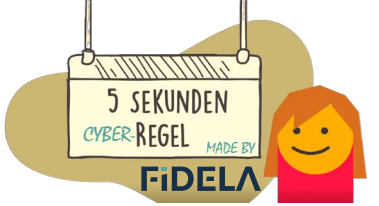
My Suppliers



Supplier / Service Provider	Role and Type of Service	Contact Person / Details	Impact on GF Process	Required Evidence	Relevant Assets
Google Cloud Platform (Firebase, Firestore, Storage, Cloud Run, GCP)	Cloud-Infrastruktur; Auth; Datenbank; Dateispeicher; Serverless; Secret Manager	cloud.google.com/support (kein dedizierter Account-Manager; Standard GCP Support)	Hoch	ISO 27001 (vorhanden); SOC 2; DSGVO-DPA (Auftragsverarbeitungsvertrag abschließen); EU-Datenlokation (Frankfurt und Belgien) bestätigt	A_1, A_2, A_3, A_6
Render.com	Hosting API (FastAPI-Backend) und Website (textshine.com, SvelteKit)	render.com/support	Hoch	SOC 2 Bericht; DPA; EU-Region (Frankfurt) bestätigt	A_6
Anthropic	LLM-Provider (Routing via	support.anthropic.	Mittel	DPA (Datenschutz	A_5

AKT III.

TESTEN



Das Handbuch überzeugt, Zeit und Fachwissen bleiben knapp

Experten

wirksam

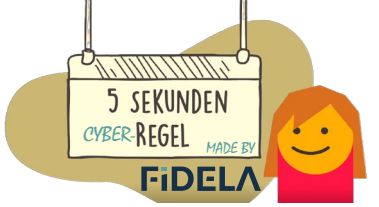
um kleine Unternehmen bei der Erfüllung von NIS2 Anforderungen zu unterstützen

Anwender

verständlich, klar, relevant

positive Einschätzung in den Interviews, aber …

Verbesserungswürdig: „Zeit und Fachkenntnisse“



Von der Masterarbeit zum Forschungsprojekt

AKT I. Analyse

AKT II. Handbuch

AKT III. Testen

Masterarbeit

AKT IV. Projekt

FFG Forschungsprojekt (beantragt)

Cyber Hygiene Managementsystem für KMUs

FFG Forschung wirkt.

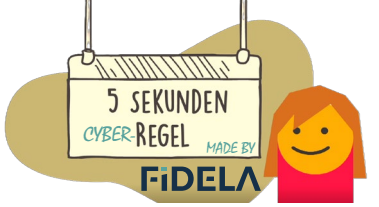
FiDELA

University of Applied Sciences St. Pölten

Textshine

AKT IV.

PROJEKT



Was gilt es zum Lösen im Forschungsprojekt?

Cyber Hygiene für kleine Unternehmen braucht eine geführte, laufend pflegbare, verhältnismäßige Umsetzungshilfe.

Wie kann man die ISO/IEC 27001 und NIS2 verhältnismäßig umsetzen?

Cyber Hygiene muss sich laufend weiterentwickeln

Mithilfe einer Community über eine Open-Source-Strategie?

„Zeit und Fachkenntnisse“ bleibt ein Problem

KI als Gamechanger?

AKT IV.

PROJEKT

Vom Pr

09/2026

Phase 1
Pilot & KI

CHMS im Pilotunt
einführen

Fehlende Erweite
ergänzen

KI-gestützte Befül
entwickeln

◆ **CHMS V1 prax**

S

03/2028

3
uung & Analyse

unity betreuen

ack auswerten

iterentwicklung?



FIDELA

Cyber-Hygiene-Managementsystem für KMUs

F&E Projektplan

mit

FFG
Forschung wirkt.

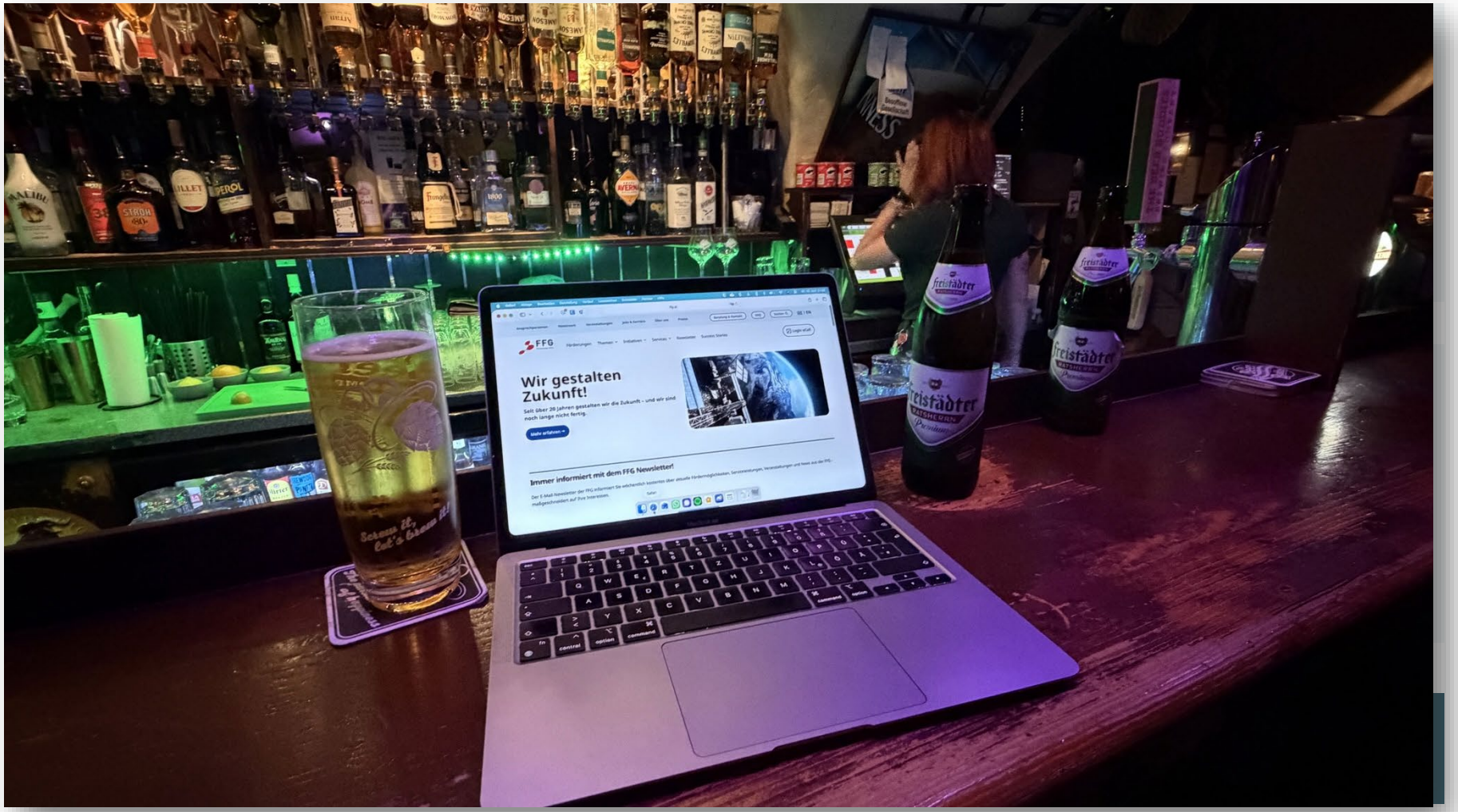
Fidela GmbH
Hofgasse 7
4020 Linz
Österreich

AKT IV.

PROJEKT

Lessons Learned

Expedition Forschungsantrag

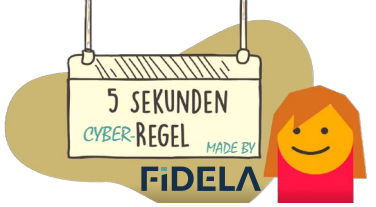


AKT IV.

PROJEKT

Warum Open Source und KI?

Open Source hält das CHMS aktuell, KI unterstützt in der Ausarbeitung



Open Source + **KI** = **Cyber-Hygiene für KMU**

Hürde: *Leitfäden für eine breite Masse aktuell halten*

- **Community hält Inhalte aktuell**
- Offene Inhalte schaffen Vertrauen
- Frei verfügbar, keine Lizenzkosten

Hürde: *Im Team fehlen Zeit und Fachwissen*

- Befüllt das Handbuch aus vorhandener Doku vor
- Schlägt passende Maßnahmen vor
- Ein Mensch prüft und entscheidet

Ergebnis: *ein lebendes Managementsystem statt Papier*

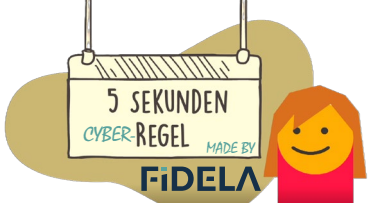
- NIS2-Maßnahmen verhältnismäßig umsetzen
- Ohne eigenes Security-Team
- Nachweis gegenüber Kunden und Lieferkette

AKT IV.

PROJEKT

Umsetzungsmöglichkeiten

Das CHMS direkt verwenden oder als Kontextbasis nutzen



KI befüllt das CHMS gemeinsam mit Verantwortlichen

Unternehmen
Doku, Antworten auf Rückfragen

KI →

CHMS befüllt
Kontextbasiertes Handbuch

→ **direkt als MS nutzen**

→ **als Kontextbasis für ein eigenes MS**
z. B. unterstützt durch Vorlagen

KI wählt Maßnahmen auf Basis des Kontexts und der Anforderungen

Anforderung
NIS2 Art. 21, NISG 2026
Kunden, usw.

↔

Kontext
Branche, Größe, Kundenanforderungen

↔

Maßnahme
passend und verhältnismäßig

AKT IV.

PROJEKT

Stand September 2026

Praxisbeispiel Textshine



Februar 2026 · Handbuch in 2 Tagen KI-gestützt ausgearbeitet

16 Aufgaben erledigt	**22** Rückfragen zum Unternehmen beantwortet	**120** Tabellenzeilen ausgefüllt	**7** Risiken bewertet	**≈2.500** Wörter Textshine-spezifisch ergänzt

↓ *ab Juli überführt, zugeschnitten auf ein kleines Cloud-Team*

Seit Juli 2026 · MS in Notion, schlank, aber verbindlich

3 Richtlinien in Kraft	**3** Richtlinien im Review	**1** Schulung im Einsatz	**8** Seiten mit MS-Inhalt	**3** Dokumente in Kunden-Audits: FAQ, TOMs, AVV

Quelle: Textshine, Praxisbericht, Stand 24.09.2026



Cyber Hygiene Management System

Teil der Community werden?

Scannen oder schreiben an:

dominik@fidela.at