Automatisierte und assistierte Erstellung von IT-Sicherheitskonzepten auf Basis des IT-Grundschutz

OMNISECURE 2026

Prof. Dr.-Ing. habil. Gerhard Wunder
Freie Universität Berlin & Fraunhofer AISEC

PhD Cand. Lea Muth

Freie Universität Berlin

19. Januar 2026

Agenda

1 Motivation

2 IT-Grundschutz

3 Unser Ansatz

4 Zukünftige Entwicklung

Motivation

- Bewältigung der wachsenden Bedrohungslage im Bereich Cyberkriminalität in Europa
- Schreibt EU-Organisationen robuste Cybersicherheitsrahmenwerke vor
- Inkrafttreten: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz 6. Dezember 2025
- Strafen: Bis zu 10 Millionen Euro oder 2 % des weltweiten Umsatzes bei Nichteinhaltung

NIS-2-Richtlinie

Netzwerk- und Informationssicherheit Richtlinie

Mangel an Fachkräften

Rückgang des Anteils der Beschäftigten im Sicherheitsbereich

Hohe Zertifizierungskosten

31,2 Milliarden Euro pro Jahr in der gesamten EU

Komplexität der Anforderungen

Rapide Entwicklung im Bereich der “Compliance”

Kleine und mittlere Unternehmen (KMU)

Zielgruppe

* Bitkom-Studie „Wirtschaftsschutz 2024“
** Enisa

Klassische IT-Sicherheitskonzepte:

- Hohe Kosten
- Geringe Verfügbarkeit
  + lange Wartezeiten (Fachkräftemangel)
- Änderungen an der Infrastruktur und der Bedrohungslage erfordern eine Neubeauftragung

Der Einsatz von KI bietet:

- Niedrige Kosten durch Automatisierung
- Sofort verfügbar
- Ermöglicht fortlaufende KI-gestützte Änderungen zu geringen Kosten

Der Vorteil der Automatisierung

Idee

IT-Grundschutz Methodik

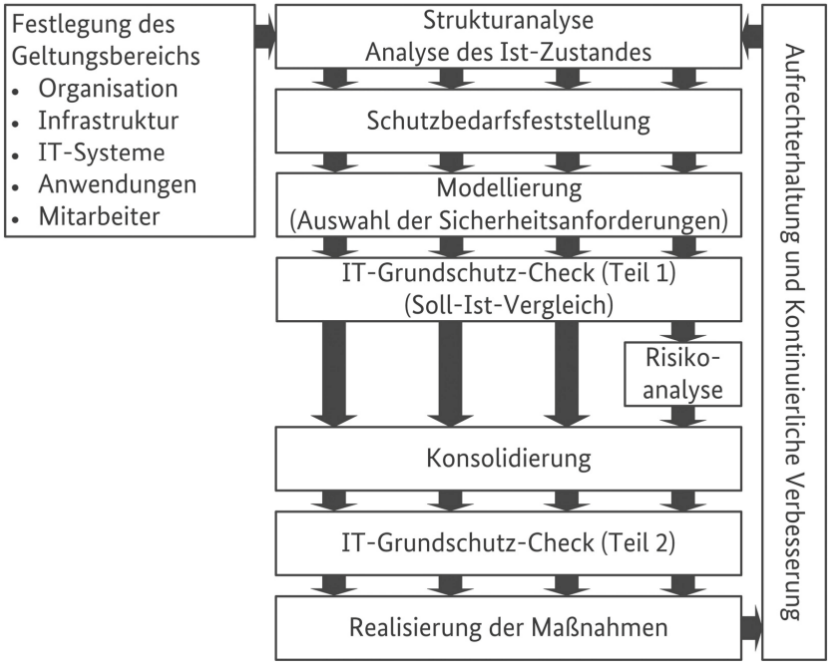
Das etablierte Sicherheitsframework des BSI’s für ein kontinuierliches Sicherheitskonzept

Überblick

- Das etablierte Sicherheitsframework des deutschen BSI (ISO/IEC 27001 kompatibel)
- Grundlage für die Zertifizierung; modular, deckt mehrere Organisationstypen ab
- Bestehend aus vier Standards:
  - 200-1: Managementsysteme für Informationssicherheit
  - 200-2: IT-Grundschutz Methodik
  - 200-3: Risikomanagement
  - 200-4: Business continuity management

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz Methodik

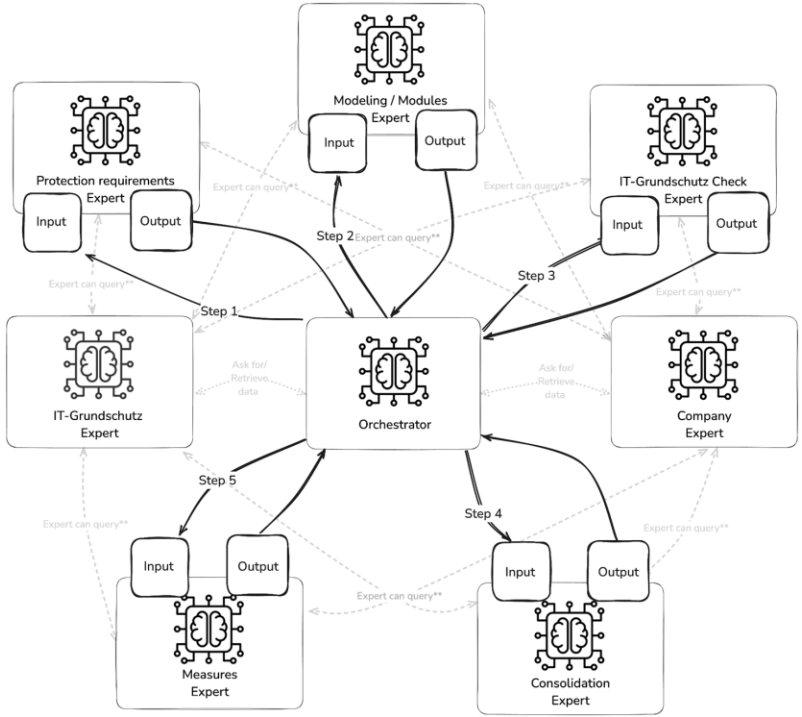


Neunstufiger Zertifizierungsprozess

IT-Grundschutz Methodik

Unser Ansatz

KI-gestützte Erstellung von IT-Sicherheitskonzepten

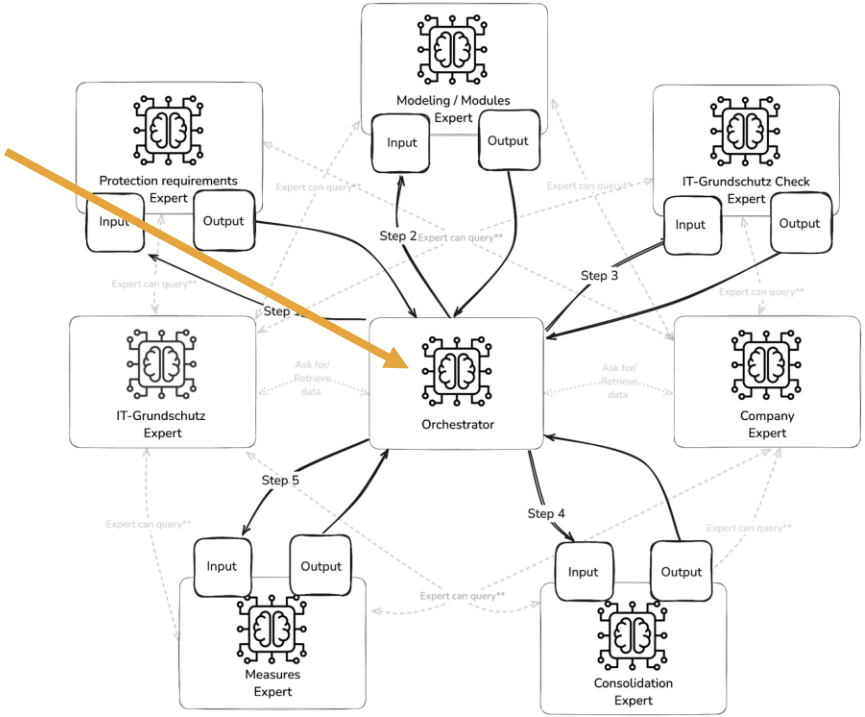


1x Orchestrator, 2x Wissensexperten und 5x Aufgabenexperten

Multi-Agenten System Architektur

Experts:

- Orchestrator: Plant und verteilt Aufgaben + Überprüft die Eingaben und Ausgaben.

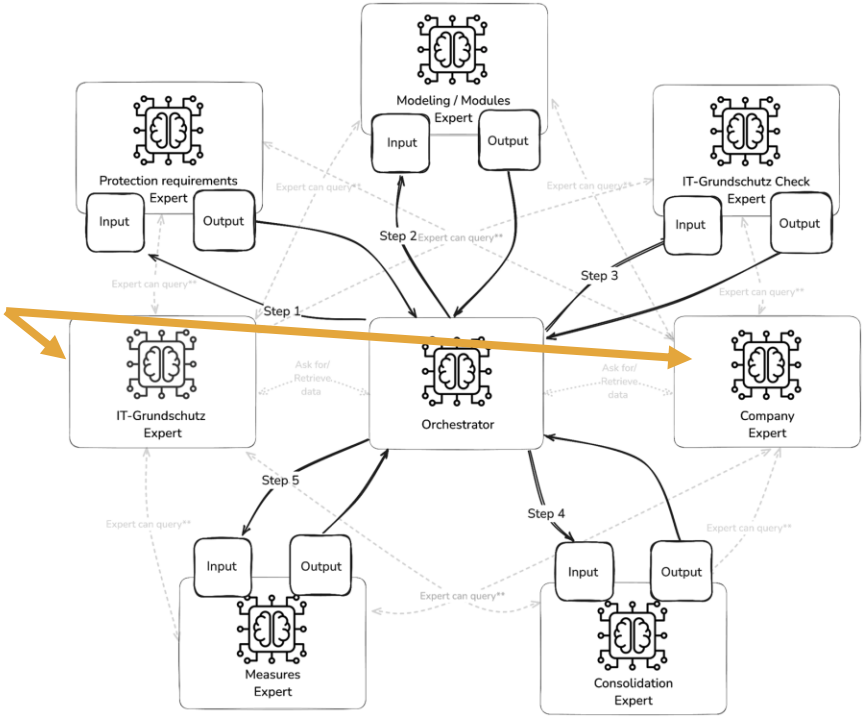


1x Orchestrator, 2x Wissensexperten und 5x Aufgabenexperten

Multi-Agenten System Architektur

Experts:

- Orchestrator: Plant und verteilt Aufgaben + Überprüft die Eingaben und Ausgaben.
- Knowledge Experts: IT-Grundschutz Experte, Unternehmens Experte.

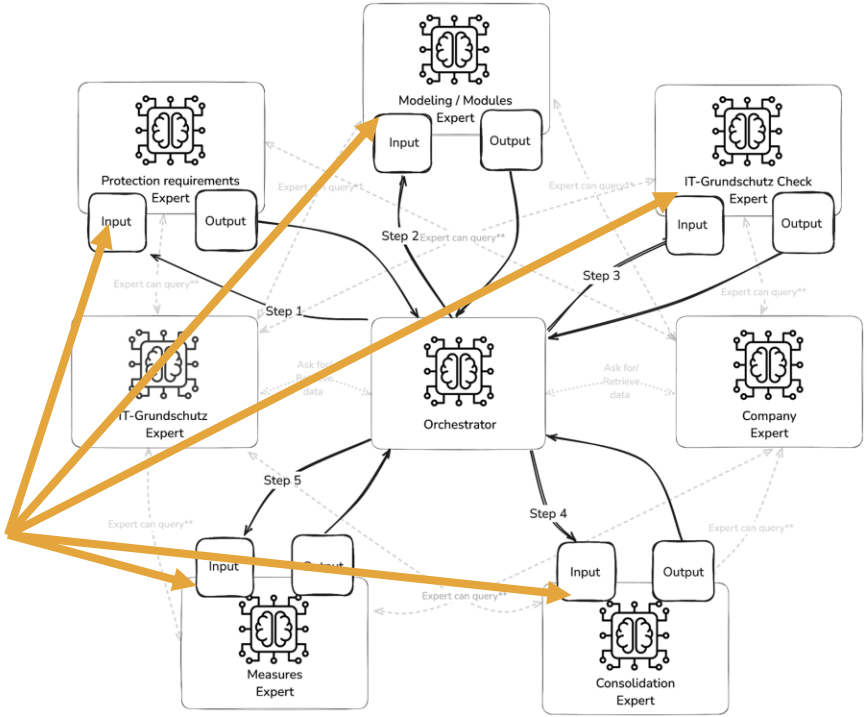


1x Orchestrator, 2x Wissensexperten und 5x Aufgabenexperten

Multi-Agenten System Architektur

Experts:

- Orchestrator: Plant und verteilt Aufgaben + Überprüft die Eingaben und Ausgaben.
- Knowledge Experts: IT-Grundschutz Experte, Unternehmens Experte.
- Task Experts: Schutzbedarfsfestellung, Modellierung, IT-Grundschutz Check, Konsolididierung und Umsetzung.

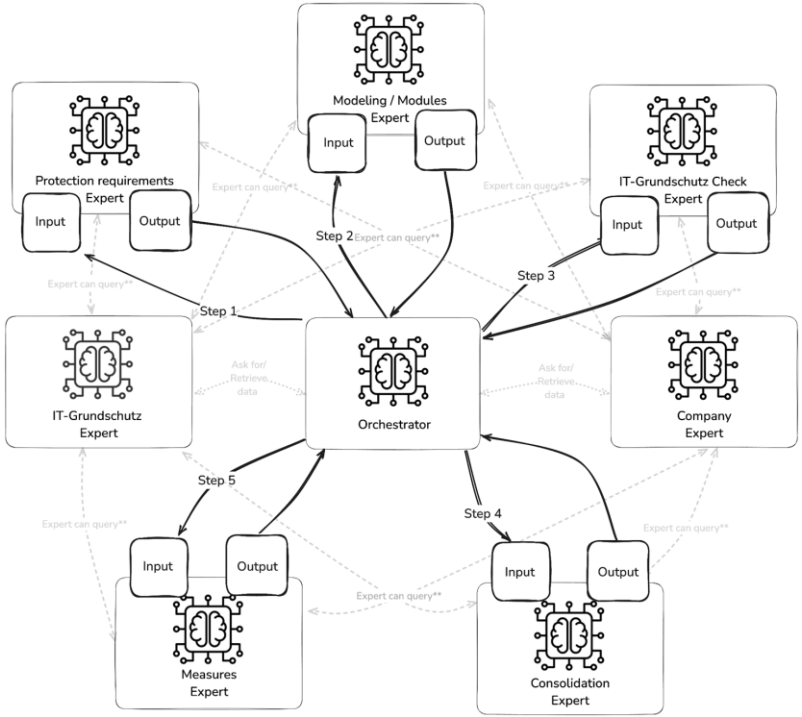


1x Orchestrator, 2x Wissensexperten und 5x Aufgabenexperten

Multi-Agenten System Architektur

Wissensbasen:

- Mehrere aufgabenspezifische Agenten.

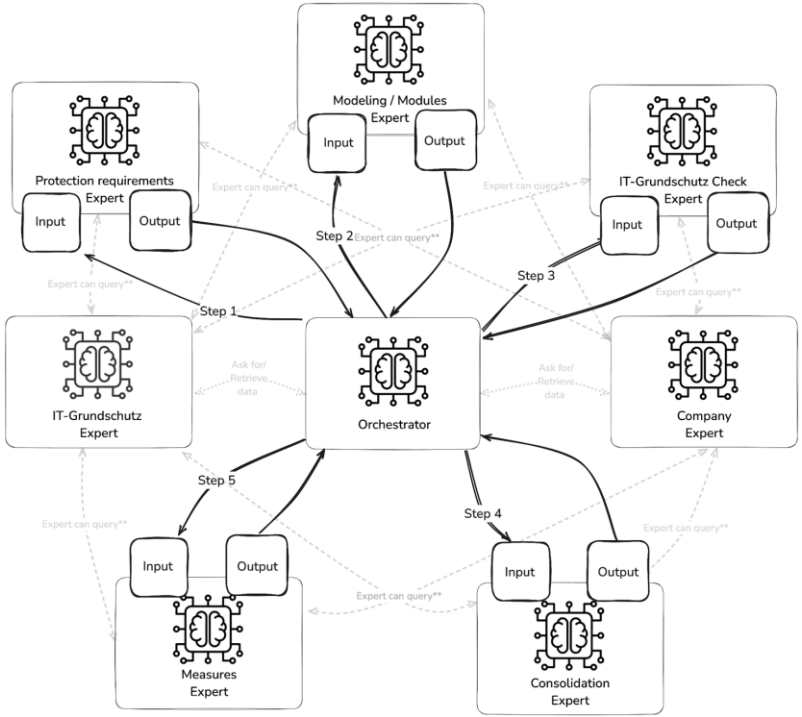


Wissensgraph, HybridRag und aufgabenbezogene LLMs

Multi-Agenten System Architektur

Wissensbasen:

- Mehrere aufgabenspezifische Agenten.
- Hybrid Retrieval-Augmented Generation (HybridRAG).

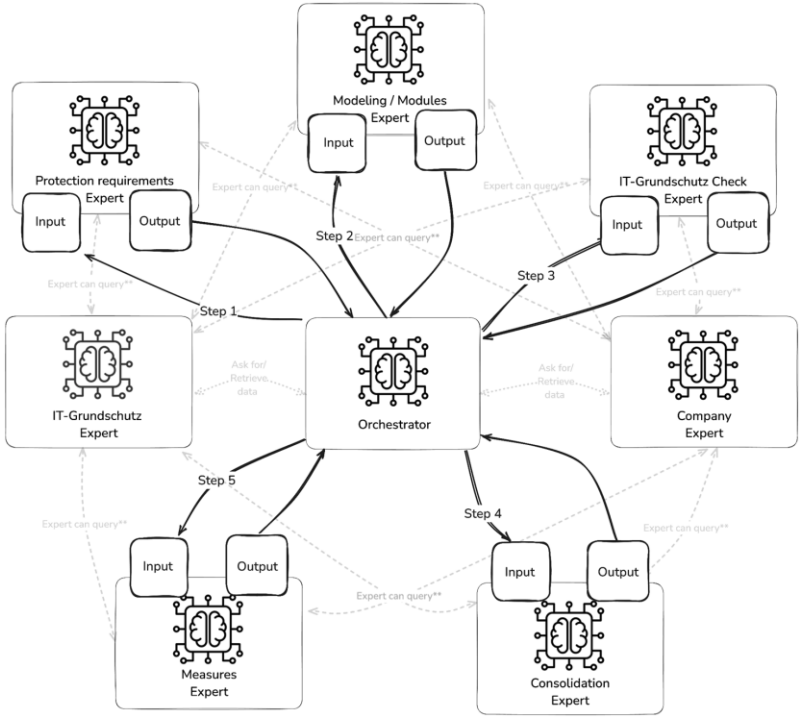


Wissensgraph, HybridRAG und aufgabenbezogene LLMs

Multi-Agenten System Architektur

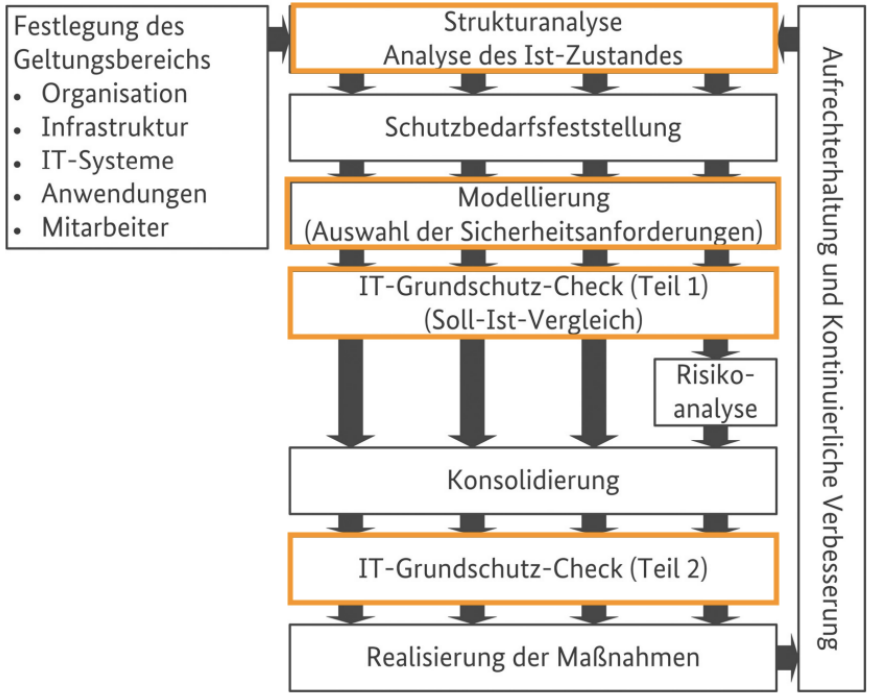
Wissensbasen:

- Mehrere aufgabenspezifische Agenten.
- Hybrid Retrieval-Augmented Generation (HybridRAG).
- Knowledge Graphen für eine strukturierte Datenrepresentation.



Wissensgraph, HybridRag und aufgabenbezogene LLMs

Multi-Agenten System Architektur



Neunstufiger Zertifizierungsprozess

IT-Grundschutz Methodik

Zukünftige Entwicklung

- Ausweitung auf IT-Grundschutz++ ab 2026
- Erweiterung des Prototyps für eine vollständige Bewertung
- Umfassende Tests mit authentischen Unternehmensdaten

&
Limitierungen

- Ein Werkzeug, kein Ersatz für den Menschen: Die endgültige Entscheidungsgewalt liegt weiterhin bei den zertifizierten Sachverständigen

Kooperationspartner

Pinnipedia Technologies

Dr. Jürgen Laartz

Enterpreneur; Berater Anwendungen der Künstlichen Intelligenz und digitale Transformation

1993 -2017 Partner McKinsey

Prof. Dr. Marian Margraf

Lehrstuhl Informationssicherheit an der Freien Universität Berlin und Abteilungsleitung am Fraunhofer-AISEC

2003-2013 Referent im BSI und BMI

Prof. Dr. Gerhard Wunder

Lehrstuhl Cybersecurity and AI an der Freien Universität Berlin und KI-Abteilungsleitung am Fraunhofer-AISEC

Prof. Dr. Sören Werth

Professur für IT-Sicherheit an der Berliner Hochschule für Technik und Berater Bundesagentur für Digitalfunk

2008-2017 Referent im BSI und BMI

Benedikt Groß

Wissenschaftlicher Mitarbeiter an der Freien Universität Berlin am Lehrstuhl Cybersecurity and AI.

Weitere Kooperationspartner

Quellen

1. European Parliament and Council of the European Union, “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive),” Official Journal of the European Union, vol. L333, pp. 80–152, Dec. 2022.

2. Frontier Economics, “Assessing the economic impact of EU initiatives on cybersecurity,” Jul. 2023. Available: https://www.frontier-economics.com/media/izyk5rgz/assessing-theeconomic- cost-of-eu-initiatives-on-cybersecurity.pdf.(Accessed: 2025-03-08)

3. Bundesamt für Sicherheit in der Informationstechnik, “ITGrundschutz-Kompendium,” Edition 2023. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/ITGS-Kompendium/IT Grundschutz

Vielen Dank für Ihre Zeit!

Kontakt Information

Name: Lea Muth

Linked-In: QR-Code

E-Mail: Lea.Muth@fu-berlin.de