Sichere Informationsnetze bei kleinen und mittleren Energieversorgern

SIDATE

VDI-Fachtagung IT-Sicherheit für Kritische Infrastrukturen

Stand zur IT-Sicherheit deutscher Stromnetzbetreiber

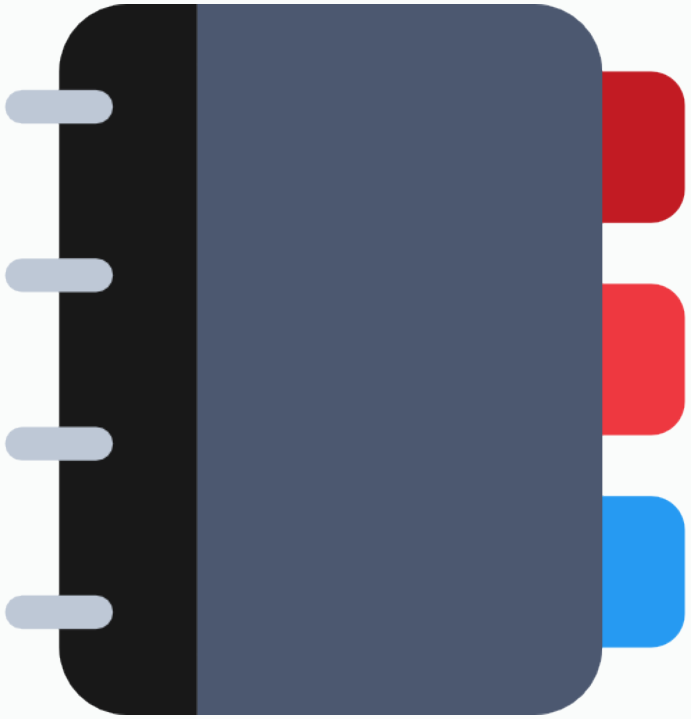
GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Dr. Sebastian Pape

15.05.2018/VDI, Neuss

Agenda

- SIDATE-Projekt
- Umfrage-Überblick
- Ausgewählte Ergebnisse
  - Prozesse und Organisation
  - Leitsystem
  - ISMS
- Fazit



SIDATE – Projekt Partner

Federal Ministry of Education and Research

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

TÜVRheinland®
Genau. Richtig.

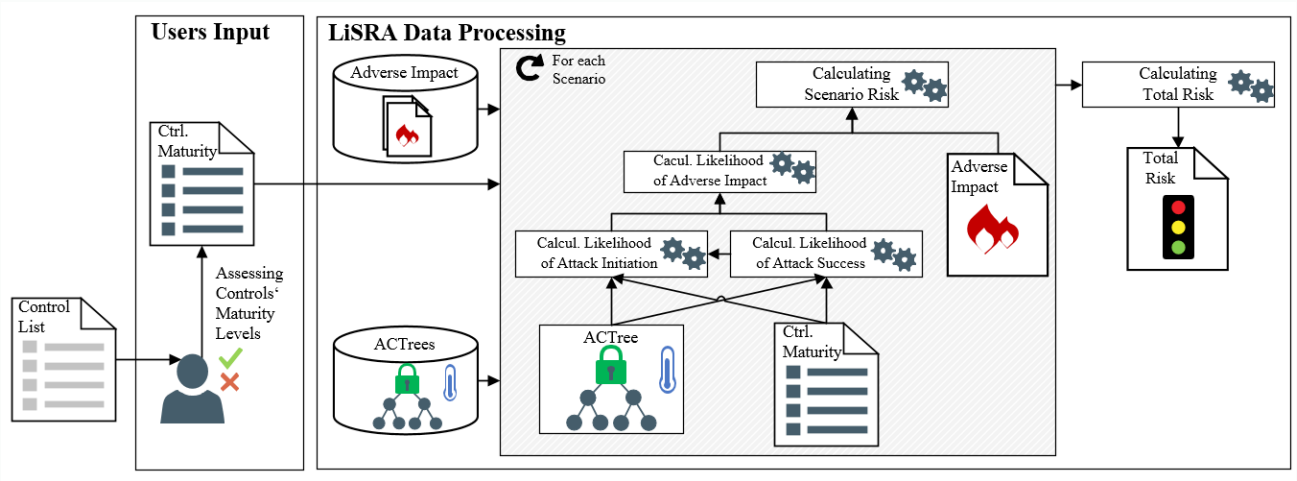
UNIVERSITÄT SIEGEN

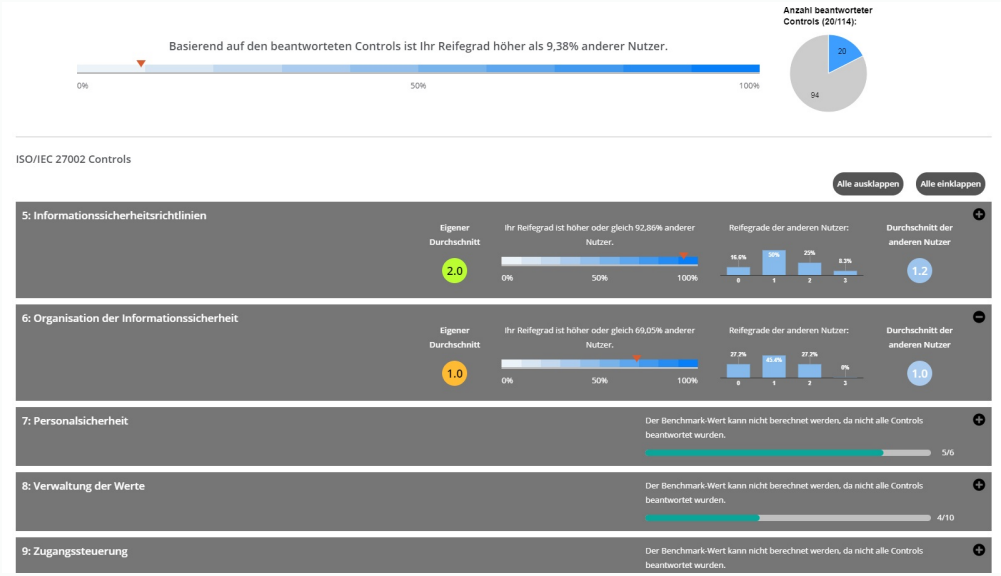
regio iT

ASEW DAS EFFIZIENZ-NETZWERK FÜR STADTWERKE

Projektziele und -ergebnisse

- Unterstützung kleiner und mittlerer Energieversorger
  - Messung von Sicherheit
  - Aufbau einer interorganisationalen Wissensdatenbank und Austauschplattform





DASHBOARD

MASSNAHMEN

FRAGEN&ANTWORTEN

SELBSTBEWERTUNG

DOKUMENTE

FEEDBACK

IMPRESSUM

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

5. Informationssicherheitsrichtlinien

Ihr Durchschnitt: 2

Sie gehören zu den besten: 50% (0% – 50% – 100%)

Reifegrade der anderen Nutzer: 25% | 25% | 25% | 25% | 0% | 0% (0;1) | (1;2) | (2;3) | (3;4) | (4;5) | N/A

Durchschnitt der anderen Nutzer: 1,6

Subgroup 5.1: Vorgaben der Leitung für Informationssicherheit

Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.

Ihr Durchschnitt: 2

Sie gehören zu den besten: 50% (0% – 50% – 100%)

Reifegrade der anderen Nutzer: 25% | 25% | 25% | 25% | 0% | 0% (0;1) | (1;2) | (2;3) | (3;4) | (4;5) | N/A

Durchschnitt der anderen Nutzer: 1,6

Control 5.1.1: Informationssicherheitsrichtlinien

Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.

Ihr Reifegrad: 3

Sie gehören zu den besten: 50% (0% – 50% – 100%)

Reifegrade der anderen Nutzer: 0% | 0% | 0% | 25% | 25% | 0% | 50% (0 | 1 | 2 | 3 | 4 | 5 | N/A)

Durchschnitt der anderen Nutzer: 3,5

Control 5.1.2: Überprüfung der Informationssicherheitsrichtlinien

Die Informationssicherheitsrichtlinien werden in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

Ihr Reifegrad: 1

Sie gehören zu den besten: 50% (0% – 50% – 100%)

Reifegrade der anderen Nutzer: 50% | 0% | 0% | 50% | 0% | 0% | 0% (0 | 1 | 2 | 3 | 4 | 5 | N/A)

Durchschnitt der anderen Nutzer: 1,5

6. Organisation der Informationssicherheit

Ihr Durchschnitt

Sie gehören zu den besten: 38,89%

Reifegrade der anderen Nutzer

Durchschnitt der anderen Nutzer

Umfrage - Überblick

881 Briefe im August 2016

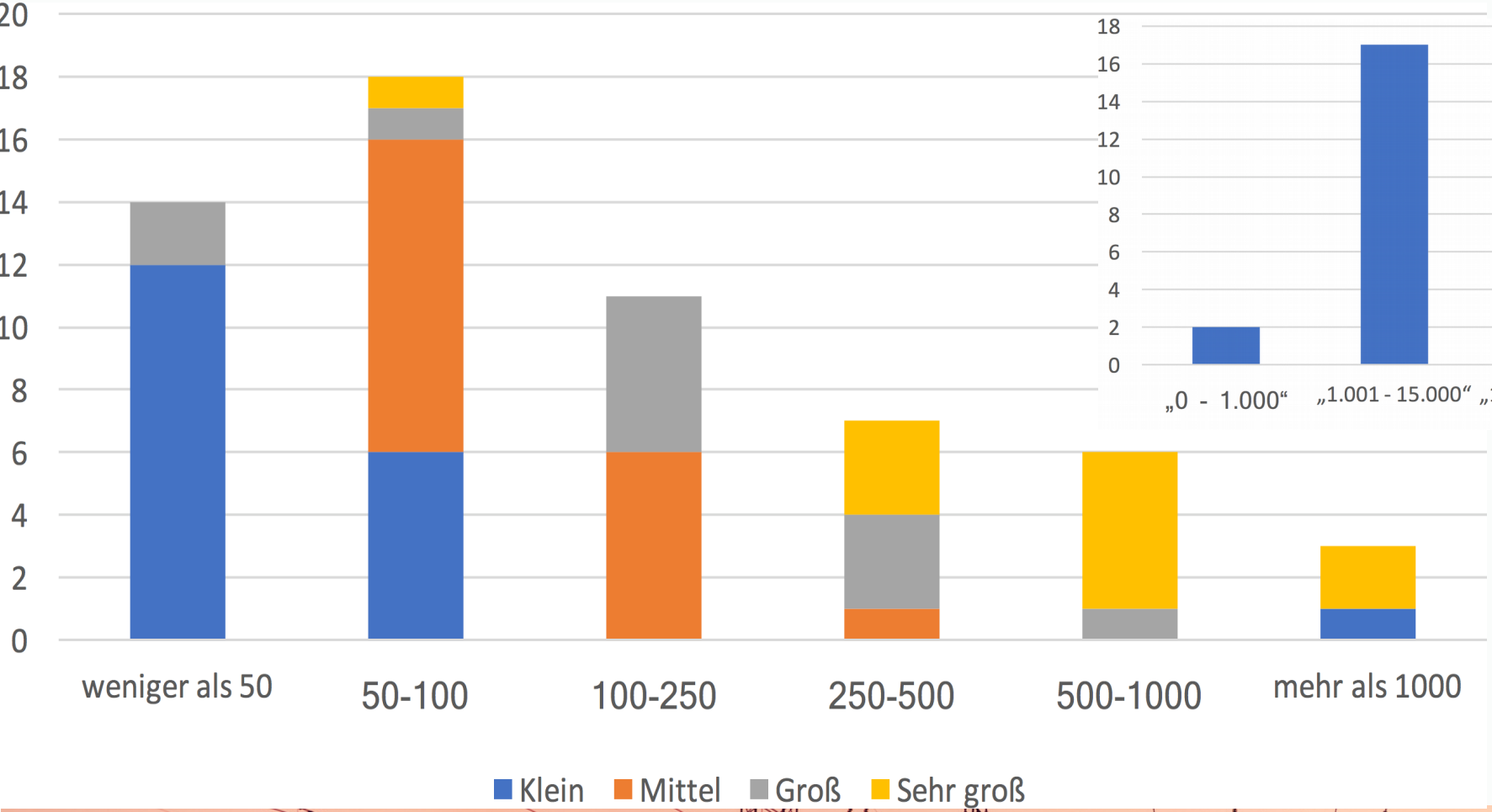
An BNetzA gelistete Energieversorger

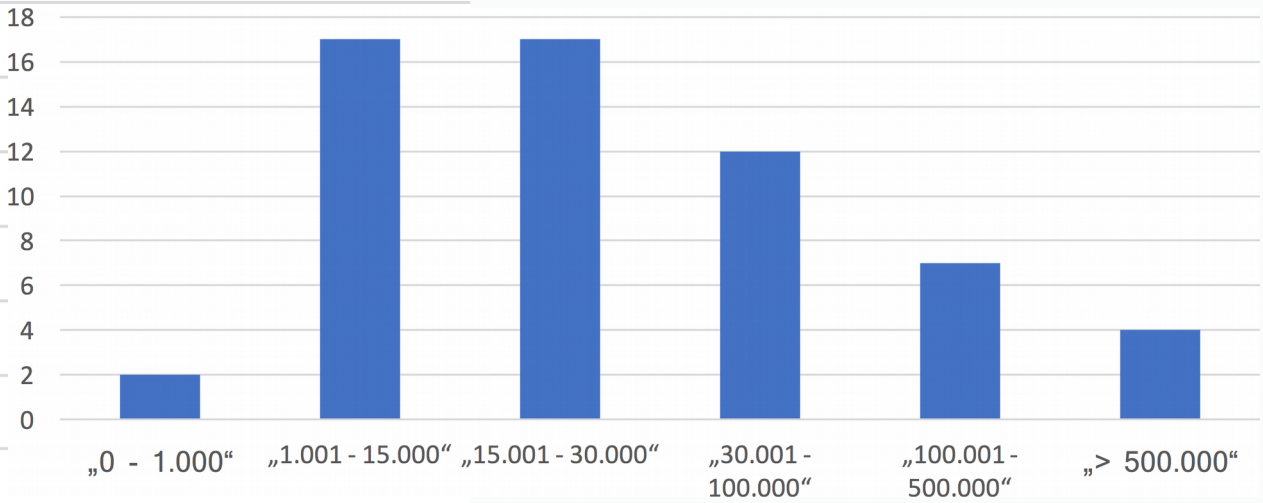
61 Antworten (6,9%)

51 Fragen

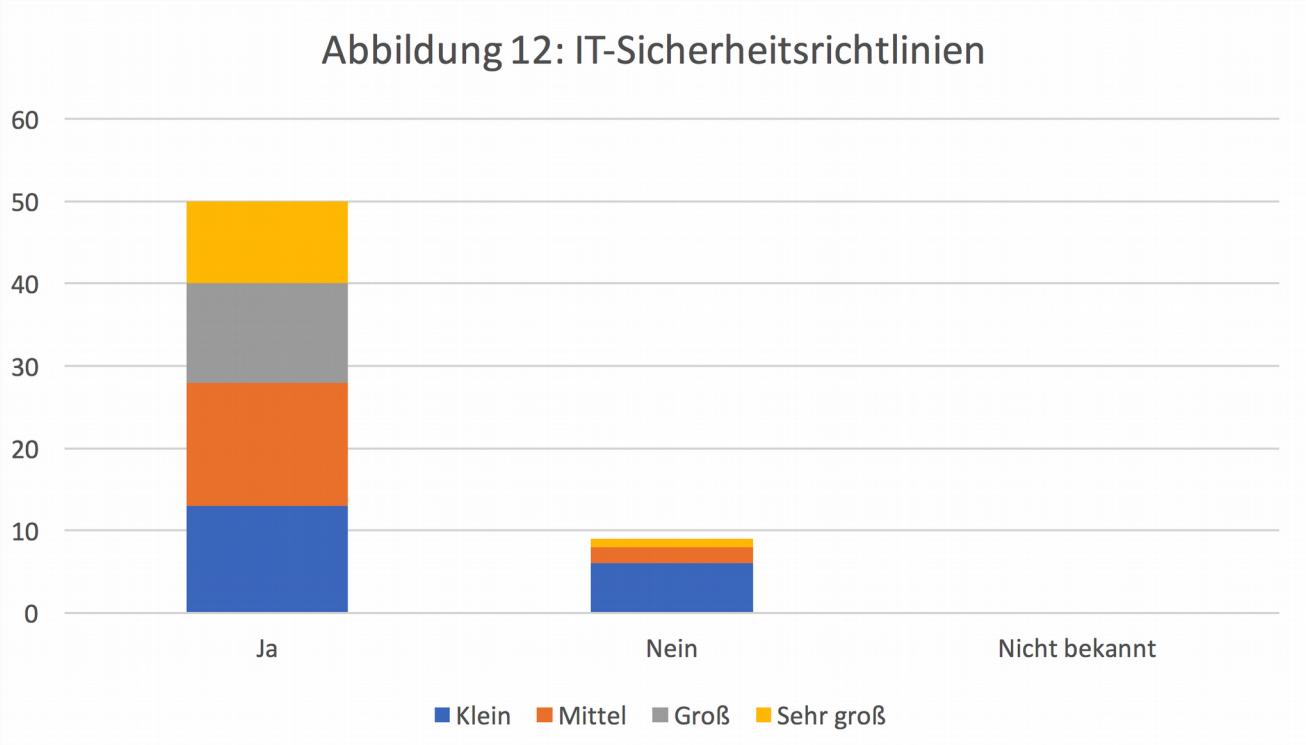
- Allgemeine Informationen
- Prozesse und Organisation
- ISMS
- Büro IT
- Leitsystem

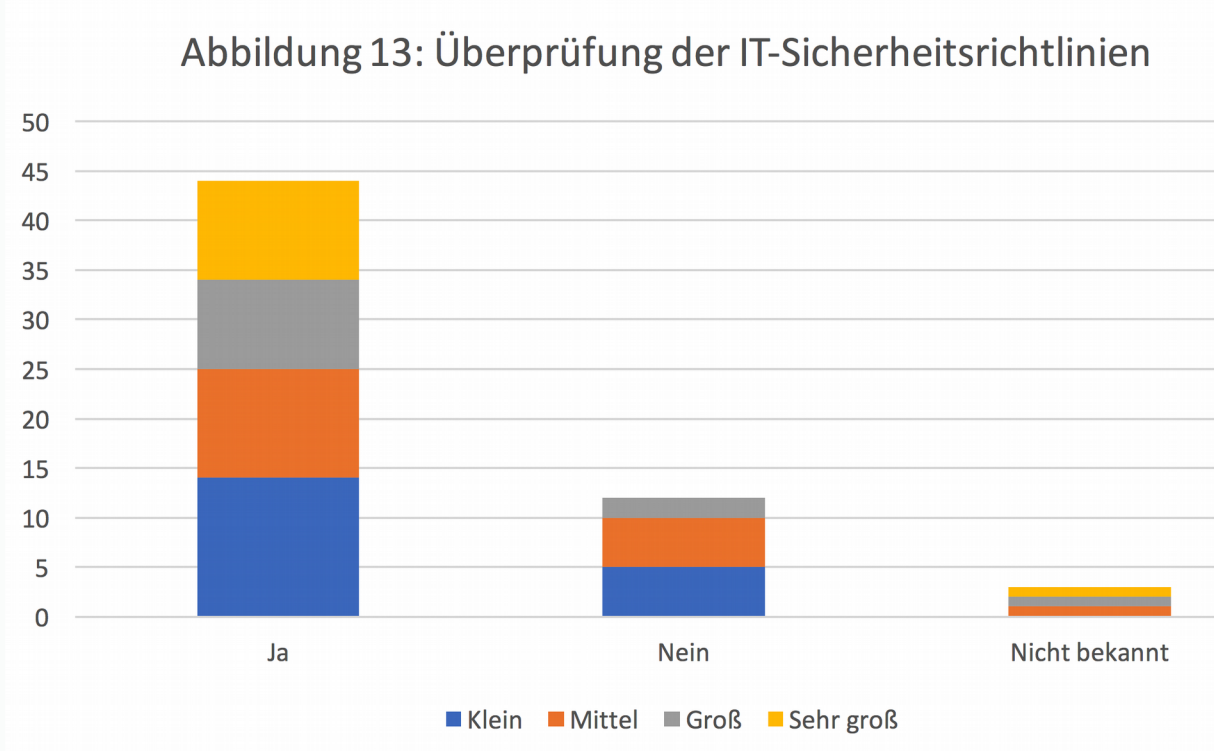
Mitarbeiter und Zählpunkte





Sicherheitsrichtlinien





Sicherheitsaudits

Abbildung 29: Durchführung von Sicherheitsaudits, Schwachstellentests oder Penetrationstests

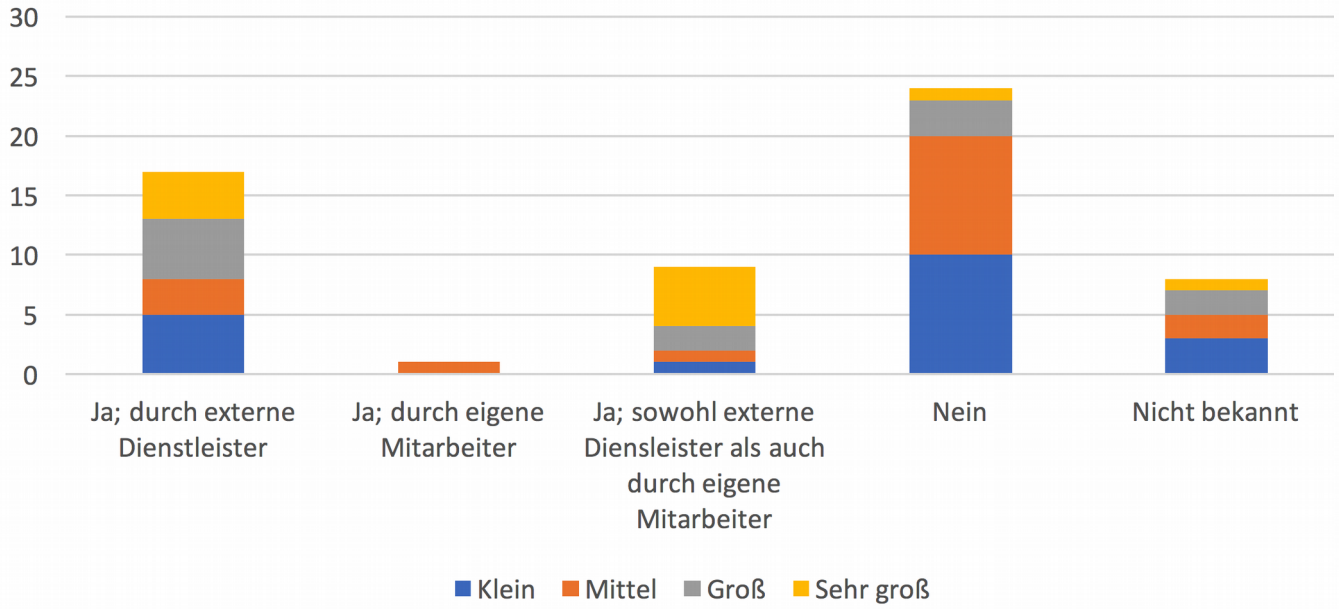
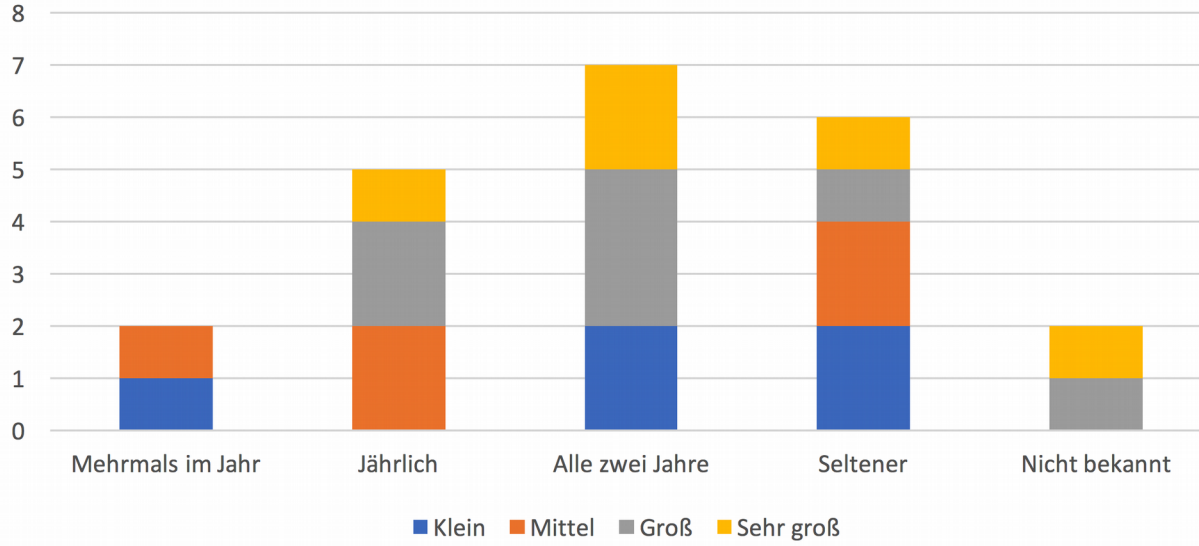


Abbildung 30: Häufigkeit zur Durchführung von Schwachstellenscans oder Penetrationstests



Risikoanalysen

Abbildung 27: IT-Risikoanalysen für Prozesse und IT-Systeme der Netzsteuerung

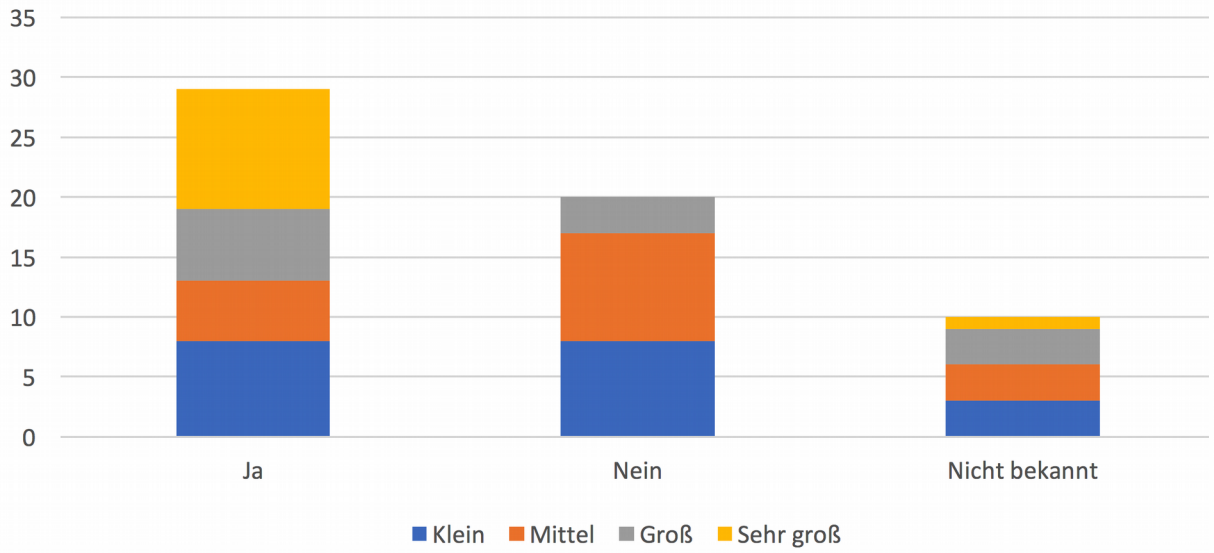
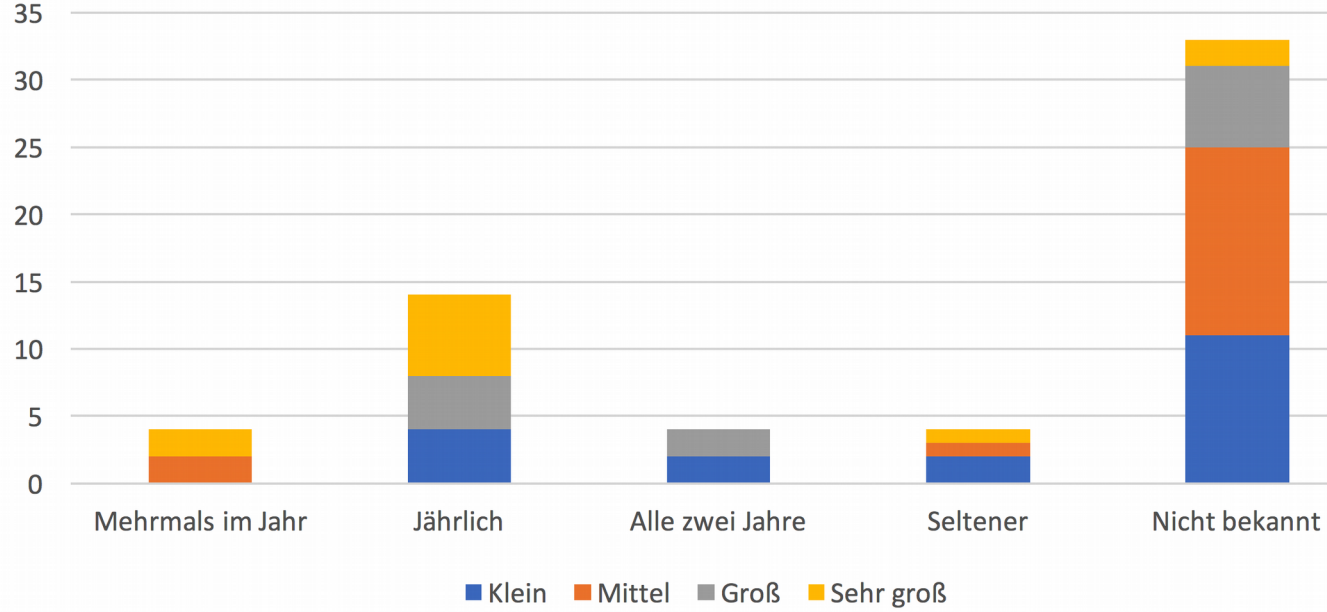


Abbildung 28: Häufigkeit der Durchführung der Risikoanalysen



Leitsystem

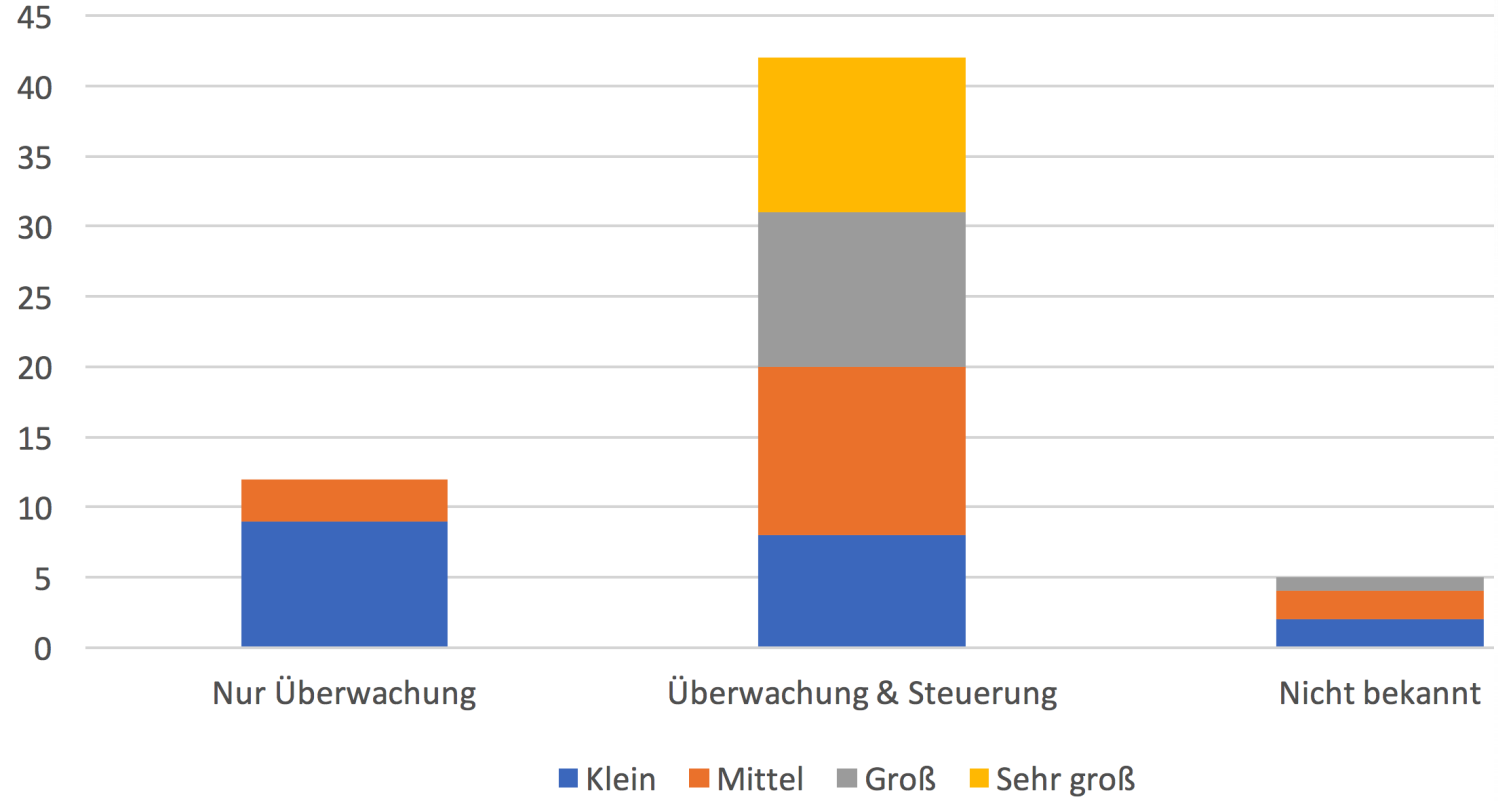


Abbildung 14: Aufgaben des Leitsystem
45
40
35
30
25
20
15
10
5
0
Nur Überwachung
Überwachung & Steuerung
Nicht bekannt
Klein
Mittel
Groß
Sehr groß

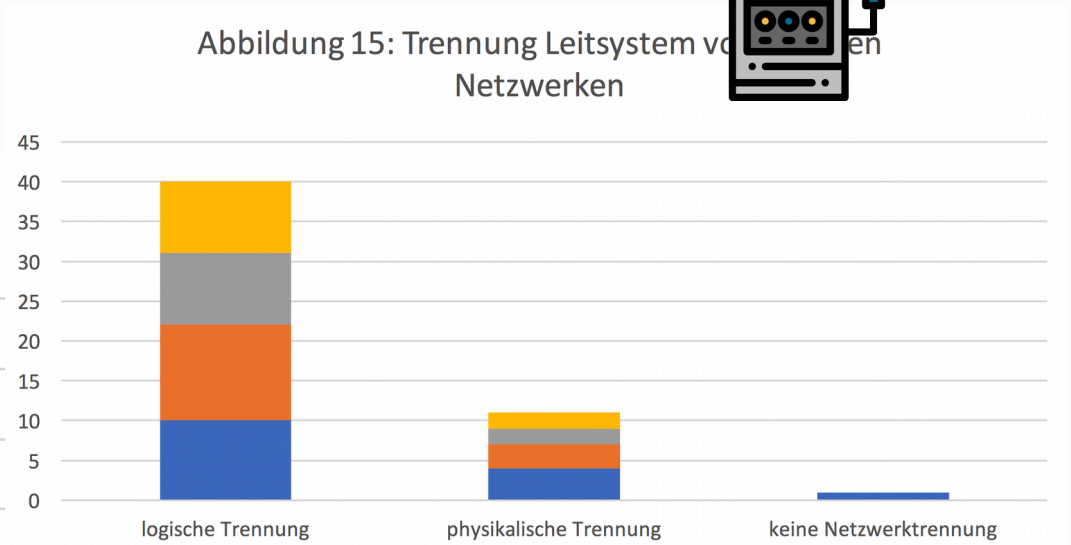


Abbildung 15: Trennung Leitsystem vo en Netzwerken
45
40
35
30
25
20
15
10
5
0
logische Trennung
physikalische Trennung
keine Netzwerktrennung

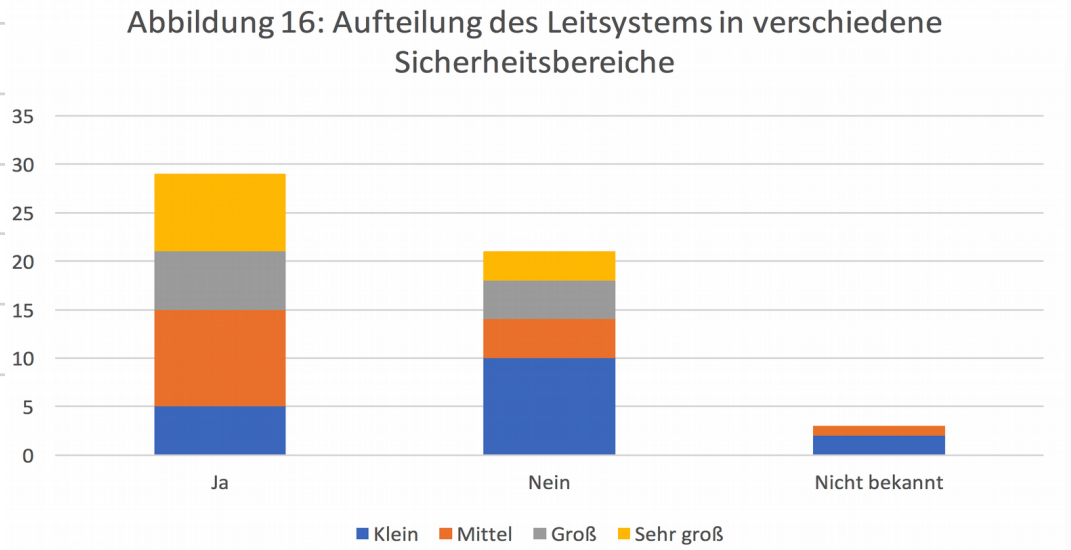
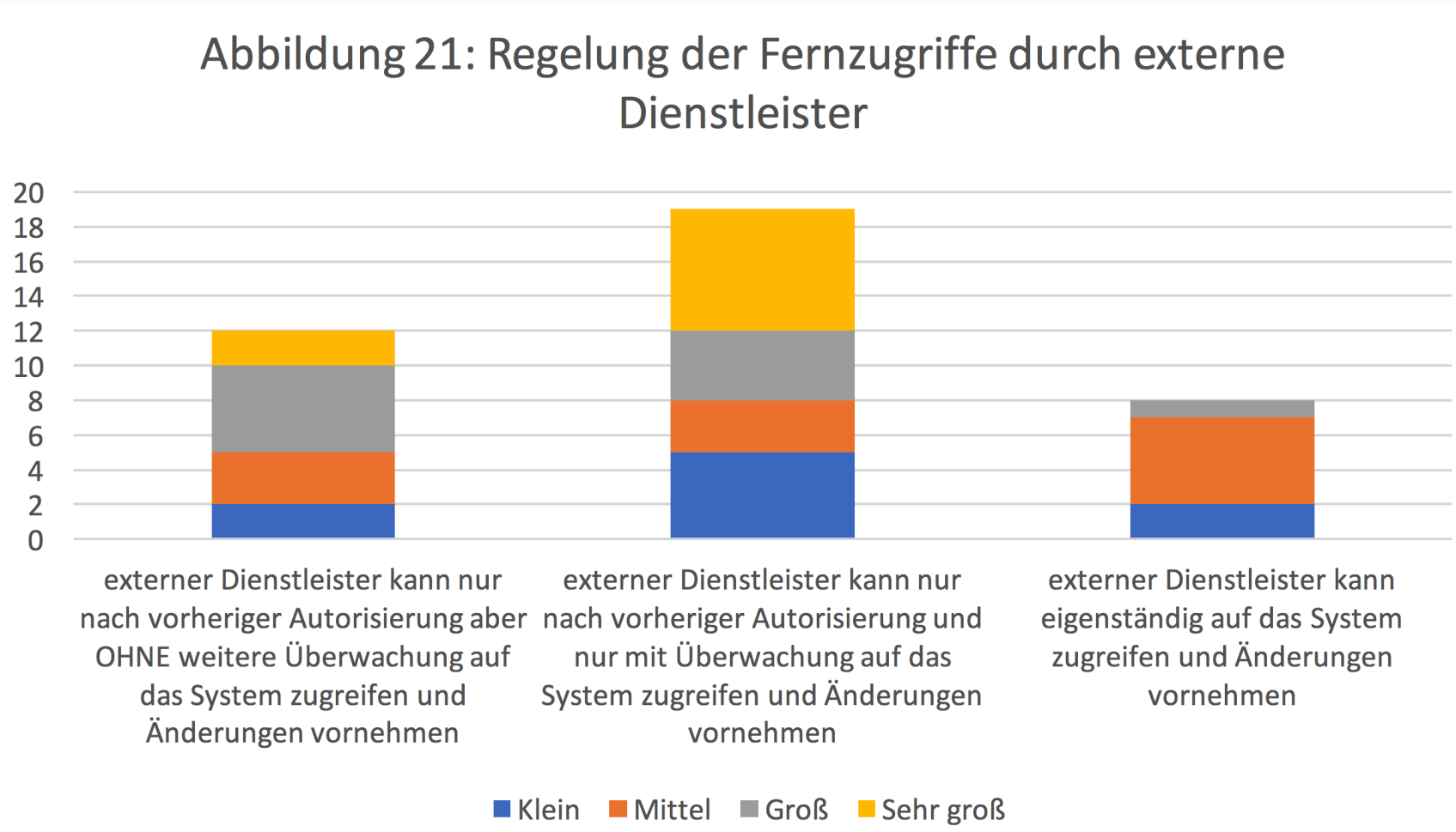
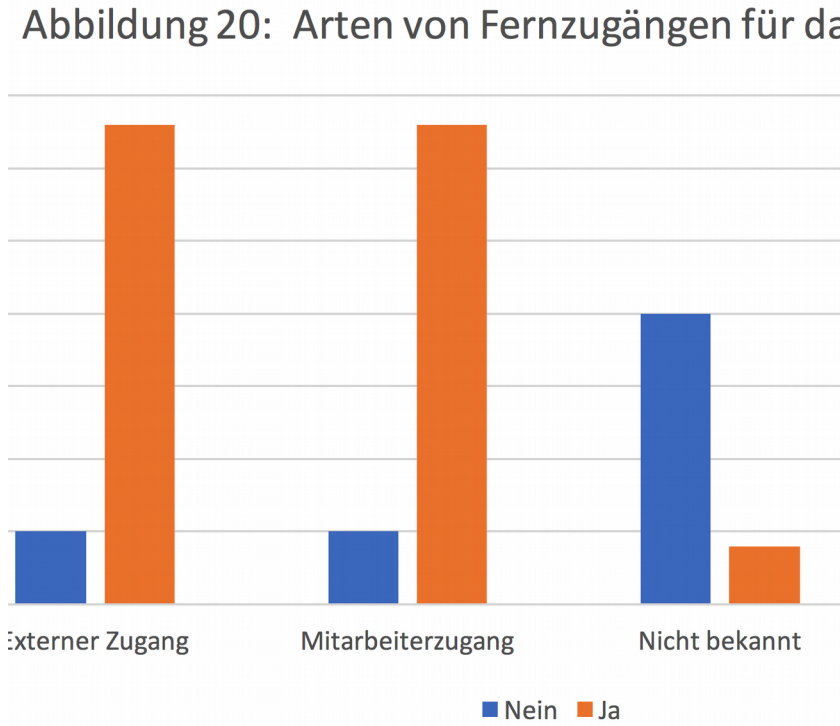


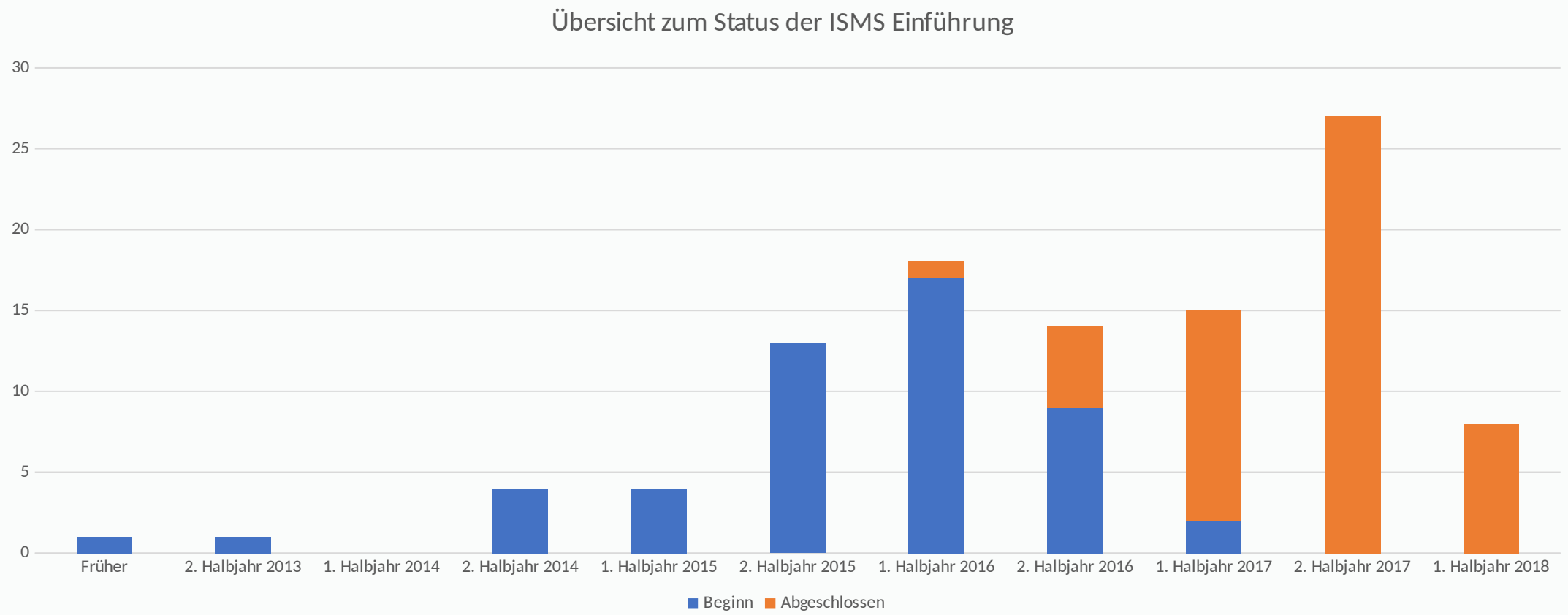
Abbildung 16: Aufteilung des Leitsystems in verschiedene Sicherheitsbereiche
35
30
25
20
15
10
5
0
Ja
Nein
Nicht bekannt
Klein
Mittel
Groß
Sehr groß

Fernzugänge

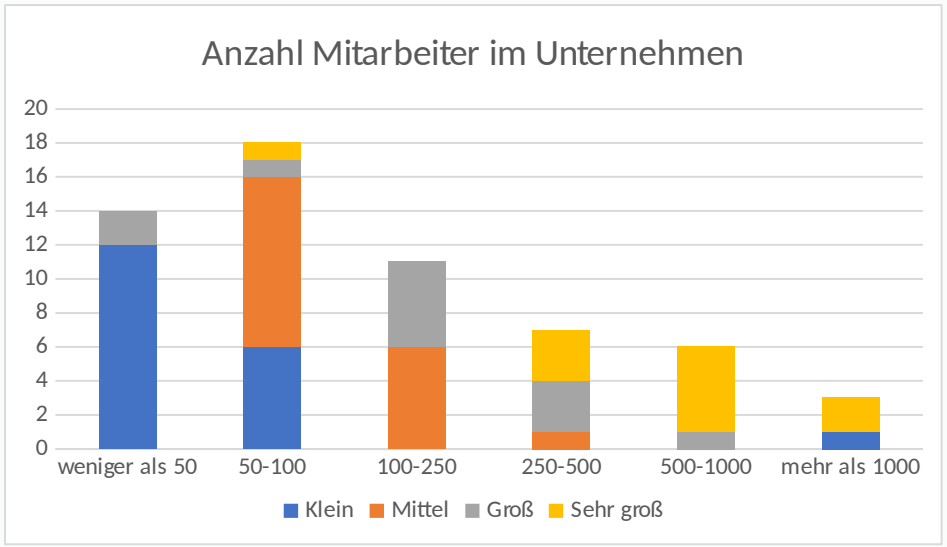


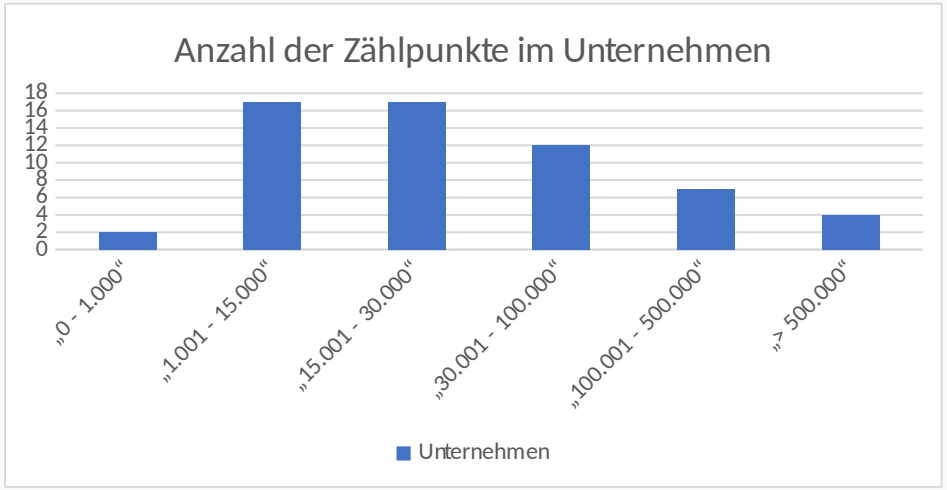


Status ISMS-Einführung



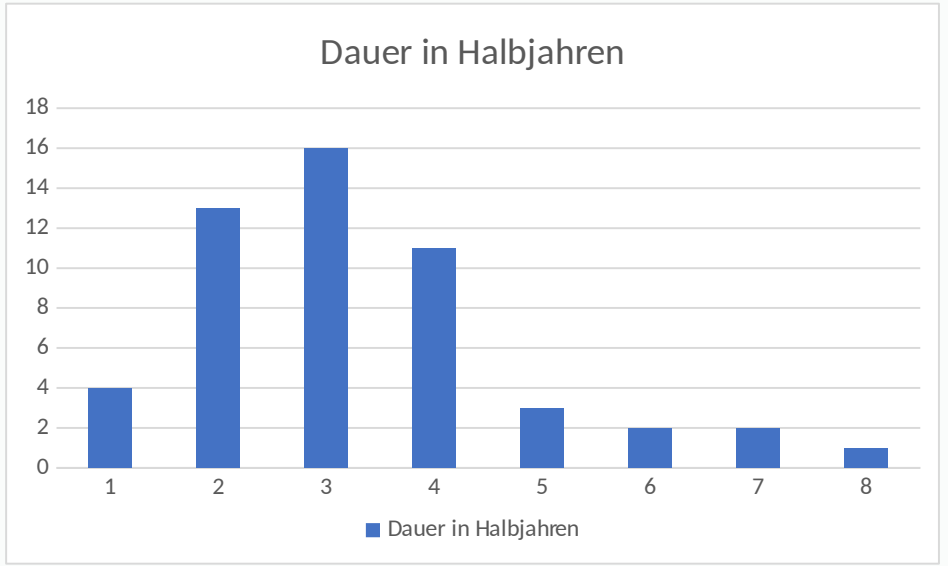
ISMS-Dauer





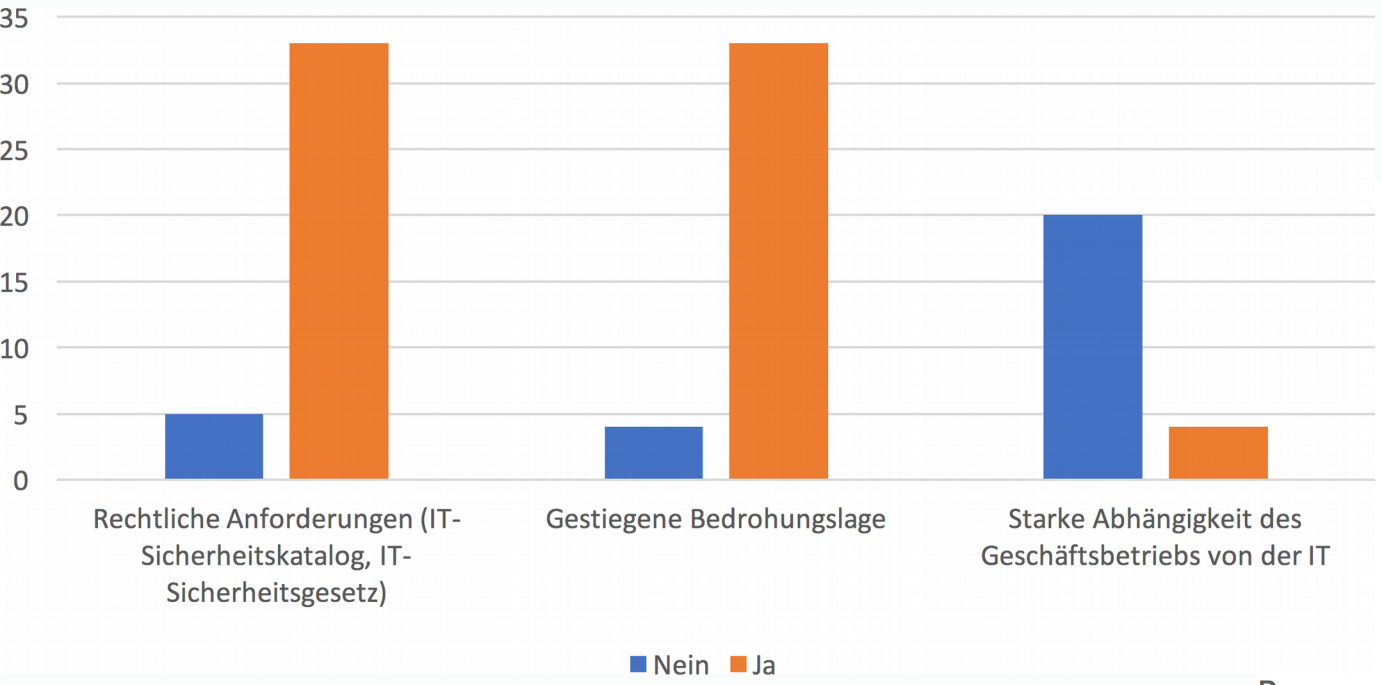
Starker Effekt
(Korr.-koeff.~0.5, signifikant)

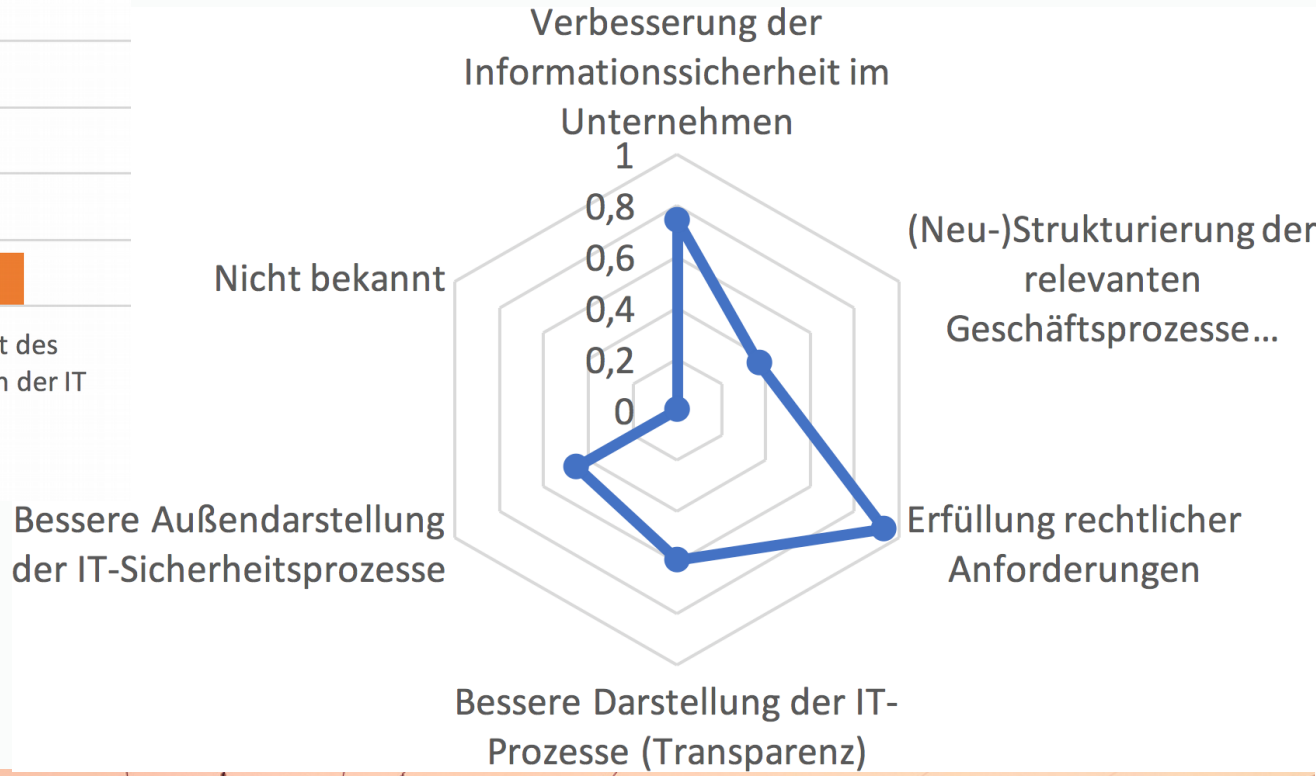
Kein Effekt gefunden



Wer hat den Fragebogen ausgefüllt?

Gründe und Erwartungen

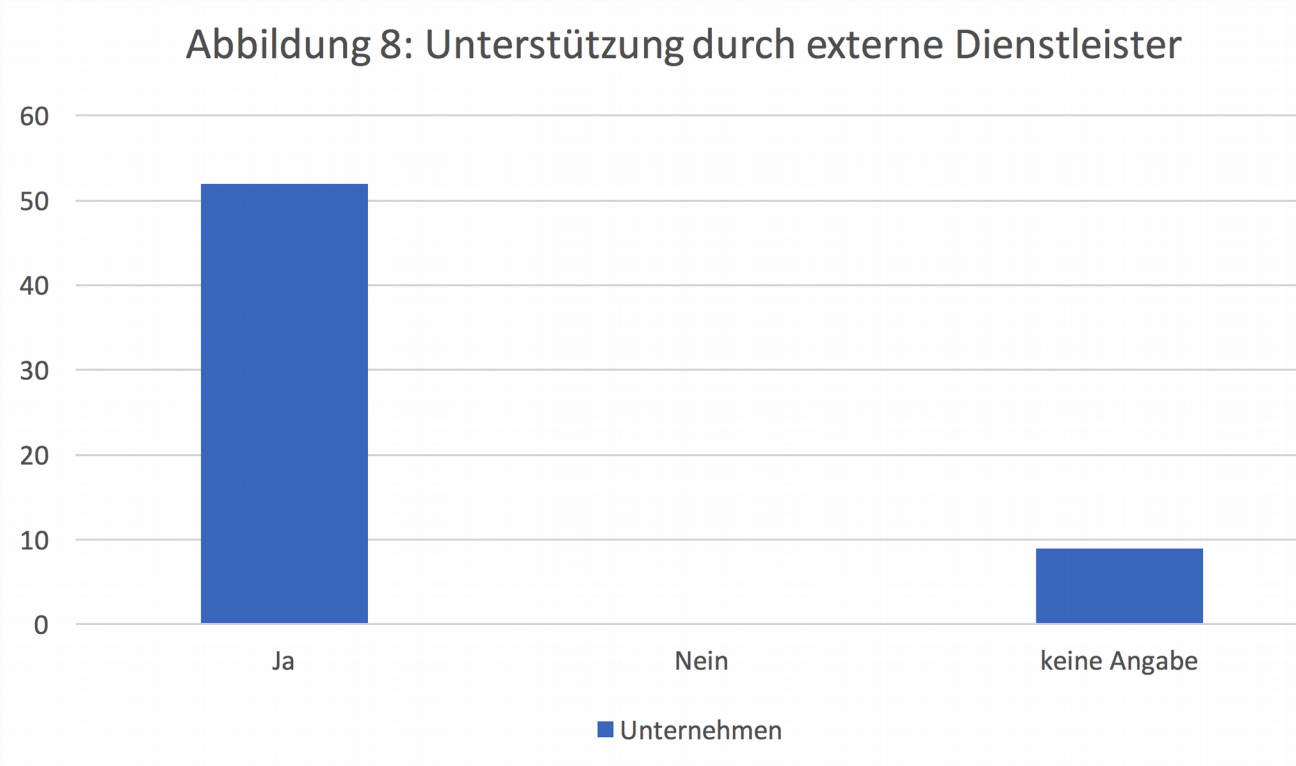




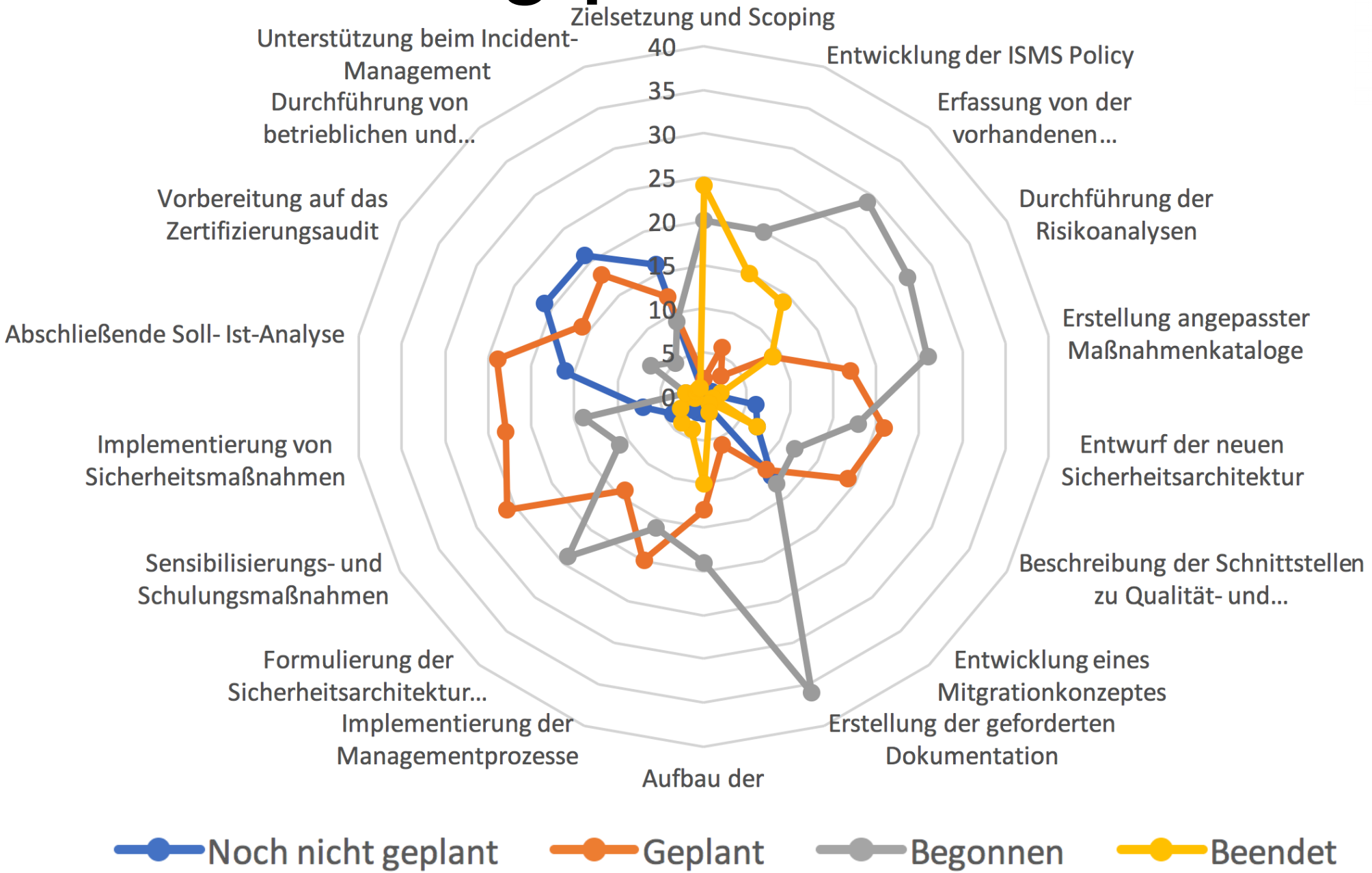
Einflussfaktoren für die Einführung von Maßnahmen

Workshop-Resultate

- Ziel: Minimaler Aufwand zur Erfüllung der gesetzlichen Anforderungen (Bestätigung der Umfrageergebnisse)
- Wunsch: Einmalig Black-Box kaufen und “einbauen” (Bestätigung siehe rechts)

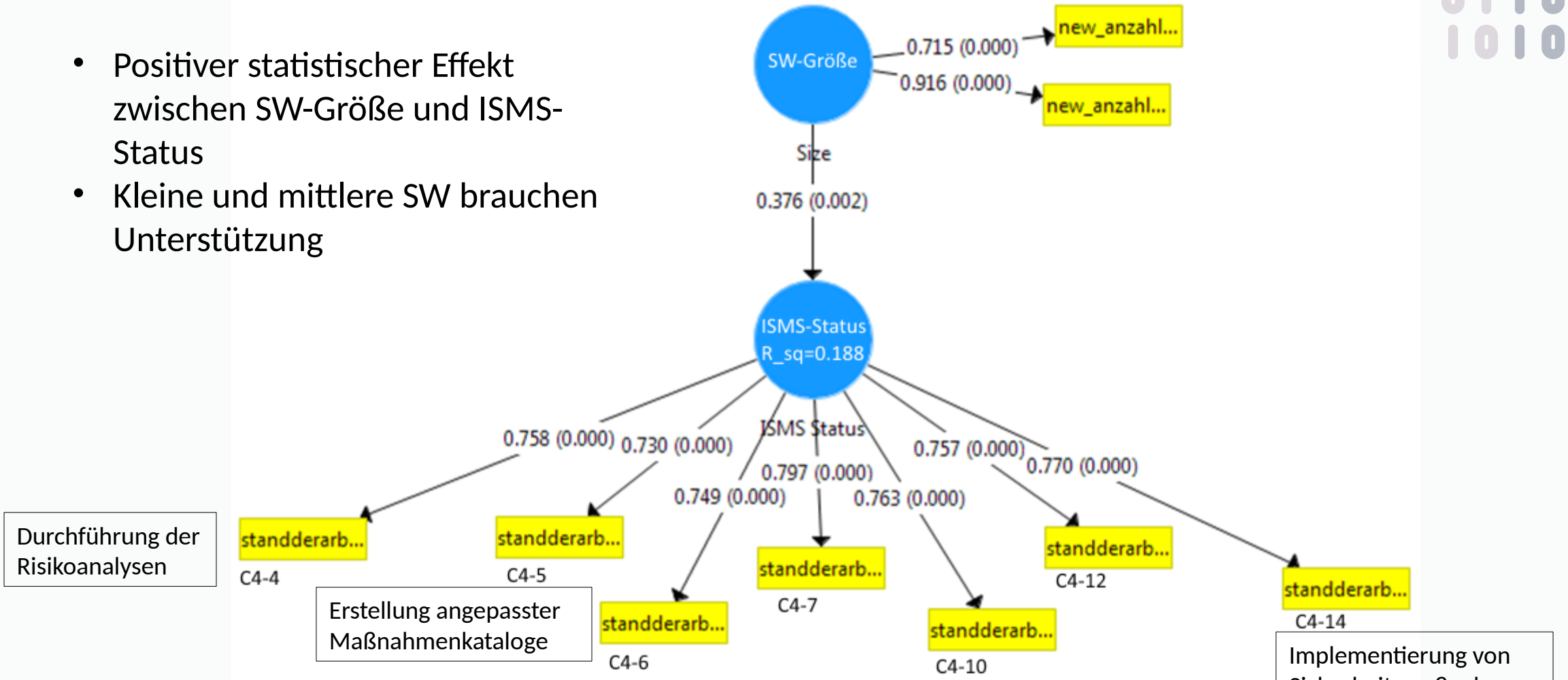


ISMS Umsetzungsphase



ISMS Stand - Größe

- Positiver statistischer Effekt zwischen SW-Größe und ISMS-Status
- Kleine und mittlere SW brauchen Unterstützung



Durchführung der Risikoanalysen

Erstellung angepasster Maßnahmenkataloge

Implementierung von Sicherheitsmaßnahmen

Fazit

- Energieversorger
  - Hilfe von externen
  - Folgen Regulierung
  - Suchen minimalen Aufwand

- Future Work
  - Evtl. Wiederholung
  - Einführung und Zertifizierung sollte bis 31. Januar 2018 abgeschlossen sein

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60629 Frankfurt, Germany

Phone +49 (0)69 798 34668
Fax +49 (0)69 798 35004

E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de