NIS2 bringt die CyberSicherhiets-Anforderungen der kritischen Infrastruktur in den Mittelstand

Teil 3 von 4: Die allgemeine Lösung für NIS2

1. Ein ISMS hilft, wenn IT-Sicherheit nicht mehr reicht
2. Sie müssen das Rad nicht neu erfinden
3. Erfahrungen aus der Praxis
4. Wann ist der richtige Zeitpunkt, um zu starten?

Christian Kreß

Externer ISB und
CyberSecurity Coach

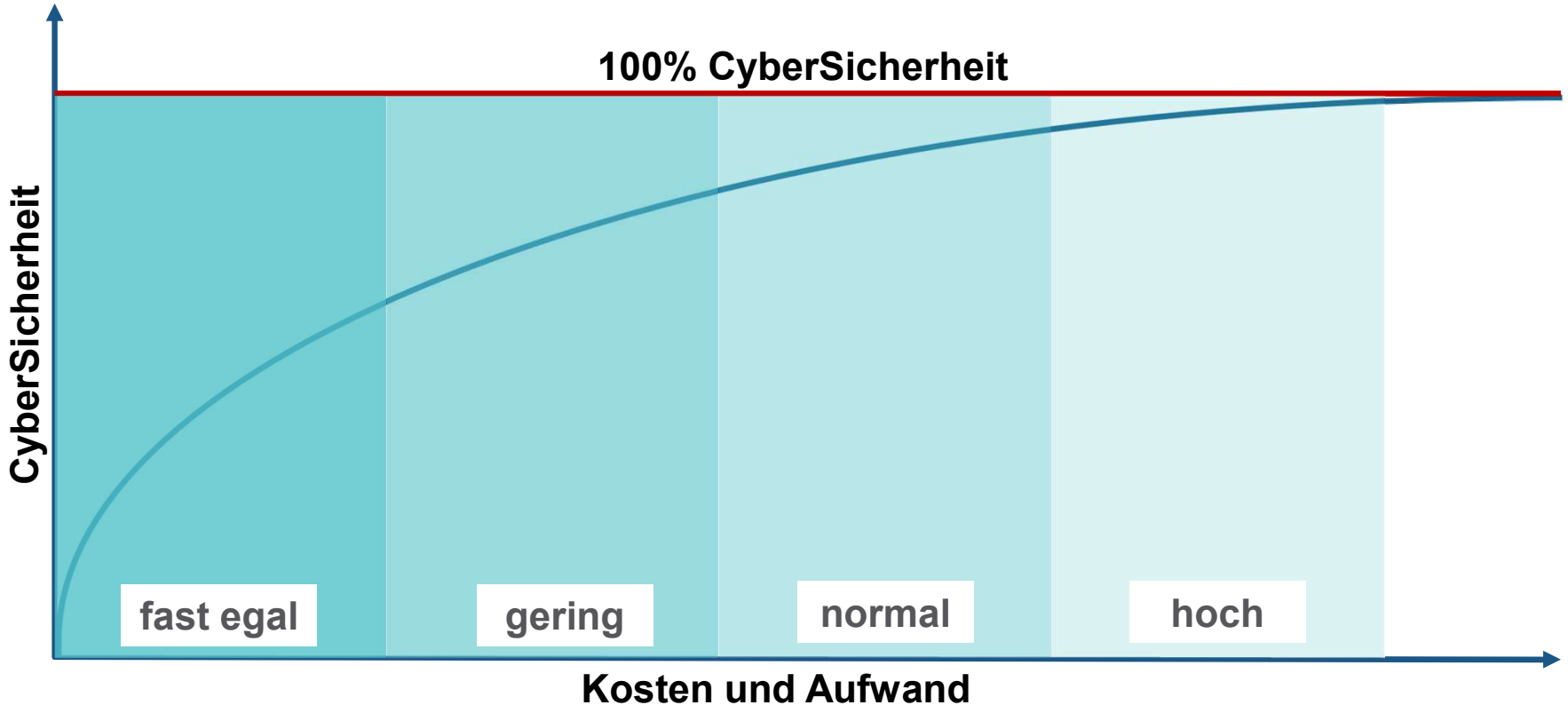
INOVASEC GmbH
Christian Kreß
In den Obergärten 28
63329 Egelsbach

E-Mail: christian.kress@inovasec.de
Tel: +49 6103 8038055
Mobil: +49 1520 9276920
Web: www.inovasec.de

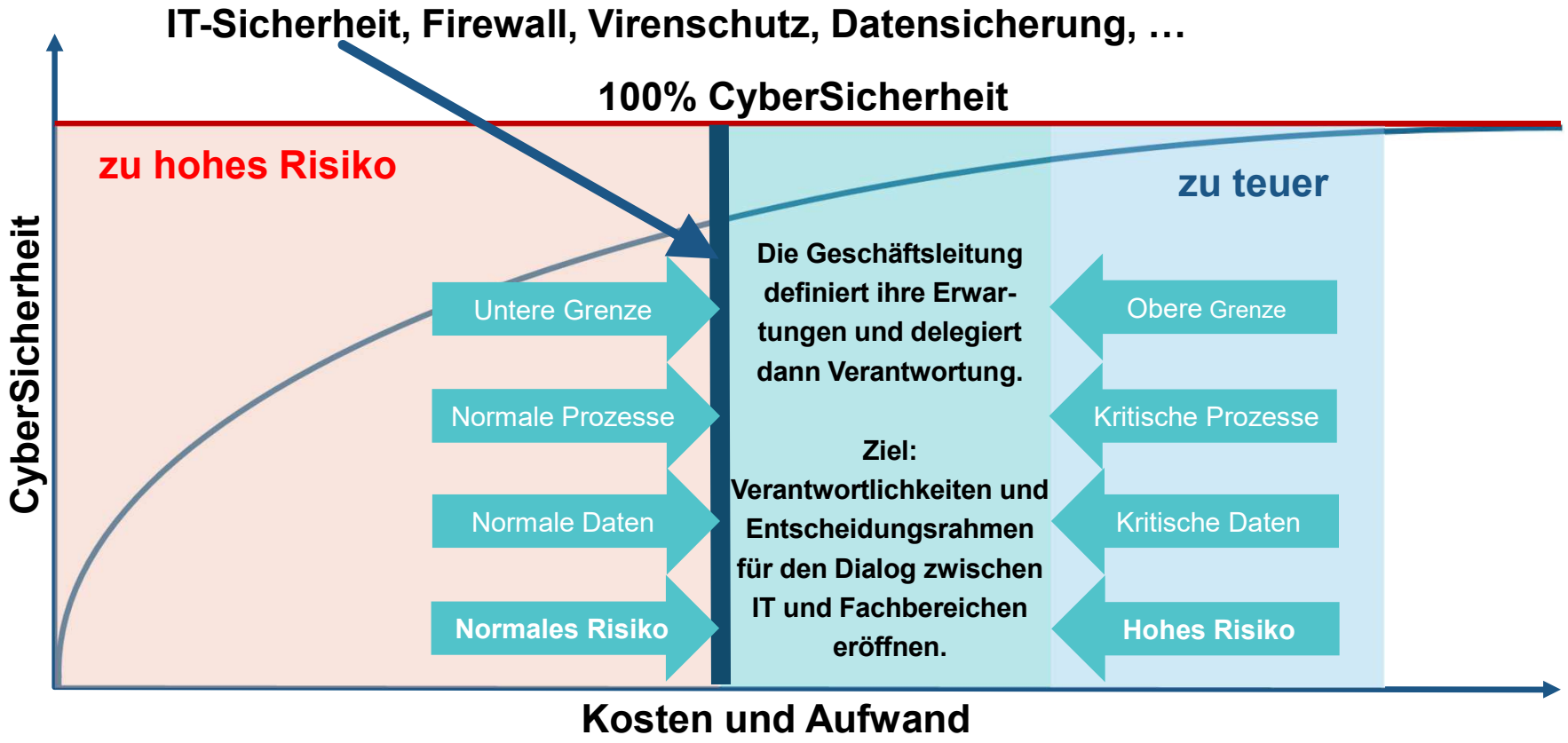
NIS2 ist ein Kooperations- und Kommunikationsprojekt

Ein ISMS hilft, wenn IT-Sicherheit nicht mehr reicht

Wieviel CyberSicherheit wollen sie?

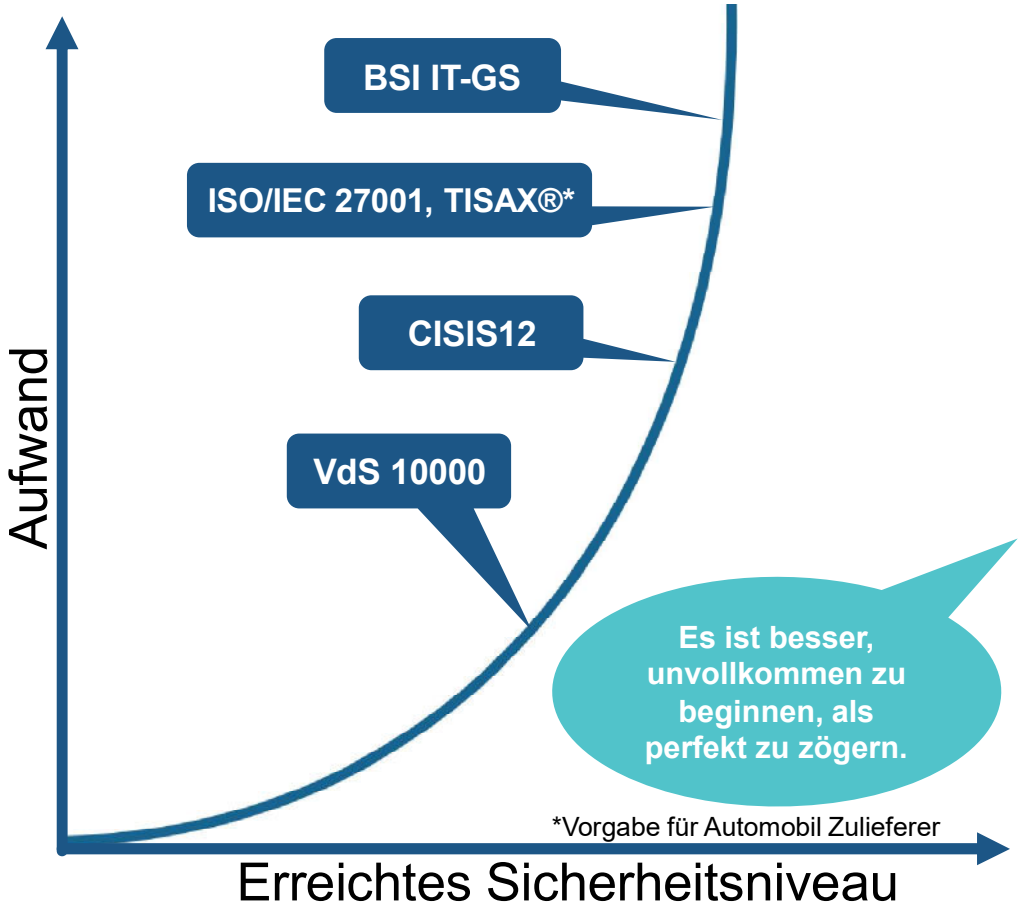


Die Geschäftsführung entscheidet über den „Risikoappetit“



Sie müssen das Rad nicht neu erfinden

Bewährte CyberSicherheits-Standards
(ISMS Information Security Management System)



*Vorgabe für Automobil Zulieferer

1. Vertraulichkeit, Integrität u. Verfügbarkeit
2. Basiert auf Best Practice
3. Technik und Organisation
4. Risikobasiert
5. Herstellerneutral, Prozesse statt Produkte
6. Wird an den Stand der Technik angepasst
7. Berücksichtigt den Lebenszyklus
8. Flexibel durch den kontinuierlichen Verbesserungsprozess
9. (IT-)Compliance (z.B. Datenschutz, PCI-DSS, BAIT, GMP, SOX)
10. Durch Dritte überprüf- und zertifizierbar

Sie unterstützen das Vertrauen ihrer Kunden, Partner, Investoren und Mitarbeiter!

Die ISMS-Standards im Überblick

Standard	ISO/IEC 27001 TISAX®	BSI IT-Grundschutz Standard-absicherung	BSI IT-Grundschutz Basis-absicherung	CISIS12	VdS 10000	VdS 10005	E-Check IT
Herausgeber	International Standards Organisation	Bundesamt für Sicherheit in der Informationstechnik		IT-Sicherheitscluster e.V.	VdS Schadenverhütung GmbH	VdS Schadenverhütung GmbH	Zentralverband der Deutschen Elektro- und Informations-technischen Handwerke
Zielgruppe	Organisationen jeder Größenordnung	Organisationen jeder Größenordnung, öffentliche Verwaltung	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen	Klein- und Kleinstunternehmen < 20 Mitarbeitende, Handwerksbetriebe	Handwerksbetriebe (Klein- und Kleinstbetriebe)
Umfang des Standards im Vergleich	ISMS	ISMS		ISMS	ISMS	Mindestanforderungen an die Informationssicherheit	IT-Sicherheitscheck
	groß (ca. 400 Seiten)	sehr groß (ca. 5.000 Seiten)	klein bis mittel (ca. 90 Seiten)	mittel (ca. 170 Seiten)	klein (ca. 40 Seiten)	sehr klein (ca. 15 Seiten)	klein (ca. 60 Seiten)
	Generisch formulierte Maßnahmen	Konkret formulierte Maßnahmen		Konkret formulierte Maßnahmen	Generisch formulierte Maßnahmen	Generisch formulierte Maßnahmen	Konkret formulierte Maßnahmen
Aufwand der Implementation	Externer Aufwand: 30 - 300 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	Externer Aufwand: 30 - 300 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	Verhältnismäßig geringer Aufwand im Vergleich zur Standard-absicherung	Externer Aufwand: 5 - 40 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	Ca. 20 – 30 % des Aufwandes im Vergleich zu ISO/IEC 27001	-	-
	Interner Aufwand: Faktor 1,5 - 2	Interner Aufwand: Faktor 2 - 4	15 – 20 Tage Aufwand für einen erfahrenen Informationssicherheits-beauftragten	Interner Aufwand: angepasst an KMU und damit geringer im Vergleich zu ISO/IEC 27001 und BSI IT-Grundschutz, aber abhängig vom individuellen Umfang	angepasst an KMU, ca. 20 – 30 % des Aufwandes im Vergleich zu ISO/IEC 27001	-	Aufwand für den Betrieb abhängig vom Ist-Stand der IT-Sicherheit im Unternehmen. Mindestens 14 PT.

Quelle: Begleitforschung Mittelstand-Digital, 2022

VdS 10000 bekommt „Ritterschlag“ vom BSI

Bundesamt für Sicherheit in der Informationstechnik

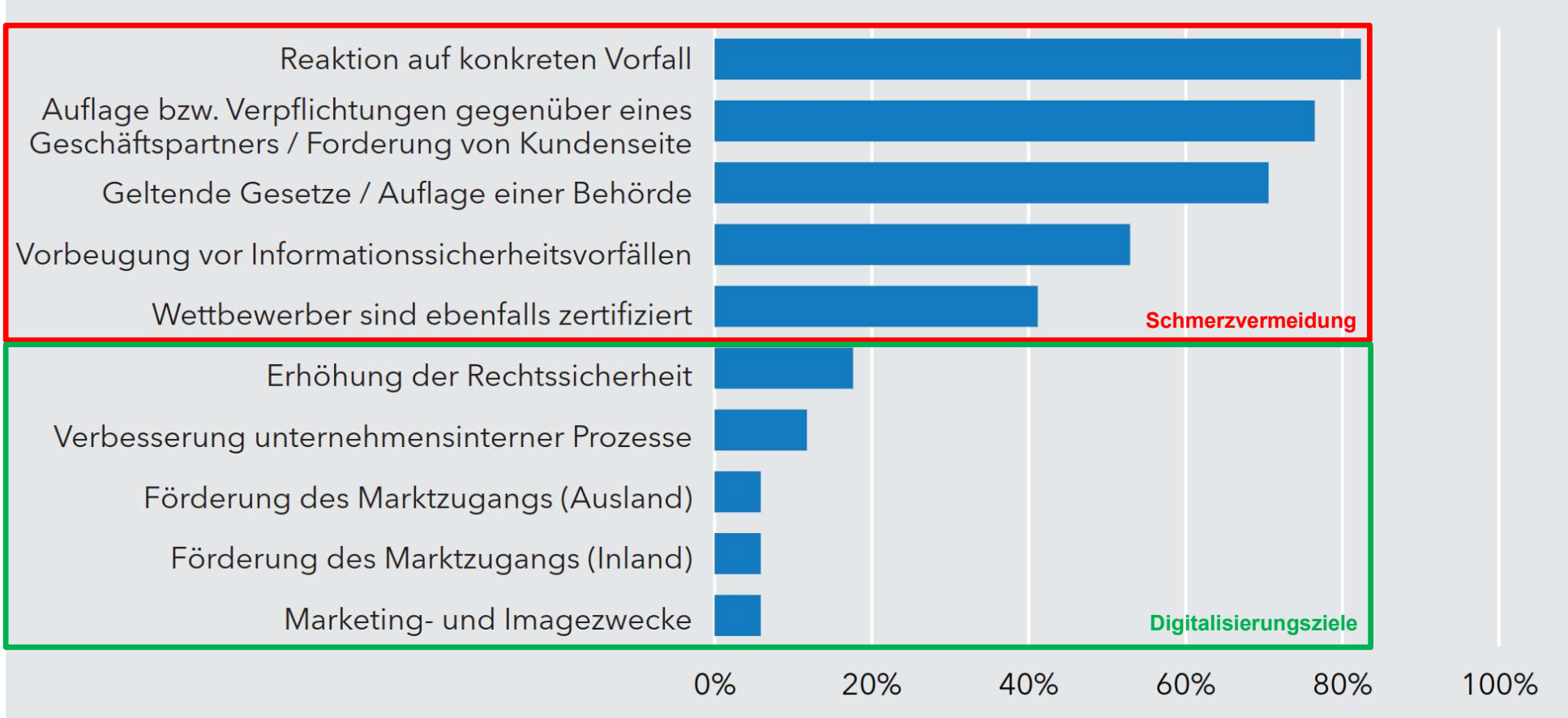
Stellungnahme vom Leitungsstab des Bundesamt für Sicherheit in der Informationstechnik BSI:

"Das Regelwerk VdS 10000 'Informationssicherheitsmanagementsystem für KMU' stellt ebenso wie die Basis-Absicherung des IT-Grundschutzes einen geregelten Prozess zur Einführung eines ISMS dar. Ebenfalls vergleichbar sind die beschriebenen Handlungsfelder, Unterschiede ergeben sich jedoch in der Ausprägung der einzelnen Anforderungen, die das VdS-Regelwerk in einigen Handlungsfeldern weniger konkret ausformuliert. **Somit stellen die Anforderungen der VdS 10000 eine Teilmenge der Basis-Absicherung des IT-Grundschutzes dar und bilden eine gute Basis zur Implementierung eines ISMS gemäß IT-Grundschutz oder ISO 27001.**"

26.03.2019

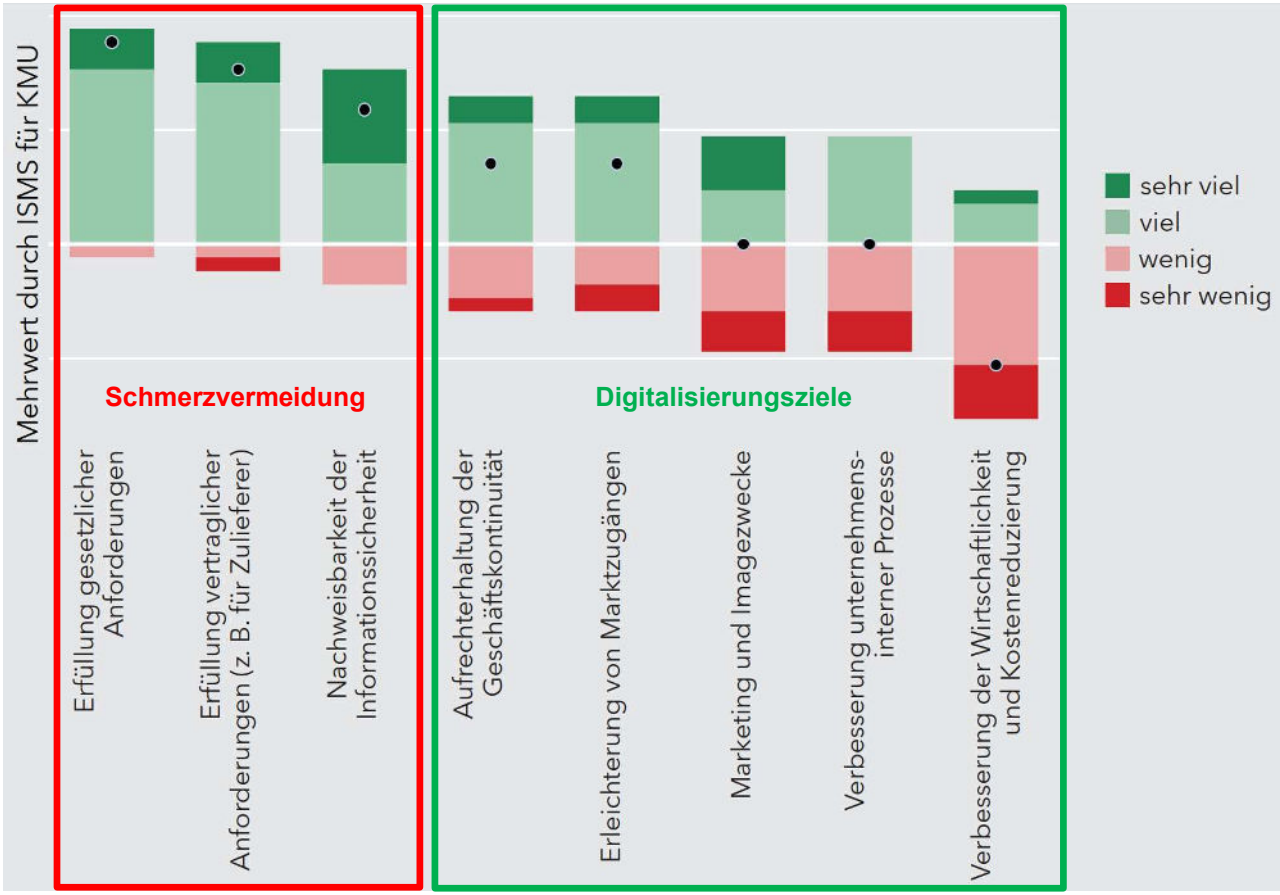
Erfahrungen aus der Praxis

Gründe, um ein ISMS einzuführen



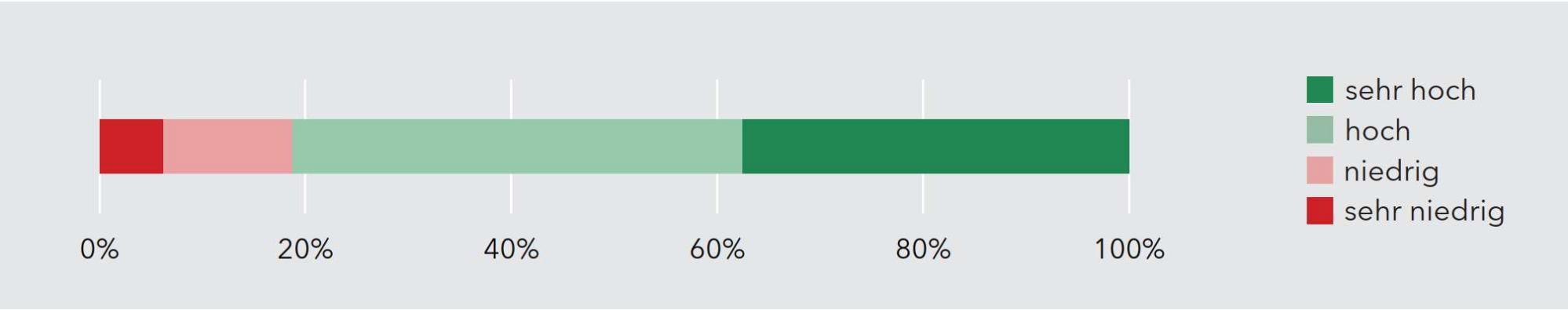
Quelle: Begleitforschung Mittelstand-Digital, 2022

Worin liegt der Mehrwehrt bei der Einführung eines ISMS?



Quelle: Begleitforschung Mittelstand-Digital, 2022

Nutzen von ISMS bei kleinen und mittelständischen Unternehmen

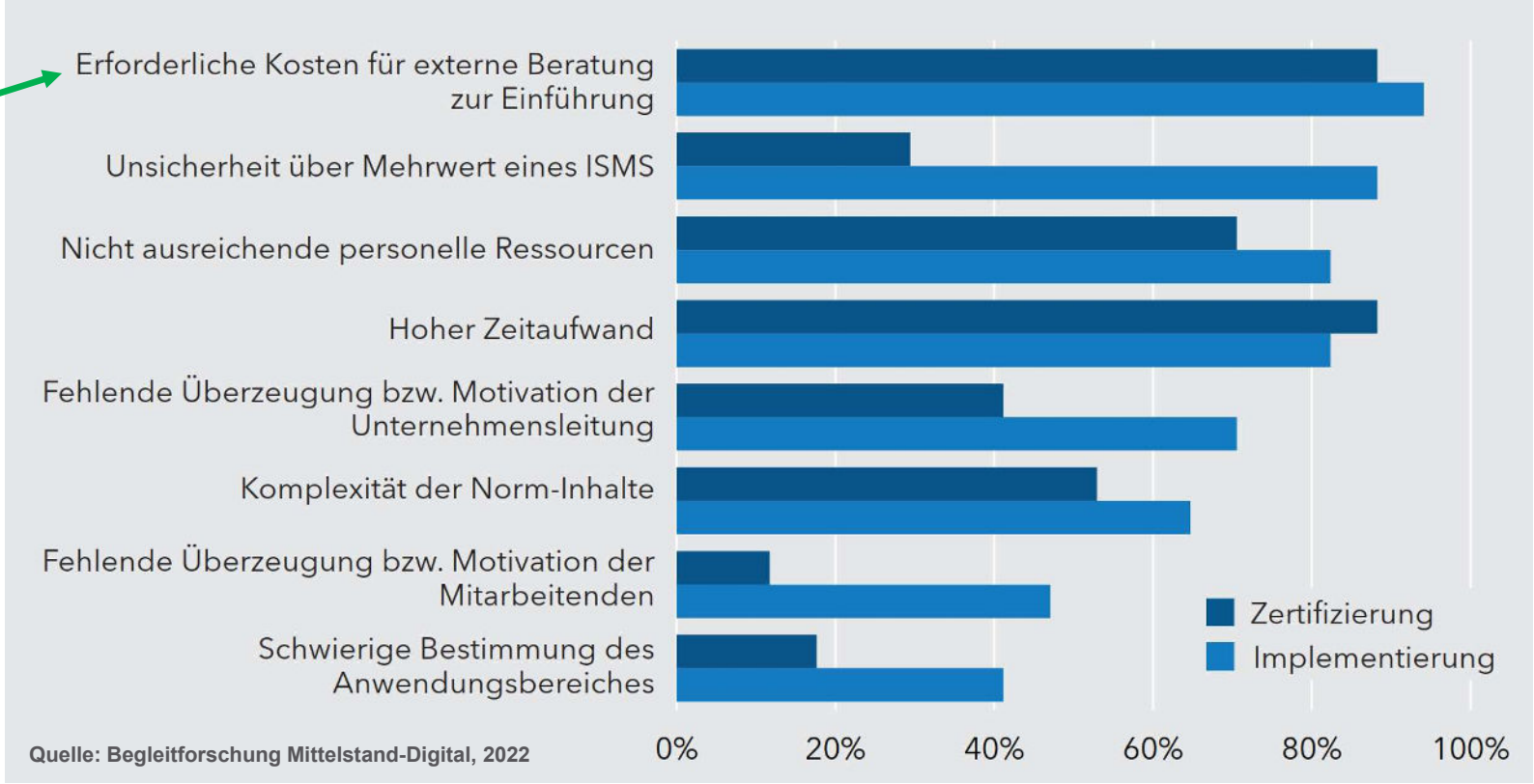


Quelle: Begleitforschung Mittelstand-Digital, 2022

Meine Kunden bewegen sich übrigens in der rechten Hälfte 😉

Was waren die Hemmnisse bei der Einführung und Zertifizierung eines ISMS?

Mögliche Förderungen



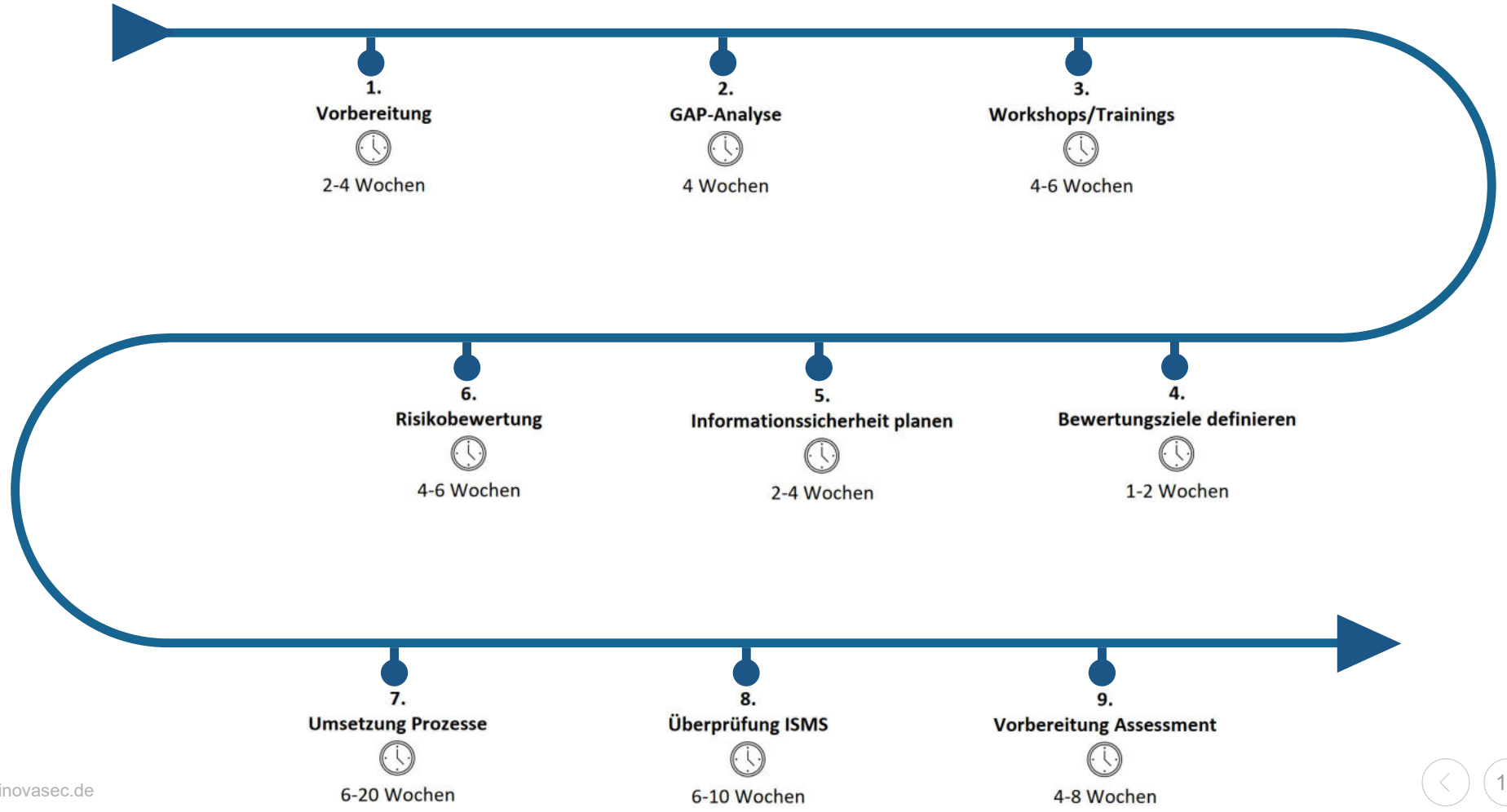
Es gibt bereits heute zu jedem Punkt eine leistbare Lösung.

Wann ist der richtige Zeitpunkt, um zu starten?

Sie ahnen es bereits ….

- Der beste Zeitpunkt war GESTERN!
- Der zweitbeste ist HEUTE

Der übliche Weg für ISMS-Einführung



Typischer Aufwand einer ISMS-Einführung

Inhalt/Aufgabe	Min. Dauer	Max. Dauer
Vorbereitung	2	4
GAP-Analyse	4	4
Workshop/Trainings	4	6
Risikobewertung	4	6
Informationssicherheit planen	2	4
Bewertungsziele definieren	1	2
Umsetzung Prozesse	6	20
Überprüfung ISMS	6	10
Vorbereitung Assessment	4	8
Wochen	**33**	**64**
Monate	**Ca. 8**	**Ca. 16**

Warum ist eine ISMS-Einführung so komplex?

Die Daten gehören nicht der IT!

Leider ignorieren viele diese Tatsache.

NIS2 ist ein Kooperations- und Kommunikationsprojekt

- **Teil 1 von 4: Die Grundlagen** 
- **Teil 2 von 4: Hintergründe (persönliche Einschätzung)** 
- **Teil 3 von 4: Die allgemeine Lösung für NIS2** 
- Teil 4 von 4: Eine konkrete Lösung für den Mittelstand