BAM
Bundesanstalt für Materialforschung und -prüfung

Sicherheit in Technik und Chemie

QI-FoKuS
Forschung für Konformitätsbewertung und Sicherheit

Die Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheit in Unternehmen in Deutschland

Eine Studie im Rahmen der Initiative QI-FoKuS

Vol. 2

Autor*innen

Mona Mirtsch, Dr. Claudia Koch, Dr. Gabriele Dudek (BAM)
Prof. Dr. Knut Blind (Technische Universität Berlin)

Herausgeber

Bundesanstalt für Materialforschung und -prüfung (BAM)

Impressum

Bundesanstalt für Materialforschung
und -prüfung (BAM)
Unter den Eichen 87
12205 Berlin

☎ +49 30 8104-0
✉ qi-fokus@bam.de
🌐 www.qi-fokus.de
🌐 www.bam.de

QI-FoKuS
Forschung für
Konformitätsbewertung
und Sicherheit

doi: 10.26272/opus4-51792

urn: nbn:de:kobv:b43-517922

Unterstützt durch das

Bundesministerium
für Wirtschaft
und Energie

BAM
Bundesanstalt für
Materialforschung
und -prüfung

Technische
Universität
Berlin

INHALT

QI-FOKUS

Die nationale Qualitätsinfrastruktur (QI) als ein System aus regulatorischen Rahmenbedingungen, Institutionen, Prozessen und Instrumenten dient der Qualitätssicherung und stellt somit die Erreichung sicherheits-, umwelt-, gesundheits- und verbraucherschutzpolitischer Ziele sicher. Sie bedient sich dabei verschiedener Elemente, die unterschiedliche Funktionen übernehmen und systematisch ineinandergreifen.

Abbildung 1: Die Elemente einer nationalen Qualitätsinfrastruktur. Quelle: BAM / TU Berlin

Konformitätsbewertungen spielen in diesem System eine zentrale Rolle. Für Wirtschaft und Verbraucher*innen sind sie eine wichtige Grundlage für Vertrauen und Sicherheit. Durch Prüfungen, Inspektionen bzw. Zertifizierungen kann bestätigt werden, ob bestimmte Anforderungen an Produkte, Dienstleistungen, Prozesse, Systeme oder Personen erfüllt sind und ob vertragliche Vereinbarungen und rechtliche bzw. normative Vorgaben an Sicherheit, Gesundheits- oder Umweltschutz eingehalten werden. Auch die Akkreditierung als Bestätigung, dass eine Konformitätsbewertungsstelle die Kompetenz besitzt, bestimmte Konformitätsbewertungsaufgaben durchzuführen, ist eine wichtige Säule der QI.

Die Entwicklung und wirtschaftliche Bedeutung von Konformitätsbewertungen in Deutschland sind nicht zuletzt aufgrund unzureichender empirischer Daten bislang noch wenig erforscht. QI-FoKuS – Qualitätsinfrastruktur - Forschung für Konformitätsbewertung und Sicherheit – strebt auf Basis einer wiederkehrenden Befragung von Unternehmen und Konformitätsbewertungsstellen in Deutschland die Schaffung einer besseren Datengrundlage für die Forschung an.

Datenbasis schaffen, Trends erkennen

QI-FoKuS soll das Zusammenwirken von Elementen der QI verständlicher machen. Mit QI-FoKuS soll es gelingen:

- eine Datenbasis für neue wissenschaftliche Erkenntnisse zu Einflussfaktoren und Effekten in der Konformitätsbewertung und Akkreditierung zu schaffen
- Wirkungsmechanismen zu identifizieren
- notwendige Veränderungen in Folge von technischen und ökonomischen Entwicklungen frühzeitig zu erkennen
- aktuelle Trends in Konformitätsbewertung und Akkreditierung und daraus resultierenden Regelsetzungsbedarf zu identifizieren
- politische Entscheidungsträger, die Wirtschaft und die Öffentlichkeit durch datenbasierte Analysen zu Konformitätsbewertung und Akkreditierung fachgerecht zu informieren.

Die aus den Ergebnissen der Befragung abgeleiteten Erkenntnisse können nicht nur als Entscheidungshilfen für die Handelnden in der Politik dienen, sondern sind auch für Unternehmen, Konformitätsbewertungsstellen und die Deutsche Akkreditierungsstelle eine wichtige Unterstützung, um aktuelle und zukünftige Herausforderungen besser einschätzen und darauf reagieren zu können.

Das Projekt QI-FoKuS wurde im Herbst 2019 von der

Bundesanstalt für Materialforschung und -prüfung (BAM), und der Technischen Universität Berlin (TU Berlin), Fachgebiet für Innovationsökonomie unter Prof. Dr. Knut Blind initiiert. Das Projekt wird aus Mitteln der BAM finanziert.

QI-FoKuS wird unterstützt vom Bundesministerium für Wirtschaft und Energie (BMWi) sowie einem Netzwerk aus QI-Institutionen und Industrieverbänden.

In einer ersten Erhebung im Rahmen von QI-FoKuS wurden Unternehmen in Deutschland zur Nutzung von genormten Managementsystemen befragt. Neben der Motivation hinsichtlich der Anwendung verschiedener Normen, die Anforderungen an Managementsysteme darlegen, sowie den Wirkungen, wurden insbesondere die Zertifizierung für diese Normen und die Rolle und Funktion der Akkreditierung adressiert. Ein Spezialteil widmete sich der Wirkung von Informationssicherheitsmanagementsystemen (ISMS), die der internationalen Norm ISO/IEC 27001 folgen. Die Bedeutung des Themas Informationssicherheit in der untenehmerischen Praxis wächst mit zunehmender Digitalisierung. Die Verbreitung der ISO/IEC 27001 unterliegt daher aktuell einer wachsenden Dynamik, die auch durch Regulierungsbestrebungen hinsichtlich Informationssicherheit beeinflusst wird. Dies begründet ein besonderes Forschungsinteresse.

Aufbauend auf der ersten Studie fasst die vorliegende Publikation die Ergebnisse einer zweiten, gesonderten Befragung von Unternehmen in Deutschland zusammen, die nach der Norm ISO/IEC 27001 zertifiziert sind.

Dazu wurden nach ISO/IEC 27001 zertifizierte Unternehmen in Deutschland identifiziert und branchenübergreifend zu den Motiven der Implementierung und der Zertifizierung dieses ISMS befragt sowie nach ihren Wahrnehmungen zu den Wirkungen. Auch die Hürden, denen die Unternehmen bei der Implementierung gegenüberstehen, wurden beleuchtet, um mögliche Maßnahmen für eine weitere Verbreitung ableiten zu können. Abschließend richtet diese Studie einen Fokus auf Kriterien für die Wahl der Zertifizierungsstelle.

QI-FoKuS Report Vol.1: Studie zur Nutzung und Wirkung genormter Managementsysteme

In einer ersten Studie im Rahmen der Initiative QI-FoKuS wurde bereits die Nutzung verschiedener genormter Managementsysteme in Deutschland untersucht, inkl. ISMS nach ISO/IEC 27001. Der Report steht unter www.qi-fokus.de zum Download bereit.

Die Umfrageergebnisse wurden differenziert ausgewertet hinsichtlich verschiedener Unternehmenscharakteristika, beispielsweise die Zugehörigkeit zu spezifischen Branchen, insbesondere die Informations- und Kommunikationstechnologiebranche (IKT). Diese Studie trägt somit zu einem besseren Verständnis hinsichtlich der branchenübergreifenden Nutzung und Wirkung von ISMS nach ISO/IEC 27001 bei und ermöglicht die Ableitung von Handlungsoptionen für eine mögliche weitere Verbreitung der Norm in der Zukunft.

ZUSAMMENFASSUNG UND ZENTRALE ERGEBNISSE

Das Ziel der Initiative QI-FoKuS ist es, eine Datenbasis für neue wissenschaftliche Erkenntnisse zu Einflussfaktoren und Effekten in der Konformitätsbewertung und Akkreditierung zu schaffen und hierbei insbesondere auch auf aktuelle Trends und Entwicklungen einzugehen. Von Januar bis März 2020 wurden in einer Online-Erhebung Unternehmen verschiedener Branchen und Größenklassen in

Deutschland zur Nutzung und den Wirkungen ihres zertifizierten Managementsystems für Informationssicherheit nach ISO/IEC 27001 befragt. Es konnten 125 vollständig ausgefüllte Fragebögen für die vorliegende Studie ausgewertet werden.

Folgende zentrale Erkenntnisse können aus der Befragung abgeleitet werden:

1. **Die ISMS Zertifizierung nach ISO/IEC 27001 ist hauptsächlich in der Informations- und Kommunikationstechnologiebranche (IKT) anzutreffen:** 58% aller zertifizierten teilnehmenden Unternehmen gehören zur IKT-Branche. Damit zeigt sich ein eindeutiger Branchenschwerpunkt unter den zertifizierten Unternehmen.

2. **Bei weniger als der Hälfte der nach ISO/IEC 27001 zertifizierten Unternehmen bezieht sich der Anwendungsbereich auf das gesamte Unternehmen:** Bei denen, die nur bestimmte Bereiche nach ISO/IEC 27001 zertifizieren lassen, ist dies am häufigsten der IT-Bereich, gefolgt von der Produktion und dem Entwicklungsbereich.

3. **Ein ISMS nach ISO/IEC 27001 ist teilweise das einzige Managementsystem im Unternehmen:** 39% aller Befragten geben an, keine weiteren zertifizierten Managementsysteme zu haben. Falls doch, ist dies überwiegend ein Qualitätsmanagementsystem nach ISO 9001.

4. **Präventionsmotive sind dominierend bei der Implementierungsentscheidung:** Insbesondere streben die Unternehmen mit der Implementierung eines ISMS nach ISO/IEC 27001 die Vorbeugung von Informationssicherheitsvorfällen an. Weiterhin zeigen sich auch hier deutliche Branchenunterschiede: So stehen markt- und marketingbezogene Motive bei Unternehmen der IKT-Branche deutlich höher im Ranking als bei Unternehmen außerhalb der IKT-Branche.

5. **Präventionsbezogene Wirkungen sind am stärksten:** Insbesondere wird das Bewusstsein der Mitarbeitenden im Hinblick auf Informationssicherheit im Zuge der Implementierung des ISMS nach ISO/IEC 27001 geschärft. Unternehmen profitieren weniger von direkten finanziellen Vorteilen durch Umsatzsteigerung oder Kostenreduktion, sondern vielmehr langfristig strategisch aufgrund der Verminderung von Risiken und Folgen aus Vorfällen bzgl. ihrer Informationssicherheit.

6. **Unterschiede zeigen sich zwischen der Motivation zur Einführung von Managementsystemen und realisierten Wirkungen:** Die wahrgenommene Wirkung durch das ISMS nach ISO/IEC 27001 übersteigt die Motivationswerte insbesondere hinsichtlich des Bewusstseins der Mitarbeitenden und der Erhöhung der Informationssicherheit des Unternehmens.

7. **Insgesamt wird die Kosten-Nutzen-Relation positiv bewertet:** Unternehmen der IKT-Branche sind hierbei noch leicht zufriedener bzgl. der Implementierung als Unternehmen anderer Branchen. Keine branchenspezifischen Zufriedenheitsunterschiede gibt es hingegen bei der Bewertung hinsichtlich der zusätzlichen Zertifizierung.

8. **Aufwand und fehlende unternehmensinterne Expertise wirken als Hürden bei der Implementierung und Zertifizierung:** Zeitaufwand, nötige Beratungsleistungen und Kosten werden als größte Schwierigkeiten bei der Implementierung und Zertifizierung gesehen. Dies trifft insbesondere bei kleineren Unternehmen zu.

9. **Unterstützungsangebote können bei der Verbreitung helfen:** Insbesondere die kleineren Unternehmen bewerten spezifische finanzielle Hilfen sowie Informationsangebote, bspw. in Form von Handlungsleitfäden und Praxisbeispielen, als hilfreiche fördernde Maßnahmen.

10. **Kompetenz und deren Nachweis sind die Hauptkriterien bei der Wahl der Zertifizierungsstelle:** Die Ergebnisse unterstreichen die wichtige Bedeutung von Akkreditierung, die von den Befragten als das mit Abstand wichtigste Auswahlkriterium gewertet wird.

EINLEITUNG

Genormte und standardisierte (im Folgenden zusammengefasst als genormte) Managementsysteme sind ein globaler Erfolg. Millionen Unternehmen weltweit integrieren diverse Managementsysteme in ihre operativen Prozesse. Dies betrifft nicht nur die bekannten Normen für Qualitäts- und Umweltmanagementsysteme (ISO 9001 und ISO 14001). Nach und nach steigt auch die Verbreitung weiterer Systeme für das Management spezifischer Aspekte.

Managementsysteme

Ein Managementsystem umfasst Aktivitäten, mit denen eine Organisation ihre Ziele identifiziert und den Prozess und die Ressourcen bestimmt, die zur Erreichung der gewünschten Ergebnisse erforderlich sind.[1] Diese Ziele können sich auf eine Reihe verschiedener Aspekte beziehen, einschließlich Produkt- oder Dienstleistungsqualität, betriebliche Effizienz, Umweltleistung, Gesundheit und Sicherheit am Arbeitsplatz und viele andere mehr.

Managementsystem-Normen

Normen von internationalen Normungsorganisationen wie ISO oder IEC legen die Anforderungen fest, um Organisationen bei der Gestaltung und Umsetzung ihrer Vorgaben und Prozesse zur Erreichung der jeweiligen Ziele zu unterstützen. Allein bei ISO gibt es mittlerweile mehr als 80 Managementsystem-Normen in den verschiedensten Bereichen.[2] Diese Normen sind so konzipiert, dass sie in unterschiedlichen Organisationen, unabhängig von Branche, Größe, Art, Organisationsform, oder geographischen, kulturellen und sozialen Bedingungen, anwendbar sind.

Mit fortschreitender Digitalisierung spielt die Informationssicherheit eine immer größere Rolle in Unternehmen. Die ISO/IEC 27001 bietet Organisationen seit 2005 die Möglichkeit, ein entsprechendes international genormtes Managementsystem zu implementieren und sich zertifizieren zu lassen. Eine solche Zertifizierung gewinnt auch im Lichte der jüngsten europäischen und deutschen regulativen Initiativen an Bedeutung, bspw. im Rahmen des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und des Cybersecurity Acts (Verordnung EU 2019/881 über die Zertifizierung von Cybersicherheit von Informations- und Kommunikationstechnik).

Informationssicherheit

Als Informationssicherheit wird laut ISO/IEC 27000 die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen verstanden. Mit Hilfe der Vertraulichkeit von Informationen soll sichergestellt werden, dass Informationen nicht Unbefugten verfügbar gemacht werden. Die Integrität sichert, dass die Informationen richtig und vollständig sind und nicht unbefugt verändert werden. Die Verfügbarkeit beschreibt hingegen die Eigenschaft, dass eine Information den Berechtigten zugänglich und nutzbar ist.

ISO/IEC 27001

Die internationale Norm ISO/IEC 27001 ist Teil der ISO/IEC 27000 Familie, die Ende 2005 von der Internationalen Organisation für Normung (ISO) gemeinsam mit der Internationalen Elektrotechnischen Kommission (IEC) veröffentlicht wurde, und legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) fest. Nach der Implementierung eines ISMS auf Basis von ISO/IEC 27001 können Organisationen sich auf Wunsch auch zertifizieren lassen.

Steigende Verbreitung auf jedoch insgesamt niedrigem Niveau

Laut ISO-Survey, einer weltweiten jährlichen Erhebung von ISO zur Verbreitung genormter Managementsysteme, gab es nach stetigem Anstieg seit 2006 zum 31. Dezember 2019 weltweit insgesamt 36.362 gültige ISO/IEC 27001-Zertifikate an 68.930 Unternehmensstandorten *(Sites)*.[3] Mit 1.175 Zertifikaten (an 2.095 Standorten) liegt Deutschland im internationalen Vergleich an sechster Stelle. Für ca. 44% der Zertifikate weltweit wurden sektorale Daten im Rahmen des ISO-Surveys erhoben. Demnach entfiel im Jahr 2019 jedes zweite ISO/IEC 27001-Zertifikat auf den IT-Sektor, gefolgt vom Dienstleistungssektor mit 13% und dem Sektor Verkehr und Nachrichtenübermittlung mit 6%.

Auch wenn diese Zahlen nur gemeldete Zertifikate akkreditierter Zertifizierungsstellen enthalten, zeigen sie dennoch deutlich die Verbreitung der Norm. Die tatsächliche Anwendung dürfte durchaus höher sein, berücksichtigt man die Limitierungen der ISO-Erhebung[4] sowie die Tatsache, dass viele Unternehmen Managementsysteme implementiert haben, ohne sich zertifizieren zu lassen.[5]

Anzahl ausgestellter ISO/IEC 27001 Zertifikate in Deutschland

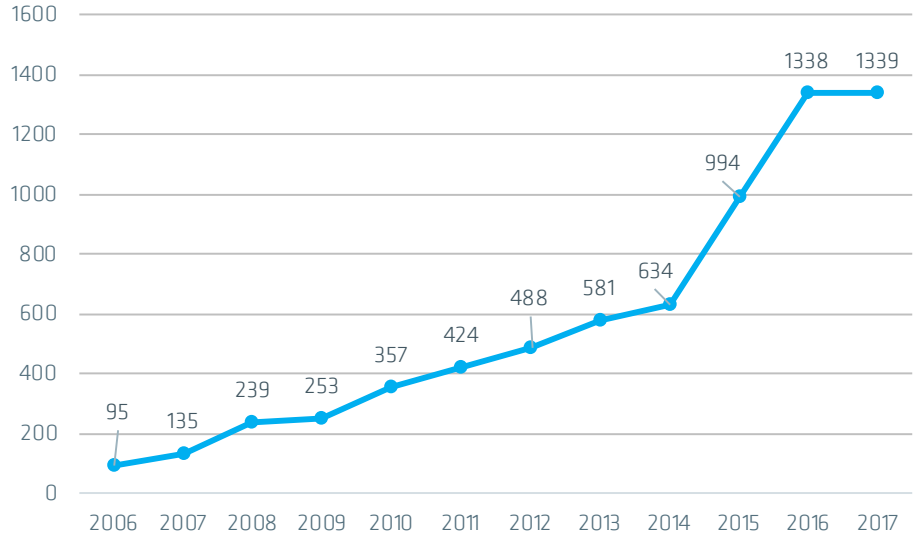


Abbildung 2: Anzahl der ausgestellten Zertifikate für ISMS nach ISO/IEC 27001 in Deutschland.
Quelle: ISO Survey (2019).[6]

Trotz zunehmender Zertifizierungen hat diese Norm dennoch weniger Verbreitung in Deutschland und weltweit gefunden als dies die fortschreitende Digitalisierung und damit einhergehende Bedeutung der Informationssicherheit digital gespeicherter Daten erwarten lässt. Aus diesem Grund wurde im Rahmen dieser Erhebung nicht nur nach den Motiven und der Wirkung gefragt, sondern zusätzlich nach Hürden bei der Einführung sowie potenziellen Maßnahmen zur Förderung der Nutzung des ISMS nach ISO/IEC 27001 in Deutschland.

Mangel an wissenschaftlichen Studien

Wissenschaftliche Erhebungen zur Nutzung und Wirkung von Managementsystemen in Unternehmen gibt es zahlreiche – insbesondere in den Bereichen Qualitäts- und Umweltmanagement. Trotz der zunehmenden Bedeutung von IKT und unzähligen Sicherheitsvorkommnissen[7] blieben Managementsysteme nach ISO/IEC 27001 in der Forschung dabei jedoch weitgehend unbeachtet. Dies hängt auch damit zusammen, dass im Vergleich zu anderen Managementsystemen noch relativ wenige Unternehmen weltweit und auch in Deutschland nach ISO/IEC 27001 zertifiziert sind und sich diese damit nur mit größerem Aufwand für eine Erhebung identifizieren lassen.

Tabelle 1: Anzahl der ausgegebenen Zertifikate für verschiedene genormte Managementsysteme in Deutschland im Jahr 2019 gemäß dem ISO Survey (2020) bzw. im Fall der IATF 16949 (Stand 30.06.2020) gemäß IATF.*

Norm/Standard	Titel	Anzahl Zertifikate in Deutschland[8] (Standorte)
ISO 9001	Qualitätsmanagementsysteme – Anforderungen	47.868 (71.963)
ISO 14001	Umweltmanagementsysteme – Anforderungen mit Anleitung zur Anwendung	8.465 (14.388)
ISO 50001	Energiemanagementsysteme – Anforderungen mit Anleitung zur Anwendung	5.786 (13.122)
IATF 16949	Qualitätsmanagementsysteme – Besondere Anforderungen bei Anwendung von ISO 9001 für die Serien- und Ersatzteilproduktion in der Automobilindustrie	3.039*
ISO/IEC 27001	**Informationssicherheit- IT-Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen**	**1.175 (2.095)**
ISO 20000-1	IT-Service-Management – Teil 1: Spezifikation für Service Management	44 (122)

Bisherige Studien zur ISO/IEC 27001 greifen daher auf sehr kleine Stichproben von zertifizierten Unternehmen[9] oder spezielle Branchen wie beispielsweise Energieversorger zurück.[10]

Für Deutschland liegen noch keine branchenübergreifenden Untersuchungen vor, obwohl auch in Deutschland insbesondere vor dem Hintergrund der fortschreitenden Digitalisierung und regulativer Initiativen Normen im Bereich der Informationssicherheit, wie der ISO/IEC 27001, und dem Nachweis der wirksamen Anwendung durch eine Zertifizierung eine wachsende Bedeutung zukommt.

In der ersten QI-FoKuS-Studie zur Nutzung und Wirkung verschiedener Managementsysteme wurde neben etablierten genormten Managementsystemen bspw. für Qualität und Umwelt (ISO 9001 und ISO 14001) auch ein Schwerpunkt auf das ISMS nach ISO/IEC 27001 gelegt.[11] Diese Erhebung stellt eine erste weitergehende empirische Erhebung zu dieser Norm dar. Die vorliegende Studie baut darauf auf und nimmt explizit nach ISO/IEC 27001 zertifizierte Unternehmen in Deutschland in den Fokus, die online befragt wurden. Die Erhebung gibt somit auf Basis einer Stichprobe von 125 nach ISO/IEC 27001 zertifizierten Unternehmen erstmals umfassende Einblicke in die Implementierung und Zertifizierung von ISMS nach ISO/IEC 27001 in Deutschland.

Die Studie trägt zu einem besseren Verständnis bei, welche Unternehmen nach dieser Norm bereits zertifiziert sind, welche Motive sie zur Nutzung eines ISMS nach ISO/IEC 27001 hatten, welche Wirkungen die Anwendung dieser Norm entfaltet und wie der Nutzen der Implementierung und darüber hinaus der Zertifizierung von den Unternehmen bewertet wird. Dies kann anderen als Entscheidungshilfe dienen, die sich mit der Frage befassen, ob sie ein ISMS nach dieser Norm einführen und sich dafür zertifizieren lassen sollen. Insbesondere die Betrachtung der Hürden, die bei der Implementierung auftraten, sowie der Einschätzung der Sinnhaftigkeit von Maßnahmen für eine mögliche weitere Verbreitung zeigt Entscheidungsträgern Handlungsoptionen auf.

FRAGENKATALOG UND METHODIK

Vorgehen

Im Vorfeld der Befragung wurden in einer separaten Studie mittels Web Mining und einer öffentlich verfügbaren Zertifizierungsdatenbank Unternehmen in Deutschland identifiziert, die gemäß eines Hinweises auf ihrer Unternehmenswebseite oder Listung in der Datenbank nach ISO/IEC 27001 zertifiziert sind.[12] Insgesamt 806 nach ISO/IEC 27001 zertifizierte Unternehmen wurden von Januar bis März 2020 direkt telefonisch kontaktiert und zur Teilnahme an der Online-Umfrage eingeladen. 125 vollständig ausgefüllte Fragebögen konnten schließlich ausgewertet werden. Dies entspricht einer Rücklaufquote von 15,5% bezogen auf die identifizierte und kontaktierte Grundgesamtheit.

Der Fragebogen

Der Fragebogen wurde in einem iterativen Prozess entwickelt, in dem das Feedback verschiedener Stakeholder und Experten einfloss. Schließlich wurde ein Pre-Test mit fünf Unternehmen unterschiedlicher Größe und aus verschiedenen Branchen durchgeführt.

Der Fragebogen unterteilt sich in sechs Themengebiete:
- Angaben zum teilnehmenden Unternehmen (z.B. Zahl der Mitarbeitenden, Umsatz etc.),
- Motive zur Implementierung und Zertifizierung eines ISMS nach ISO/IEC 27001,
- Wirkungen durch die Nutzung des ISMS nach ISO/IEC 27001,
- Kosten-Nutzen-Einschätzung,
- Hürden bei der Implementierung sowie hilfreiche fördernde Maßnahmen und
- Wahl der Zertifizierungsstelle.

Teilnehmende und Stichprobe

In den meisten Fällen (n=70) wurde der Fragebogen von Mitarbeitenden der IT/Datenverarbeitung ausgefüllt, gefolgt von der Gruppe der Verwaltung/Organisation (n=46) sowie des Qualitätsmanagements (n=40). Des Weiteren haben viele der Befragten angegeben, der Geschäftsführung/Betriebsleitung anzugehören (n=30) oder auch in der Normung/Standardisierung (n=16) tätig zu sein.[13]

97% der befragten Unternehmen haben ihren Hauptsitz in Deutschland. Jeweils ein Fünftel gehört zu einer nationalen oder internationalen Unternehmensgruppe, 53% sind Einzelunternehmen.

Unternehmensform

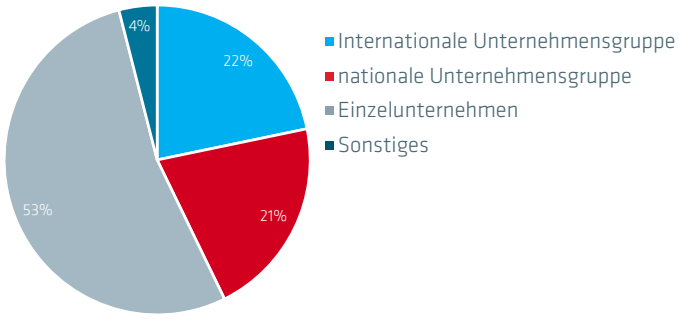


Abbildung 3: Zugehörigkeit zu einer Unternehmensform (N=124).

Die Zuordnung der Branchenzugehörigkeit erfolgte entsprechend der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE). 58% aller teilnehmenden Unternehmen gehören demnach zur IKT-Branche. Damit zeigt sich ein eindeutiger Branchenschwerpunkt zertifizierter Unternehmen – insbesondere, wenn man berücksichtigt, dass IKT-Unternehmen nur 3,5% aller Unternehmen in Deutschland darstellen.[14] Die Gruppe der Beratungsunternehmen, d.h. Anbieter von freiberuflichen, wissenschaftlichen und sonstigen Dienstleistungen, stellen die zweitgrößte Branchengruppe unserer Stichprobe dar. Weiterhin ist fast jedes zehnte

Branchen

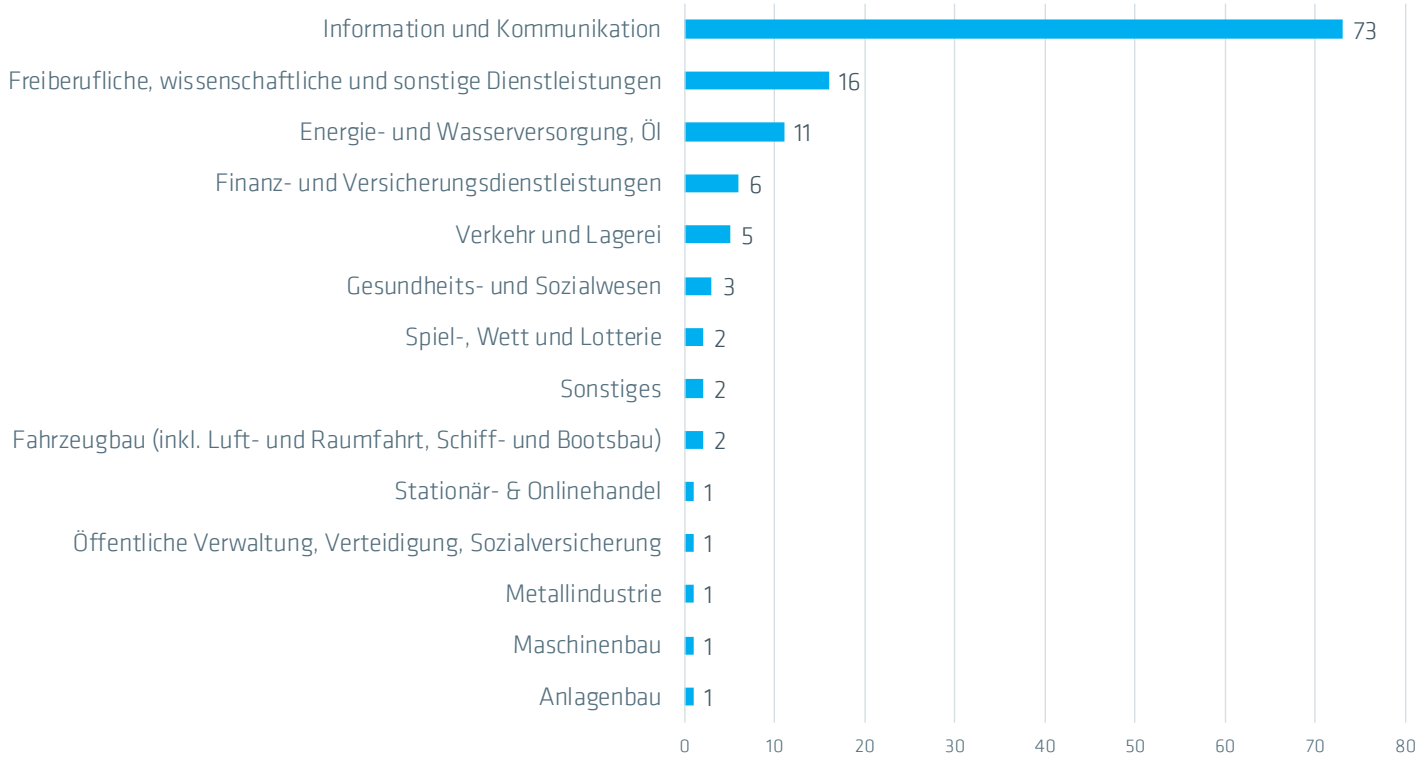


Abbildung 4: Branchenzugehörigkeit der teilnehmenden Unternehmen (N=125).

teilnehmende zertifizierte Unternehmen ein Energie- und Wasserversorger – und gehört damit zu einer Branche, deren Unternehmen als Kritische Infrastruktur besonders schützenswert und gemäß IT-Sicherheitsgesetz und BSI-KRITIS-Verordnung bei entsprechender Größe verpflichtet sind, mit einem Zertifikat nachzuweisen, die Anforderungen der ISO/IEC 27001 zu erfüllen.[15]

Im Hinblick auf die Branchenverteilung der per Web Mining ermittelten, nach ISO/IEC 27001 zertifizierten Unternehmen[16] und die branchenspezifischen ISO Survey Zahlen[17] können die Ergebnisse der Stichprobe weitgehend auf die Grundgesamtheit übertragen werden, wobei IKT-Unternehmen und Energieanbieter im Vergleich leicht über- und Banken und Finanzanbieter leicht unterrepräsentiert sind.[18]

Die Einordnung der Unternehmen nach Größe folgt der Definition der Europäischen Kommission (2003/361/EG) für kleine und mittelständische Unternehmen (KMU), die unterscheidet zwischen

- kleinen Unternehmen bis 50 Mitarbeitende bzw. höchstens 10 Mio. Euro Umsatz,
- mittleren Unternehmen mit 50 bis 250 Mitarbeitenden und 10 bis 50 Mio. Euro Umsatz und
- großen Unternehmen mit mehr als 250 Mitarbeitenden und über 50 Mio. Euro Umsatz.

41% der Unternehmen haben weniger als 50 Mitarbeitende sowie 40% weniger als 10 Mio. Euro Umsatz im letzten Geschäftsjahr und gehören damit entsprechend dieser Einteilung zu den kleinen Unternehmen. Zu den mittleren Unternehmen gehört nach Mitarbeitendenzahl ein Drittel der befragten Unternehmen bzw. 21% gemessen am Umsatz. Jedes zehnte Unternehmen der Stichprobe beschäftigt mindestens 1000 Mitarbeitende.

36% der befragten Unternehmen geben an, auch im Ausland Umsatz zu erwirtschaften. Insgesamt lag ihr durchschnittlicher Exportanteil bei 7,4%. Der wesentliche Absatzmarkt für 89% der Unternehmen hierbei ist

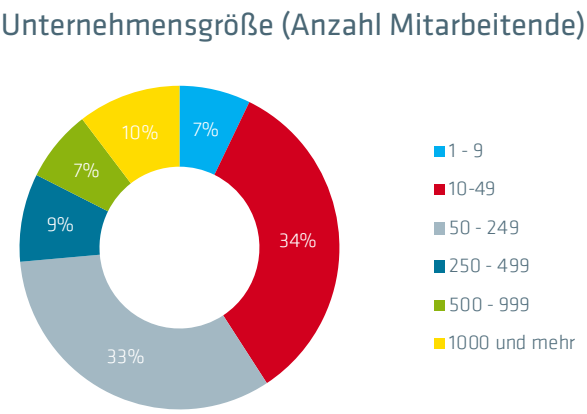


Abbildung 5: Unternehmensgröße nach Anzahl der Mitarbeitenden im letzten Geschäftsjahr (N=125).

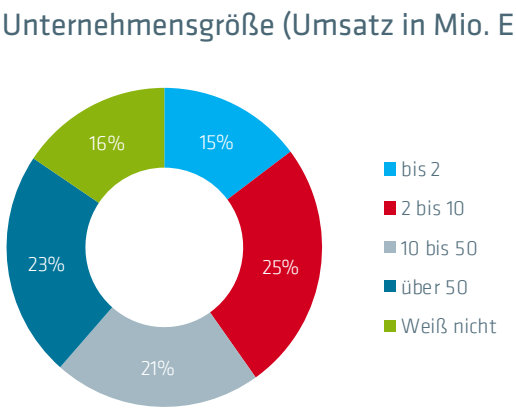


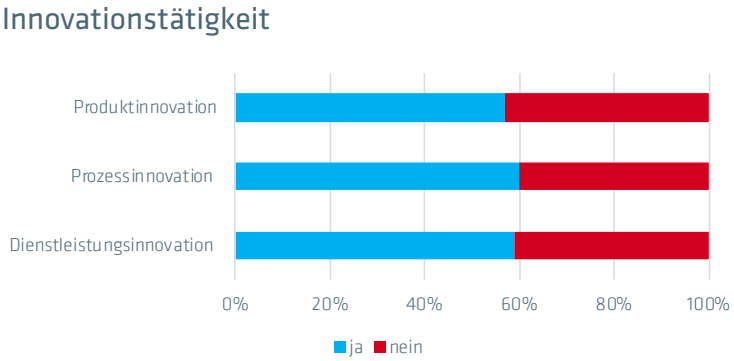
Abbildung 6: Unternehmensgröße nach Umsatz in Mio. Euro im letzten Geschäftsjahr (N=122).

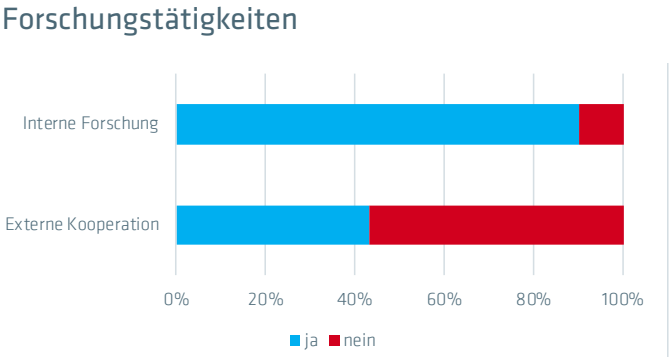
die Europäische Union, gefolgt von den USA (7%) und dem asiatischen Markt (4%).

Auch die Innovationstätigkeit der teilnehmenden Unternehmen wurde erfasst. Dafür wurde erhoben, ob das jeweilige Unternehmen im Vorjahr Innovationen in Bezug auf Produkte oder Dienstleistungen auf den Markt gebracht oder merklich verbesserte Prozesse eingeführt hat. Falls dies der Fall ist, wird das Unternehmen im Folgenden als innovativ bezeichnet. Von den 125 Unternehmen der Stichprobe sind 89 Unternehmen (=71%) in mindestens einem Bereich (Produkt, Prozess, Dienstleistung) innovativ. Konkret gaben 57% (aus n=111) an, eine Produktinnovation eingeführt zu haben. Etwa 59% (aus n=107) waren an Dienstleistungsinnovationen beteiligt und 60% (aus n=110) der Befragten gaben an, Prozessinnovationen eingeführt zu haben. Etwa jedes vierte Unternehmen (28%) war in allen drei Dimensionen innovativ.

90% (aus n=80) der Unternehmen üben diese Forschungs- und Innovationsaktivitäten selbst intern aus, und 43% (aus n=79) geben an, (auch) mit externen Forschungseinrichtungen zu kooperieren.

Im vorliegenden Bericht werden vor allem die Unternehmensgröße, Exporttätigkeit sowie Innovationstätigkeiten als Unterscheidungskriterien herangezogen, um





Abbildungen 7 und 8: Innovationstätigkeit (N=107-111) und Forschungstätigkeiten (N=79-80).

die Ergebnisse zu strukturieren und einzelne Besonderheiten herauszuarbeiten. Insbesondere wird unterschieden zwischen Unternehmen, die zur IKT-Branche gehören, und jenen, die anderen Branchen angehören. Unterschiede werden dann gesondert hervorgehoben, wenn diese statistisch signifikant sind (d.h. einen p-Wert von mindestens < 0,10 aufweisen).

NUTZUNG EINES ISMS NACH ISO/IEC 27001

Managementsysteme nach ISO- und anderen Normen erfreuen sich international und auch in Deutschland wachsender Beliebtheit. Seit 1986 gibt es die Qualitätsmanagementsystem-Norm ISO 9001 und mittlerweile sind fast eine Million Unternehmen nach dieser Norm zertifiziert. Im Zuge dieses Erfolges wurden nach und nach weitere Standards für andere Managementbereiche entwickelt, so bspw. für das Management umwelt- und energiebezogener Aspekte in Organisationen. Die 2005 eingeführte ISO/IEC 27001 für Informationssicherheit gehört zu den jüngeren internationalen ISO bzw. ISO/IEC Managementsystem-Normen.

Unternehmen können ISMS implementieren und sich darüber hinaus bezüglich der Anforderungen der zugrundeliegenden Norm zertifizieren lassen. Eine Zertifizierung bestätigt von dritter (d.h. unabhängiger) Seite, dass die in der gültigen Norm definierten Anforderungen erfüllt sind. Zertifikate sind damit ein wichtiger transparenzschaffender Nachweis gegenüber Kunden oder anderen interessierten Kreisen und können zu einem einheitlichen Qualitäts- und Sicherheitsniveau beitragen.[19]

Die grundsätzliche Struktur verschiedener ISO bzw. ISO/IEC Managementsystemnormen ist mittlerweile angeglichen, was den Unternehmen eine leichtere und integrative Implementierung verschiedener Managementsysteme ermöglicht und somit Synergien bei der Nutzung freisetzen kann. So kann bspw. für Nutzende eines Qualitätsmanagementsystems nach ISO 9001 die Implementierung weiterer Managementsysteme aufgrund der gewonnenen Erfahrungen und Kenntnisse mit weniger Aufwand verbunden sein.

Jedes zweite nach ISO/IEC 27001 zertifizierte Unternehmen der Stichprobe hat gleichzeitig auch ein nach ISO 9001 zertifiziertes Qualitätsmanagementsystem. Weitere 6% haben ein solches ohne Zertifizierung implementiert. 17% haben ein Energiemanagementsystem nach ISO 50001, 16% ein Umweltmanagementsystem nach ISO 14001, mehrheitlich mit Zertifikat. 39% aller befragten Unternehmen der vorliegenden Studie geben jedoch an, keine weiteren Zertifizierungen außer für das ISMS nach ISO/IEC 27001 zu haben.

Anwendung anderer Managementsystem-Normen

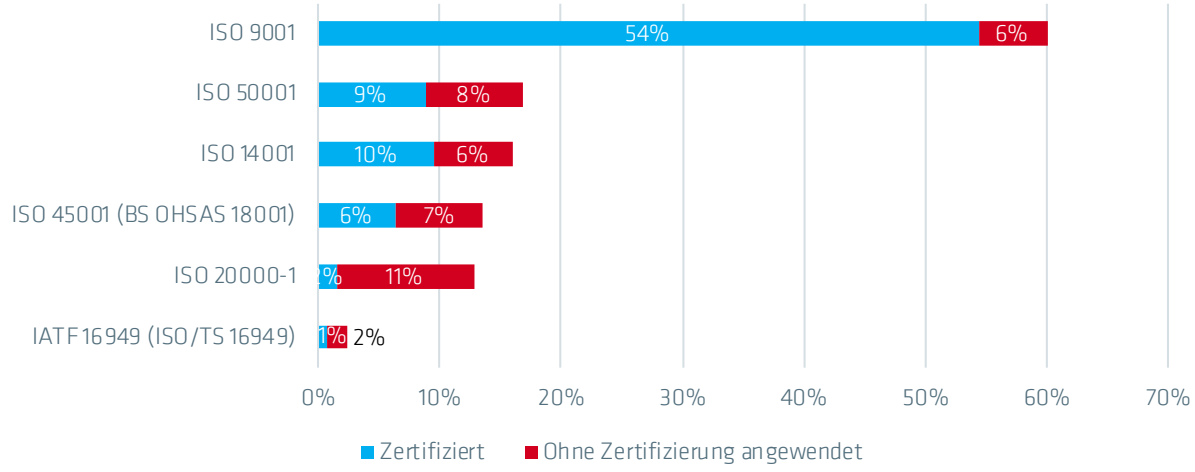


Abbildung 9: Anteil der nach ISO/IEC 27001 zertifizierten Unternehmen, die auch andere Managementsystem-Normen anwenden (N=125).

Gemäß IT-Sicherheitsgesetz können Unternehmen verpflichtet werden, ein ISMS einzuführen und sich entsprechend zertifizieren zu lassen. 13% geben an, dass dies auf ihr Unternehmen zutrifft, wobei 53% davon zu den Energieanbietern (n=9) gehören. Bei 77% der Befragten ist dies hingegen nicht der Fall. Jedes zehnte befragte Unternehmen gab außerdem an, nicht zu wissen, ob es gemäß IT-Sicherheitsgesetz zur Zertifizierung verpflichtet ist.

Jeweils 45% der nach der Norm ISO/IEC 27001 zertifizierten Unternehmen geben an, seit 1-3 bzw. bereits seit 4-9 Jahren zertifiziert zu sein. Jedes zehnte Unternehmen gehört zu den frühen Nutzern und hält sein Zertifikat bereits mindestens 10 Jahre. Betrachtet man die Branchenzugehörigkeit genauer, zeigt sich, dass Unternehmen der IKT-Branche einen kleinen Vorsprung beim Zertifizierungszeitpunkt gegenüber Unternehmen anderer Branchen haben. Während nur 6% der Letzteren seit mindestens 10 Jahren zertifiziert sind, gehören bei den IKT-Unternehmen 14% zu diesen „Early Adoptern". Energieversorgungsunternehmen können bei entsprechender Größe und Wichtigkeit seit 2015 gemäß IT-Sicherheitsgesetz zur Zertifizierung

Verpflichtung zur Zertifizierung eines ISMS gem. IT-Sicherheitsgesetz

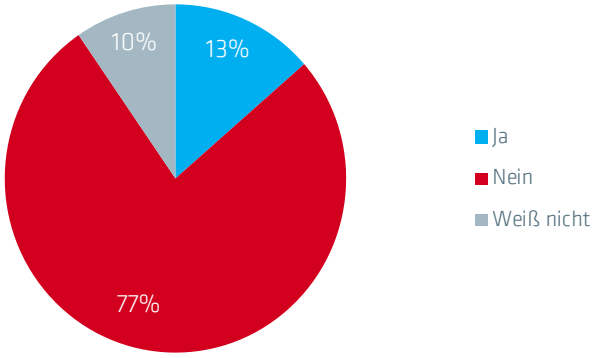


Abbildung 10: Angabe, ob die befragten Unternehmen gemäß IT-Sicherheitsgesetz verpflichtet sind, ein ISMS zu implementieren und sich zertifizieren zu lassen (N=125).

verpflichtet sein: Entsprechend geben 82% der befragten Unternehmen dieser Branche an, seit maximal drei Jahren zertifiziert zu sein, nur 18% sind dies schon länger (seit 4-9 Jahren).

Jahre seit Erstzertifizierung

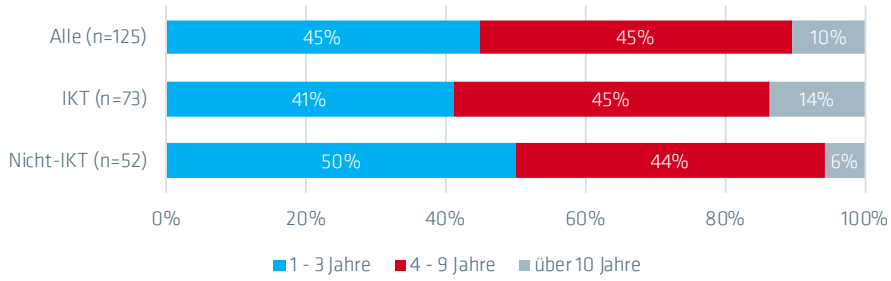


Abbildung 11: Jahre seit Erstzertifizierung. Basis bilden alle antwortenden Unternehmen (N=125), Unternehmen, die zur IKT-Branche gehören (N=73) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=52).

Unternehmen, die sich nach ISO/IEC 27001 zertifizieren lassen, können dabei entscheiden, auf welchen Geltungsbereich sich diese Zertifizierung erstreckt. Bei 43% deckt das ISMS das gesamte Unternehmen ab. Vor allem Unternehmen, die sonstige Dienstleistungen anbieten (8 von 12 Unternehmen) und Unternehmen, die der IKT Branche angehören (32 von 73 Unternehmen), lassen vergleichsweise häufig das ISMS des gesamten Unternehmens nach ISO/IEC 27001 zertifizieren.

Von Unternehmen, bei denen nicht das gesamte Unternehmen zertifiziert ist, geben 86% an, dass sich der Geltungsbereich auf die IT bezieht. Mit Abstand folgen die Produktion sowie die Entwicklung. Finanzen und Einkauf fallen hingegen seltener in den Geltungsbereich einer ISO/IEC 27001 Zertifizierung.

MOTIVE ZUR NUTZUNG EINES ISMS NACH ISO/IEC 27001

Geltungsbereich der Zertifizierung für das gesamte Unternehmen?

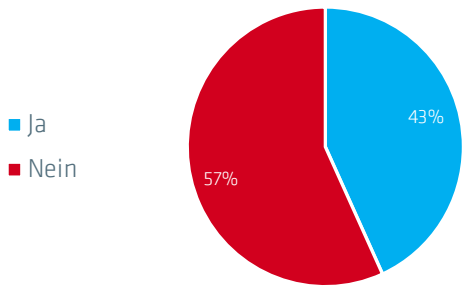


Abbildung 12: Geltungsbereich der ISO/IEC 27001 Zertifizierung für das gesamte Unternehmen. Basis bilden alle antwortenden Unternehmen (N=125).

Geltungsbereich der Zertifizierung (falls nicht für das gesamte Unternehmen zertifiziert)

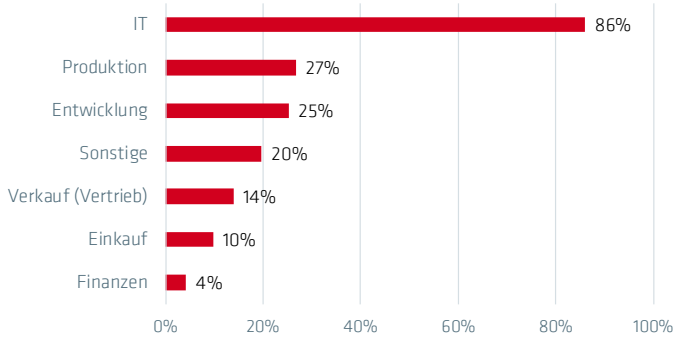


Abbildung 13: Geltungsbereich der ISO/IEC 27001 Zertifizierung, falls nicht das gesamte Unternehmen zertifiziert ist (N=71), Mehrfachnennungen möglich.

Die befragten Unternehmen nutzen ihr ISMS nach ISO/IEC 27001 aus verschiedenen internen und externen Gründen. Die Teilnehmenden wurden gebeten, die Relevanz vorgegebener Motive auf einer Skala von "trifft gar nicht zu" (1) bis „trifft voll zu" (5) zu bewerten.

Die „Vorbeugung von Informationssicherheitsvorfällen" ist das führende Motiv für die Einführung und Zertifizierung eines ISMS nach ISO/IEC 27001. Gleich dahinter folgen vier fast gleich stark bewertete Motive, die überwiegend auch im Zusammenhang mit der Prävention von Informationssicherheitsvorfällen und damit der Erhöhung der Informationssicherheit stehen. So werden die Verbesserung unternehmensinterner Prozesse, die Erhöhung der Rechtssicherheit und die Erhöhung des Bewusstseins der Mitarbeitenden als wichtige interne Motive genannt. Letzteres wird von innovativen Unternehmen als wichtiger angesehen als von nicht-innovativen Unternehmen (Mittelwert (MW) 4,1 ggü. 3,7). Kundenforderungen nach entsprechender Zertifizierung sind als externer Treiber insgesamt ebenfalls ein führendes Motiv.

Während der Marktzugang im Inland als zweithäufigstes Motiv für die Einführung und Zertifizierung eines ISMS nach ISO/IEC 27001 folgt, spielt der Marktzugang im Ausland eine vergleichsweise untergeordnete Rolle. Allerdings wertet die Gruppe der exportierenden Unternehmen letzteres Motiv erwartungsgemäß signifikant höher (MW 3,0 ggü. 1,9 bei nicht-exportierenden Unternehmen). Für sie sind weiterhin Forderungen von Kundenseite signifikant wichtiger als für nicht-exportierende Unternehmen (MW 4,3 ggü. 3,7). Für letztere spielt auch eine mögliche Zertifizierung der Konkurrenz eine signifikant geringere Rolle als dies bei exportorientierten Unternehmen der Fall ist (MW 2,9 ggü. 2,3). Unterschiede bei der Bewertung der Motive zeigen sich auch hinsichtlich der Unternehmensgröße: Für große Unternehmen mit mehr als 50 Mio. Euro Jahresumsatz sind der inländische Marktzugang und Kundenforderungen signifikant weniger wichtige Motive für die Zertifizierung nach ISO/IEC 27001 als für den Rest (MW 2,8 ggü. 3,9 sowie 3,4 ggü. 4,2).

Die geringste Rolle bei der Entscheidung für eine Zertifizierung des ISMS spielt die Reaktion auf einen konkreten Informationssicherheitsvorfall. Die Entscheidung für ein solches Managementsystem scheint also eher strategisch getrieben als aufgrund konkreter Vorfälle.

Vergleicht man die Motive von Unternehmen, die im IKT-Sektor tätig sind, mit Unternehmen anderer Branchen, so zeigen sich fünf signifikante Unterschiede. Markt- und marketingbezogene Motive stehen bei Unternehmen der IKT-Branche deutlich höher im Ranking als bei anderen Unternehmen: Sowohl die Forderungen von Kundenseite, die Förderung des Marktzugangs (im In- und Ausland), die Nutzung für Marketing- und Imagezwecke als auch, dass konkurrierende Unternehmen ebenfalls zertifiziert sind, werden als Motive für die Einführung und Zertifizierung eines ISMS nach ISO/IEC 27001 signifikant höher bewertet.

Motive zur Anwendung von ISO/IEC 27001

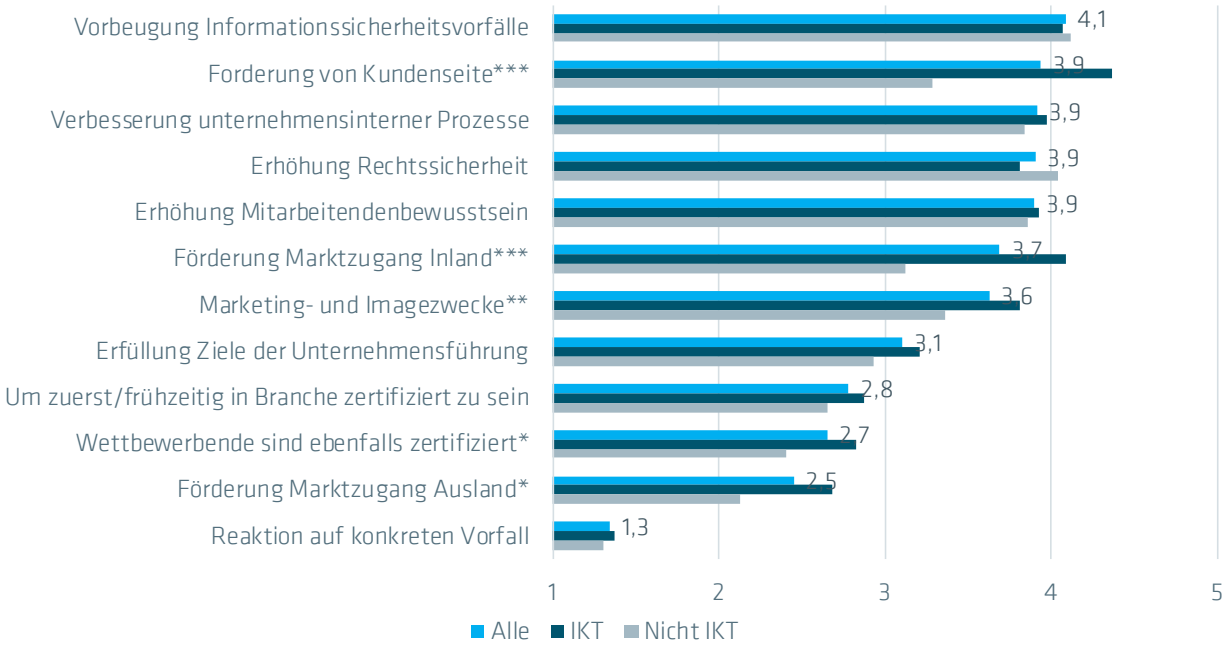


Abbildung 14: Durchschnittliche Einschätzung der Motive für die Implementierung der Norm ISO/IEC 27001 und Zertifizierung. Basis bilden alle antwortenden Unternehmen (N=117-123), Unternehmen, die zur IKT-Branche gehören (N=65-73) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=46-52).
*Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu). Signifikante Unterschiede bei Branchenzugehörigkeit werden durch * angezeigt (* p < 0,10; ** p < 0,05; *** p < 0,01).*

WIRKUNG VON ISMS NACH ISO/IEC 27001

Die Teilnehmenden wurden gebeten, die Wirkungen zu bewerten, die ihrer Meinung nach durch die Umsetzung der ISMS-Norm ISO/IEC 27001 realisiert wurden. Auch hier wurden vorgegebene Wirkungen auf einer Skala von 1 („trifft gar nicht zu“) bis 5 („trifft voll zu“) gewertet.

Die wichtigste Wirkung für die Befragten ist die Erhöhung des Mitarbeitendenbewusstseins für Informationssicherheit. Es folgen weitere präventionsbezogene Wirkungen: Sowohl die Erhöhung der Informationssicherheit als auch die Reduktion der Gefahr von Informationssicherheitsvorfällen werden als wichtige Folgen der ISO/IEC 27001-Zertifizierung wahrgenommen – unabhängig davon, ob die Unternehmen zur IKT-Branche gehören oder nicht. Es folgen Imageverbesserungen und – mit Abstand – Umsatzsteigerungen durch Verweise auf das Zertifikat als eher marktbezogene Wirkungen. Hier zeigen sich jedoch deutliche Branchenunterschiede: Unternehmen der IKT-Branche profitieren in beiden Fällen signifikant mehr als Unternehmen anderer Branchen (MW 4,1 ggü. 3,7 und 3,5 ggü. 2,5). Große Unternehmen mit mehr als 50 Mio. Euro Jahresumsatz hingegen bewerten diese Wirkungen signifikant geringer als kleinere Unternehmen (MW 3,5 ggü. 4,1 bzw. 2,5 ggü. 3,3). Auch bei der Unternehmensgröße gemessen nach Anzahl der Mitarbeitenden zeigt sich, dass kleine Unternehmen mit weniger als 50 Mitarbeitenden signifikant mehr positive Wirkung auf ihr Image durch Verweis auf ein ISO/IEC 27001-Zertifikat verzeichnen als größere Unternehmen mit über 250 Mitarbeitenden (MW 4,2 ggü. 3,6). Des Weiteren bewerten Unternehmen, die laut IT-Sicherheitsgesetz verpflichtet sind, die Konformität ihres ISMS durch ein Zertifikat zu belegen, die Umsatzeffekte signifikant geringer als alle anderen (MW 1,9 ggü. 3,2).

Während die Erhöhung der Rechtssicherheit im Mittelfeld der Wirkungen liegt, spielen Kosten nur eine untergeordnete Rolle: Die Reduktion unternehmensinterner, durch Informationssicherheitsvorfälle

Wirkung von ISO/IEC 27001

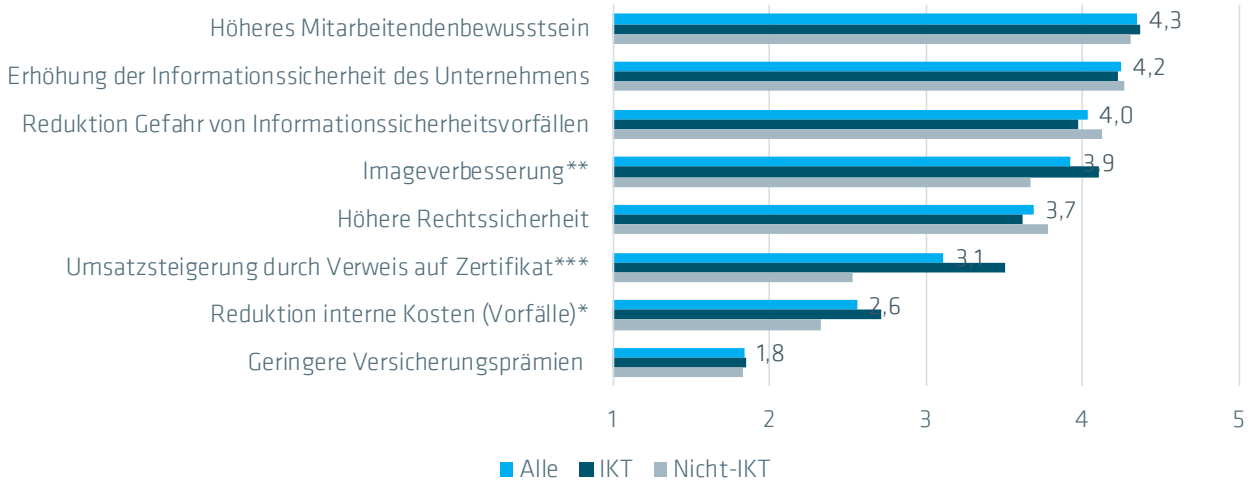


*Abbildung 15: Durchschnittliche Einschätzung der Wirkung durch die Nutzung des Managementsystems nach ISO/IEC 27001. Basis bilden alle antwortenden Unternehmen (N=96-123), Unternehmen, die zur IKT-Branche gehören (N=54-72) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=42-52). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu). Signifikante Unterschiede bei Branchenzugehörigkeit werden durch * angezeigt (* p < 0,10; ** p < 0,05; *** p < 0,01).*

verursachter Kosten und insbesondere von Versicherungsprämien stehen auf den letzten beiden Plätzen. Für IKT-Unternehmen entfaltet eine ISO/IEC 27001-Zertifizierung jedoch hinsichtlich der Reduktion interner Kosten signifikant mehr Wirkung als für Nicht-IKT-Unternehmen (MW 2,7 vs. 2,3).

Die Befragungsergebnisse unterstreichen damit den eher präventionsbezogenen Fokus der Implementierung und Zertifizierung eines ISMS nach ISO/IEC 27001. Unternehmen profitieren weniger von direkten finanziellen Vorteilen durch Umsatzsteigerung oder Kostenreduktion (bedingt durch weniger Informationssicherheitsvorfälle), sondern vielmehr von der Verminderung von Risiken und Folgen aus Vorfällen bzgl. ihrer Informationssicherheit und damit strategisch langfristig.

GESAMTBEWERTUNG DES ISMS NACH ISO/IEC 27001

Unterschiede zwischen Motivation zur Einführung von Managementsystemen und tatsächlich realisierten Wirkungen

Vergleicht man die ursprünglichen Motive zur Einführung eines ISMS nach ISO/IEC 27001 mit den Bewertungen bzgl. der tatsächlich realisierten Wirkungen, zeigt sich, dass die Erwartungen, insbesondere hinsichtlich der Imagewirkungen, der internen Verbesserungen bzgl. der Informationssicherheit sowie des Bewusstseins der Mitarbeitenden für die Thematik, übertroffen wurden. Leicht negative Abweichungen zeigen sich hingegen bei der angestrebten Verbesserung der Rechtssicherheit sowie der Vorbeugung und Reduktion der Gefahr von Informationssicherheitsvorfällen. Alle Abweichungen sind gleichsam sowohl bei Unternehmen der IKT als auch in anderen Branchen zu sehen.

Abweichungen zwischen Motiven und tatsächlich wahrgenommenen Wirkungen (bezogen auf die jeweiligen Durchschnittswerte)

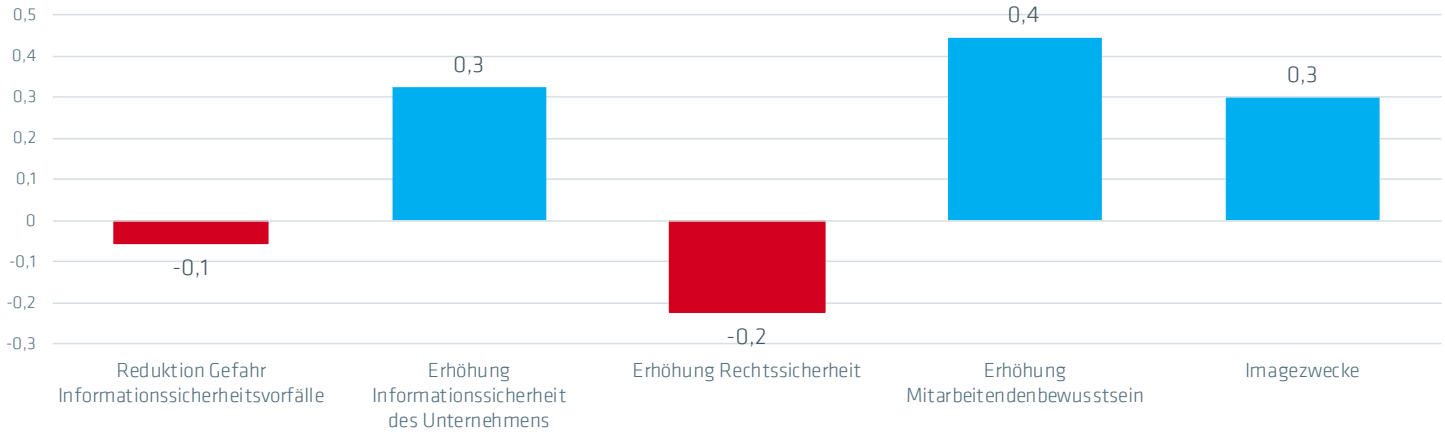


Abbildung 16: Abweichungen der Bewertung der tatsächlich wahrgenommenen Wirkungen von der ursprünglichen Bewertung der Motive (bezogen auf die jeweiligen Mittelwerte); (N=96-123).

Positive Bewertung der Kosten-Nutzen-Relation

Diese positive Bewertung spiegelt sich auch in der Gesamtbewertung des Nutzens des ISMS nach ISO/IEC 27001 wider. Die Teilnehmenden wurden abschließend gefragt, ob die Implementierung sowie zusätzlich die Zertifizierung insgesamt eine gute Investition in Bezug auf Kosten und Nutzen seien (auf einer 5-stufigen Skala von „trifft gar nicht zu“ (1) bis „trifft voll zu“ (5)).

Während die Einschätzungen hier insgesamt positiv sind, zeigt sich eine signifikant positivere Bewertung des Nutzens der Implementierung durch Unternehmen der IKT-Branche im Vergleich zu anderen Unternehmen (MW 4,3 ggü. 3,9). In der Bewertung des Nutzens der zusätzlichen Zertifizierung zeigen sich hier hingegen keine signifikanten Branchenunterschiede. Die Zertifizierung wird insbesondere von nur im Inland tätigen Unternehmen lohnender gewertet als von auch exportierenden Unternehmen (MW 4,2 ggü. 3,7). Dies passt auch zu der Einschätzung der Wichtigkeit der Motive, dass der Marktzugang im Inland höher bewertet wurde als der Marktzugang im Ausland. Und auch innovative Unternehmen werten den Nutzen der zusätzlichen Zertifizierung insgesamt positiver als nicht-innovative Unternehmen (MW: 4,1 ggü. 3,8).

ISO/IEC 27001 gute Investition?

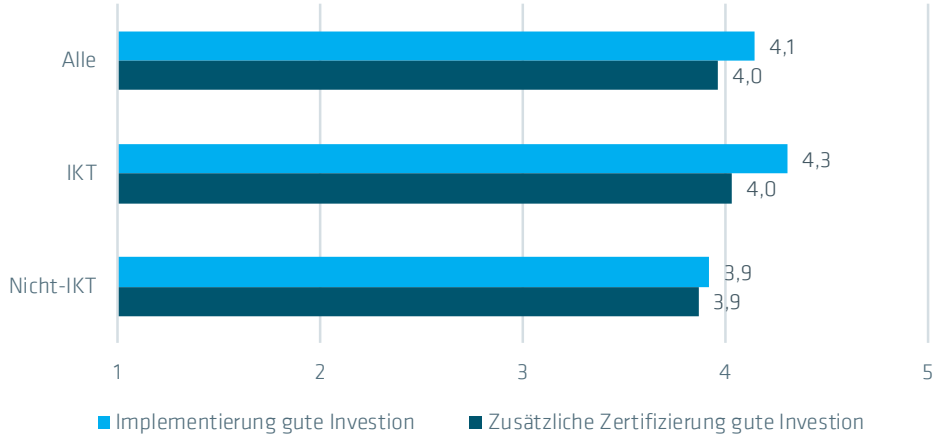


Abbildung 17: Einschätzung, ob alles in allem die Implementierung und zusätzlich die Zertifizierung eine gute Investition in Bezug auf Kosten und Nutzen für die Unternehmen darstellen. Basis bilden alle antwortenden Unternehmen (N=108-123), Unternehmen, die zur IKT-Branche gehören (N=63-72) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=45-51). Bewertungsskala: 1 (trifft gar nicht) bis 5 (trifft voll zu).

Unternehmen, deren Erstzertifizierung schon mehr als drei Jahre zurückliegt und die somit eine Re-Zertifizierung durchlaufen haben, wurden befragt, wie sich ihre Kosten-Nutzen-Einschätzung im Zeitverlauf seither geändert hat. Im Durchschnitt hat sich die Wahrnehmung nicht verändert (MW: 3,1), wobei für IKT-Unternehmen eine minimal positivere Tendenz (MW: 3,3) zu verzeichnen ist und für Unternehmen anderer Branchen eine leicht negativere (MW: 2,9). Unter genauer Betrachtung zeigt sich, dass ein Drittel aller befragten rezertifizierten Unternehmen eine geringe oder sogar starke Verschlechterung der Kosten-Nutzen-Relation feststellen; 44% hingegen berichten eine geringe oder starke Verbesserung. Sonstige signifikante Unterschiede bei spezifischen Unternehmenscharakteristika zeigen sich hingegen nicht.

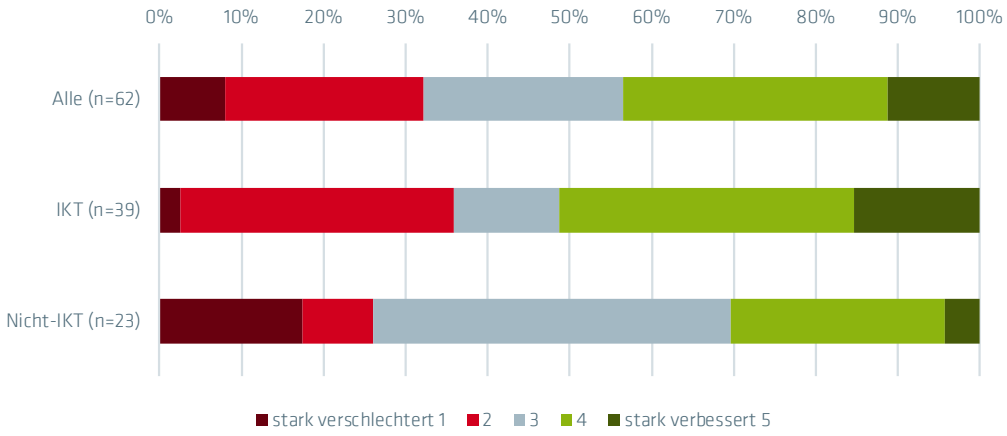


Abbildung 18: Einschätzung der befragten Unternehmen, die erstmals vor mehr als 3 Jahren nach ISO/IEC 27001 zertifiziert wurden, wie sich im Vergleich zur Erstzertifizierung die Kosten-Nutzen Relation bis heute entwickelt hat. Basis bilden alle antwortenden Unternehmen (N=62), Unternehmen, die zur IKT-Branche gehören (N=39) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=23). Bewertungsskala: 1 (stark verschlechtert) bis 5 (stark verbessert).

IMPLEMENTIERUNGSHÜRDEN UND MÖGLICHE FÖRDERNDE MASSNAHMEN FÜR EINE WEITERE VERBREITUNG

Die Unternehmen wurden zu den Hürden bei der Implementierung des ISMS nach ISO/IEC 27001 befragt. Sie konnten dabei vorgegebene Optionen auf einer Skala von 1 („trifft gar nicht zu“) bis 5 („trifft voll zu“) bewerten.

Hürden bei der Implementierung vor allem durch Zeitaufwand und fehlende Expertise

Die größten Schwierigkeiten werden im hohen Zeitaufwand, nötigen externen Beratungsleistungen und den hohen Kosten gesehen. Letztere sind jedoch erwartungsgemäß insbesondere für die Gruppe der großen Unternehmen mit mehr als 250 Mitarbeitenden oder mehr als 50 Mio. Euro Jahresumsatz wesentlich weniger problematisch (MW 2,9 bei Umsatz größer als 50 Mio. Euro ggü. 3,7 bei weniger als 50 Mio. Euro). Neben Aufwand und Kosten stellen aber auch die Komplexität der Normeninhalte und fehlende unternehmensinterne Expertise Hürden für die Einführung dar. Die Einschätzung hinsichtlich der Schwierigkeiten ist für Unternehmen der IKT-Branche und anderer Branchen weitgehend ähnlich.

Verschiedene Maßnahmen können bei der Verbreitung helfen

Falls eine Verbreitung der Anwendung der Norm ISO/IEC 27001 in Deutschland aktiv angestrebt wird, können verschiedene Maßnahmen unterstützend wirken. Die Teilnehmenden konnten mögliche Maßnahmen hinsichtlich ihrer Eignung bewerten. Von den

Schwierigkeiten bei der Implementierung und Zertifizierung der ISO/IEC 27001

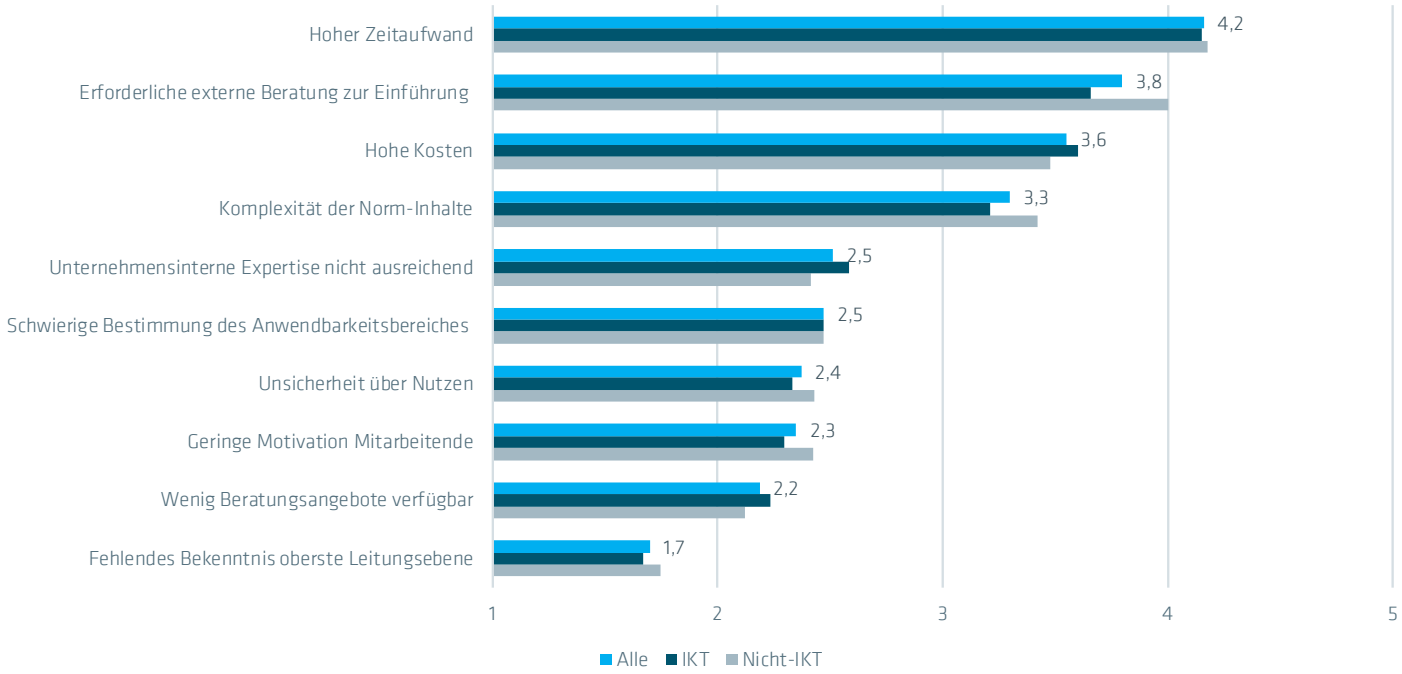


Abbildung 19: Durchschnittliche Einschätzung der Schwierigkeiten bei der Implementierung und Zertifizierung eines ISMS nach ISO/IEC 27001. Basis bilden alle antwortenden Unternehmen (N=113-124), Unternehmen, die zur IKT-Branche gehören (N=64-73) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=49-52). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

Unternehmen werden alle vorgeschlagenen Maßnahmen (mit MW zwischen 4,0 und 3,5) als sinnvoll eingeschätzt und ähnlich hilfreich bewertet. Jedoch zeigen sich bei vielen Optionen signifikante Unterschiede in der Bewertung zwischen großen und kleinen Unternehmen.

Insgesamt sei für eine weitere Verbreitung der Norm die Erhöhung ihrer Bekanntheit unter potenziellen Nutzenden am wichtigsten. Ebenso hilfreich werden finanzielle Unterstützungsleistungen für die Zertifizierung und für Beratungsleistungen speziell für KMU angesehen. Diese Maßnahmen werden von kleinen Unternehmen (mit weniger als 10 Mio. Euro Jahresumsatz) erwartungsgemäß signifikant positiver bewertet als von umsatzstärkeren Unternehmen (MW jeweils 4,4 ggü. 3,6). Auch Informationsangebote können eine wichtige Rolle spielen: KMUs könnten aus Sicht der Befragten auch durch einen Handlungsleitfaden bei der praktischen Implementierung unterstützt werden. Auch diese Maßnahme wird von den kleineren Unternehmen signifikant förderlicher bewertet – ähnlich wie die Veröffentlichung von Praxisbeispielen (MW 4,2 ggü. 3,5) und das Angebot von Schulungen für Mitarbeitende (MW 4,0 ggü. 3,6). Die Forderung eines Zertifizierungsnachweises von Seiten des Gesetzgebers wird insgesamt am wenigsten unterstützt. Eher noch wird Forderungen von Kundenseite eine fördernde Wirkung zugeschrieben (signifikant mehr von umsatzstarken als von kleinen Unternehmen mit weniger als 10 Mio. Euro Jahresumsatz; MW 4,1 ggü. 3,7).

Unternehmen der IKT-Branche bewerten sämtliche fördernden Maßnahmen tendenziell positiver als Unternehmen anderer Branchen. Insbesondere praxisorientierte Schulungen für Mitarbeitende werden signifikant hilfreicher eingeschätzt (MW 4,0 ggü. 3,6).

Maßnahmen zur Verbreitung von ISO/IEC 27001

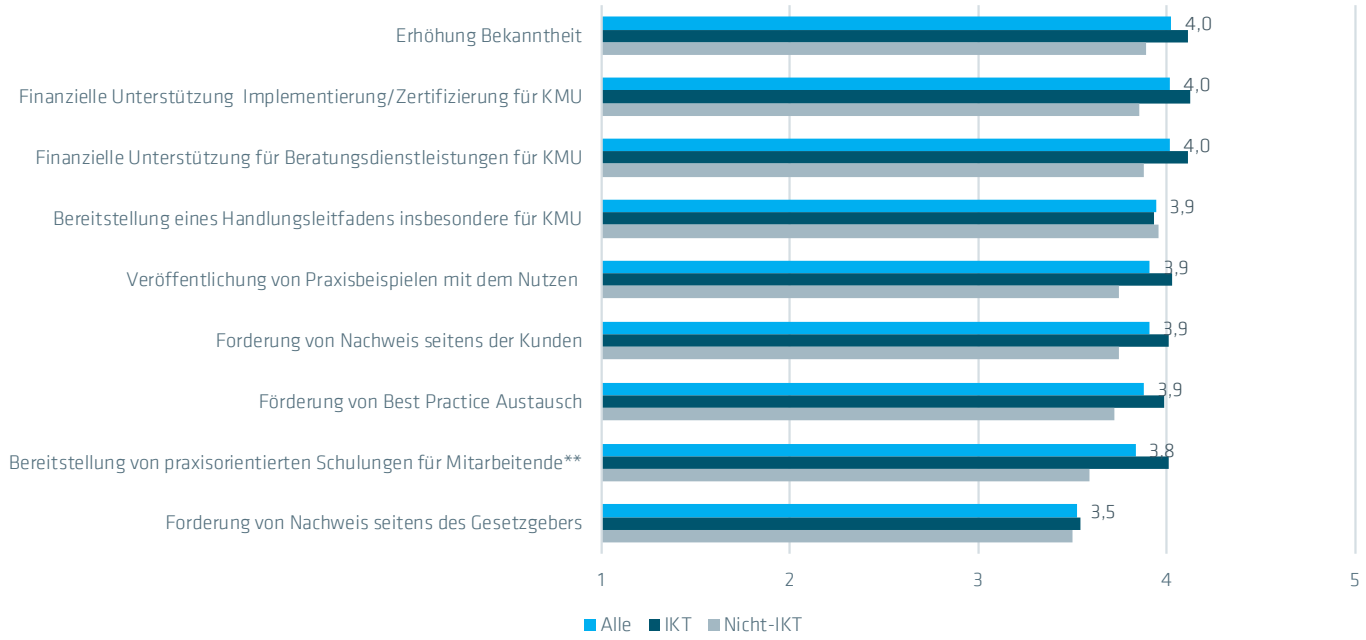


Abbildung 20: Bewertung von Maßnahmen zur Förderung der Verbreitung der Norm ISO/IEC 27001 in Deutschland. Basis bilden alle antwortenden Unternehmen (N=118-124), Unternehmen, die zur IKT-Branche gehören (N=71-73) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=47-51).
*Bewertungsskala: 1 (gar nicht sinnvoll) bis 5 (sehr sinnvoll). Signifikante Unterschiede bei Branchenzugehörigkeit werden durch * angezeigt (* p < 0,10; ** p < 0,,05; *** p < 0,01).*

WAHL DER ZERTIFIZIERUNGSSTELLE

Zertifikate können Unternehmen dabei helfen, die Erfüllung von Anforderungen an Produkte oder Arbeitsweisen und Prozesse in Form von Managementsystemen nach außen zu signalisieren und damit Informationsasymmetrien zwischen Marktteilnehmenden zu verringern. Unternehmen haben in der Regel die Wahl, durch welche Zertifizierungsstelle sie sich zertifizieren lassen. Bisher gibt es jedoch nur wenige Untersuchungen zu den Kriterien, welche die Unternehmen dabei anwenden. Die vorliegende Studie hat solche Kriterien beispielhaft adressiert. Dabei wurden die teilnehmenden Unternehmen gebeten, vorgegebene Kriterien entsprechend der Bedeutung, die sie ihnen zumessen, auf einer Skala von „überhaupt nicht wichtig“ (1) bis „sehr wichtig“ (5) zu bewerten.

Kompetenz und deren Nachweis als Hauptkriterien bei der Wahl der Zertifizierungsstelle

Das mit Abstand wichtigste Kriterium für die Teilnehmenden dieser Befragung bei der Auswahl der Zertifizierungsstelle ist deren Akkreditierung. Durch Akkreditierung lassen sich Zertifizierungsstellen ihre Kompetenz durch eine unabhängige Akkreditierungsstelle bestätigen. Vergleichsweise größere Bedeutung wird ihr insbesondere von großen Unternehmen mit

mehr als 10 Mio. Euro Jahresumsatz beigemessen (MW: 4,8 ggü. 4,5) sowie von Unternehmen, die nach dem IT-Sicherheitsgesetz verpflichtet sind, ein Zertifikat für ihr ISMS nachzuweisen (MW: 4,9 ggü. 4,7).

Daran anknüpfend ist das zweitwichtigste Kriterium bei der Auswahl der Zertifizierungsstelle die Fachkompetenz der Auditor*innen, gefolgt von der Reputation der Zertifizierungsstelle. Auch spezielles Fachwissen für die Branche des jeweiligen Kunden spielt insgesamt eine vergleichsweise große Rolle. Während es den Teilnehmenden daneben auch wichtig ist, dass die Zertifizierung schnell und einfach durchgeführt wird und branchenspezifisches Fachwissen vorhanden ist, sind die Kosten der Zertifizierung (Gebühren der Zertifizierungsstelle sowie Neben- und Reisekosten) hingegen weniger wichtig. Hier zeigen sich jedoch signifikante Unterschiede bei der Branchenzugehörigkeit der Befragten: Für Unternehmen der IKT-Branche sind die Gebühren ein signifikant wichtigeres Kriterium als für Unternehmen anderer Branchen (MW: 3,1 ggü. 2,7), ähnlich auch bei der internationalen Ausrichtung der Zertifizierungsstelle, welche von IKT-Unternehmen wesentlich wichtiger als von Nicht-IKT-Unternehmen bewertet wird (MW: 3,1 ggü. 2,3), ebenso von innovativen Unternehmen im Vergleich zu nicht-innovativen Unternehmen (MW: 3,0 ggü. 2,4).

Empfehlungen durch Dritte sind vergleichsweise unwichtig bei der Wahl der Zertifizierungsstelle – nicht-innovative Unternehmen werten diese jedoch deutlich höher als innovative (MW: 3,3 ggü. 2,7). Unternehmen, die jedoch zusätzlich gegen ISO 9001 zertifiziert sind und somit schon Erfahrungen haben, werten Empfehlungen Dritter hingegen geringer (MW: 2,7 ggü. 3,2 bei Unternehmen ohne ISO 9001 Zertifizierung). Insgesamt ähnlich bewertet wird die Möglichkeit eines integrierten Audits für verschiedene Managementsysteme. Unternehmen, die zusätzlich zur Zertifizierung nach ISO/IEC 27001 auch über eine Zertifizierung nach ISO 9001 verfügen, bewerten diese Möglichkeit jedoch erwartungsgemäß signifikant höher (MW: 3,6 ggü. 2,0).

Kriterien für die Wahl der Zertifizierungsstelle

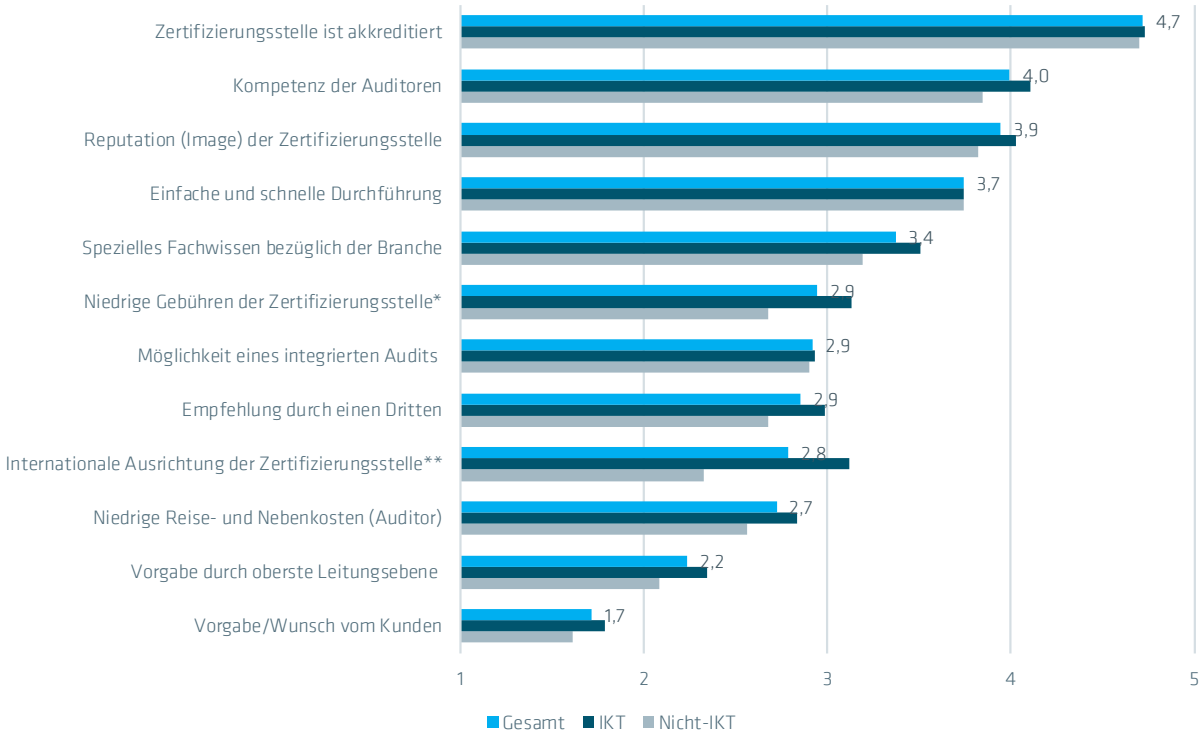


*Abbildung 21: Durchschnittliche Bewertung der Kriterien bei der Wahl von Zertifizierungsstellen. Bewertungsskala: 1 (überhaupt nicht wichtig) bis 5 (sehr wichtig). Basis bilden alle antwortenden Unternehmen (N=114-121), Unternehmen, die zur IKT-Branche gehören (N=65-71) sowie Unternehmen, die nicht zur IKT-Branche gehören (N=48-52). Signifikante Unterschiede bei Branchenzugehörigkeit werden durch * angezeigt (* p < 0,10; ** p < 0,05; *** p < 0,01).*

FAZIT

Die Studie beleuchtet die Nutzung und Wirkung der Norm ISO/IEC 27001 bei entsprechend zertifizierten Unternehmen in Deutschland. Vergleichsweise häufig lassen sich Unternehmen im IKT-Bereich nach ISO/IEC 27001 zertifizieren, gefolgt von Anbietern von freiberuflichen, wissenschaftlichen und sonstigen Dienstleistungen (wozu auch Beratungsunternehmen gehören). Energieanbieter sind zunehmend in den letzten drei Jahren nach ISO/IEC 27001 zertifiziert worden, nachdem entsprechende gesetzliche Anforderungen in Kraft getreten sind.

Die Umfrageergebnisse zeigen deutlich, dass auch Nicht-IKT-Unternehmen angeben, von der Steigerung der Informationssicherheit zu profitieren. Dies könnte – gerade im Hinblick auf die steigende Bedeutung der Informationssicherheit für die gesamte Wirtschaft im Zuge der Digitalisierung – mehr Unternehmen motivieren, ein Managementsystem nach ISO/IEC 27001 zu implementieren. Entsprechende Hürden wurden in der Studie ebenso aufgezeigt wie mögliche fördernde Maßnahmen. Hier sind Politik, Verbände und Unternehmen aufgerufen, das Bewusstsein für die Bedeutung des Themas Informationssicherheit zu stärken sowie den Beitrag, den ein Managementsystem nach ISO/IEC 27001 leisten kann, zu verdeutlichen. Diese Studie erlaubt dafür fundierte Einblicke in Motive und Wirkungen einer entsprechenden Zertifizierung.

Maßgeschneiderte fördernde Maßnahmen – speziell auch für KMU – werden von den Befragten als besonders sinnvoll bewertet. Sowohl finanzielle Hilfen als auch Informationen können bei der Entscheidung und Implementierung wertvolle Unterstützung bieten und so zu mehr Informationssicherheit, Vertrauen von Kunden und Partnern sowie einem wirtschaftlichen Mehrwert beitragen.

GLOSSAR

- **Akkreditierung:** Im Akkreditierungsverfahren weisen Konformitätsbewertungsstellen gegenüber einer unabhängigen Akkreditierungsstelle nach, dass sie ihre Tätigkeiten fachlich kompetent, unter Beachtung gesetzlicher sowie normativer Anforderungen und auf international vergleichbarem Niveau erbringen. Die Akkreditierungsstelle begutachtet und überwacht dabei das → *Managementsystem* und die Kompetenz des eingesetzten Personals der Konformitätsbewertungsstelle.[20]
- **Audit:** systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind (ISO/IEC 17000).
- **Konformitätsbewertung:** Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind (ISO/IEC 17000). Konformitätsbewertungen können von vielen Personen durchgeführt werden, einschließlich des Anbieters eines Produkts oder einer Dienstleistung, seines Käufers und anderer Parteien, die ein Interesse haben könnten, wie

Versicherungsgesellschaften und Aufsichtsbehörden.
  - Internes Audit (erste Seite/first party): durchgeführt von der Person oder Organisation, die Gegenstand der Konformitätsbewertung ist oder diesen anbietet.
  - Lieferanten- (bzw. Kunden-) Audit (zweite Seite/second party): durchgeführt von einer Person oder einer Organisation, die gegenüber dem Gegenstand der Konformitätsbewertung ein Interesse als Anwender*in hat (z.B. Käufer*in oder Anwender*in eines Produkts).
  - Externes Audit (dritte Seite/third party): durchgeführt von einer Person oder einer Stelle, die von der Person oder der Organisation, die Gegenstand der Konformitätsbewertung ist oder diesen anbietet, und von Interessen als Anwender*in dieses Gegenstandes, unabhängig ist (z.B. → *Zertifizierung*).
- **Managementsystem:** Ein Managementsystem umfasst Aktivitäten, mit denen eine Organisation ihre Ziele identifiziert und den Prozess und die Ressourcen bestimmt, die zur Erreichung der gewünschten Ergebnisse erforderlich sind.[21] Diese Ziele können sich auf eine Reihe von verschiedenen Themen beziehen, einschließlich Produkt- oder Dienstleistungsqualität, betriebliche Effizienz, Umweltleistung, Gesundheit und Sicherheit am Arbeitsplatz und viele andere. Normen, bspw. von der Internationalen Normungsorganisation ISO, legen die Anforderungen oder Leitlinien fest, um Organisationen bei der Gestaltung und Umsetzung ihrer Richtlinien und Prozesse zur Erreichung dieser Ziele zu unterstützen.
- **Qualitätsinfrastruktur:** Das System, das die Organisationen (öffentliche und private) zusammen mit dem Regelwerk, dem relevanten rechtlichen und regulatorischen Rahmen und den Maßnahmen umfasst, die zur Unterstützung und Verbesserung der Qualität, Sicherheit und Umweltverträglichkeit von Gütern, Dienstleistungen und Prozessen erforderlich sind. Sie stützt sich auf Normung, → *Konformitätsbewertung*, → *Akkreditierung*, Metrologie und Marktüberwachung.[22]
- **Zertifizierung:** Bestätigung von unabhängiger dritter Stelle, dass spezifische Anforderungen an Produkte, Prozesse, Systeme oder Personen erfüllt sind (ISO/IEC 17000). Bei der Zertifizierung von genormten → *Managementsystemen* bestätigt ein unabhängiger, externer Auditor, ob die dokumentierten Verfahren der jeweiligen Organisation angemessen sind und in der Praxis befolgt werden, so dass die Organisation die in der Managementsystem-Norm festgelegten Anforderungen erfüllt.[23]

ABKÜRZUNGEN

BSI: Bundesamt für Sicherheit in der Informationstechnik

IEC: Internationale Elektrotechnische Kommission (International Electrotechnical Commission)

IKT: Informations- und Kommunikationstechnologie

ISO: Internationale Organisation für Normung (International Organization for Standardization)

ISMS: Informationssicherheitsmanagementsystem

KMU: kleine und mittelständische Unternehmen

KRITIS: Kritische Infrastruktur

MW: Mittelwert

QI: Qualitätsinfrastruktur

DANKSAGUNGEN

Die Autor*innen danken den vielen Personen und Institutionen, die diese Studie unterstützt haben. Insbesondere dem BMWi gilt unser Dank für die allgemeine Unterstützung des Projektes. Gedankt sei auch den Interviewpartner*innen in der Vorbereitung der Befragung.

ANMERKUNGEN UND REFERENZEN

[1] *ISO 9000:2015.*

[2] *www.iso.org/management-system-standards*

[3] *Vgl. ISO (2020). The ISO Survey, abrufbar unter: https://www.iso.org/the-iso-survey.html.*

[4] *ISO-Survey erfasst nur Zertifizierungen, die von den akkreditierten Stellen gemeldet werden. Mögliche Meldefehler können ebenso zu Verzerrungen führen wie die Tatsache, dass Zertifikate nicht-akkreditierter Stellen nicht berücksichtigt sind.*

[5] *Vgl. Mirtsch, M., Koch, C., Dudek, G. & Blind, K. (2020). Die Nutzung und Wirkung genormter Managementsysteme. Eine Studie im Rahmen der Initiative QI-FoKuS. Vol. 1. Bundesanstalt für Materialforschung und -prüfung (BAM).*

[6] *Aufgrund einer Änderung der Erhebungsmethode können ab dem Jahr 2018 die gültigen ISO-Zertifikate nicht mehr mit den Vorjahren verglichen werden (ISO, 2019).*

[7] *Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018). Cyber-Sicherheits-Umfrage 2018: Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Abgerufen unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9.*

[8] *Vgl. ISO Survey (2020).*

[9] *Vgl. AbuSaad, B., Saeed, F. A., Alghathbar, K., & Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned. Papier präsentiert bei der Australian Information Security Management Conference sowie Longras, A., Pereira, T., Cameiro, P., & Pinto, P. (2018). On the Track of ISO/IEC 27001: 2013 Implementation Difficulties in Portuguese Organizations. Papier präsentiert bei der 2018 International Conference on Intelligent Systems (IS) sowie Svoboda, T., & Horalek, J. (2018). Analysis of the information security management in Czech Republic. Advanced Science Letters, 24(11), 8562-8566.*

[10] *Vgl. Müller, J, Sänn, A., & Ludwig, V. (2018). Informationssicherheits-Management-Systeme (ISMS) bei Energieversorgern 2018. Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth. Abgerufen unter: https://www.bfm-bayreuth.de/wp-content/uploads/2018/09/Studie_ISMS_2018-09-30_BFM-7P_v10.pdf.*

[11] *Vgl. Mirtsch, M., Koch, C., Dudek, G. & Blind, K. (2020).*

[12] *Vgl. Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. IEEE Transactions on Engineering Management, 1-14.*

[13] *Mehrfachnennungen waren möglich.*

[14] *Vgl. BMWi (2018). Monitoring-Report Wirtschaft DIGITAL 2018 - Der IKT-Standort Deutschland und seine Position im internationalen Vergleich. Abgerufen unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/monitoring-report-wirtschaft-digital-2018-ikt-standort-deutschland.pdf?__blob=publicationFile&v=26*

[15] *Vgl. Bundesnetzagentur (2018). IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz. Abgerufen unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4*

[16] *Vgl. Mirtsch, M., Kinne, J., & Blind, K. (2020).*

[17] *Vgl. ISO Survey (2019).*

[18] *Eine Gewichtung, z.B. hinsichtlich der Branchen fand jedoch nicht statt, da eine Aussage über die aktuelle Branchenverteilung der Grundgesamtheit nicht möglich ist: zum einen, da die Branchenzuordnung dieser Erhebung (basierend auf NACE) und dem ISO-Survey (basierend auf den EA-Codes) nicht vollständig übereinstimmen und zum anderen, da sich die Zahlen aus den anderen Quellen auf Vorjahre beziehen und damit aktuelle Entwicklungen, wie z.B. bei den Energieanbietern, nicht berücksichtigen.*

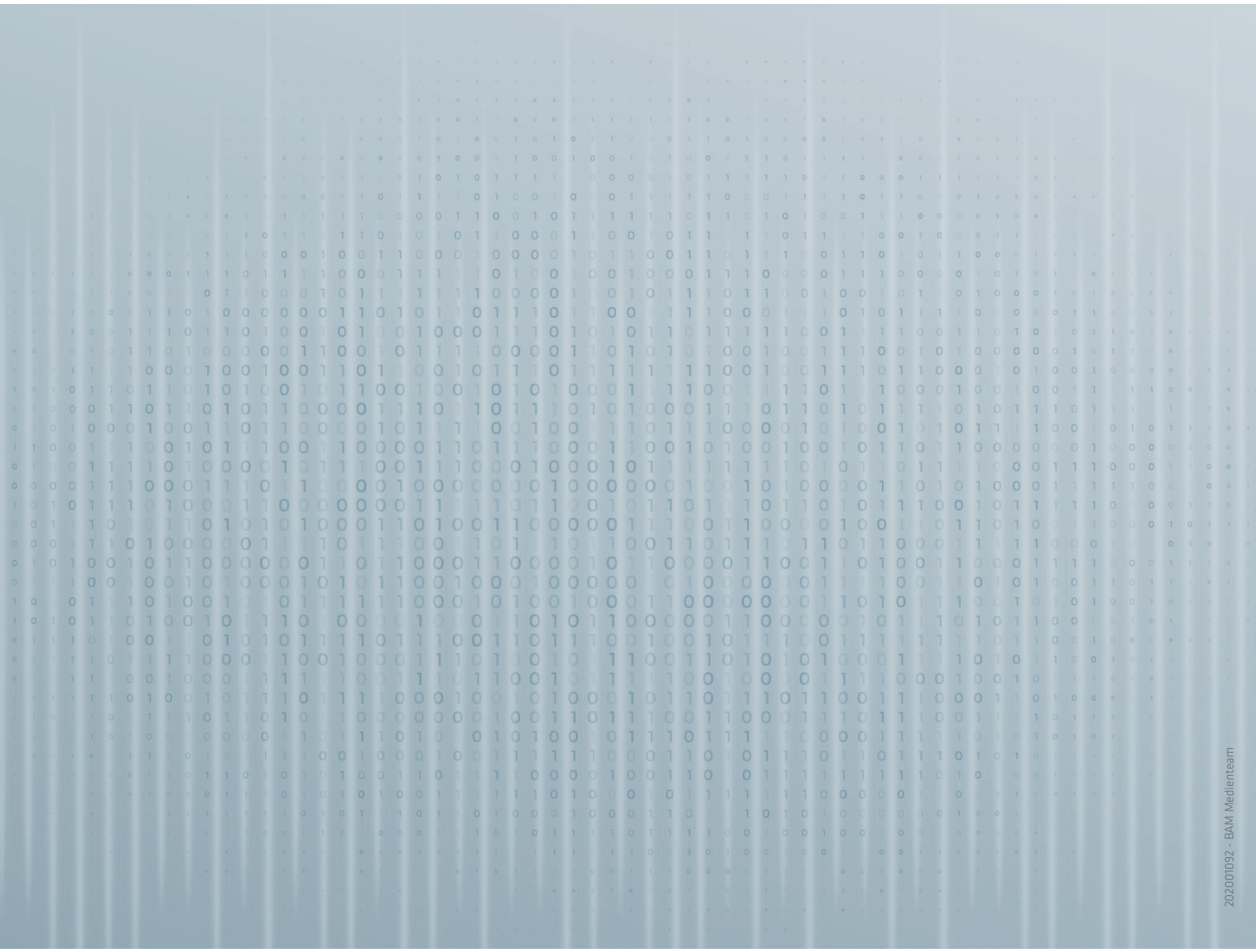
[19] *Vgl. Blind, K., & Mangelsdorf, A. (2016). Zertifizierung in deutschen Unternehmen – zwischen Wettbewerbsvorteil und Kostenfaktor. In: R. Friedel & E. A. Spindler (Eds.), Zertifizierung als Erfolgsfaktor: Nachhaltiges Wirtschaften mit Vertrauen und Transparenz (pp. 23-32), Springer.*

[20] *https://www.dakks.de/content/was-ist-akkreditierung*

[21] *ISO 9000:2015.*

[22] *UNIDO. (2018). Quality Infrastructure - UNIDO's unique approach. Abgerufen unter: https://www.unido.org/sites/default/files/files/2018-08/UNIDO_QI_CASE_FINAL_ONLINE_2.pdf*

[23] *Vgl. Castka, P., & Corbett, C. J. (2015). Management Systems Standards: Diffusion, Impact and Governance of ISO 9000, ISO 14000, and Other Management Standards. Foundations and Trends in Technology, Information and Operations Management, 7, 161-379.*



202001092 - BAM Medienteam

BAM

Bundesanstalt für Materialforschung
und -prüfung (BAM)
Unter den Eichen 87
12205 Berlin, Germany

Info@bam.de
www.bam.de