BAM
Bundesanstalt für Materialforschung und -prüfung

Sicherheit in Technik und Chemie

QI-FoKuS
Forschung für Konformitätsbewertung und Sicherheit

Inkl. Spezialteil zur ISO/IEC 27001 für Informations-sicherheit

Die Nutzung und Wirkung genormter Managementsysteme

Eine Studie im Rahmen der Initiative QI-FoKuS

Vol. 1

Autoren

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

https://doi.org/10.26272/opus4-51083
ISBN: 978-3-9818564-3-9

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 – **Fo**rschung für **K**onformitätsbewertung **u**nd **S**icherheit – 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 Befragungen 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.

Die Befragung von Unternehmen in Deutschland zur Nutzung von genormten Managementsystemen ist die erste Erhebung im Rahmen von QI-FoKuS. Neben der Motivation hinsichtlich der Anwendung verschiedener Normen, die Anforderungen an Managementsysteme darlegen, sowie den Wirkungen werden insbesondere die Zertifizierung für diese Normen sowie daran anknüpfend die Rolle und Funktion der Akkreditierung – und somit verschiedene Bausteine der QI – adressiert. Ein Schwerpunkt dieser Befragung liegt auf der Norm ISO/IEC 27001, welche Anforderungen anManagementsysteme für Informationssicherheit (ISMS) beschreibt. Die Verbreitung dieser Norm unterliegt aktuell einer Dynamik, die durch Regulierungsbestrebungen hinsichtlich Informationssicherheit beeinflusst wird. Dies begründet ein besonderes Forschungsinteresse.

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. Ende 2019 wurden in einer ersten Online-Erhebung Unternehmen verschiedener Branchen und Größenklassen in Deutschland zur Nutzung von Managementsystemen und ihren Wirkungen befragt. Diese umfasste weit verbreitete genormte Managementsysteme wie ISO 9001 und ISO 14001 genauso wie bisher wenig untersuchte Systeme wie die ISO 50001 oder ISO/IEC 27001. Es konnten 180 Fragebögen für die vorliegende Studie ausgewertet werden. Folgende zentralen Erkenntnisse können daraus abgeleitet werden:

1. **ISO 9001 ist die am weitesten verbreitete Managementsystem-Norm in der Stichprobe,** gefolgt vom Umweltmanagementsystem nach ISO 14001, Arbeits- und Gesundheitsschutzmanagementsystemen nach ISO 45001 (BS OHSAS 18001) und Energiemanagementsystemen nach ISO 50001. Noch nicht so weit verbreitet sind Informationssicherheitsmanagementsysteme nach ISO/IEC 27001. Alle weiteren untersuchten Managementsysteme finden vergleichsweise noch weniger Anwendung.

2. **Die Zertifizierungsquoten der verschiedenen Managementsysteme unterscheiden sich erheblich:** Das Qualitätsmanagementsystem nach ISO 9001 ist unter den Befragten nicht nur das am weitesten verbreitete Managementsystem, auch lassen sich die nutzenden Unternehmen am häufigsten danach zertifizieren (87%). Anwender des Managementsystems für Informationssicherheit nach ISO/IEC 27001 sind dagegen vergleichsweise selten zertifiziert (37%).

3. **Die gleichzeitige Nutzung verschiedener Managementsysteme ist weit verbreitet:** Über zwei Drittel der zertifizierten Unternehmen haben mehr als eine Managementsystem-Zertifizierung. Im Durchschnitt halten die zertifizierten befragten Unternehmen 2,6 Zertifikate, wobei hier deutliche Unterschiede zwischen kleinen und großen Unternehmen festzustellen sind. Die Befragung hat auch Managementsysteme erfasst, welche die

Unternehmen lediglich implementiert haben, ohne ein Zertifikat zu erlangen. Berücksichtigt man diese ebenfalls, zeigt sich, dass die Unternehmen im Durchschnitt deutlich mehr – nämlich 3,3 – Managementsysteme gleichzeitig implementiert haben. Der Umfang solch einer gemeinsamen Nutzung und Integration mehrerer Managementsysteme hängt entscheidend von den Charakteristika des jeweiligen Unternehmens im Hinblick etwa auf Branchenzugehörigkeit oder Größe ab.

4. **ISO 9001 dient meist als „Basis-Norm“:** Die Analyse der in den jeweiligen Unternehmen parallel implementierten Managementsysteme zeigt, dass fast alle Anwender von Umwelt-, Energie- und Arbeitsschutzmanagementsystemen auch über ein zertifiziertes Qualitätsmanagementsystem nach ISO 9001 verfügen. Die geringste gemeinsame Nutzung mit anderen genormten Managementsystemen findet sich bei der ISO/IEC 27001 für Informationssicherheit.

5. **Es zeigen sich verschiedene Hauptmotive für die Nutzung von Managementsystemen:** Während bei ISO 9001 und ISO 14001 Kundenforderungen als externe Faktoren maßgeblich die Einführung motivieren, ist bei Arbeits- und Gesundheitsschutzmanagementsystemen nach ISO 45001/BS (British Standard) OHSAS 18001 sowie bei ISMS nach ISO/IEC 27001 die Erhöhung der Rechtsicherheit das Hauptmotiv. Die Zertifizierung eines Energiemanagementsystems nach ISO 50001 wird insbesondere durch die Aussicht auf damit verbundene Steuererleichterungen motiviert. Verbesserungen im Sinne des jeweiligen Managementsystems bzw. entsprechender unternehmensinterner Prozesse sind für die Befragten bei keinem der Managementsysteme der Hauptantrieb für die Implementierung.

6. **Nicht-zertifizierte Anwender von Managementsystemen haben andere Motive:** Insbesondere bei anwendenden Unternehmen der ISO 9001 zeigt sich, dass diejenigen, die sich nicht zertifizieren lassen, noch stärker intrinsisch motiviert sind, ein solches Qualitätsmanagementsystem zu nutzen. Für sie stehen nicht die entsprechenden Forderungen von Kundenseite an erster Stelle, sondern das Ziel interner Verbesserungen.

7. **Die Managementsystem-Normen erfüllen ihren Zweck:** Bei den Managementsystemen nach ISO 9001, ISO 45001 (BS OHSAS 18001) und ISO/IEC 27001 wird die Hauptwirkung unter den Befragten in Verbesserungen im Sinne des Zwecks der jeweiligen Norm gesehen, also Qualität, Arbeits- und Gesundheitsschutz sowie Informationssicherheit. Energie- und Kosteneinsparungen werden als ein Hauptnutzen bei der Etablierung von Energiemanagementsystemen nach ISO 50001 angegeben. Wesentliche Wirkungen des Umweltmanagementsystems nach ISO 14001 ist eine Sensibilisierung der Mitarbeitenden für Umweltfragen.

8. **Die Gesamtzufriedenheit mit den Managementsystemen variiert:** Die Wahrnehmung, ob die Zertifizierung gegen die jeweiligen Managementsystem-Normen insgesamt eine gute Investition in Bezug auf Kosten und Nutzen sei, variiert deutlich. So sind die nach ISO 9001 zertifizierten befragten Unternehmen unabhängig von Größe oder Branche insgesamt deutlich zufriedener als insbesondere die Anwender des Umweltmanagementsystems ISO 14001. Gestützt wird die insgesamt positive Bewertung der Managementsysteme auch durch die tendenziell positiveren Bewertungen der realisierten Wirkungen im Vergleich zu den ursprünglichen Erwartungen bei Einführung eines Managementsystems.

9. **Kompetenz und deren Nachweis sind die Hauptkriterien bei der Wahl der Zertifizierungsstelle:** Die Studienergebnisse bestätigen deutlich die hohe Bedeutung der Akkreditierung, die für die Befragten das wichtigste Kriterium für die Auswahl der Zertifizierungsstelle darstellt. Überdies geben 99% an, dass mindestens eines ihrer Zertifikate von einer akkreditierten Stelle ausgestellt worden ist. Die hohe Bedeutung fachlicher Kompetenz bei der Wahl des Zertifizierenden spiegelt sich auch darin wider, dass fachliche Unzufriedenheit als Hauptgrund für einen Wechsel der Zertifizierungsstelle genannt wird.

10. **Jede*r zweite Befragte kennt die handelserleichternden internationalen Anerkennungsabkommen für Akkreditierung:** Sofern bekannt, wird diesen auch eine hohe Bedeutung beigemessen.

11. **Kundenaudits haben eine hohe Relevanz in der Praxis:** Jedes zweite befragte Unternehmen gibt an, auch von Kunden auditiert zu werden, insbesondere hinsichtlich ihres Qualitätsmanagementsystems, aber auch beim Umweltmanagement sowie Arbeits- und Gesundheitsschutz. Laut den Befragten können diese Audits jedoch keine Zertifizierungen ersetzen. Insgesamt werden Kundenaudits als strenger wahrgenommen als Auditierungen im Rahmen des Zertifizierungsprozesses.

12. **Die Studie gewährt erste branchenübergreifende Einblicke in die Nutzung von ISO/IEC 27001 für Informationssicherheit:**

    - ISO/IEC 27001 hat unter den Managementsystem-Normen dieser Studie eine der geringsten Zertifizierungsquoten: Lediglich jedes dritte anwendende Unternehmen ist zertifiziert. Die Analyse der Hauptantriebe zur Einführung der Norm zeigt entsprechend überwiegend intrinsische Motive. Und auch Wirkungen nach innen, d. h. innerhalb der Unternehmen, insbesondere hinsichtlich Prävention und Gefahrenabwehr, sind dominierend – unabhängig von spezifischen Unternehmenscharakteristika wie Branche oder Größe.
    - Aktuell fehlt es der Norm noch an breiter Bekanntheit (29% der nicht-anwendenden Unternehmen kennen sie nicht). Unter denen, die ISO/IEC 27001 kennen, plant nur jedes fünfte Unternehmen, sie in Zukunft zu implementieren. Die geringe Verbreitung wird insbesondere durch fehlenden Druck von extern (Gesetzgeber bzw. Kunden) begründet. Konkrete Hürden für die Einführung in dem eigenen Unternehmen werden besonders im damit verbundenen Aufwand und fehlender Expertise, auch angesichts der Komplexität der Norminhalte, gesehen. Zur Unterstützung einer weiteren Verbreitung des Managementsystems für Informationssicherheit werden eine Reihe von Maßnahmen als sinnvoll erachtet: u.a. Handlungsleitfäden für kleine und mittlere Unternehmen (KMUs) oder Schulungen und finanzielle Unterstützung. Insbesondere nach ISO/IEC 27001 zertifizierte Unternehmen betrachten auch die Forderung des Nachweises seitens der Kunden oder des Gesetzgebers als verbreitungsfördernd.

EINLEITUNG

Genormte und standardisierte (im Folgenden zusammengefasst als genormte) Managementsysteme sind ein globaler Erfolg: Millionen Unternehmen weltweit arbeiten in verschiedensten Management-Bereichen nach internationalen Normen. Dies betrifft nicht nur die bekannten Normen für Qualitäts- und Umweltmanagement ISO 9001 und ISO 14001; nach und nach steigt auch die Verbreitung weiterer Managementsysteme für spezielle Bereiche wie dem Energie- oder Informationssicherheitsmanagement.

Die allgemeine wirtschaftliche und gesellschaftliche Bedeutung von Normen und Standards ist wissenschaftlich gut belegt. Sie ermöglichen nicht nur ökonomischen Nutzen für Unternehmen, sondern tragen auch insgesamt zu Vorteilen für Verbraucher*innen, Umwelt- und Arbeitsschutz bei, minimieren Risiken und verbessern so die gesamtwirtschaftliche Wohlfahrt.[1] Insbesondere für ISO 9001 und ISO 14001 gibt es eine Vielzahl von Studien, die die Wirkungen dieser Managementsystem-Standards weltweit untersucht und belegt haben.[2] Andere Managementsystem-Normen blieben jedoch bisher weitgehend unbeachtet, so z. B. die erst 2005 und 2011 eingeführten Normen ISO/IEC 27001 für ISMS und ISO 50001 für Energiemanagementsysteme. Zudem

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.[3] 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 mehr.

Managementsystem-Normen

Normen, bspw. von internationalen Normungsorganisationen wie ISO, 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.[4] Diese Normen sind so konzipiert, dass sie in unterschiedlichen Organisationen, unabhängig von Branche, Größe, Art, Organisationsform, oder geographischen, kulturellen und sozialen Bedingungen, anwendbar sind.

erfassen nur wenige Studien mehrere Managementsysteme zusammen; die meisten widmen sich lediglich einer Norm. Dies verkennt jedoch, dass die Managementsysteme miteinander kompatibel sind und in der Praxis oft auch Managementsysteme in verschiedenen Bereichen gleichzeitig genutzt werden. Ein weiterer Aspekt ist die oftmals sehr eingeschränkte Sichtweise vorhandener Studien auf ausschließlich zertifizierte Unternehmen, während in der Praxis jedoch oft Managementsysteme implementiert werden, ohne dass ein Zertifikat erteilt wurde bzw. angestrebt wird. Darüber hinaus bleibt die Zertifizierung in den meisten Erhebungen an sich oftmals unbeachtet. Dies betrifft sowohl die Rolle der Zertifizierungsstellen als auch deren Kompetenz, nachgewiesen in Form einer Akkreditierung.

Der vorliegende Report präsentiert Ergebnisse einer branchenübergreifenden Online-Befragung von Unternehmen in Deutschland zur Nutzung von diversen genormten Managementsystemen. Die Studie bietet nicht nur Einblicke in die Motive zur Implementierung und die Einschätzung der Wirkungen; vielmehr richtet sie auch einen Fokus auf die Konformitätsbewertung als ein zentrales Element der Qualitätsinfrastruktur (QI). Dazu schreiben Managementsystem-Normen in der Regel sogenannte interne Audits vor, die von den Unternehmen selbst durchgeführt werden. Weit verbreitet ist darüber hinaus die Zertifizierung als Bestätigung durch eine unabhängige dritte Seite. Die vorliegende Untersuchung unterscheidet daher explizit zwischen den Unternehmen, die sich gegen die implementierte Norm zertifizieren lassen, und jenen, die die Norm ohne Zertifizierung anwenden.

Gründe für die Zertifizierung werden ebenso beleuchtet wie die Kriterien für die Wahl einer Zertifizierungsstelle oder deren Wechsel. Da es zur Bekanntheit und Bewertung des Nutzens und der Wirkung von Akkreditierung bisher nur wenige empirische Daten gibt, widmet sich die vorliegende Studie auch diesem Instrument.

Des Weiteren können Audits bspw. auch durch Geschäftspartner erfolgen, z. B. Abnehmern entlang der Lieferkette (sogenannte Kunden- bzw. Lieferantenaudits). Auch die vorliegende Studie bestätigt die Bedeutung dieser in der Praxis weit verbreiteten Form der Konformitätsbewertung und zieht Vergleiche zur Zertifizierung.

Ein Spezialteil der Studie behandelt die Managementsystem-Norm ISO/IEC 27001 für Informationssicherheit im Detail. Zu dieser Norm gibt es bisher noch keine branchenübergreifende Untersuchung für Deutschland. Insbesondere vor dem Hintergrund der fortscheitenden Digitalisierung und regulativer Initiativen wie dem IT-Sicherheitsgesetz und dem europäischen Cybersecurity Act kommt Normen im Bereich der Informationssicherheit, wie der ISO/IEC 27001, und des Nachweises der wirksamen Anwendung durch eine Zertifizierung eine wachsende Bedeutung zu.

Die Studie trägt zu einem umfänglichen Abbild der Nutzung von Managementsystemen in Deutschland bei und hilft dabei insbesondere, Konformitätsbewertungen in diversen Facetten zu verstehen. Unternehmen, die sich mit genormten Managementsystemen bisher wenig oder gar nicht aktiv befasst haben, ermöglicht diese Studie einen Einblick in die Motive und Wirkweise bei anderen Unternehmen. Zertifizierungsstellen können von den Ergebnissen zu den Auswahlkriterien der

Zertifizierungsstelle und den Gründen für den Wechsel eines Zertifizierers profitieren. Die Ergebnisse der Erhebung bieten ferner die Möglichkeit, im Bereich der Informationssicherheit aktiv Strategien für die Erhöhung der Verbreitung dieser Norm abzuleiten.

Insgesamt soll QI-FoKuS dazu beitragen, den ökonomischen und gesellschaftlichen Wert und Nutzen sowie die Wirkweisen der Konformitätsbewertungen und Akkreditierung als wichtige Elemente der QI besser zu verstehen und relevante Stakeholder dafür zu sensibilisieren.

Wachsende Beliebtheit genormter und standardisierter Managementsysteme

Managementsysteme nach ISO- und anderen Normen erfreuen sich international und auch in Deutschland wachsender Beliebtheit. 1986 eingeführt, sind mittlerweile bspw. über eine Million Unternehmen nach der Qualitätsmanagementsystem-Norm ISO 9001 zertifiziert. Im Zuge dieses Erfolges wurden nach und nach Standards auch für andere Managementbereiche geschaffen, so bspw. für Umwelt, Arbeitssicherheit, Informationssicherheit und Energie.

Erhebungen der Internationalen Organisation für Normung (ISO) zeigen, dass Deutschland international bei der absoluten Zahl der ausgestellten Zertifikate[5] weit vorne liegt: Nur in China gibt es mehr ISO 9001-Zertifikate, bei Zertifikaten für ISO 50001 ist Deutschland sogar auf Platz 1 und bei ISO/IEC 27001 auf dem fünften sowie bei ISO 14001 auf dem sechsten Platz.[6]

Auch wenn diese Zahlen nur gemeldete Zertifikate akkreditierter Zertifizierungsstellen enthalten, zeigen sie dennoch deutlich die weite Verbreitung genormter Managementsysteme. Die tatsächliche Anwendung dürfte weitaus höher sein, berücksichtigt man die Limitierungen der ISO-Erhebung[7] sowie die Tatsache, dass viele Unternehmen Managementsysteme implementiert haben, ohne sich zertifizieren zu lassen.

Tabelle 1: Im Rahmen der Studie untersuchte genormte Managementsysteme und Anzahl der ausgegebenen Zertifikate in Deutschland im Jahr 2018 gemäß dem ISO Survey.

Norm/Standard	Titel	Anzahl Zertifikate in Deutschland (Standorte)[8]
ISO 9001	Qualitätsmanagementsysteme – Anforderungen	47.482 (73.559)
ISO 14001	Umweltmanagementsysteme – Anforderungen mit Anleitung zur Anwendung	8.028 (14.525)
ISO 50001	Energiemanagementsysteme – Anforderungen mit Anleitung zur Anwendung	6.243 (14.736)
ISO 13485	Medizinprodukte – Qualitätsmanagement – Anforderungen für regulatorische Zwecke	2.662 (3.249)
ISO/IEC 27001	Informationssicherheit- IT-Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen	1.057 (2.003)
ISO 22000	Managementsysteme für die Lebensmittelsicherheit – Anforderungen an Organisationen in der Lebensmittelkette	257 (479)

Norm/Standard	Titel	Anzahl Zertifikate in Deutschland (Standorte)[8]
ISO 45001 (zuvor BS OHSAS 18001)	Arbeits- und Gesundheitsschutz-Managementsysteme – Anforderungen mit Anleitung zur Anwendung	147 (483)
ISO 20000-1	IT Service-Management – Teil 1: Spezifikation für Service Management	48 (148)
IATF 16949 (zuvor ISO/TS 16949)	Qualitätsmanagementsysteme – Besondere Anforderungen bei Anwendung von ISO 9001 für die Serien- und Ersatzteilproduktion in der Automobilindustrie	Nicht verfügbar in der aktuellen ISO Erhebung

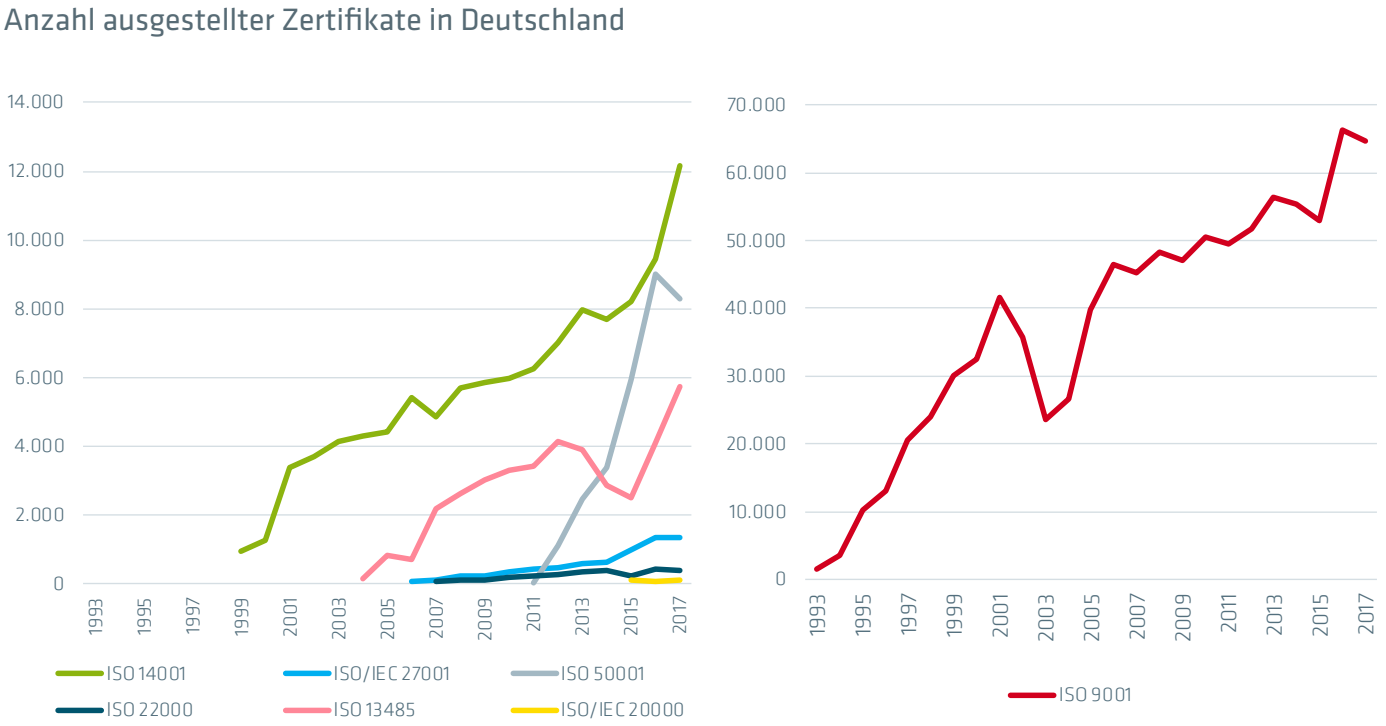


Abbildung 2: Anzahl der ausgestellten Zertifikate für ausgewählte Managementsystem-Normen in Deutschland. Quelle: ISO Survey (2018).

FRAGENKATALOG UND METHODIK

Der Fragenkatalog

Im Mittelpunkt der Erhebung standen die Nutzung und Wirkung von international genormten Managementsystemen. Der Fragebogen wurde aufbauend auf Interviews mit Industrievertreter*innen und Zertifizierungsstellen sowie einer umfassenden Literaturrecherche zu vorherigen Studien zu Managementsystemen entwickelt und vorab hinsichtlich der Verständlichkeit der Fragen und der Befragungsdauer getestet. Während viele Studien nur zertifizierte Unternehmen erfassen, liegt eine Besonderheit dieser Befragung darin, dass auch jene Unternehmen abgebildet werden, die genormte Managementsysteme implementiert haben, ohne dafür zertifiziert zu sein. Der Fragebogen erfasste und unterschied entsprechend beide Möglichkeiten. Ein besonderer Fokus der Umfrage lag auf den Kriterien für die Auswahl der Zertifizierungsstelle und ggf. Gründen eines Wechsels. Im Weiteren wurde die Bedeutung von Akkreditierung als einer wichtigen Säule der QI sowie von internationalen Akkreditierungsabkommen erfasst. Schließlich wurde eine in der Praxis weit verbreitete jedoch wissenschaftlich-empirisch oftmals vernachlässigte Form der Konformitätsbewertung, die Auditierung durch Geschäftspartner, ebenfalls in der Umfrage adressiert.

Entsprechend der genannten Themen ist der Fragebogen mit insgesamt 137 Fragen in die folgenden Teilbereiche untergliedert:

- Angaben zum teilnehmenden Unternehmen
- Einsatz und Bedeutung von Managementsystemen
- Motive und Wirkungen von Managementsystemen
- Spezialteil zu Informationssicherheitsmanagementsystem nach ISO/IEC 27001
- Auswahlkriterien von Zertifizierungsstellen
- Akkreditierung und Bedeutung von internationalen Anerkennungsabkommen
- Verbreitung und Bedeutung von Lieferanten- bzw. Kundenaudits

Der Fragebogen beinhaltete überwiegend geschlossene und einige offene Fragen. Bei ersteren wurden den Befragten eine Auswahl von Antwortmöglichkeiten vorgegeben, wobei bei den Einschätzungen Skalenfragen mit einer fünfstufigen Ratingskala genutzt wurden. Bei den meisten Fragen, abgesehen jenen zur Zahl der Mitarbeitenden und Branchenzugehörigkeit, handelt es sich nicht um Pflichtfragen.

Die Umfrage wurde als Online-Fragebogen im Rahmen der neu geschaffenen Initiative QI-FoKuS mithilfe von Multiplikatoren verteilt. Die Deutsche Gesellschaft für Qualität (DQG), der Bundesverband der Deutschen Industrie (BDI), Branchenverbände (z. B. der Verband der Chemischen Industrie (VCI) sowie der Verband der Automobilindustrie (VDA)) sowie Zertifizierungsstellen, Industrie- und Handelskammern und weitere Interessensverbände haben ihre Mitglieder in Newslettern und auf ihren Webseiten auf die Umfrage aufmerksam gemacht. Eine Teilnahme an der Umfrage war von Ende September bis Ende Dezember 2019 möglich.

Insgesamt 248 Fragebögen wurden ausgefüllt, 134 davon vollständig. Diese Publikation umfasst die Auswertung der Antworten all jener 180 Teilnehmenden, die den kompletten Hauptteil des Fragebogens (zur Nutzung von Managementsystemen) ausgefüllt haben. Die statistische Auswertung erfolgte durch die Bundesanstalt für Materialforschung und -prüfung gemeinsam mit der Technischen Universität Berlin.

Teilnehmende und Stichprobe

In den meisten Fällen (n=99) wurde der Fragebogen von den zuständigen Qualitätsmanager*innen ausgefüllt, gefolgt von der Gruppe der Geschäftsführung (n=30) sowie der Verwaltung (n=26). Des Weiteren

Branchen

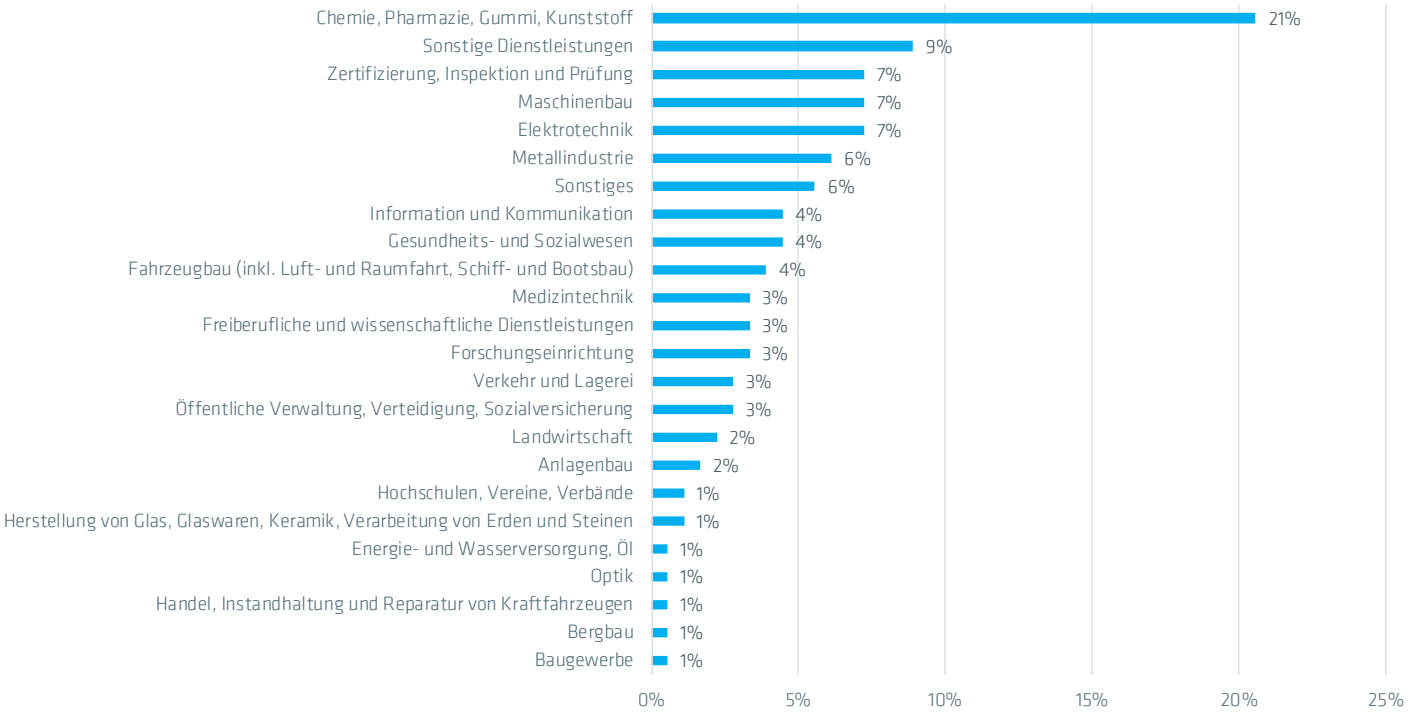


Abbildung 3: Branchenzugehörigkeit der teilnehmenden Unternehmen (N=180).

haben viele der Befragten angegeben, im Bereich Normung und Standardisierung, oder auch in der Ausbildung und Schulung tätig zu sein. Wenig vertreten sind Mitarbeitende aus den Bereichen Konstruktion, Produktion und Fertigung, sowie aus dem Exportgeschäft und dem Marketing.

93% der teilnehmenden Unternehmen haben ihren Hauptsitz in Deutschland, wobei ein Drittel zu einer internationalen und ein Fünftel zu einer nationalen Unternehmensgruppe gehören. 44% sind Einzelunternehmen.

Die Zuordnung der Branchenzugehörigkeit erfolgte entsprechend der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE). Diverse Branchen wurden zusammengefasst, um Unterschiede darzustellen, im speziellen das Verarbeitende Gewerbe/Herstellung von Waren[9], Dienstleistungen sowie „alle anderen". Über die Hälfte der Teilnehmenden der Umfrage kommt aus dem Verarbeitenden Gewerbe. Insbesondere die Chemie- und Pharma-Industrie ist überproportional stark vertreten (20,6%). Dies liegt an der sehr erfolgreichen Unterstützung durch einen entsprechenden Branchenverband. Aber auch der deutsche Maschinenbau und die Elektrotechnikbranche (jeweils 7,2%) sowie die Metallindustrie (6,1%) sind stark repräsentiert. Die zweitstärkste Branchengruppe insgesamt sind sonstige Dienstleister (8,9%). Unternehmen des IKT-Sektors stellen 4,4% der Stichprobe. Nur wenig Teilnehmende gab es aus dem Baugewerbe und Handel (nur jeweils 0,6%).

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

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

Da auch sehr große Unternehmen an der Befragung teilgenommen haben, wird im Folgenden auch auf sehr große Unternehmen mit 500-999 oder über 1000 Mitarbeitenden bei den Ergebnissen als eigene Gruppe hingewiesen.

45% der teilnehmenden Unternehmen beschäftigen bis

Unternehmensgröße (Mitarbeitende)

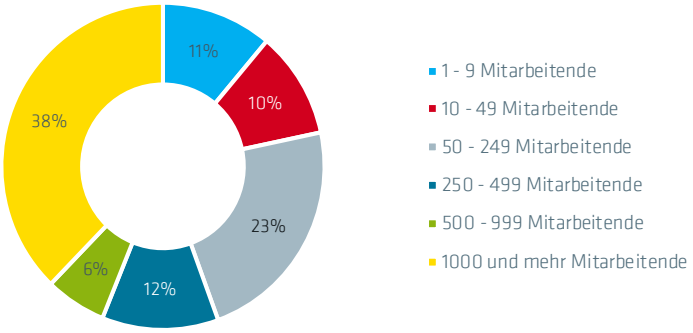


Abbildung 4: Unternehmensgröße nach Anzahl der Mitarbeitenden (N=180).

Unternehmensgröße (Umsatz in Mio. Euro)

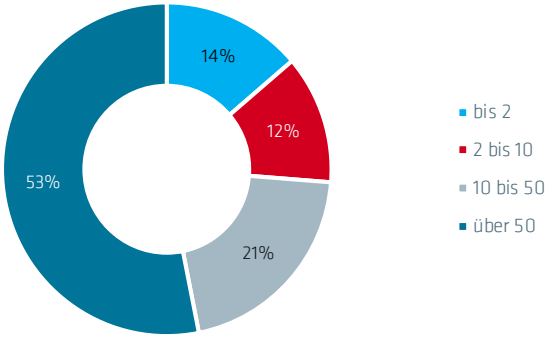


Abbildung 5: Unternehmensgröße nach Umsatz in Mio. Euro (N=160).

zu 250 Mitarbeitende und gehören damit zum klassischen Mittelstand, 12% haben zwischen 250 und 500 Mitarbeitende. 38% der Befragten sind Unternehmen mit einer Mitarbeitendenzahl von über 1000. Knapp über die Hälfte der Unternehmen (53%) hat 2018 mindestens 50 Mio. Euro Umsatz erwirtschaftet, 14% maximal 2 Mio. Euro.

Während ein Drittel der Unternehmen ihre Produkte und Dienstleistungen dabei ausschließlich im Inland verkauft, gibt ein weiteres Drittel der Teilnehmenden an, mindestens die Hälfte des Umsatzes im Export zu erwirtschaften. Dies trifft vor allem auf Unternehmen aus der Branche des Verarbeitenden Gewerbes zu (jedes zweite Unternehmen (56%)).

Der durchschnittliche Exportanteil bei den kleinen Unternehmen bis max. 50 Mitarbeitenden liegt unter 10%, bei den größeren Unternehmen beträgt er im Mittel mindestens 29% (führend hierbei sind die Unternehmen mit 500-999 Mitarbeitenden mit durchschnittlich 36%).

Auch die Innovationstätigkeit der teilnehmenden Unternehmen wurde im Fragebogen erfasst: So wurde erhoben, ob das jeweilige Unternehmen im Jahr 2018 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 180 Unternehmen der Stichprobe sind 130 Unternehmen in mindestens einem Bereich (Produkt, Prozess, Dienstleistung) innovativ. Konkret geben 46% an, im Vorjahr Produktinnovationen eingeführt zu haben (insbesondere große Unternehmen mit mehr als 1000 Mitarbeiter*innen und über 50 Mio.

Exportanteile im Mittel nach Mitarbeitendenanzahl

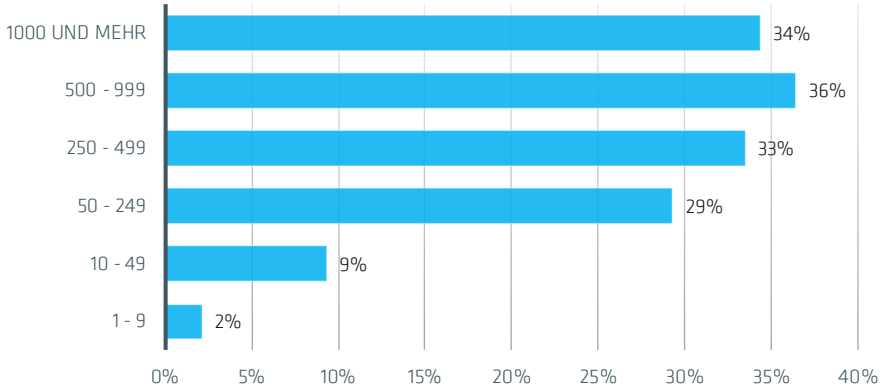
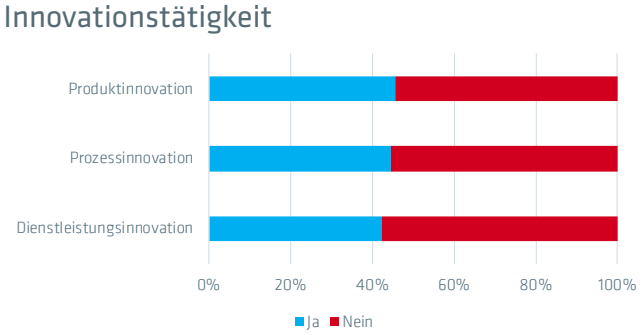
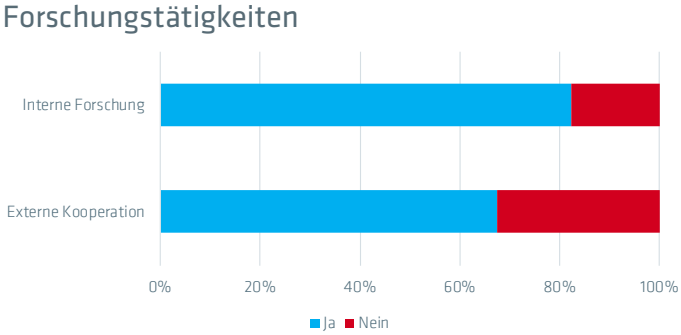


Abbildung 6: Exportanteile nach Unternehmensgröße (gemessen an Anzahl der Mitarbeitenden (N=137)).

Euro Umsatz sind hier relativ aktiver als kleine Unternehmen bis 49 Mitarbeiter*innen, von denen nur 28% angeben, Produktinnovationen auf den Markt gebracht zu haben). 45 bzw. 42% der Befragten geben zudem an, Prozess- bzw. Dienstleistungsinnovationen eingeführt zu haben. Relativ häufig beteiligt an Produktinnovationen sind hierbei die Gruppen der exportintensiven Unternehmen mit Exportquoten zwischen





Abbildungen 7 und 8: Innovationstätigkeiten (N=134-137) und Forschungsaktivitäten (N=86).

10% und 50%, sowie höher als 50%. In diesen beiden Gruppen geben 65% bzw. 62% der Befragten an, Prozessinnovationen eingeführt zu haben, während es bei Unternehmen, die keinen Export betreiben, gerade einmal 25% sind. 82% der Unternehmen üben diese Forschungs- und Innovationsaktivitäten selbst intern aus, und 67% geben an, darüber hinaus mit externen Forschungseinrichtungen zu kooperieren.

Im vorliegenden Bericht werden vor allem die Branchenzugehörigkeit, Unternehmensgröße, Exporttätigkeit sowie Forschungs- und Innovationstätigkeiten als Unterscheidungskriterium herangezogen, um die Ergebnisse zu strukturieren und einzelne Besonderheiten herauszuarbeiten.

NUTZUNG VON MANAGEMENTSYSTEMEN

Unternehmen können Managementsysteme implementieren und sich darüber hinaus bezüglich der Anforderungen der jeweiligen Norm zertifizieren lassen. Eine Zertifizierung ist eine Bestätigung 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.[10]

Zertifizierungsquote schwankt erheblich: Anwendende der ISO 9001 am häufigsten, der ISO/IEC 27001 selten zertifiziert

Laut ISO-Survey ist ISO 9001 für Qualitätsmanagement die weltweit und in Deutschland am weitesten verbreitete Managementsystem-Norm. Dies spiegelt sich auch in den Ergebnissen dieser Befragung wider: 83% der 180 Teilnehmenden geben an, diese Norm anzuwenden. 130 Teilnehmende sind dabei nach ISO 9001 zertifiziert, 20 weitere wenden die Norm ohne Zertifizierung an. Weit verbreitet sind in unserer

Stichprobe auch die Umweltmanagementsystem-Norm ISO 14001 (insg. 51%), ISO 45001 (BS OHSAS 18001) für Managementsysteme in den Bereichen Arbeits- und Gesundheitsschutz (41%) und die Energiemanagementsystem-Norm ISO 50001 (37%).

Auffällig sind große Unterschiede in der **Zertifizierungsquote**: So zeigen die Befragungsergebnisse für ISO 9001 nicht nur eine generell große Verbreitung, sondern auch, dass anwendende Unternehmen tendenziell öfter zertifiziert sind als Anwender anderer Managementsysteme. Insbesondere Unternehmen des Verarbeitenden Gewerbes sind vergleichsweise oft zertifiziert. Nur ein befragtes anwendendes Unternehmen der ISO 9001 dieser Branche ist nicht zertifiziert. Auch die Unternehmensgröße spielt eine Rolle: Die Gruppe der Kleinunternehmen (bis 49 Mitarbeitenden) weist deutlich niedrigere Zertifizierungsquoten auf als die Unternehmen aller Vergleichsgruppen (63% vs. 90%).

Andere Normen werden oft auch implementiert, ohne ein Zertifikat zu erlangen. Während Umweltmanagementsysteme nach ISO 14001 ebenfalls eine hohe Zertifizierungsquote aufweisen (81% der Nutzenden haben ein Zertifikat), lässt sich nur gut jeder dritte Anwender eines Managementsystems nach ISO/IEC 27001 für Informationssicherheit zertifizieren (37%). Und auch bei Managementsystemen für Arbeits- und Gesundheitsschutz nach ISO 45001 (BS OHSAS 18001) verzichtet mehr als jeder zweite Anwender auf eine Zertifizierung. 5% geben hier sogar an, eine frühere Zertifizierung aufgegeben zu haben. Während allgemeine Qualitätsmanagementsysteme nach ISO 9001 eine Zertifizierungsquote von 87% aufweisen, sind nur zwei Drittel der Unternehmen, die branchenspezifische Qualitätsmanagementsystem-Normen implementieren (ISO 13485 für Medizinprodukte und IATF 16949 für die Automobilindustrie), auch dafür zertifiziert. Das nächste Kapitel beleuchtet die jeweiligen Motive genauer.

Gleichzeitige Nutzung von verschiedenen Managementsystemen weit verbreitet: 70% der zertifizierten Unternehmen haben mehr als eine Managementsystem-Zertifizierung

Von den 180 Teilnehmenden der Umfrage nutzen 169 mindestens ein genormtes Managementsystem. Davon haben 151 mindestens ein entsprechendes Zertifikat. Unternehmen, die nicht nur ein, sondern mehrere verschiedene Managementsysteme (entweder gleichzeitig oder sukzessive) implementieren und zertifizieren, können dabei allgemein von verschiedenen Vorteilen einer kombinierten Nutzung bzw. Integration profitieren. Mögliche Synergien ergeben sich bspw. aus den ähnlichen Dokumentationsanforderungen oder Normenstrukturen und -prozessen (z. B. dem Plan-Do-Check-Act-Cycle, den viele der betrachteten Normen gemeinsam haben). Die Vertrautheit mit den Anforderungen, Arbeitsprinzipien, nötigen Ressourcen und Maßnahmen, die mit der Implementierung eines

Anzahl Zertifikate und Zertifizierungsquote

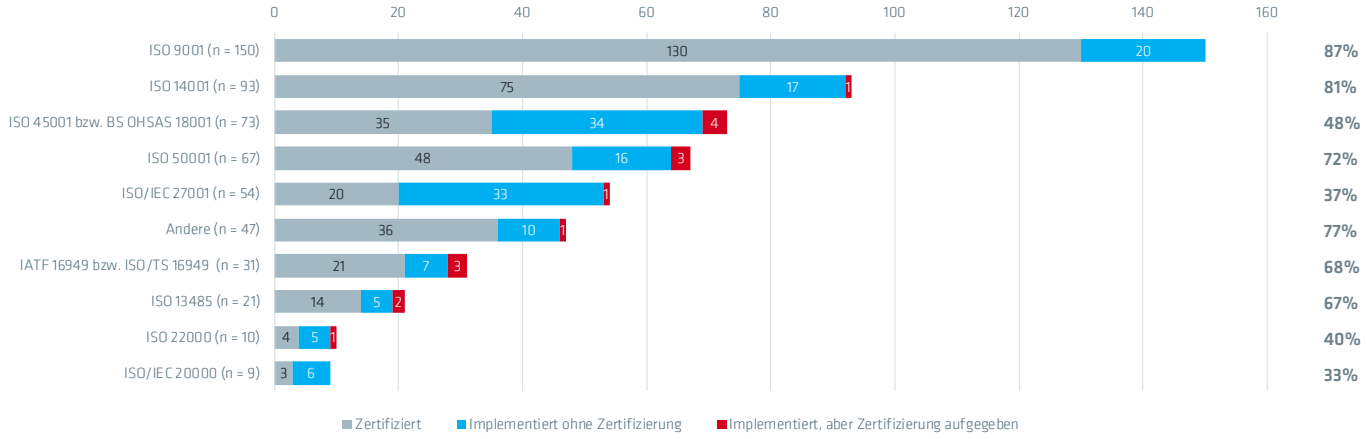


Abbildung 9: Nutzung von ausgewählten Managementsystemen und Anteil der Unternehmen, die eine Zertifizierung aufweisen (Zertifizierungsquote).

Mitarbeitendenzahl	Anzahl Zertifikate/ Unternehmen	n
1000 und mehr	3,4	59
500 - 999	2,6	9
250 - 499	2,4	17
50 - 249	2,1	38
10 - 49	1,5	17
1 - 9	1,5	11
Summe		151

Umsatz	Anzahl Zertifikate/ Unternehmen	n
über 50	3,1	76
10 bis 50	2,2	31
2 bis 10	1,7	18
bis 2	1,5	13
keine Angabe	1,5	2
Weiß nicht	2,4	11
Summe		151

Unternehmensform	Anzahl Zertifikate/ Unternehmen	n
internationale Unternehmensgruppe	3,3	55
nationale Unternehmensgruppe	2,7	32
Einzelunternehmen	1,8	59
Sonstiges	1,8	4
keine Angabe	1	1
Summe		151

Exportorientierung	Anzahl Zertifikate/ Unternehmen	n
kein Export	2,1	31
EU (außerhalb DE)	2,6	64
Amerika (exkl. USA)	2,5	2
USA	2,8	8
Asien	3,0	9
Afrika	1,0	1
keine Angabe	2,9	36
Summe		151

Tabelle 2: Durchschnittliche Zahl von Zertifikaten pro Unternehmen, unterteilt nach Mitarbeitendenzahl des Unternehmens, Umsatz (in Mio. Euro), Unternehmensform und Exportorientierung (mit jeweiligem Hauptexportmarkt). Basis bilden Unternehmen, die mindestens ein Zertifikat halten (N= 151).

Managementsystems verbunden sind, kann Unternehmen die Implementierung eines weiteren genormten Managementsystems erleichtern.

Die Studie kann einen seltenen detaillierten empirischen Einblick in diese integrierte Zertifizierung geben. Auch wenn aus der vorliegenden Erhebung nicht der Grad der Integration in den einzelnen Unternehmen abgeleitet werden kann, so zeigen die Umfrageergebnisse dennoch, dass die gleichzeitige Nutzung mehrerer Managementsysteme weit verbreitet ist. So sind 70% der zertifizierten Unternehmen gegen mehr als eine Managementsystem-Norm erfolgreich zertifiziert worden. Wenn man auch zusätzlich die Implementierungen ohne Zertifikat betrachtet, so nutzen 80% mehr als ein genormtes Managementsystem. Im Durchschnitt aller zertifizierten Teilnehmenden ergeben sich 2,6 Zertifikate pro Unternehmen. Dabei zeigen sich mitunter erhebliche Unterschiede: So steigt die Zahl der Zertifikate pro Unternehmen mit der Mitarbeitendenzahl und dem Umsatz: kleine Unternehmen bis max. 50 Mitarbeitenden bzw. bis max. 2 Mio. Euro Umsatz haben im Durchschnitt 1,5 Zertifikate, die mit über 1000 Mitarbeitenden hingegen 3,4. Auch bei den verschiedenen Unternehmensformen zeigen sich Differenzen: Einzelunternehmen haben erwartungsgemäß die wenigsten Zertifikate, nationale und internationale Unternehmensgruppen haben deutlich mehr Zertifizierungen. Exportierende Unternehmen halten im Durchschnitt mehr Zertifikate als nicht-exportierende Unternehmen. Dies gilt vor allem für Unternehmen mit Hauptexportmärkten in Asien, gefolgt von den USA.

Berücksichtigt man zusätzlich auch noch alle Implementierungen ohne Zertifikat, zeigt sich, dass jedes teilnehmende Unternehmen im Durchschnitt 3,3 genormte Managementsysteme nutzt (zertifiziert und/ oder nur implementiert).

Anzahl Zertifizierungen und Implementierungen pro Unternehmen
(0 bis max. 10 gleichzeitig)

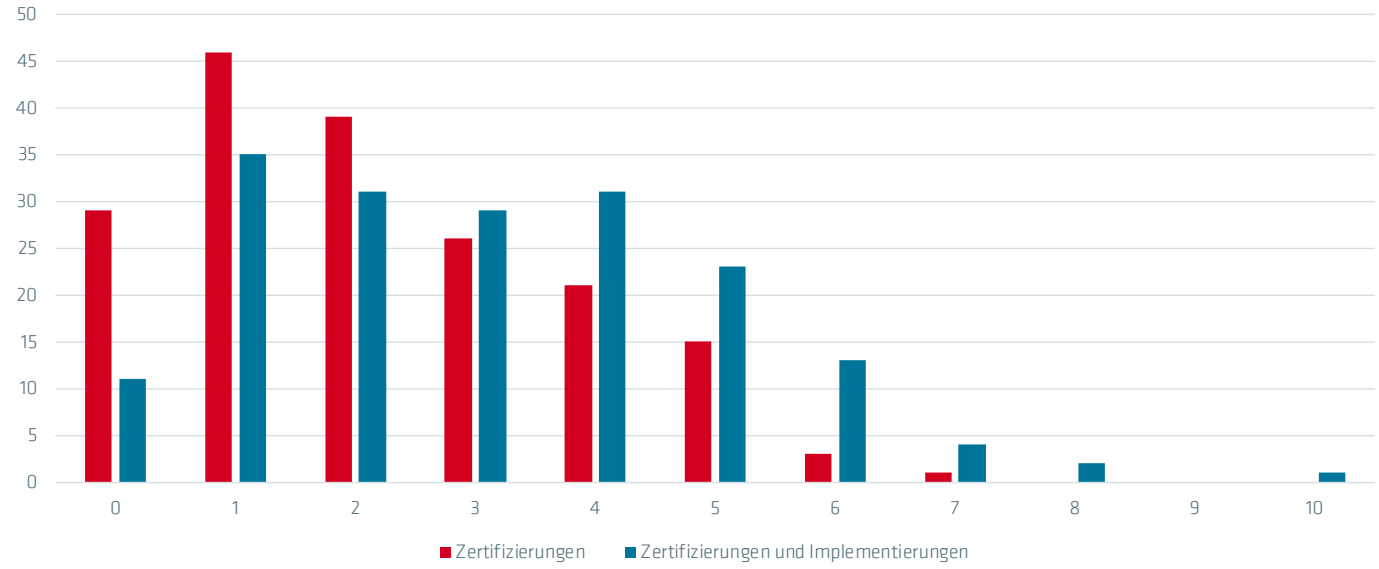


Abbildung 10: Anzahl der Zertifizierungen und Implementierungen von Managementsystemen pro Unternehmen (0 bis max. 10 gleichzeitig). Basis: Zertifizierte Unternehmen (N=151), Zertifizierte und/oder implementierende Unternehmen (N=169).

Jedes vierte zertifizierte teilnehmende Unternehmen hat genau zwei zertifizierte Managementsysteme, 17% haben drei, 14% vier. Jeder achte Zertifizierte unserer Stichprobe ist sogar gegen mindestens fünf verschiedene Managementsysteme zertifiziert. Betroffen sind hier ausschließlich Unternehmen des Verarbeitenden Gewerbes sowie der Branchen Verkehr und Lagerei. Außerdem ist dies vornehmlich bei sehr großen Unternehmen der Fall: Alle der mindestens fünfmal Zertifizierten haben mehr als 10 Mio. Euro Umsatz (84% sogar über 50 Mio. Euro), mit nur einer Ausnahme gehören alle zu nationalen oder internationalen Unternehmensgruppen. Umgekehrt sind es überwiegend (zu 59%) Einzelunternehmen mit zumeist unter 250 Mitarbeitenden, die lediglich gegen ein einziges Managementsystem zertifiziert sind. Hier ist die Branchenverteilung auch wesentlich durchmischter: zwei Drittel gehören nicht dem Verarbeitenden Gewerbe an.

Die Erhebung erlaubt auch Einblicke darin, welche Managementsysteme gemeinsam genutzt werden. Hier zeigt sich, dass die ISO 9001 für das Qualitätsmanagementsystem als „Basis-Norm“ dient. Fast alle Anwender von Umwelt-, Energie- und Arbeitsschutzmanagementsystemen sind auch gegen diese ISO-Norm zertifiziert. Auch die Umwelt- und Energiemanagementsysteme werden sehr häufig gemeinsam genutzt. Das deckt sich mit früheren Studien, die zeigen, dass ISO 50001 nur sehr selten implementiert und zertifiziert wird, wenn noch kein anderes Managementsystem implementiert ist, insbesondere ISO 14001 und ISO 9001.[11] Die geringste gemeinsame Nutzung mit anderen genormten Managementsystemen findet sich bei der ISO/IEC 27001 für Informationssicherheit. Hier hatte sich bereits eine geringe Zertifizierungsquote bei den Anwendern gezeigt. Eine gemeinsame Nutzung von Managementsystemen mit anderen zertifizierten Managementsystemen (Kookkurrenz) zeigt sich hingegen beim Arbeits- und Gesundheitsschutz nach ISO 45001 (BS OHSAS 18001).

Der Umfang solch einer gemeinsamen Nutzung und Integration mehrerer Systeme hängt entscheidend von den Charakteristika der jeweiligen Unternehmen bspw. im Hinblick auf Branchenzugehörigkeit oder Unternehmensgröße ab. Dies deckt sich mit früheren Studien anderer Länder, in denen ähnliche Trends gefunden wurden. Unterstützt wird diese Entwicklung insgesamt auch davon, dass die ISO Managementsystem-Normen aufgrund der 2012 eingeführten gemeinsamen High-Level Structure (einheitliche Grundstruktur, Anforderungen und Begriffe) kompatibel sind.

		...sind x% auch zertifiziert nach					
		ISO 9001	ISO 14001	ISO 50001	ISO/IEC 27001	ISO 45001	IATF 16949
von den Zertifizierten nach...	ISO 9001 (n=130)	100,0%	56,9%	34,6%	9,2%	26,2%	15,4%
	ISO 14001 (n=75)	98,7%	100,0%	53,3%	13,3%	44,0%	22,7%
	ISO 50001 (n=48)	93,8%	83,3%	100,0%	14,6%	43,8%	29,2%
	ISO/IEC 27001 (n=20)	60,0%	50,0%	35,0%	100,0%	20,0%	20,0%
	ISO 45001 (n=35)	97,1%	94,3%	60,0%	11,4%	100,0%	25,7%
	IATF 16949 (n=21)	95,2%	81,0%	66,7%	19,0%	42,9%	100,0%

Tabelle 3: Integration verschiedener Managementsystem-Normen: Anteil der nach jeweils zwei Managementsystem-Normen zertifizierten Unternehmen. Basis bilden Unternehmen, die gegen die jeweilige(n) Norm(en) zertifiziert sind. Insgesamt haben 151 Unternehmen mindestens ein Zertifikat (N=151).

Große Unterschiede beim Zeitpunkt der Erstzertifizierung

Große Unterschiede zwischen den verschiedenen Managementsystemen ergaben sich beim Zeitpunkt der Erstzertifizierung. Über 80% der nach ISO 9001 zertifizierten Unternehmen verfügen bereits seit mindestens 10 Jahren über ihre Zertifizierung. Lediglich jedes achte Unternehmen unserer Stichprobe hat sich erst in den letzten 3 Jahren erstmalig zertifizieren lassen. Auch ein Qualitätsmanagement speziell für die Automobilbranche nach IATF 16949 (ISO/TS 16949) sowie ein Umweltmanagement nach ISO 14001 haben viele teilnehmende Unternehmen schon seit über 10 Jahren zertifiziert (68% bzw. 60%).

Tendenziell zeigt sich damit, dass genau diejenigen Normen relativ mehr Zertifizierungen aufzeigen, die bereits länger verfügbar sind. Jüngere Normen – für die entsprechend eine Zertifizierung überhaupt erst seit wenigen Jahren möglich ist – haben eine geringere Zertifizierungsquote. Für die Normen, die erst nach der Jahrtausendwende eingeführt wurden (ISO/IEC 20000, ISO 22000, ISO/IEC 27001), sind jeweils weniger als die Hälfte der anwendenden Unternehmen zertifiziert. Diese Zertifizierungen sind im Durchschnitt entsprechend auch jünger: 47% der für ihr ISMS nach der 2005 veröffentlichten ISO/IEC 27001 zertifizierten Unternehmen sind maximal 3 Jahre (nach Erstzertifizierung) zertifiziert, 43% geben an, zwischen 4 und 9 Jahren zertifiziert zu sein. Hier bleibt abzuwarten, ob es in den kommenden Jahren eine ähnliche Entwicklung wie bei den länger etablierten Normen gibt.

Eine Ausnahme unter den jüngeren Normen bildet ISO 50001 für Energiemanagementsysteme, die erst 2011 eingeführt wurde, aber schon früh eine vergleichsweise hohe Zertifizierungsquote erreicht (72% der befragten anwendenden Unternehmen sind zertifiziert): jedes fünfte zertifizierte Unternehmen erhielt ihr Erstzertifikat in den vergangenen 3 Jahren, 75% gaben an, erstmalig vor 4-9 Jahren zertifiziert worden zu sein. Das nachfolgende Kapitel zu den Motiven einer Zertifizierung zeigt einen eindeutigen Grund für diesen Trend.

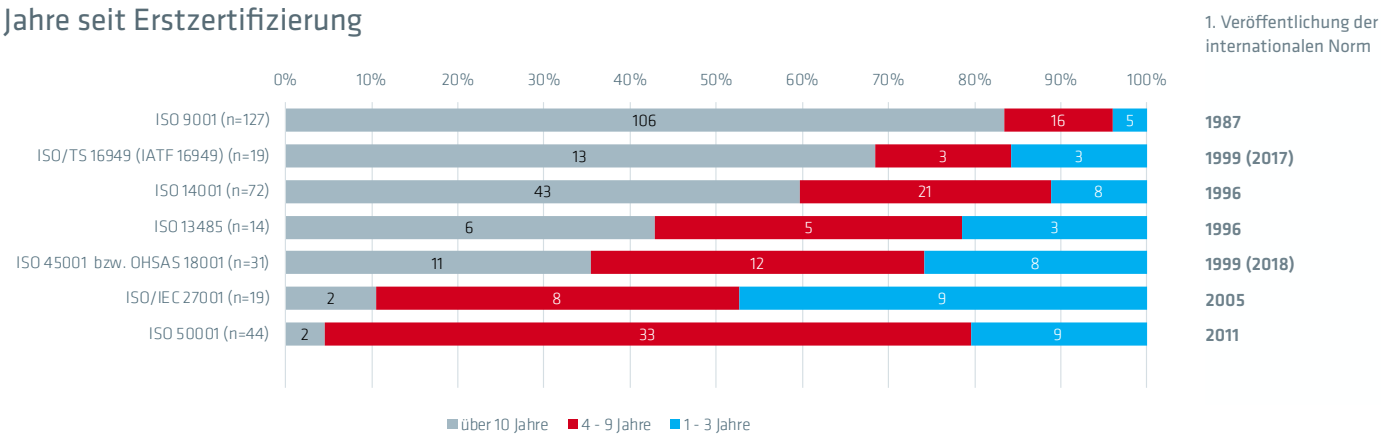


Abbildung 11: Jahre seit Erstzertifizierung für verschiedene Managementsystem-Normen.

MOTIVE ZUR NUTZUNG VON MANAGEMENTSYSTEMEN

Neben dem primären Ziel des jeweiligen genormten Managementsystems (bspw. Erhöhung der Qualität von Produkten und Dienstleistungen bzw. Erhöhung der Arbeitssicherheit) nutzen Unternehmen die Managementsysteme aus verschiedenen internen und externen Gründen. Hierbei unterscheidet sich die Wichtigkeit der Motive je nach Managementsystem. Die Teilnehmenden wurden gebeten, die Relevanz vorgegebener Motive auf einer Skala von "trifft gar nicht zu" (1) bis „trifft voll zu" (5) zu bewerten.

Verschiedene Hauptmotive für die Implementierung und Zertifizierung von Managementsystemen

Während Kundenforderungen der Hauptantrieb für die Einführung und Zertifizierung von ISO 9001 und ISO 14001 sind, ist es bei ISO 45001/BS OHSAS 18001 (Gesundheit und Sicherheit) und ISO/IEC 27001 (Informationssicherheit) die Erhöhung der Rechtsicherheit. Im Falle des Qualitätsmanagementsystems nach ISO 13485 für den Bereich Medizinprodukte wird die Norm als Türöffner für den Marktzugang insbesondere im Ausland angesehen. Die wichtigste Triebfeder für die Zertifizierung nach ISO 50001 (Energiemanagement) ist das Ziel, damit verbundene Steuererleichterungen zu realisieren. Der Wunsch nach internen Verbesserungen durch ein genormtes Managementsystem ist bei ISO 9001 und ISO 45001 (BS OHSAS 18001) vergleichsweise am größten.

Qualitätsmanagement: getrieben von Kundenforderungen und interner Verbesserung

Kundenforderungen sind für die Teilnehmenden an der Umfrage der wichtigste Grund, ISO 9001 zu implementieren bzw. sich dagegen zertifizieren zu lassen. Dies trifft im besonderen Maße für Unternehmen mit mehr als 1000 Mitarbeitenden zu (Mittelwert: 4,5). Für kleine Unternehmen bis 49 Mitarbeitenden ist dies vergleichsweise weniger wichtig (MW: 3,3). Für sie stehen unternehmensinterne Verbesserungen an erster

Motive zur Anwendung von ISO 9001

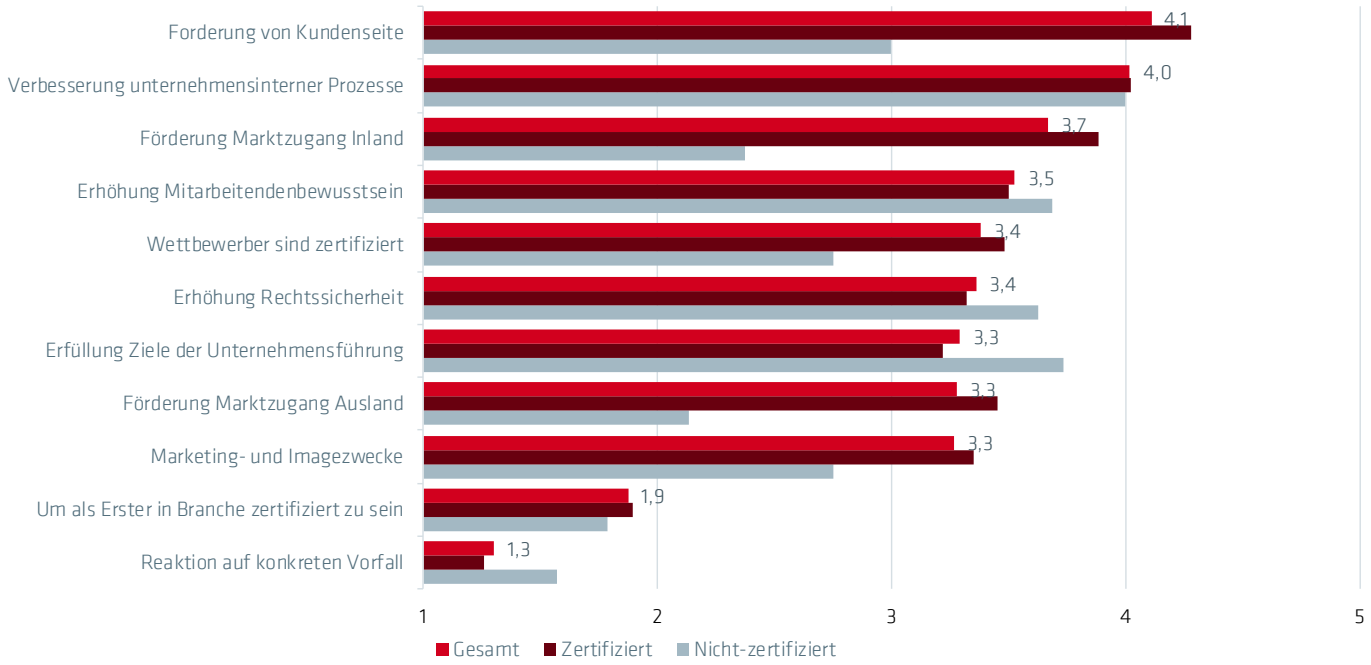


Abbildung 12: Durchschnittliche Einschätzung der Motive für die Implementierung der Norm ISO 9001. Basis bilden antwortende Unternehmen, die diese Norm mit (N=92-103) oder ohne Zertifizierung (N=14-16) implementieren, gesamt (N=106-119). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

Stelle (MW: 3,8), welche für die gesamte Stichprobe die zweitwichtigste Motivation sind.

Auch die Exportorientierung spielt eine Rolle: Während Kundenanforderungen bei Unternehmen, die einen Exportanteil von über 50% haben, ein entscheidender Motivator sind (MW: 4,6), sinkt deren Bedeutung bei Unternehmen, die ausschließlich im Inland aktiv sind (MW: 3,6). Die sehr exportorientierten Unternehmen nennen den Marktzugang im Ausland sowie die Tatsache, dass Wettbewerber ebenfalls zertifiziert sind, ebenfalls als weitere wichtige Beweggründe (MW: 4,1 und 3,9). Der Marktzugang ins Ausland ist insgesamt ein Hauptgrund für eine Zertifizierung nach ISO 9001 – und damit höher bewertet als für den heimischen Marktzugang. Dies hängt jedoch auch mit der insgesamt hohen Exportorientierung der Befragten zusammen.

Deutliche Unterschiede bei den Motiven zur Einführung von ISO 9001 zeigen sich insgesamt bei den verschiedenen Branchen: Während das Verarbeitende Gewerbe hauptsächlich durch Kundenforderungen (MW: 4,5), Marktzugang im Inland (MW: 4,1), und dann erst internen Verbesserungen (MW: 3,9) motiviert wird, ist letzteres mit Abstand der wichtigste Grund für Dienstleister (MW: 4,2). Sie zielen mit der Implementierung von ISO 9001 auch insbesondere darauf ab, das Mitarbeitendenbewusstsein in Bezug auf Qualität zu erhöhen und Rechtsicherheit zu schaffen (MW: je 3,6). Auch Konzernvorgaben und die Erfüllung von Zielen der Unternehmensführung spielen eine weitere wichtige Rolle (MW: 3,5) für Dienstleister.

Die Daten zeigen auch, dass ein Qualitätsmanagementsystem nicht als Reaktion auf bestimmte Vorfälle eingeführt wird, sondern vielmehr eine strategische Entscheidung auf Grundlage der o.g. Motive ist.

Da die Umfrage nicht nur Unternehmen erfasst hat, die nach ISO 9001 zertifiziert sind, sondern auch jene, die die Norm ohne Zertifizierung anwenden, lassen sich hier auch Unterschiede bei der Motivation erkennen: Während zertifizierte Unternehmen externe Kundenforderungen als Hauptmotiv nennen (MW: 4,3), zielen Unternehmen, die auf Zertifizierung verzichten, mit der Implementierung von ISO 9001 in erster Linie auf interne Verbesserungen (MW: 4,0) und die Erhöhung des Mitarbeitendenbewusstseins in Bezug auf Qualität ab (MW: 3,7).

Motive zur Anwendung von ISO 14001 und ISO 50001

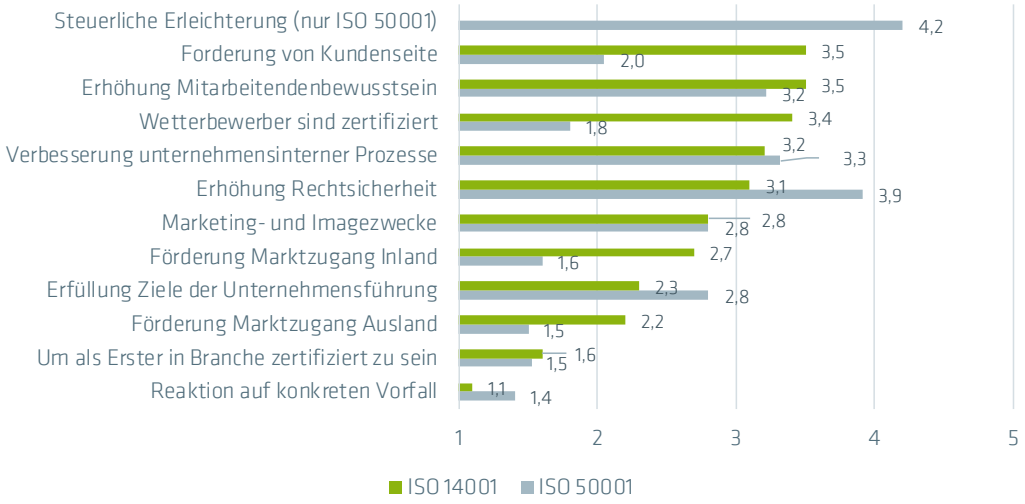


Abbildung 13: Durchschnittliche Einschätzung der Motive für die Implementierung der Normen ISO 14001 und ISO 50001. Basis bilden antwortende Unternehmen, die diese Normen mit oder ohne Zertifizierung implementieren (N=10 für ISO 14001 bzw. N=22-26 für ISO 50001). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

Im speziellen Fall des Qualitätsmanagementsystems für die Medizinproduktebranche nach ISO 13485 zeigt sich, dass der Marktzugang sowohl im Inland als auch im Ausland das entscheidende Kriterium für die Einführung und Zertifizierung sind (MW: 4,9 und 4,8). Hier limitiert jedoch der geringe Stichprobenumfang von nur neun Unternehmen die Aussagekraft.

Umwelt- und Energiemanagement: gemischte Motive

Nicht nur bei Qualitätsmanagementsystemen sind Kundenforderungen der Hauptmotivator für die Implementierung und Zertifizierung. Auch die Einführung eines Umweltmanagementsystems nach ISO 14001 ist – wenn auch vergleichsweise insgesamt auf niedrigerem Niveau – von Kundenforderungen getrieben. Hier spielt auch eine wichtige Rolle, dass Wettbewerber zertifiziert sind. Das zweite Hauptmotiv ist jedoch intrinsisch: Tatsächlich wollen Unternehmen erreichen, dass ihre Mitarbeitenden bewusster mit Umweltthemen umgehen und insgesamt unternehmensinterne Prozesse mithilfe des Managementsystems verbessert werden.

Bei der Implementierung eines Energiemanagementsystems nach ISO 50001 spielt die Forderung von Kundenseite hingegen eine untergeordnete Rolle. Vielmehr sind die Erfüllung von gesetzlichen Vorgaben und die Erhöhung der Rechtsicherheit sowie insbesondere der Anreiz, Steuern zu sparen, die Haupttreiber. Zertifizierte Unternehmen in Deutschland können von Steuererleichterungen profitieren und Unternehmen sind teilweise sogar gesetzlich verpflichtet, die Anwendung eines Energiemanagementsystems nachzuweisen. Dies erklärt die hohe Bedeutung, die diesen Motiven von den Befragten beigemessen wird. Erst dann folgen intrinsische Motive wie die Erhöhung des Mitarbeitendenbewusstseins oder Verbesserung interner Prozesse. Letzteres hat bei Unternehmen, die nur implementieren und sich nicht zertifizieren lassen, jedoch einen höheren Stellenwert (MW: 3,8). Kundenforderungen oder Marktzutritt spielen bei keinen der Befragten eine bedeutende Rolle. Obwohl die Norm hauptsächlich von großen Unternehmen, vorrangig aus dem Verarbeitenden Gewerbe implementiert wird, sind die Motive dennoch über die gesamte Stichprobe ähnlich.

Informationssicherheit nach ISO/IEC 27001: Prävention das wichtigste Motiv

Mit der Implementierung der ISO/IEC 27001 wollen die befragten Unternehmen – unabhängig von Branche oder Größe – an erster Stelle die Rechtsicherheit erhöhen bzw. gesetzliche Anforderungen erfüllen. Hierbei gibt es keine signifikanten Unterschiede zwischen Unternehmen, die die Norm anwenden bzw. zusätzlich dagegen zertifiziert sind.

Im Sinne der Norm sollen mit ihrer Einführung insbesondere im präventiven Sinne Informationssicherheitsvorfällen (z. B. Hackerangriffen) vorgebeugt, das Mitarbeitendenbewusstsein bzgl. Informationssicherheit

Motive zur Anwendung von ISO/IEC 27001

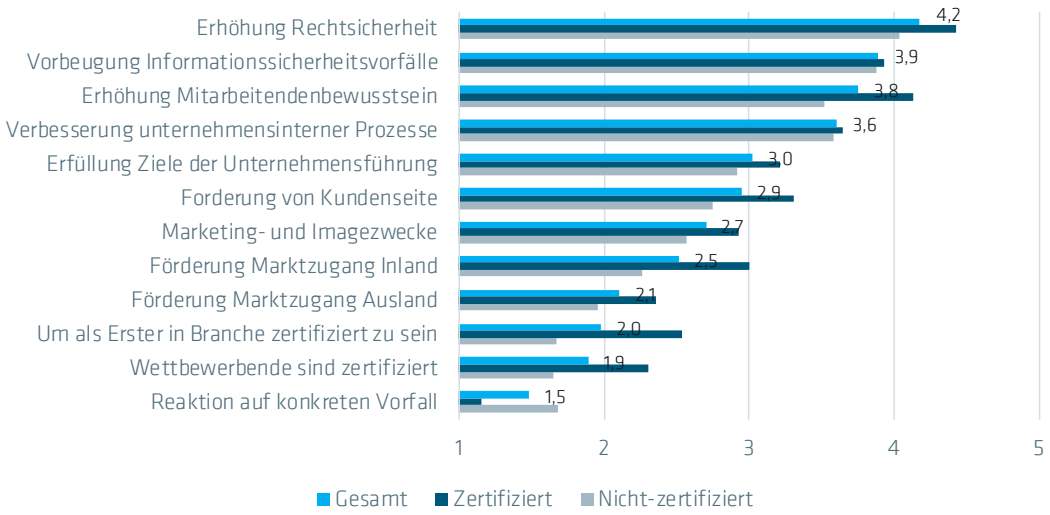


Abbildung 14: Durchschnittliche Einschätzung der Motive für die Implementierung der Norm ISO/IEC 27001. Basis bilden antwortende Unternehmen, die diese Norm mit (N=22-25) oder ohne Zertifizierung (N=12-15) implementieren, gesamt (N=34-40). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

erhöht sowie unternehmensinterne Prozesse verbessert werden. Die externe Forderung von Kundenseite nimmt einen unterschiedlich hohen Stellenwert je nach Unternehmensgröße ein. Während bei kleineren Unternehmen (unter 50 Mitarbeitenden) die Forderung von Kundenseite keine große Rolle spielt (MW: 1,7) ist dies das wichtigste Motiv bei Unternehmen mit 250 bis 1000 Mitarbeitenden (MW 4,0). Die Bedeutung des Marktzugangs im Ausland steigt erwartungsgemäß mit der Größe sowie der Exportorientierung.

Bei kleineren Unternehmen hingegen steht die Erhöhung des Mitarbeitendenbewusstseins in Bezug auf Informationssicherheit im Vordergrund. Auffallend ist, dass die weniger innovativen Unternehmen stärker motiviert sind hinsichtlich möglicher interner Verbesserungen als innovative Unternehmen (MW 4,3 ggü. 3,4).

Eine Abgrenzung gegenüber der Konkurrenz spielt allgemein eine untergeordnete Rolle. Beim Vergleich der Motive zwischen zertifizierten und nicht-zertifizierten anwendenden Unternehmen dieser Norm wird jedoch ersichtlich, dass erstere den Wettbewerb bei ihrer Entscheidung berücksichtigen: Zum einen bewerten zertifizierte Unternehmen das Motiv höher, als erster

Vergleich Motive für Managementsysteme

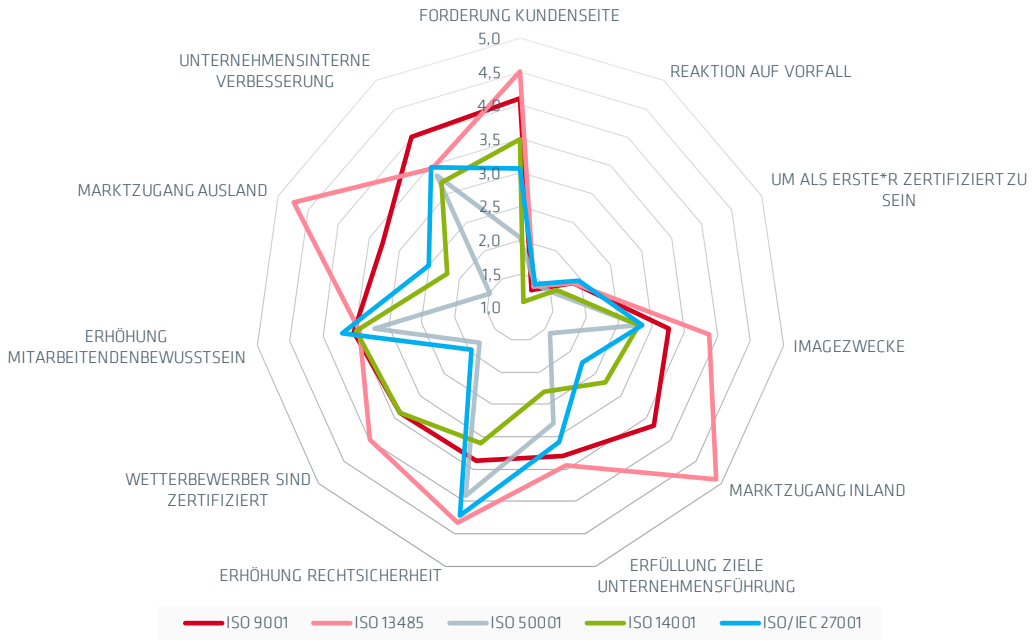


Abbildung 15: Vergleich der durchschnittlichen Einschätzung der Motive für die Implementierung diverser Managementsystem-Normen. ISO 9001 (N=106-119), ISO 13485 (N=8-9), ISO 50001 (N=22-26), ISO 14001 (N=10), ISO/IEC 27001 (N=35-40). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

(bzw. als einer der ersten) in der Branche dieses Managementsystem zu nutzen und zum anderen auch die Tatsache, dass die Konkurrenz diese Norm bereits anwendet.

Ein konkreter Informationssicherheitsvorfall ist für die teilnehmenden Unternehmen kein entscheidender Motivator für die Einführung eines Managementsystems nach ISO/IEC 27001, was erneut auf einen intrinsisch motivierten, präventiven Antrieb deutet.

Der Spezialteil dieser Befragung beleuchtet zusätzlich Schwierigkeiten bei der Einführung von ISO/IEC 27001 sowie Gründe für eine Nicht-Nutzung dieses Managementsystems und mögliche Maßnahmen zur Erhöhung der Verbreitung.

Abbildung 15 stellt die Motive für die Nutzung der verschiedenen Managementsysteme vergleichend gegenüber. Im folgenden Abschnitt werden die realisierten Wirkungen durch die Anwendung der Normen dargestellt.

WIRKUNG VON MANAGEMENTSYSTEMEN

Die einzelnen Managementsysteme entfalten bei den betroffenen Unternehmen ganz unterschiedliche Wirkungen. Die Teilnehmenden wurden gebeten, die Wirkungen zu bewerten, die ihrer Meinung nach durch die Umsetzung der jeweiligen Managementsystem-Normen realisiert wurden. Auch hier wurden vorgegebene Wirkungen auf einer Skala von 1 („trifft gar nicht zu“) bis 5 („trifft voll zu“) gewertet.

Managementsystem-Normen erfüllen ihren Zweck

Bei den Managementsystemen nach ISO 9001, ISO 45001 (BS OHSAS 18001) und ISO/IEC 27001 wird der Hauptnutzen in Verbesserungen im Sinne des Zwecks der jeweiligen Norm gesehen, also Qualität, Arbeits- und Gesundheitsschutz sowie Informationssicherheit. Nennenswerte Auswirkungen auf den Umsatz durch die Managementsystem-Normen werden von den Umfrageteilnehmenden nicht berichtet, mit Ausnahme der anwendenden Unternehmen von ISO 13485 (Qualitätsmanagement für Medizinprodukte). Steuererleichterungen sowie Energie- und Kosteneinsparungen wiederum sind der Hauptvorteil des Energiemanagementsystems nach ISO 50001. Eine größere Sensibilisierung der Mitarbeitenden ist die wichtigste Wirkung im Falle von ISO 14001 und auch eine wesentliche Wirkung durch die Nutzung der Managementsysteme nach ISO/IEC 27001 und ISO 9001.

ISO 9001 erzielt mit Qualitätsverbesserung die gewünschte Wirkung

Eine Verbesserung im Sinne von ISO 9001, also eine Sicherstellung bzw. Verbesserung der Qualität der hergestellten Produkte bzw. Dienstleistungen (z. B. geringere Ausschussquoten oder Kundenbeschwerden), wird als stärkste Wirkung durch die Teilnehmenden bestätigt.[12] In diesem Sinne ist auch das stärkere Mitarbeitendenbewusstsein für Qualitätsfragen eine zweite Hauptwirkung des Managementsystems nach ISO 9001.

Auch was die finanziellen Effekte angeht, nehmen die Befragten allgemein Kosteneinsparungen als einen der wichtigsten Vorteile wahr. Auswirkungen auf Versicherungsprämien ließen sich bei den teilnehmenden Unternehmen durch ISO 9001 jedoch kaum realisieren. Imageverbesserungen zählen zu den Hauptwirkungen, Umsatzsteigerungen hingegen werden vergleichsweise gering eingeschätzt. Insbesondere Unternehmen, die ausschließlich im Inland verkaufen, realisierten geringere Umsatzeffekte durch ISO 9001 im Vergleich zu

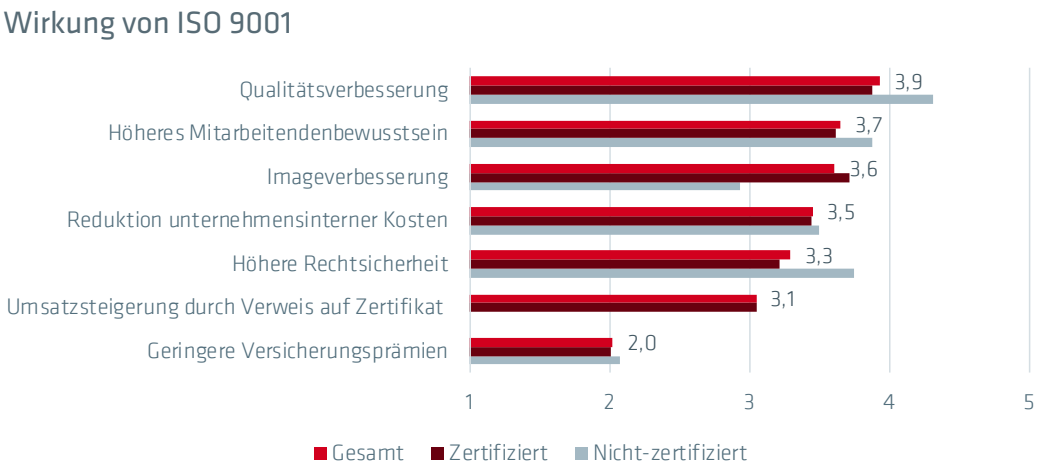


Abbildung 16: Durchschnittliche Einschätzung der Wirkung durch die Nutzung des Managementsystems nach ISO 9001. Basis bilden antwortende Unternehmen, die diese Norm mit (N=76-104) oder ohne Zertifizierung (N=14-16) implementieren, gesamt (N=90-120). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

exportierenden Unternehmen (MW 2,1 im Vergleich zu 3,2).

Unternehmenscharakteristika spielen bei den Wahrnehmungen der Wirkungen von ISO 9001 kaum eine Rolle, die von allen Befragten ähnlich bewertet werden, — unabhängig von Branche, Zahl der Mitarbeitenden, Umsatz oder Exportorientierung. Unterschiede zeigen sich jedoch zwischen den Unternehmen, die nach ISO 9001 zertifiziert sind und jenen, die die Norm nur implementiert haben: Für beide Gruppen sind die unternehmensinternen Verbesserungen durch das Qualitätsmanagementsystem zwar die wichtigsten Wirkungen. Nicht-Zertifizierte nehmen sie aber stärker wahr als Zertifizierte (MW: 4,3 versus 3,9). Auch das gewachsene Mitarbeitendenbewusstsein wird mit 3,9 auf dem zweiten Platz höher bewertet als bei den Zertifizierten. Auffällig ist auch, dass Nicht-Zertifizierte eine erhöhte Rechtsicherheit als drittwichtigste Wirkung benennen (MW: 3,8), während dies für Zertifizierte nur für Platz 5 reicht (MW: 3,2). Die Effekte auf Kosten und Versicherungsprämien werden bei beiden Gruppen vergleichsweise geringer eingeschätzt.

Umweltmanagementsysteme erhöhen das Mitarbeitendenbewusstsein – finanzielle Vorteile als Hauptwirkung von Energiemanagementsystemen

Ein erhöhtes Bewusstsein für Umweltfragen sowie tatsächliche Verbesserungen im Sinne des Managementsystems sind die größten wahrgenommenen Wirkungen unter den befragten Anwendern des Umweltmanagementsystems nach ISO 14001. Auch Imageverbesserungen und Kosteneinsparungen sind wichtige Wirkungen.

Für Nutzende eines Energiemanagementsystems nach ISO 50001 sind die finanziellen Vorteile hingegen am wichtigsten: Neben der Reduktion der unternehmensinternen Energiekosten spielen hier in erster Linie die steuerlichen Erleichterungen, die mit der Zertifizierung gewährt werden, die mit Abstand entscheidende Rolle. Doch selbst nicht-zertifizierte Unternehmen profitieren: Für sie ist die erhöhte Rechtsicherheit durch die Anwendung der ISO 50001 die wesentlichste Hauptwirkung (MW: 4,8). Dahinter steckt auch die verbindliche EU-Richtlinie 2012/27/EU zur Energieeffizienz, nach der Nicht-KMUs ein Energieaudit durchführen müssen. ISO 50001 kann Unternehmen hier bei der Erfüllung der Anforderungen aus der Richtlinie unterstützen. Die Umfrageergebnisse zeigen in diesem Sinne auch, dass insbesondere große Unternehmen als die Betroffenen der EU-Richtlinie das Managementsystem nach ISO 50001 nutzen. Berücksichtigt man deren tendenziell höheren Energieverbrauch, sind sie auch diejenigen, die überdurchschnittlich von einem besseren Energiemanagement profitieren können. Die Stichprobe identifizierte entsprechend fast ausschließlich energieintensive verarbeitende Branchen wie die Chemische Industrie als hauptanwendende Unternehmen der Norm.

ISO/IEC 27001 wird oft ohne Zertifizierung implementiert – Erhöhung der Sicherheit steht im Vordergrund

Mit 20 zertifizierten Unternehmen und weiteren 33, die ein Managementsystem für Informationssicherheit nach ISO/IEC 27001 ohne eine Zertifizierung implementiert haben, gehört diese Norm zu denen mit den kleinsten Zertifizierungsquoten. Während die Analyse der

Wirkungen von ISO 14001 und ISO 50001

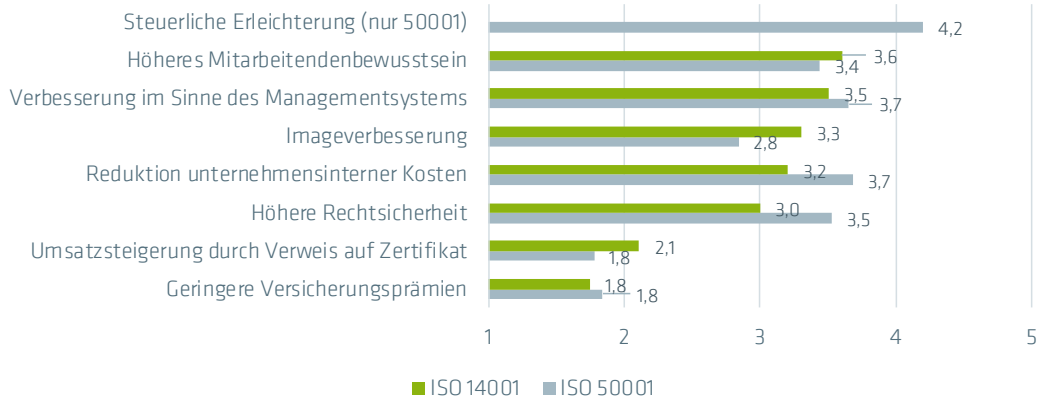


Abbildung 17: Durchschnittliche Einschätzung der Wirkung durch die Nutzung des Managementsystems nach ISO 14001 und ISO 50001. Basis bilden Unternehmen, die diese Norm mit oder ohne Zertifizierung implementieren (N=8-10 für ISO 14001 bzw. N=18-26 für ISO 50001). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

Hauptantriebe zur Einführung der Norm bereits hauptsächlich intrinsische Motive gezeigt hat, findet sich auch ein Schwerpunkt bei internen Wirkungen, insbesondere hinsichtlich Prävention.

Die Erhöhung der Informationssicherheit der Unternehmen wird von allen Unternehmen, unabhängig von Größe und Branche, als wichtigste Wirkung eingeschätzt. Auch die Gefahr von Informationssicherheitsvorfällen konnte reduziert werden.

Die Erhöhung des Mitarbeitendenbewusstseins in Bezug auf Informationssicherheit war eine Hauptmotivation für die Einführung eines Managementsystems nach ISO/IEC 27001 und tritt tatsächlich als weitere wesentliche Wirkung ein. Eine Erhöhung der Rechtsicherheit – obgleich das Hauptmotiv zur Einführung (MW: 4,2) – ist lediglich auf Platz vier der realisierten Wirkungen (MW: 3,7).

Direkte finanzielle Vorteile in Form von Kostenersparnissen (durch weniger Informationssicherheitsvorfälle) oder Umsatzsteigerungen treten nur in geringem Maße als Wirkung ein, unabhängig von der Unternehmensgröße, Branche oder der Innovationstätigkeit. Unterschiede gibt es jedoch hinsichtlich einer Reduktion von Versicherungsprämien: größere Unternehmen und das Verarbeitende Gewerbe (MW: 3,1 gegenüber 1,3 bei Dienstleistern) verzeichnen hier eine vergleichsweise hohe Wirkung durch die Anwendung von ISO/IEC 27001.

Zertifikate haben grundsätzlich eine Signalfunktion gegenüber den interessierten Kreisen. Zertifikatshalter können ihnen zeigen, dass sie die Anforderungen der Norm erfüllen. Gegenüber den Unternehmen, die die Norm zwar implementieren, aber kein Zertifikat halten, können die zertifizierten Befragten entsprechend auch einen höheren Imagegewinn verzeichnen (MW: 2,5 gegenüber 3,4). Insgesamt ist diese Wirkung jedoch

Wirkung von ISO/IEC 27001

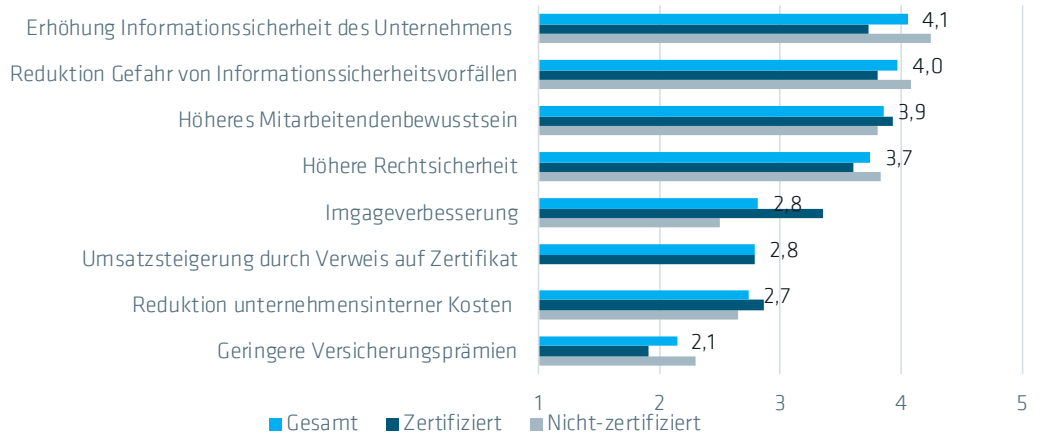


Abbildung 18: Durchschnittliche Einschätzung der Wirkung durch die Nutzung des Managementsystems nach ISO/IEC 27001. Basis bilden Unternehmen, die diese Norm mit (N=11-15) oder ohne Zertifizierung (N=17-25) implementieren, gesamt (N=28-40). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

Vergleich Wirkungen von Managementsystemen

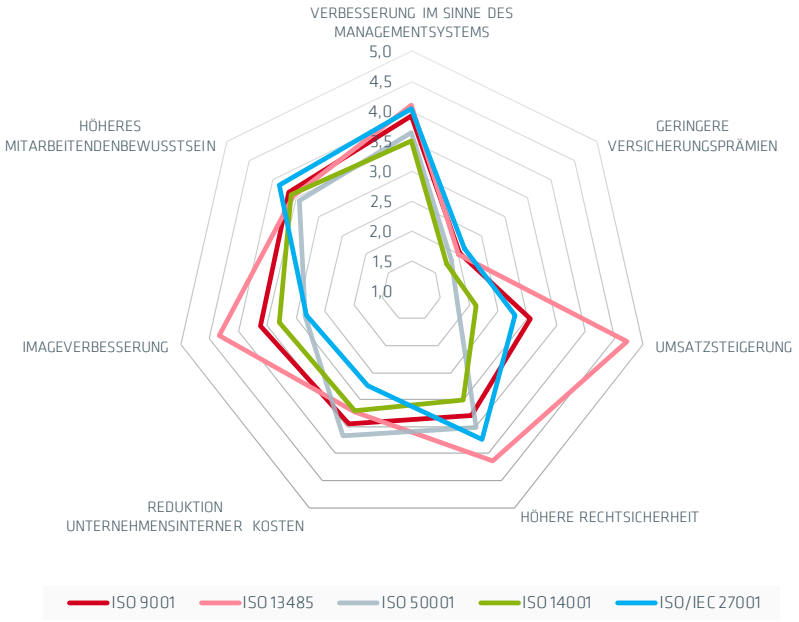


Abbildung 19: Vergleich der durchschnittlichen Einschätzung der Wirkungen durch die Implementierung diverser Managementsystem-Normen. ISO 9001 (N=90-120) ISO 13485 (N=5-9), ISO 50001 (N=18-26), ISO 14001 (N=8-10), ISO/IEC 27001 (N=28-40). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

vergleichsweise geringer als bei den Normen ISO 9001 oder ISO 14001.Die verschiedenen Wirkungen der Managementsysteme sind in Abbildung 19 vergleichend dargestellt. Wie die teilnehmenden Unternehmen insgesamt die Kosten-Nutzen-Relation der Zertifizierung bewerten, beleuchtet der nachfolgende Abschnitt.

Kosten-Nutzen-Relation am höchsten bei den Qualitätsmanagementsystemen

Die Teilnehmenden wurden abschließend gefragt, ob die Zertifizierung insgesamt eine gute Investition in Bezug auf Kosten und Nutzen sei (auf einer 5-stufigen Skala von „trifft gar nicht zu“ bis „trifft voll zu“). Hierbei sind die Befragten im Falle der ISO 13485 (Medizinprodukte - Qualitätsmanagementsysteme) besonders zufrieden in Bezug auf die Kosten-Nutzen-Relation (zu berücksichtigen ist jedoch die geringe Anzahl der Unternehmen von n=9). Auch die Zufriedenheit mit der ISO 9001 insgesamt ist unabhängig von Unternehmensgröße oder Branche recht hoch (MW: 3,9). Die ISO 14001-Zertifizierung hat den niedrigsten Zufriedenheitsgrad (MW: 3,4). Insgesamt gibt es keine signifikanten Unterschiede bei der Zufriedenheit im Hinblick auf die Branchenzugehörigkeit, Unternehmensgröße, sowie Forschungs- und Innovationstätigkeiten oder der Nutzung mit oder ohne Zertifikat.

Managementsysteme gute Investition?

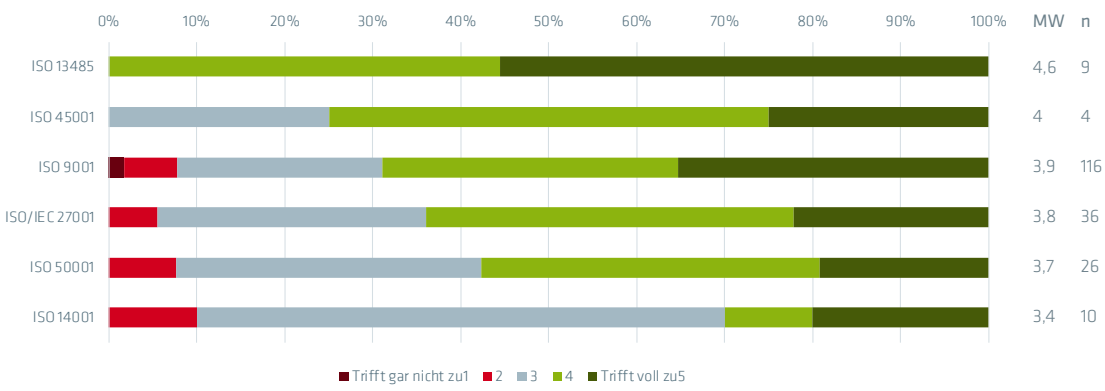


Abbildung 20: Einschätzung, ob alles in allem die genannten Managementsysteme eine gute Investition in Bezug auf Kosten und Nutzen für die Unternehmen darstellen. Bewertungsskala: 1 (trifft gar nicht) bis 5 (trifft voll zu).

Unterschiede zwischen Motivation zur Einführung von Managementsystemen und tatsächlich realisierten Wirkungen

Die insgesamt positiven Ergebnisse hinsichtlich der Gesamtzufriedenheit werden weiter gestützt, wenn man die tatsächlich eingetretenen Wirkungen mit den initialen Motiven vergleicht. Insbesondere bei ISO/IEC 27001 und ISO 13485 (Qualitätsmanagement für Medizinprodukte) werden die unternehmensinternen Verbesserungen in ihrer tatsächlichen Wirkung deutlich höher bewertet als bei der Motivation. Bei ISO 9001, ISO 13485 und ISO 14001 ist dies bei der Imageverbesserung der Fall.

Anders sieht es hingegen bei der Erhöhung der Rechtsicherheit durch die Anwendung der genormten Managementsysteme aus: Obwohl bei vielen Systemen als eine wichtige Hauptwirkung gewertet, zeigt sich dennoch im Vergleich zur ursprünglichen Motivation eine negative Abweichung. Hier bleibt die tatsächliche Wirkung hinter der offenbar hohen Erwartung zurück.

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

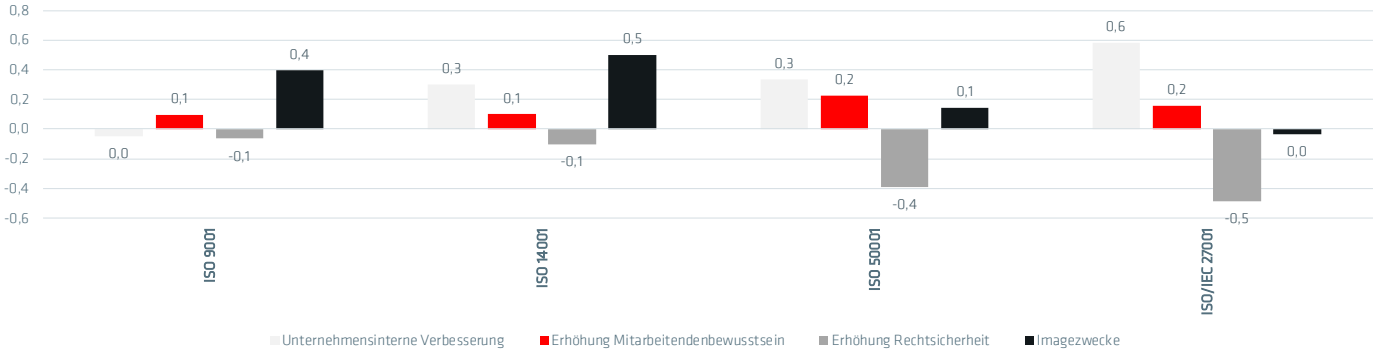


Abbildung 21: Abweichungen der Bewertung der tatsächlich wahrgenommenen Wirkungen von der ursprünglichen Bewertung der Motive (bezogen auf die jeweiligen Mittelwerte). ISO 9001: N=90-120, ISO 14001: N=8-10, ISO 50001: N=18-26, ISO/IEC 27001: N=28-40.

ZERTIFIZIERTE UND NICHT-ZERTIFIZIERTE UNTERNEHMEN IM VERGLEICH

Die Analyse der Zertifizierungsquoten hat bereits deutliche Unterschiede zwischen den einzelnen Managementsystemen gezeigt.

Bei genauerer Betrachtung zeigt sich, dass insbesondere große und sehr exportorientierte Unternehmen Managementsysteme nach ISO 9001 und ISO 14001 nicht nur implementieren, sondern sich auch eher danach zertifizieren lassen als kleine Unternehmen und solche, die ausschließlich oder hauptsächlich im Inland aktiv sind. Die Daten lassen außerdem erkennen, dass bei beiden Normen Unternehmen des Verarbeitenden Gewerbes eher zertifiziert sind als jene des Dienstleistungsgewerbes, die vergleichsweise oft auch auf eine Zertifizierung verzichten.

Betrachtet man die Motive und realisierten Wirkungen, werden teilweise auch deutliche Unterschiede zwischen zertifizierten und nur implementierenden Unternehmen

ersichtlich. So zeigen sich nicht-zertifizierte Unternehmen tendenziell noch stärker intrinsisch motiviert als zertifizierte. Bspw. sind sie im Falle der ISO 9001 oder ISO 50001 vorrangig durch interne Verbesserungen und eine Erhöhung des Mitarbeitendenbewusstseins motiviert, während bei Zertifizierten externe Kundenforderungen neben den unternehmensinternen Verbesserungen Hauptantreiber darstellen. Und auch bei ISO/IEC 27001 spielt der Wettbewerb als externer Faktor eine größere Rolle als bei Nicht-Zertifizierten.

Speziell bei ISO 9001 zeigt sich auch, dass zwar beide Gruppen unternehmensinterne Verbesserungen durch das Qualitätsmanagementsystem als wichtigste Wirkung wahrnehmen; Nicht-Zertifizierte werten sie aber höher als Zertifizierte. Ähnliche Muster zeigen sich auch beim Mitarbeitendenbewusstsein. Auch gewonnene Rechtsicherheit wird von Nicht-Zertifizierten tendenziell höher bewertet als von Zertifizierten – sowohl bei ISO 9001 als auch bei ISO 50001. Imagegewinne sind erwartungsgemäß deutlich stärker bei Zertifizierten zu verzeichnen als bei jenen, die ein Managementsystem implementieren, ohne ein Zertifikat zu erlangen (insbesondere zu beobachten bei ISO/IEC 27001).

SPEZIALTEIL: ISO/IEC 27001

Hintergrund

Im Zuge der Digitalisierung spielt die Informationssicherheit eine immer größere Rolle in den Unternehmen. Mit der ISO/IEC 27001 gibt es seit 2005 die Möglichkeit, ein entsprechendes international genormtes Managementsystem zu implementieren. Die Zertifizierung nach internationalen Normen bzw. Standards wie ISO/IEC 27001 gewinnt auch im Lichte der jüngsten europäischen und deutschen regulativen Initiativen an Bedeutung, bspw. im Rahmen des IT-Sicherheitskataloges und im Rahmen des Cybersecurity Acts (EU 2019/881 über die Zertifizierung von Cybersicherheit von Informations- und Kommunikationstechnik).

Wissenschaftliche Erhebungen zur Nutzung in Unternehmen gibt es jedoch weltweit bisher nur sehr wenige. Für Deutschland liegen noch gar keine branchenübergreifenden Daten vor. Diese Erhebung gibt somit erstmals Einblicke in die Implementierung und Zertifizierung nach ISO/IEC 27001.

Hoher Anstieg von ISO/IEC 27001 Zertifikaten weltweit – Nutzung vor allem im IKT Sektor

Laut letztem ISO-Survey gab es nach stetigem Anstieg seit 2006 zum 31. Dezember 2018 weltweit 31.910 gültige ISO/IEC 27001 Zertifikate.[13] Mit 1.057 Zertifikaten an 2.003 Standorten (Sites) liegt Deutschland weltweit an fünfter Stelle. Für ca. 40% der Zertifikate in Deutschland wurden sektorale Daten im Rahmen des ISO-Surveys erhoben. Demnach entfiel im Jahr 2018 jedes zweite ISO/IEC 27001-Zertifikat auf den IT-Sektor, gefolgt vom Dienstleistungssektor mit 23% und dem Maschinen- und Anlagenbau mit 5%.

Trotz der hohen Wachstumsraten bei den Zertifizierungen hat diese Norm 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 der 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

Definition Informationssicherheit

Als Informationssicherheit wird unter Bezug auf die Norm DIN EN ISO/IEC 27000:2017 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 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.

Managementsystems nach ISO/IEC 27001 in Deutschland.

Fehlender Druck von außen Hauptgrund ISO/IEC 27001 nicht zu implementieren

Die Motive zur Implementierung der ISO/IEC 27001 sowie die realisierten Wirkungen wurden bereits im Hauptteil des Reports beleuchtet. Die Umfrage hat jedoch auch gezielt diejenigen Unternehmen erfasst, die dieses Managementsystem nicht nutzen. Von diesen 114 Unternehmen hat mehr als jede vierte angegeben, die Norm gar nicht zu kennen (29%).

Von den Unternehmen, die die Norm kennen, plant jede fünfte, sie in Zukunft anwenden zu wollen. Von denen, die das *nicht* planen, begründen es die meisten damit, dass Kunden oder der Gesetzgeber ein ISMS nicht verlangen würden. Wenige Befragte begründen eine Nicht-Anwendung der Norm ISO/IEC 27001 damit, dass ISO 9001 die Informationssicherheit bereits abdeckt. Gut

Wieso wird ISO/IEC 27001 nicht genutzt?

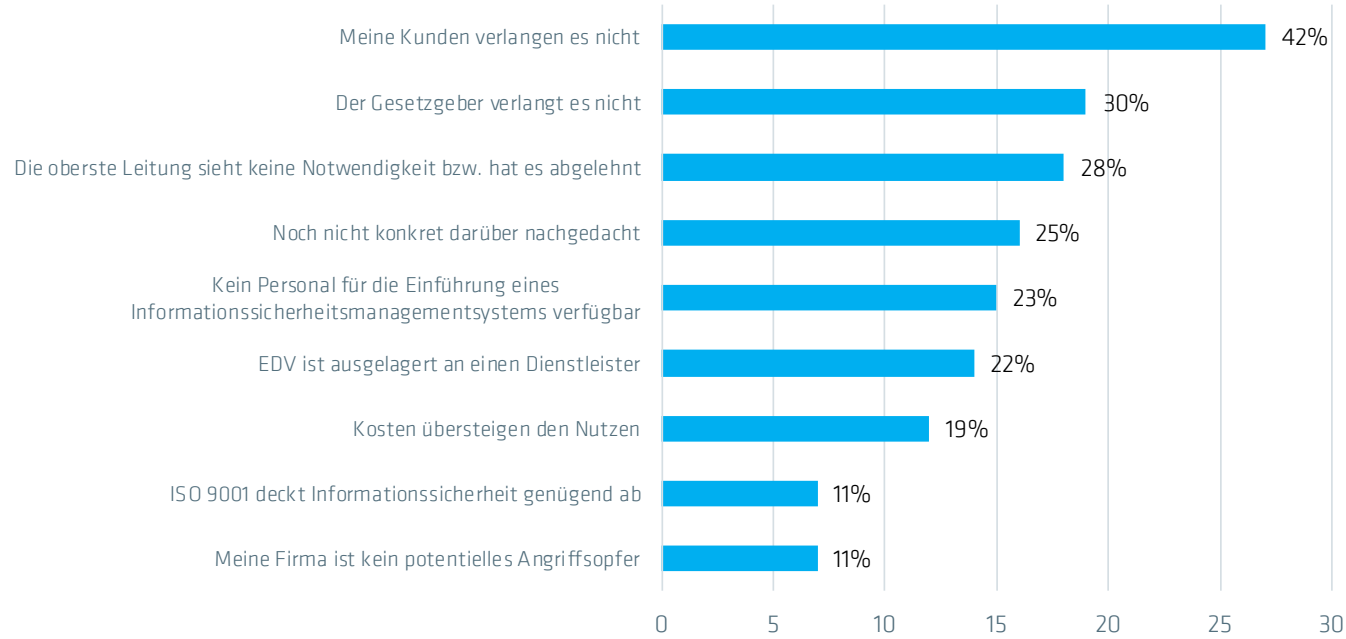


Abbildung 22: Gründe, die Norm ISO/IEC 27001 nicht zu implementieren. Basis bilden Unternehmen, die diese Norm kennen, aber nicht anwenden, N=64 (Mehrfachnennung möglich).

Gründe für Nichtzertifizierung ISO/IEC 27001

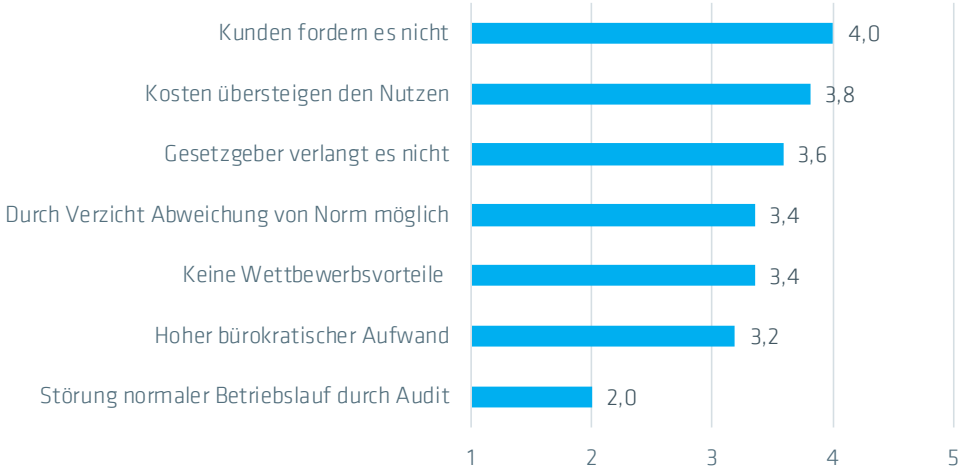


Abbildung 23: Gründe für Verzicht auf Zertifizierung nach ISO/IEC 27001. Basis bilden Unternehmen, die diese Norm anwenden aber nicht dafür zertifiziert sind (N=16-17). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

jede*r zehnte Befragte nennt hingegen als Grund, dass das eigene Unternehmen kein potenzielles Angriffsopfer sei. Insbesondere große und innovative Unternehmen sehen hier jedoch durchaus die Gefahr: innovative Unternehmen begründen eine Nicht-Anwendung nie mit fehlender Gefahr – vielmehr nennen 60% von ihnen mangelnden Druck von Kundenseite als Grund.

Fast jeder vierte Befragte gibt als Grund für die Nicht-Nutzung von ISO/IEC 27001 an, dass die Unternehmensspitze bzw. das Top-Management die Notwendigkeit einer Implementierung des Managementsystems nicht sieht. Auch der Mangel an qualifiziertem Personal wird auch von vielen Unternehmen als Hürde für die Einführung genannt. Ein Viertel der Unternehmen hat prinzipiell noch nicht über eine Implementierung der Norm ISO/IEC 27001 nachgedacht und 22% geben an, die eigene EDV an externe Dienstleister ausgelagert zu haben.

Unternehmen, die die Norm anwenden, sich aber nicht dafür zertifizieren lassen, nennen als Hauptgründe, dass die Kunden keine Zertifizierung fordern, die Kosten der Zertifizierung zu hoch sind und dass der Gesetzgeber die Zertifizierung nicht verlangt.

Aufwand und Expertise größte Schwierigkeiten bei der Implementierung von ISO/IEC 27001

Unternehmen, die ein ISMS nach ISO/IEC 27001 implementiert haben bzw. diesbezüglich zertifiziert sind, wurden zu den Hürden bei der Implementierung befragt. Der notwendige Zeitaufwand wird als größte Schwierigkeit gesehen, gefolgt von den hohen Kosten. Danach schließt sich die erforderliche externe Beratung an, die auch mit den weiteren Schwierigkeiten – der Komplexität der Norm-Inhalte und dem Mangel an interner Expertise des IT-Personals – in Zusammenhang gesehen werden kann.

Die hohen Kosten sowie die fehlende interne Expertise (in Form von qualifiziertem Personal) werden im Verarbeitenden Gewerbe als höhere Hürden erachtet als in den anderen Branchen. In den meisten Fällen werden die Hürden höher von Unternehmen bewertet, die diese Norm anwenden, ohne dafür zertifiziert zu sein. Dies trifft insbesondere bei der geringen Motivation der Mitarbeitenden und dem fehlenden Bekenntnis der obersten Leitungsebene zu.

Diverse Maßnahmen können bei der Verbreitung helfen

Falls eine Verbreitung der Norm ISO/IEC 27001 aktiv angestrebt wird, können verschiedene Maßnahmen dazu beitragen. Die Teilnehmenden konnten mögliche Maßnahmen, die die Anwendung der Norm ISO/IEC 27001 in Deutschland fördern könnten, hinsichtlich ihrer Eignung bewerten. Von den anwendenden Unternehmen der Norm werden alle vorgeschlagenen Maßnahmen (mit Mittelwerten zwischen 3,6 und 4,1) als sinnvoll eingeschätzt. Die Bereitstellung eines Handlungsleitfadens, insbesondere für KMU, wird dabei als besonders hilfreich eingeschätzt. KMU sehen

Schwierigkeiten bei ISO/IEC 27001

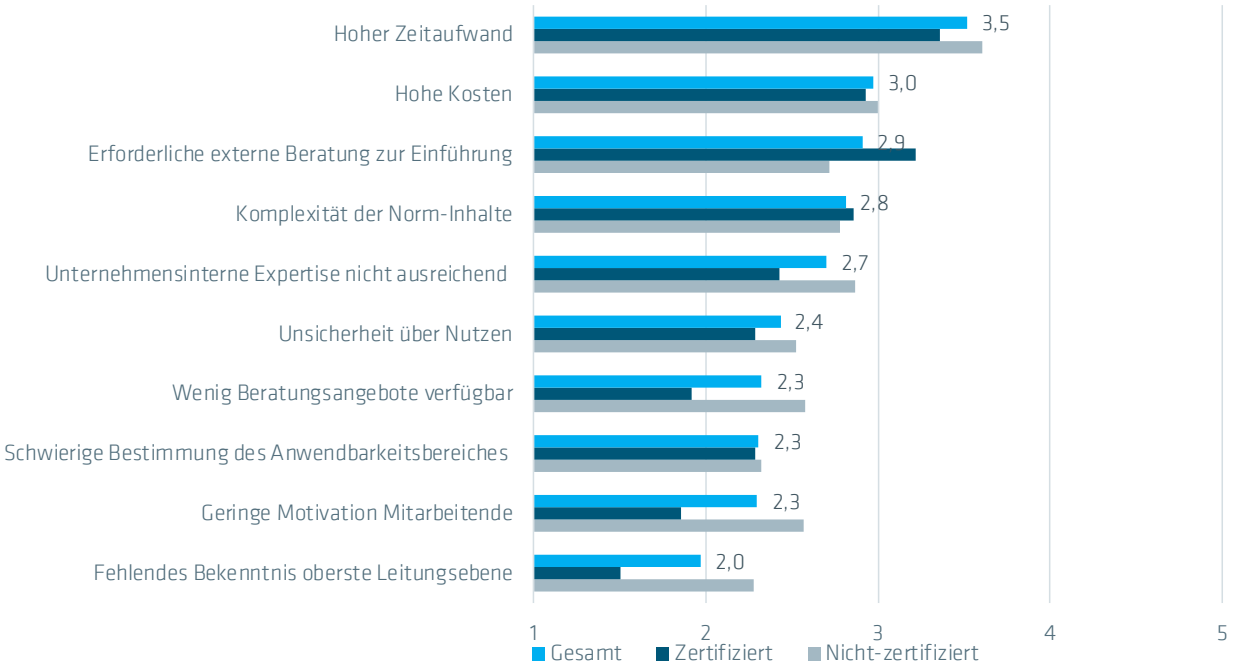


Abbildung 24: Durchschnittliche Einschätzung der Schwierigkeiten bei der Implementierung und Zertifizierung eines ISMS nach ISO/IEC 27001. Basis bilden Unternehmen, die diese Norm anwenden ohne Zertifizierung (N=19-23) und mit Zertifizierung (N=12-14). Bewertungsskala: 1 (trifft gar nicht zu) bis 5 (trifft voll zu).

eine hohe finanzielle Hürde bei der Einführung eines ISMS nach ISO/IEC 27001. Erwartungsgemäß erachten sie finanzielle Unterstützungen speziell für diese Zielgruppe als sehr sinnvoll. Dies betrifft sowohl die finanzielle Unterstützung für Beratungsdienstleistungen (MW 4,3 versus 3,4 bei großen Unternehmen) als auch für die Zertifizierung und deren Aufrechterhaltung.

Mit Mittelwerten von 3,6 bzw. sogar 3,9 werden die Forderung eines Nachweises vom Gesetzgeber bzw. der Kunden auch als sinnvolle Maßnahme von allen befragten anwendenden Unternehmen der ISO/IEC 27001 bewertet, wobei es keine großen Unterschiede hinsichtlich Unternehmensgröße oder Branche gab. Allerdings erachten nach ISO/IEC 27001 zertifizierte Unternehmen dies insgesamt als sinnvollere Maßnahme als Unternehmen, die diese Norm ohne Zertifizierung anwenden (MW 4,2 vs. 3,3 bei Forderung seitens Gesetzgeber und MW 4,5 vs. 3,5 bei Forderung seitens Kunden).

Unternehmen, die die ISO/IEC 27001 zwar kennen, aber nicht anwenden, bewerten den Nutzen eines Handlungsleitfadens besonders hoch, gefolgt von Schulungen und finanziellen Unterstützungen. Hingegen bewerten sie Forderungen seitens der Kunden bzw. des Gesetzgebers als weniger verbreitungsfördernd als jene Unternehmen, die die Norm ISO/IEC 27001 bereits anwenden.

Unternehmen unterschiedlich stark von Informationssicherheitsvorfällen betroffen

Alle teilnehmenden Unternehmen wurden gefragt, ob es schon einmal einen Vorfall gab, welcher die Vertraulichkeit, Verfügbarkeit oder Integrität wichtiger Informationen beeinträchtigt hat. Ein Viertel der Befragten beantwortet dies mit Ja, wobei es Unterschiede nach Unternehmensgröße gibt. Während nur jedes zehnte kleine Unternehmen diese Frage bejaht, ist dies bei großen Unternehmen bei mehr als jedem zweiten der Fall.[14]

Vergleicht man die Gruppen der Anwender und Nicht-Anwender eines Managementsystems nach ISO/

Maßnahmen zur Verbreitung von ISO/IEC 27001

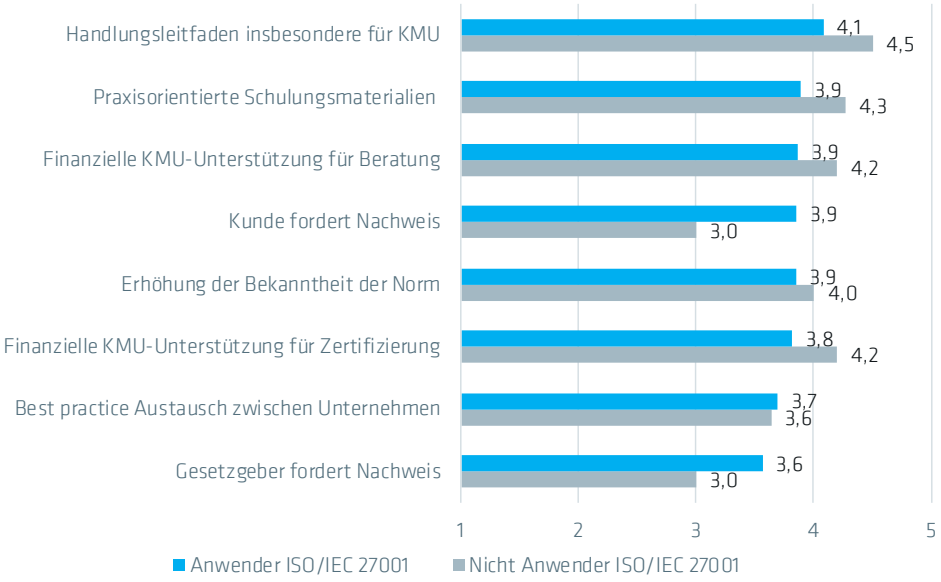


Abbildung 25: Bewertung von Maßnahmen zur Förderung der Verbreitung der Norm ISO/IEC 27001 in Deutschland. Basis bilden Unternehme, die diese Norm anwenden (N=35-40) sowie Unternehmen, die diese Norm kennen, aber nicht anwenden (N=10-12). Bewertungsskala: 1 (gar nicht sinnvoll) bis 5 (sehr sinnvoll).

IEC 27001 wird ersichtlich, dass Anwender häufiger berichten, in der Vergangenheit von Informationssicherheitsvorfällen betroffen gewesen zu sein, als jene, die diese ISMS-Norm nicht anwenden. Während nur jeder vierte Nicht- Anwender von einem Vorfall in dem Unternehmen in der Vergangenheit berichtet, tun dies 38% in der Gruppe der Unternehmen, die ISO/IEC 27001 anwenden. Die Motive hinter der Implementierung des Managementsystems nach ISO/IEC 27001 haben in diesem Zusammenhang jedoch gezeigt, dass konkrete Vorfälle kein bedeutender Antrieb für die Befragten sind, sondern vielmehr strategische Motive vorliegen.

Fazit und Ausblick

Angesichts der wachsenden Bedeutung der Informationssicherheit und steigender Risiken potenzieller Angriffe, welche die Informationssicherheit gefährden können,[15] werden ISMS nach ISO/IEC 27001 in Deutschland nur sehr verhalten implementiert. Die Erhebung konnte erste Einblicke in Motive, Wirkungen und Hürden ermöglichen. Die Ergebnisse weisen darauf hin, dass die Norm zwar vielen bekannt ist, aber oftmals keine Notwendigkeit gesehen wird, diese zu implementieren, da dies (noch) nicht aktiv von interessierten Kreisen gefordert wird. Auch wird der mit der

Vorkommen von Informationssicherheitsvorfällen

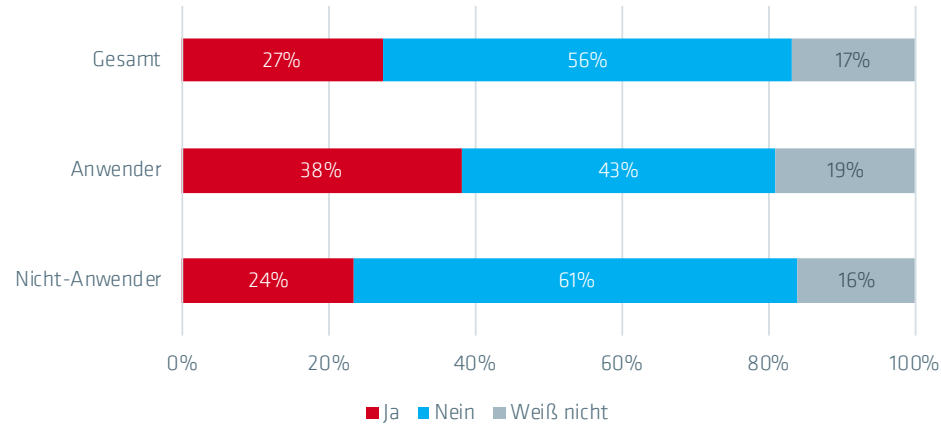


*Abbildung 26: Vorkommen von Vorfällen, welcher die Vertraulichkeit, Verfügbarkeit oder Integrität von wichtigen Informationen beeinträchtigt hat (Cyber-Angriff, Einbruch, Innentäter, Datenschutz). Basis: alle Umfrageteilnehmer*innen, N= 161 (Anwender eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001 (N=42) und Nicht-Anwender (N=119)).*

Einführung verbundene Aufwand als hindernd angesehen.

Eine Analyse der Wirkung von ISO/IEC 27001 zeigt jedoch, dass das ISMS dazu beitragen kann, die Informationssicherheit in dem Unternehmen zu erhöhen und die Gefahr von Informationssicherheitsvorfällen zu reduzieren, u.a. durch eine Erhöhung des Mitarbeitendenbewusstseins in Bezug auf Informationssicherheit. Insgesamt ist die allgemeine Zufriedenheit hinsichtlich der Kosten-Nutzen-Relation der ISO/IEC 27001 unter den befragten zertifizierten Unternehmen hoch.

Möglichkeiten zur Unterstützung der weiteren Verbreitung werden sowohl in finanziellen und informativen Maßnahmen als auch durch Forderungen des Nachweises von Kunden oder des Gesetzgebers gesehen.

Spezial-Studie zu ISO/IEC 27001

Aufbauend auf den ersten Erkenntnissen dieser Erhebung wurden Anfang 2020 125 nach ISO/IEC 27001 zertifizierte Unternehmen gesondert befragt. Die Ergebnisse dieser Studie werden in einem separaten QI-FoKuS Report (Vol. 2) veröffentlicht.

DIE ROLLE VON ZERTIFIZIERUNG, AKKREDITIERUNG UND KUNDENAUDITS

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 Marktteilnehmern 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 für die am weitesten verbreitete Managementsystem-Norm ISO 9001 sowie für ISO/IEC 27001 für Informationssicherheit 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. Der folgende Abschnitt beleuchtet die Ergebnisse im Detail.

Kompetenz und deren Nachweis 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. Diese hohe Bedeutung spiegelt sich auch in der tatsächlichen Zertifizierungspraxis wider: 99% der Antwortenden geben an, dass mindestens eines ihrer Zertifikate von einer akkreditierten Zertifizierungsstelle ausgestellt wurde.

Daran anknüpfend ist das zweitwichtigste Kriterium bei der Auswahl der Zertifizierungsstelle die Fachkompetenz der Auditor*innen, im Falle der ISO 9001 gefolgt von der Reputation der Zertifizierungsstelle. Auch spezielles Fachwissen für die Branche des jeweiligen Kunden spielt eine vergleichsweise große Rolle.

Kriterien für die Wahl der Zertifizierungsstelle

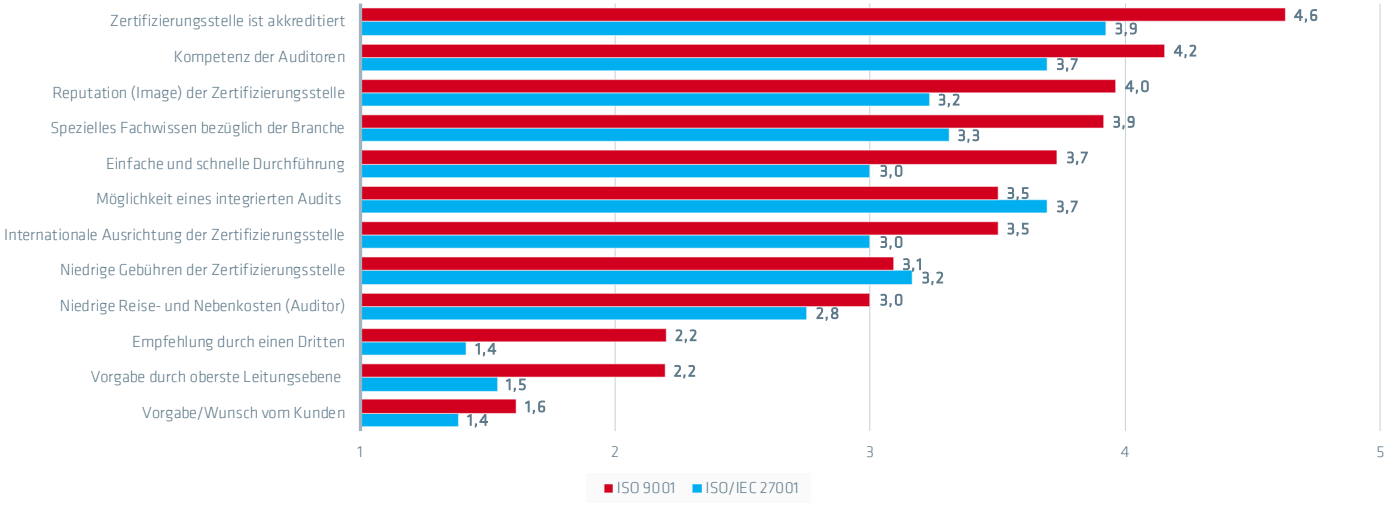


Abbildung 27: Durchschnittliche Bewertung der Kriterien bei der Wahl von Zertifizierungsstellen für die Normen ISO 9001 (N=76-87) und ISO/IEC 27001 (N=12-13). Bewertungsskala: 1 (überhaupt nicht wichtig) bis 5 (sehr wichtig).

Während es den Teilnehmenden daneben auch wichtig ist, dass die Zertifizierung schnell und einfach durchgeführt wird, sind die Kosten der Zertifizierung (Gebühren der Zertifizierungsstelle und Neben- und Reisekosten) hingegen weniger wichtig. Gerade stark exportorientierte Unternehmen mit mehr als der Hälfte des Umsatzes im Ausland, die nach ISO 9001 zertifiziert sind, bewerten die internationale Ausrichtung der Zertifizierungsstelle als besonders wichtig (MW: 4,2 gegenüber MW von 2,5-3,4 bei Vergleichsgruppen). Die geringste Bedeutung bei der Wahl der Zertifizierungsstelle wird von den Teilnehmenden der Empfehlung bzw. Vorgabe von Dritten beigemessen.

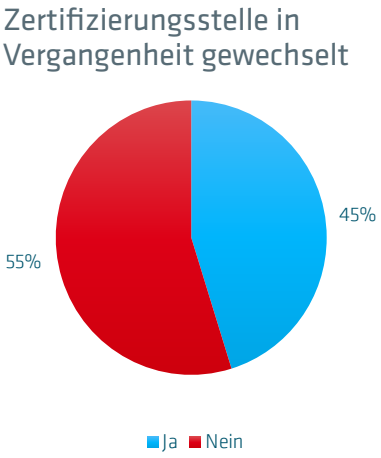
Unternehmen nutzen unterschiedliche ISO-Managementsysteme häufig parallel. Insbesondere anwendende Unternehmen der ISO/IEC 27001 nennen die Möglichkeit eines integrierten Audits als wichtiges Kriterium bei der Wahl ihrer Zertifizierungsstelle. 60% sind bereits nach ISO 9001 zertifiziert, jeder zweite nach ISO 14001. Durch integrierte Audits durch eine Zertifizierungsstelle können Unternehmen von einheitlichen Strukturen profitieren, Ressourcen bündeln und Synergien nutzen.

Fachliche Unzufriedenheit Hauptgrund für Wechsel der Zertifizierungsstelle

Für den Wechsel einer Zertifizierungsstelle kann es verschiedene Gründe geben. 45% der 104 Teilnehmenden, die hierzu Auskunft gaben, haben schon einmal die Zertifizierungsstelle in der Vergangenheit gewechselt. Als Grund nennen die Teilnehmenden am häufigsten die Unzufriedenheit mit der fachlichen Leistung des Zertifizierers. Dicht dahinter folgt der Wunsch, die Zertifizierungen im Unternehmen auf einen Anbieter zu bündeln. Obwohl Kosten bei der Auswahl der Zertifizierungsstelle wie oben beschrieben nicht zu den wichtigsten Gründen gehören, so können sie dennoch Grund für einen Wechsel sein: 40% der Antwortenden nennen dies. Für 17% boten unterschiedliche Auslegungen der Anforderungen aus der betreffenden Managementsystem-Norm durch die Auditoren Grund zum Wechsel der Zertifizierungsstelle.

Hohe Bedeutung von Akkreditierung und internationalen Anerkennungsabkommen

Gerade im internationalen Warenverkehr ist die gegenseitige Anerkennung von Zertifikaten eine wichtige Handelserleichterung. Anerkennungsabkommen für Akkreditierungen spielen daher eine bedeutende Rolle. Jedoch kennt nur jeder zweite der Befragten dieses Instrument (56% von n=138). Ob es ein Anerkennungsabkommen für ihre Zertifikate gibt, können indes nur 64% bestätigen, jeweils ca. 18% verneinen dies oder geben an, es nicht zu wissen. Die



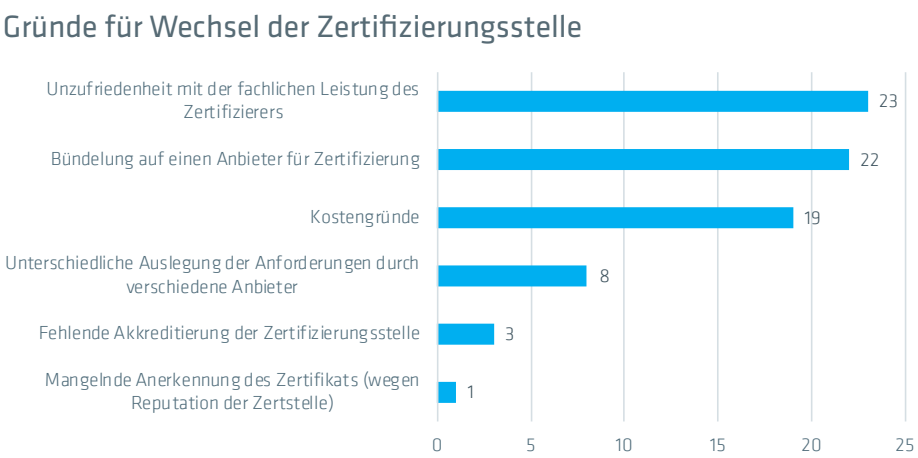


Abbildung 28 und 29: Anteil von Teilnehmenden, die die Zertifizierungsstelle in der Vergangenheit schon einmal gewechselt haben (links, N=104) und Anzahl der Nennungen zu Gründen für den Wechsel der Zertifizierungsstelle (rechts), N=47 (Mehrfachnennung möglich).

Befragten bestätigen jedoch die Wirkung solcher Abkommen: von 40 Befragten stimmen 78% zu, dass sie zu einer besseren Anerkennung der Zertifikate im Ausland beitragen.

Kundenaudits mit hoher Relevanz in der Praxis

Neben der Durchführung von internen Audits (erste Seite) und der Auditierung durch unabhängige Externe (dritte Seite/Zertifizierung) werden Unternehmen in der Praxis oft auch von deren Kunden (zweite Seite) auditiert. Von 134 teilnehmenden Unternehmen unserer Umfrage gibt jede zweite an, dass sie auch von Kunden auditiert wird. Dies ist insbesondere bei den Qualitätsmanagement-Normen der Fall: Neben ISO 9001 (51 Teilnehmende) betrifft das auch die branchenspezifischen Managementsysteme im Medizinproduktesektor und der Automobilbranche (12 und 15). Auch Umweltmanagementsysteme nach ISO 14001 und Arbeits- und Gesundheitsschutz-Managementsysteme nach ISO 45001 (BS OHSAS 18001) werden von Kunden der befragten Unternehmen auditiert (20 und 15 Fälle).

Dabei ersetzen Kundenaudits in den meisten Fällen keine Zertifikate, umgekehrt geben jedoch 27% der

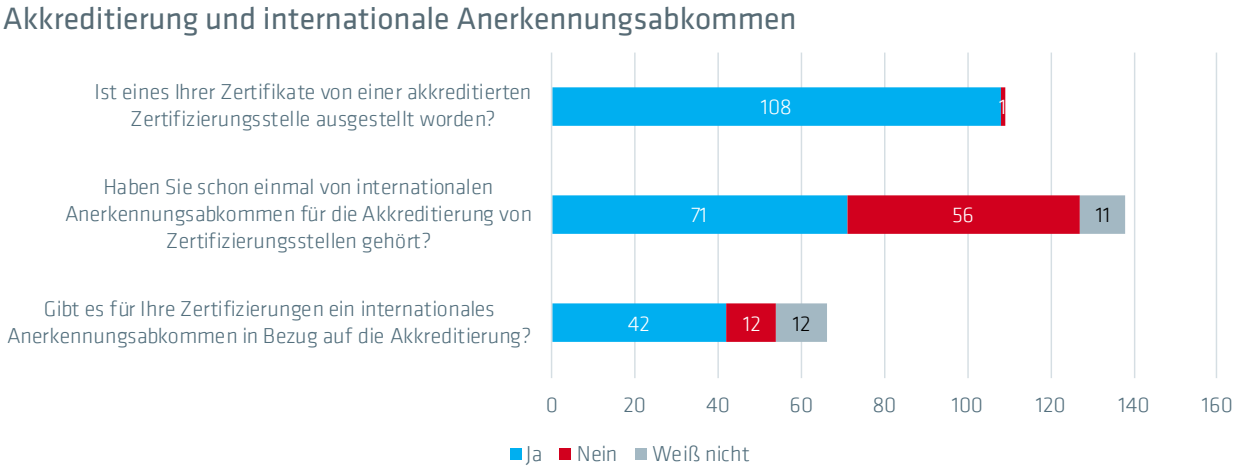


Abbildung 30: Anzahl von Teilnehmenden, die angeben ob ihr Unternehmen ein Zertifikat hält, das von einer akkreditierten Zertifizierungsstelle ausgestellt worden ist (N=109), ob sie internationale Anerkennungsabkommen für Akkreditierung kennen (N=138) und ob für die Zertifizierungen ihrer Unternehmen ein internationales Anerkennungsabkommen existiert (N=66).

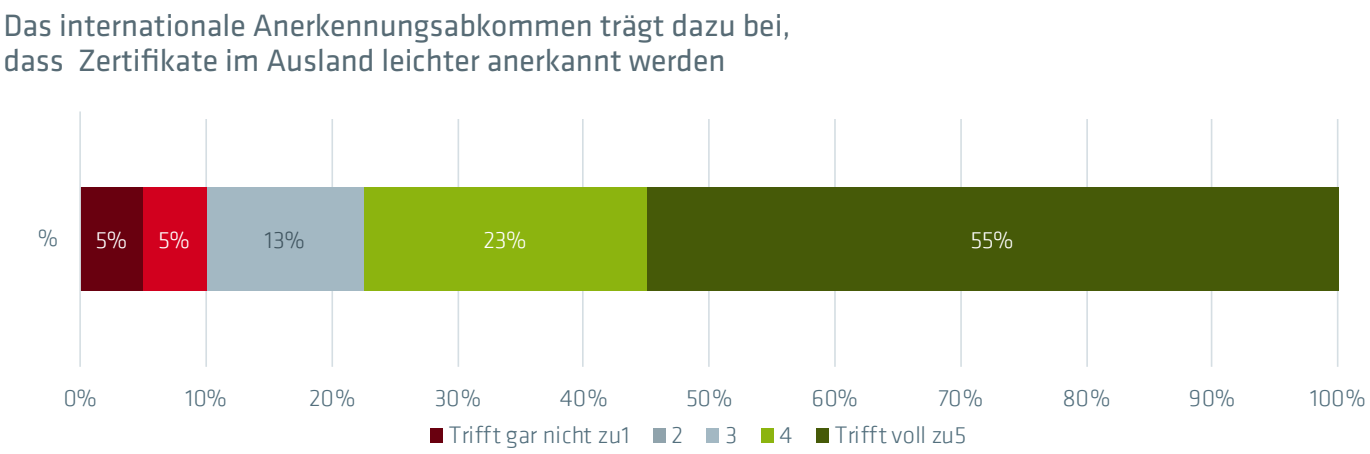


Abbildung 31: Einschätzung ob Anerkennungsabkommen dazu beitragen, dass Zertifikate im Ausland leichter anerkannt werden (N=40).

Teilnehmenden an, dass Zertifikate mindestens teilweise die Kundenaudits ersetzen. Für 69% der Antwortenden vereinfacht eine vorhandene Zertifizierung den Kunden-audit-Prozess. Die Anforderungen der Kundenaudits werden tendenziell als strenger beschrieben als die der Zertifizierung: 63% der Befragten geben an, dass die Anforderungen der Kundenaudits über die Anforderungen der Zertifizierer hinausgehen.

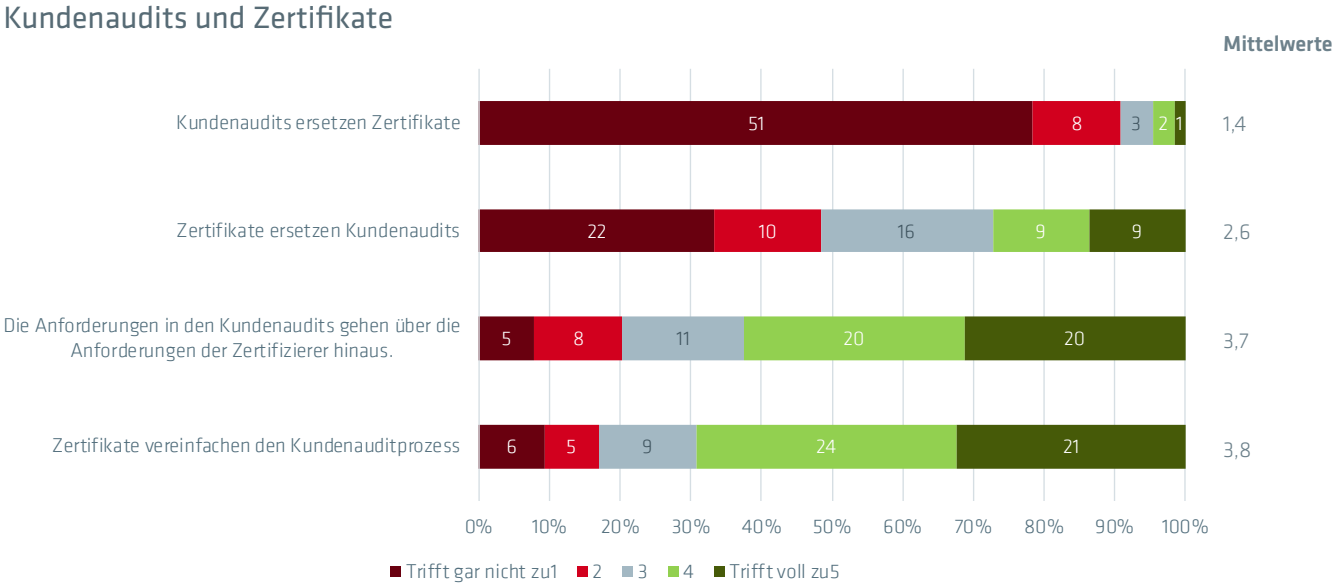


Abbildung 32: Verhältnis von Kundenaudits und Zertifizierung (N=64-66). Bewertungsskala: 1 (trifft gar nicht zu) und 5 (trifft voll zu).

FAZIT

Die Studie beleuchtet die Nutzung und Wirkungen von Managementsystemen in Deutschland und setzt dabei einen Schwerpunkt auf die Konformitätsbewertung. Die teilnehmenden Unternehmen wurden hierbei zu den weit verbreitetsten genormten Managementsystemen befragt. Die Erhebung ermöglicht somit Einblicke nicht nur zu den etablierten Normen wie ISO 9001 oder ISO 14001, sondern auch zu jüngeren wie ISO 50001 für Energiemanagementsysteme und erstmals branchenübergreifend auch ISO/IEC 27001 für Informationssicherheitsmanagementsysteme. Die Daten zeigen, dass die Nutzung von zwei oder mehr Managementsystemen weit verbreitet ist und Unternehmen dabei offenbar von Synergien Gebrauch machen können. Es zeichnet sich nicht nur ein differenziertes Bild verschiedener Hauptmotive und -wirkungen, vielmehr erlauben die Daten insbesondere auch die systematische Unterscheidung der Bewertungen zertifizierter und nicht-zertifizierter Unternehmen.

Für die noch wenig verbreitete Managementsystem-Norm für Informationssicherheit ISO/IEC 27001 zeigen sich die anwendenden Unternehmen zufrieden hinsichtlich ihres Beitrags, die Informationssicherheit in dem Unternehmen zu erhöhen und die Gefahr von Informationssicherheitsvorfällen zu reduzieren. Hürden werden jedoch insbesondere im mit der Implementierung verbundenen Aufwand gesehen. Falls eine weitere Verbreitung dieser Managementsystem-Norm gewünscht ist, können dafür die von den Teilnehmenden als sinnvoll erachteten Maßnahmen ergriffen werden, welche insbesondere darauf abzielen, mehr Informationen und finanzielle Unterstützung bei der Implementierung und Zertifizierung besonders für KMUs bereitzustellen.

Einen Schwerpunkt der Studie stellt die Betrachtung der verschiedenen Parteien dar, die die Konformitätsbewertung durchführen können. Die Ergebnisse unterstreichen die hohe Bedeutung kompetenter Zertifizierungsstellen sowie die wichtige Rolle der Akkreditierung in diesem Bereich – auch wenn sich zeigt, dass vielen Teilnehmenden der Umfrage die zugrundeliegenden Mechanismen wie die internationalen Anerkennungsabkommen für Akkreditierung nicht bekannt sind. Weiterhin wird die wichtige Stellung von Lieferanten- bzw. Kundenaudits in der unternehmerischen Praxis bestätigt.

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 u.a. das → *Managementsystem* und die Kompetenz des eingesetzten Personals der Konformitätsbewertungsstelle.[16]
- **Anerkennungsabkommen**: Zentrales Ziel des internationalen Netzwerks der Akkreditierung ist deren gegenseitige Anerkennung. Dies fördert die Anerkennung der Kompetenz akkreditierter Stellen und dient damit der weltweiten Akzeptanz ihrer Dienstleistungen und Ergebnisse. Ermöglicht wird dies durch multilaterale Vereinbarungen und Abkommen der europäischen bzw. internationalen Akkreditierungsorganisationen (EA MLA, IAF MLA und ILAC MRA)[17]. Der Beitritt zu diesen Abkommen verlangt die Einhaltung gemeinsamer Grundsätze und Regularien durch die Akkreditierungsstellen, die Unterzeichner dieser Abkommen sind.
- **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.[18] 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.[19]
- **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 wirksam sind und in der Praxis befolgt werden, so dass die Organisation die in der Managementsystem-Norm festgelegten Anforderungen erfüllt.[20]

ABKÜRZUNGEN

DAkkS: Deutsche Akkreditierungsstelle

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

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. Weiterhin danken wir der DGQ sowie den Verbänden VCI, VDA und dem Dachverband BDI sowie diversen Zertifizierungsstellen für die Bekanntmachung der Umfrage unter ihren Mitgliedern bzw. Kund*innen.

Gedankt sei auch Philipp Heß (TU Berlin), dem VdTÜV sowie den Interviewpartner*innen in der Vorbereitung der Befragung.

ANMERKUNGEN UND REFERENZEN

[1] *Blind, K. (2015). From standards to quality infrastructure - A review of impact studies and an outlook. In: P. Delimatsis (Hrsg.), The law, economics and politics of international standardization; Cambridge University Press.*

[2] *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 sowie Power, D., & Terziovski, M. (2007). Quality audit roles and skills: Perceptions of non-financial auditors and their clients. Journal of operations management, 25(1), 126-147.*

[3] *ISO 9000:2015*

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

[5] *Die Erhebung bezieht sich auf die Anzahl der gültigen Zertifikate von ausgewählten ISO-Management-Normen, die von Zertifizierungsstellen ausgestellt wurden, die von Mitgliedern des Internationalen Akkreditierungsforums (IAF) akkreditiert wurden.*

[6] *Was die relative Zahl der jeweiligen Zertifizierungen angeht (also die Zertifizierungen bezogen auf die Anzahl der Unternehmen im Land), liegt Deutschland jedoch deutlich hinter Ländern wie Italien oder Spanien (siehe dazu Heras- Saizarbitoria, I., & Boiral, O. (2013). ISO 9001 and ISO 14001: towards a research agenda on management system standards. International Journal of Management Reviews, 15(1), 47-65.) Für das Qualitätsmanagement speziell für die Automobilindustrie nach IATF 16949 (zuvor ISO/TS 16949) liegen keine Daten aus dem ISO Survey 2018 vor, da es sich seit 2016 um einen IATF (International Automotive Task Force) Standard handelt. Im Bereich Arbeitsschutzmanagement beziehen sich die Zahlen nur auf die Norm ISO 45001, die seit dem Jahr 2018 den Standard BS (British Standard) OHSAS 18001 – jedoch für zertifizierte Unternehmen mit einer Übergangsfrist bis 2021 - abgelöst hat.*

[7] *Das 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. Vgl. ISO (2019), The ISO Survey, abrufbar unter: https://www.iso.org/the-iso-survey.html*

[8] *Vgl. ISO Survey (2019). Der Rückgang der im Jahr 2018 erfassten gültigen Zertifikate gegenüber dem Vorjahr erklärt sich durch eine Änderung der Erhebungsmethode im Rahmen des jährlichen ISO Surveys.*

[9] *Im Folgenden „Verarbeitendes Gewerbe" genannt.*

[10] *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.*

[11] *Vgl. Karcher, P., & Jochem, R. (2015). Success factors and organizational approaches for the implementation of energy management systems according to ISO 50001. The TQM Journal, 27(4), 361-381. doi:10.1108/TQM-01-2015-0016 sowie Wulandari, M., Laskurain, I., Casadesús, M., & Heras-Saizarbitoria, I. (2015). Early Adoption of ISO 50001 Standard: An Empirical Study. In A. Chiarini (Ed.), Sustainable Operations Management: Advances in Strategy and Methodology (pp. 183-202). Cham: Springer International Publishing.*

[12] *Noch stärker wird dieser Effekt von Nutzenden des Qualitätsmanagementsystems für Medizinprodukte nach ISO 13485 erfahren (4,1). Diese stellen generell tendenziell stärkere Wirkungen fest als Anwender des allgemeinen Qualitätsmanagements nach ISO 9001. Dies betrifft*

besonders die positiven Wirkungen auf den Umsatz (sowohl stärkste Wirkung mit 4,7 für ISO 13485 als auch höchste Differenz zu ISO 9001 mit nur 3,0); (n=5-9).

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

[14] *Ähnlich dazu gaben auch im Rahmen der Cyber-Sicherheitsumfrage der Allianz für Cyber-Sicherheit 2018 43% der großen und 26% der mittelständischen Unternehmen an, im Jahr 2018 von Cyber-Sicherheits-Vorfällen betroffen gewesen zu sein. 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*

[15] *ebenda*

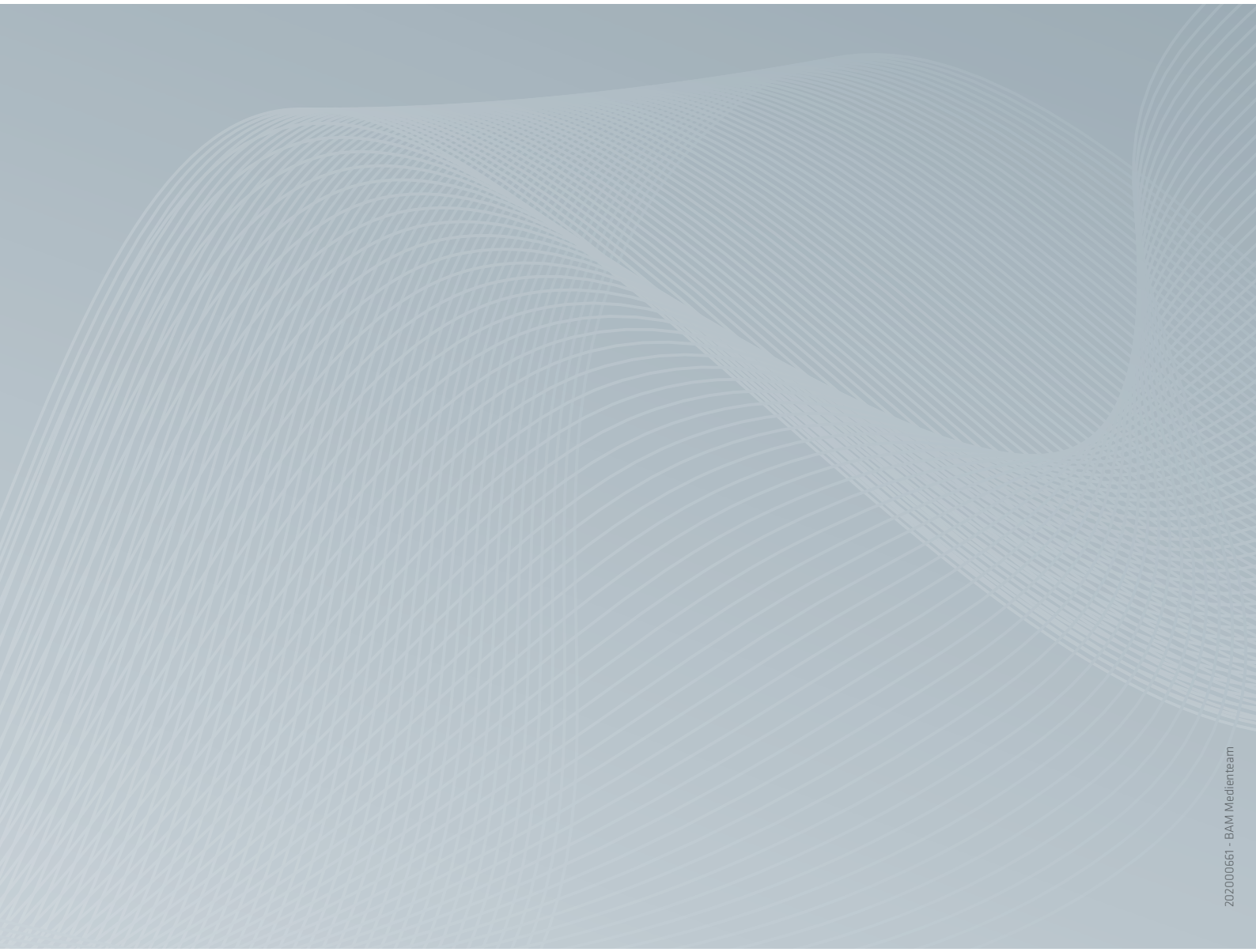
[16] *https://www.dakks.de/content/was-ist-akkreditierung*

[17] *https://www.dakks.de/content/internationales-netzwerk*

[18] *ISO 9000:2015*

[19] *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*

[20] *Vgl. Castka, P., & Corbett, C. J. (2015).*



202000661 - BAM Medienteam

BAM

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

Info@bam.de
www.bam.de