einfachISO

DIE ESSENZIELLE ISO 27001 CHECKLISTE FÜR IHRE ZERTIFIZIERUNG

Ihr Leitfaden für den Compliance-Erfolg

Kapitel 1

Ihr Weg zur ISO 27001-Zertifizierung

Willkommen auf der Reise

Willkommen in „Die Essenzielle ISO 27001 Checkliste für Ihre Zertifizierung“. Dieses E-Book ist Ihr Leitfaden zum Verständnis und Erreichen der prestigeträchtigen ISO 27001-Zertifizierung, *dem* Maßstab für Exzellenz im Informationssicherheitsmanagement.

einfachISO

Was ist ISO 27001?

ISO 27001 ist mehr als nur ein Standard; Es handelt sich um ein Framework für den Aufbau eines robusten Informationssicherheits-Managementsystems (ISMS), das Ihre Daten schützt und den Weiterbetrieb Ihres Unternehmens im Krisenfall gewährleistet.

Dieser internationale Standard beschreibt die Anforderungen für die Erstellung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines ISMS.

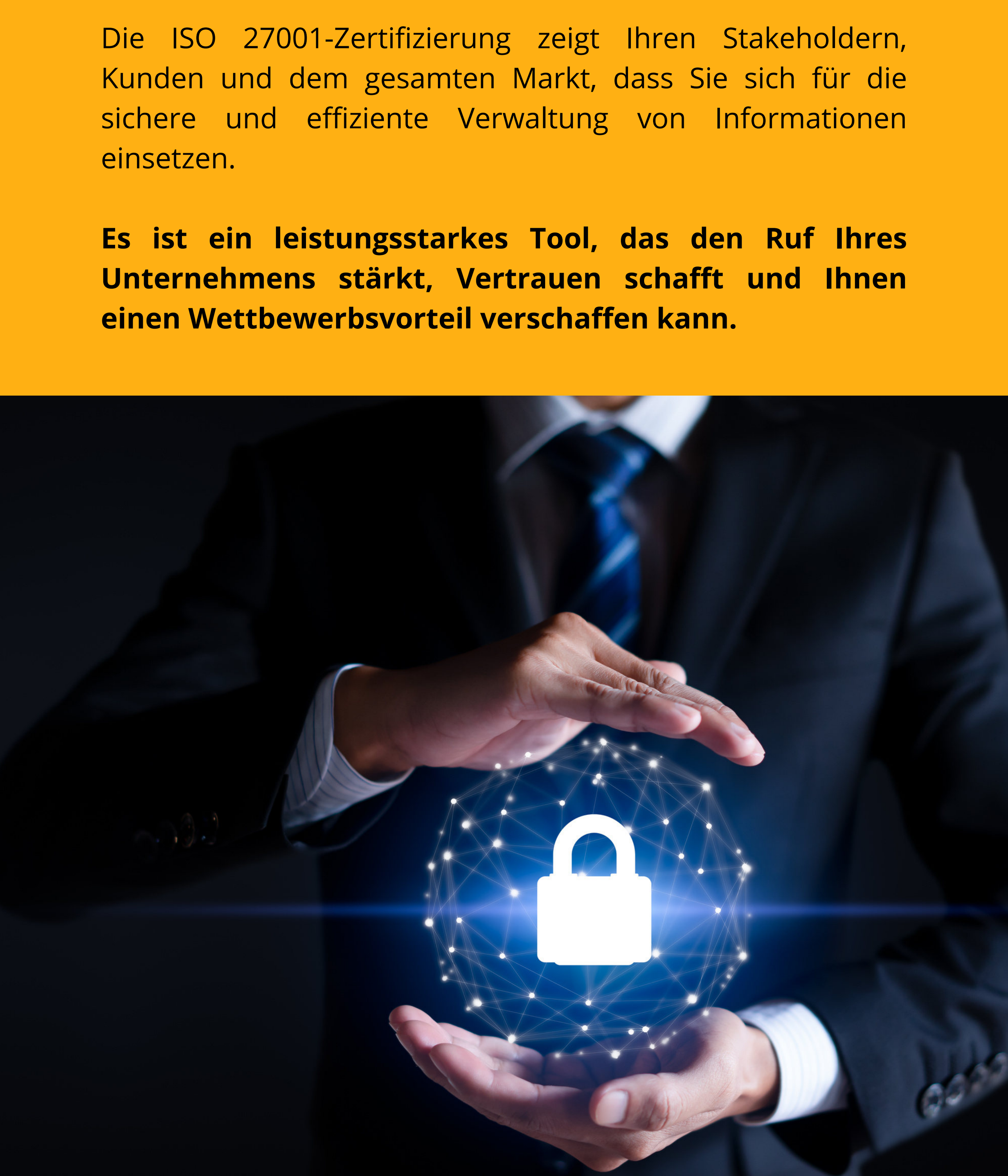
Es enthält auch Anforderungen zur Bewertung und Behandlung von Informationssicherheitsrisiken, die auf die Bedürfnisse Ihrer Organisation zugeschnitten sind.

Warum ist das Interessant für Sie?

In unserem digitalen Zeitalter sind Informationen Herz und Nieren vieler Unternehmen. Der Schutz dieser Informationen ist nicht nur oft eine behördliche Anforderung, sondern eine geschäftliche Notwendigkeit.

Die ISO 27001-Zertifizierung zeigt Ihren Stakeholdern, Kunden und dem gesamten Markt, dass Sie sich für die sichere und effiziente Verwaltung von Informationen einsetzen.

Es ist ein leistungsstarkes Tool, das den Ruf Ihres Unternehmens stärkt, Vertrauen schafft und Ihnen einen Wettbewerbsvorteil verschaffen kann.



einfachISO

Wir begleiten Sie bei jedem Schritt

Dieses E-Book führt Sie durch den gesamten Prozess zur ISO 27001-Zertifizierung.

Wir legen zunächst den Grundstein und helfen Ihnen, den Standard und seine Relevanz für Ihr Unternehmen zu verstehen.

Von dort aus gehen wir Schritt für Schritt vor und decken alles von der ersten Bewertung über das Risikomanagement bis hin zu den letzten Vorbereitungen für die Zertifizierung ab.

Jeder Abschnitt ist so gestaltet, dass er umsetzbare Einblicke und praktische Tipps bietet, um sicherzustellen, dass Sie für den Weg zur Zertifizierung gut gerüstet sind.

Ganz gleich, ob die ISO 27001 ganz neu für Sie ist oder Sie Ihr bestehendes ISMS verfeinern möchten, dieser Leitfaden ist eine unschätzbar wertvolle Ressource. Lassen Sie uns gemeinsam auf diese Reise gehen und das volle Potenzial Ihres Informationssicherheitsmanagements ausschöpfen.

Kapitel 2

ISO 27001 verstehen

ISO 27001 ist nicht nur einfach ein Regelwerk. In ihrem Kern steht die Philosophie der kontinuierlichen Verbesserung bei der Verwaltung und dem Schutz von Informationen.

Dieses Kapitel befasst sich mit den Schlüsselkonzepten und -prinzipien, die die Grundlage dieses Standards bilden, und vermittelt Ihnen das Wissen, das Sie benötigen, um seine Bedeutung und Anwendbarkeit für Ihr Unternehmen vollständig zu verstehen.

Schlüsselkonzepte der ISO 27001

Im Mittelpunkt der ISO 27001 stehen folgende Kernkonzepte:

Risikobasierter Ansatz

Im Mittelpunkt der ISO 27001 steht das Konzept des Risikomanagements für Ihre Informationsressourcen.
Dabei geht es darum, potenzielle Risiken zu identifizieren und Maßnahmen zu implementieren, um diese zu mindern.

Prozessorientierung

Der Standard betont einen prozessbasierten Ansatz für die Einrichtung, Implementierung, den Betrieb, die Überwachung, die Überprüfung, die Wartung und die Verbesserung Ihres ISMS.

einfachISO

Ständige Verbesserung

ISO 27001 fordert eine kontinuierliche Verbesserung des ISMS und stellt sicher, dass sich Ihr Informationssicherheits-management sich mit ändernden Bedrohungen und Geschäftsanforderungen weiterentwickelt.

Führungsverpflichtung

Effektive Informationssicherheit erfordert das Engagement und die Führung des Top-Managements, um sicherzustellen, dass die Sicherheitsrichtlinien mit den Geschäftszielen übereinstimmen.

Informations- ≠ IT-Sicherheit

Anstatt Informationssicherheit als technisches Problem zu betrachten, sieht die ISO 27001 sie als integralen Bestandteil der Unternehmensführung.

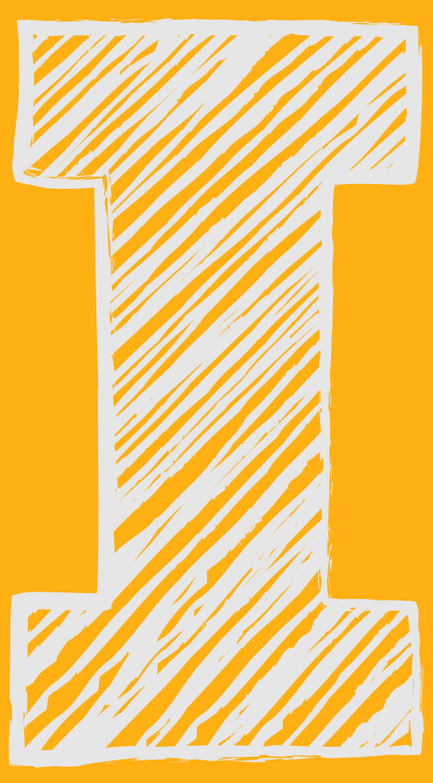
einfachISO

Schutzziele

Der Standard konzentriert sich auf diese drei Standardziele, um einen umfassenden und anpassungsfähigen Ansatz zur Informationssicherheit sicherzustellen:

Vertraulichkeit

Sicherstellen, dass Informationen nur für zugriffsberechtigte Personen zugänglich sind.



Integrität

Nur autorisierte Personen können Informationen ändern.

Verfügbarkeit

Sicherstellen, dass autorisierte Benutzer bei Bedarf Zugriff auf Informationen und zugehörige Assets haben.

Umfang und Anwendbarkeit des Standards

Die ISO 27001 ist universell anwendbar, unabhängig von der Größe, Art oder Branche Ihrer Organisation.

Sie ist relevant für Organisationen, die sensible Daten aller Art verarbeiten, von kleinen Unternehmen bis hin zu multinationalen Konzernen, in jedem Sektor, einschließlich öffentlicher, privater und gemeinnütziger Organisationen.

Ein Standardkonformes ISMS kann an die spezifischen Bedürfnisse und das Risikoprofil Ihres Unternehmens angepasst werden und bietet einen flexiblen Ansatz zur Sicherung einer Vielzahl von Informationsarten.

Kapitel 3

Aufbau Ihres Informationssicherheits-Managementsystems (ISMS)

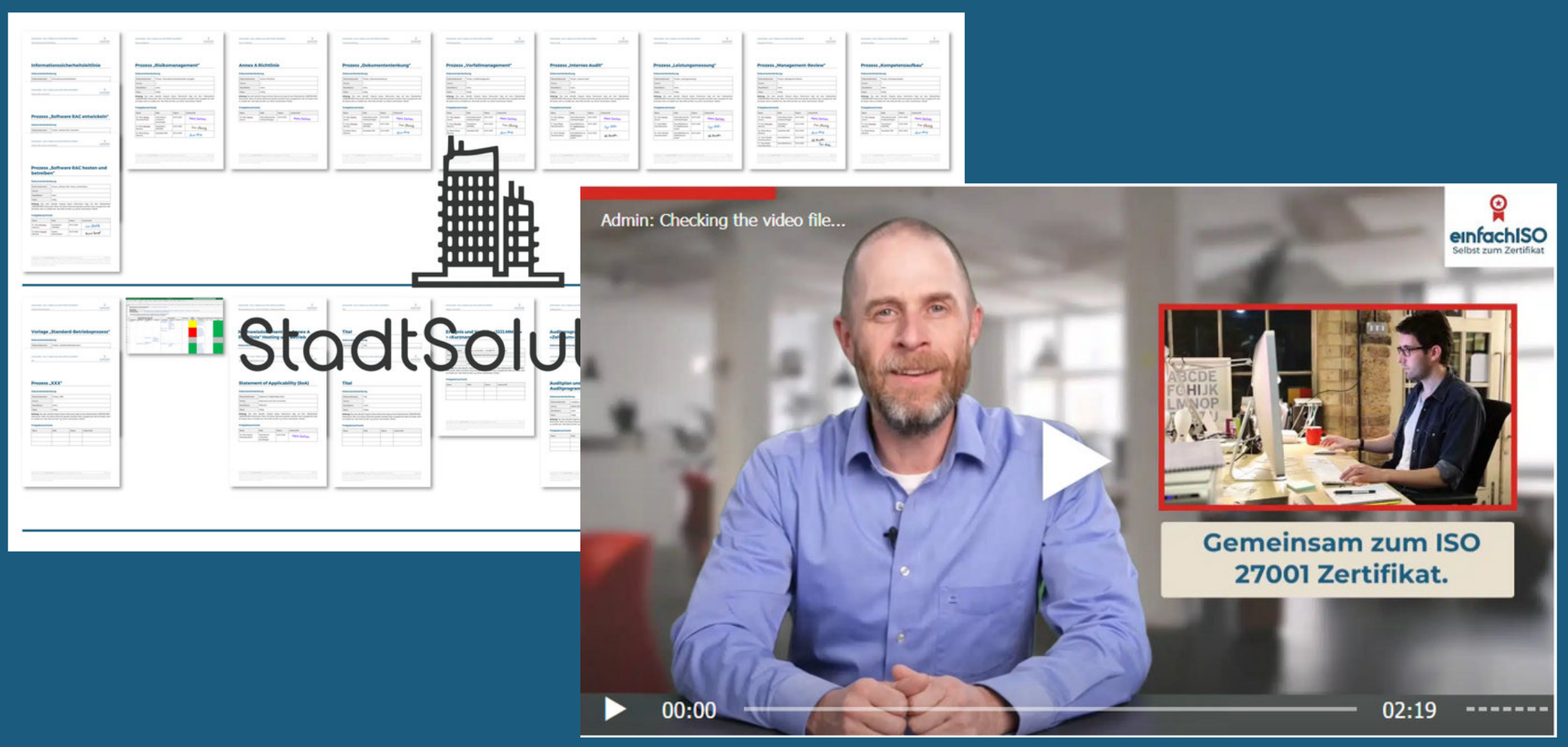
In diesem Kapitel befassen wir uns mit den praktischen Aspekten der Einrichtung eines robusten Informationssicherheits-Managementsystems (ISMS).

Pro-Tipp

Sparen Sie Tage Zeit, indem Sie Ihr ISMS auf der Grundlage unserer Vorlagen starten, die alle erforderlichen Dokumente für ein Musterunternehmen enthalten. Und es gibt ein 20-stündiges Video, das Ihnen genau erklärt, was zu tun ist.

Und das Beste: Es ist kostenlos!

https://einfachiso.de/27001-isms



einfachISO

Schlüsselkomponenten Ihres ISMS

Ein effektives ISMS basiert auf mehreren Schlüsselkomponenten, die jeweils eine entscheidende Rolle bei der Verwaltung und dem Schutz von Informationen spielen:

1. **Geltungsbereich des ISMS**: Definieren der Grenzen und Anwendbarkeit des ISMS in Ihrer Organisation. Dazu gehört die Identifizierung, welche Daten, Abteilungen und Prozesse einbezogen werden.
2. **Informationssicherheitsrichtlinie**: Erstellen einer Richtlinie, die den Ansatz Ihrer Organisation zur Informationssicherheit festlegt und Ihre Geschäftsziele und Compliance-Anforderungen widerspiegelt.
3. **Risikobewertung und -behandlung**: Identifizierung potenzieller Informationssicherheitsrisiken und Entscheidung über die erforderlichen Maßnahmen zu deren Minderung.
4. **Ziele und Planung**: Festlegung klarer Informationssicherheitsziele und Planung, wie diese im Einklang mit der gesamten Geschäftsstrategie erreicht werden können.
5. **Ressourcen und Kompetenz**: Sicherstellen, dass die erforderlichen Ressourcen verfügbar sind und dass das Personal für die Implementierung des ISMS geschult und kompetent ist.
6. **Betriebskontrollen**: Implementierung und Verwaltung der betrieblichen Aspekte des ISMS, einschließlich Datenverarbeitung, Zugangskontrolle und physische Sicherheit.
7. **Leistungsbewertung**: Überwachung und Messung der Leistung des ISMS anhand der festgelegten Ziele und Berichterstattung der Ergebnisse an das Management.
8. **Verbesserung**: Möglichkeiten zur kontinuierlichen Verbesserung des ISMS identifizieren und notwendige Anpassungen vornehmen.

Kapitel 4

Risikobewertung und -behandlung

Risikobewertung und -behandlung sind der Kern eines wirksamen ISMS.

Dieses Kapitel führt Sie durch die Durchführung einer umfassenden Risikobewertung, gefolgt von der Entwicklung von Strategien zur Risikominderung und -behandlung im Einklang mit der ISO 27005 (kein Tippfehler - in dieser Norm ist ein ISO 27001-konformes Risikomanagement geregelt).

Risikobewertung

Bei der Risikobewertung handelt es sich um einen systematischen Prozess zur Identifizierung und Bewertung von Risiken für die Informationsressourcen Ihres Unternehmens. Das ISO 27005-Framework bietet dazu einen strukturierten Ansatz:

Auf den Kontext kommt es an

Definieren Sie den externen und internen Kontext Ihres Unternehmens. Sie definieren den Umfang der Risikobewertung, einschließlich der zu schützenden Informationsbestände.

einfachISO

Risiko-Analyse

Identifizieren Sie potenzielle Risiken, die sich auf die Informationsressourcen auswirken könnten.
Ermitteln Sie Bedrohungen (sowohl interne als auch externe), auf welche Schwachstellen diese einwirken können und welche potenzielle Auswirkungen sich ergeben.

Verwenden Sie Techniken wie die SWOT-Analyse (Stärken, Schwächen, Chancen, Bedrohungen) oder die Analyse von Vorfällen und Beinaheunfällen, um Risiken zu identifizieren.

Eine gute und umfangreiche Liste häufiger Bedrohungen finden Sie auch im BSI-Grundschutzkompandium.

einfachISO

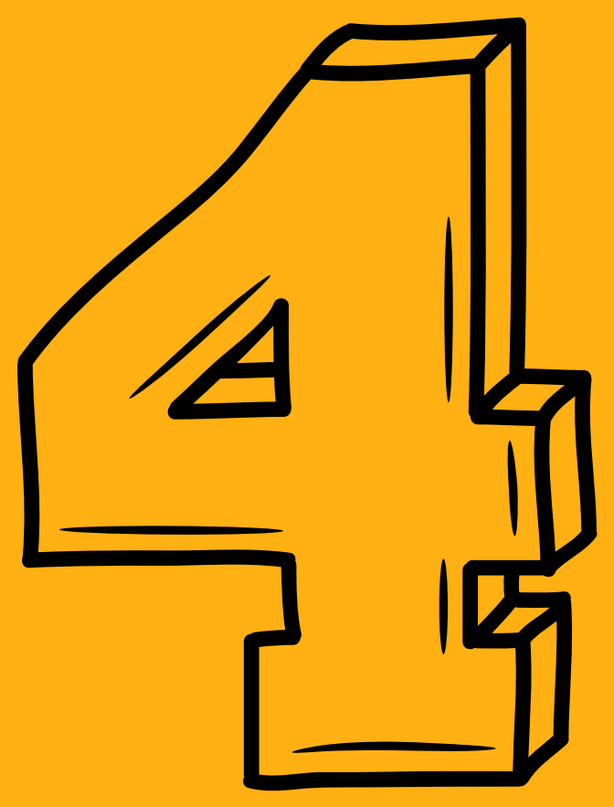
Risikobewertung

Bestimmen Sie die Wahrscheinlichkeit und Schadensausmaß jedes identifizierten Risikos. Diese Bewertung kann qualitativ, quantitativ oder als Kombination aus beidem erfolgen.

Die Kombination aus Wahrscheinlichkeit und Auswirkung bestimmt die Risikoklasse.

Die meisten Klassifizierungsschemata (auch Risikomatrizen genannt) klassifizieren Risiken in grüne, gelbe und rote Risiken.

Risikobehandlung



Sobald die Risiken bewertet sind, besteht der nächste Schritt darin, sie effektiv zu verwalten und zu mindern.

Entscheiden Sie, wie mit jedem Risiko umgegangen werden soll.

Zu den Optionen gehören:

- das Risiko **vermeiden**,
- **Reduzierung** durch Kontrollen, z. B. Verschlüsselung
- **Teilen oder Übertragen** des Risikos, z. B. durch eine Versicherung
- **Akzeptieren** Sie es (sofern es im Rahmen Ihrer Risikobereitschaft liegt).

Der Risikobehandlungsplan - Ein Schlüsselelement Ihres ISMS

Das Herzstück jedes wirksamen ISMS gemäß ISO 27001 ist der Risikobehandlungsplan (RBP).

Dieses Dokument erfüllt wichtige Funktionen:

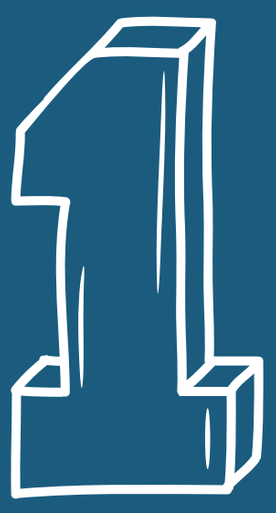
1. **Strategischer Ansatz für das Risikomanagement:** Der RBP bietet einen strukturierten Ansatz für das Management identifizierter Risiken und stimmt diese mit der gesamten Informationssicherheitsstrategie ab.
2. **Umsetzbare Risikominderung**: Er beschreibt spezifische Maßnahmen, die zur Bewältigung jedes identifizierten Risikos ergriffen werden müssen, und stellt sicher, dass diese Maßnahmen wirtschaftlich und erreichbar sind.
3. **Ressourcenzuweisung**: Der Plan weist die erforderlichen Ressourcen zu sowie Verantwortlichkeiten für die Risikobehandlung zu und gewährleistet so eine wirksame Umsetzung.

Kapitel 4

Zertifizierung erhalten

Nachdem Sie Ihr ISMS fertig aufgebaut haben, Ihre Risikoanalyse abgeschlossen, alle darin enthaltenen Richtlinien implementiert und Ihr Team geschult haben – wie erhalten Sie endlich Ihr Zertifikat?

einfachISO



Beauftragen Sie Ihre Zertifizierungsstelle

Berater und Unternehmen, die Sie bei der Vorbereitung auf die Zertifizierung unterstützen, können Sie nicht gleichzeitig auditieren und zertifizieren.
Es ist einfach nicht erlaubt – und das aus guten Gründen.

Der erste Schritt zur Zertifizierung ist also ganz einfach: die Suche nach einem akkreditierten Zertifizierungs-dienstleister. Jedes Land verfügt über eine zentrale Organisation, die Zertifizierungsstellen akkreditiert. In Deutschland ist dies beispielsweise die DAkkS. Diese führen Listen akkreditierter Zertifizierungsstellen.

Die Wahl des richtigen Zertifizierungsdienstleisters ist entscheidend – dieser wird Sie über mehrere Jahre begleiten (mehr dazu weiter unten). Deshalb ist es wichtig, eine gute Wahl zu treffen – der Preis allein ist nicht alles. Wenn Sie Tipps benötigen, können Sie sich gerne an uns wenden.

einfachISO

Es gibt auch Unternehmen, die nicht akkreditiert sind, aber dennoch ISO 27001-Zertifizierungen durchführen!

Dies ist nicht verboten und die Zertifizierungen können durchaus von guter Qualität sein.

Allerdings ist das Zertifikat, das Sie danach erhalten, nicht viel Wert.

Möglicherweise wird es von Ihren Kunden abgelehnt und Ihre Konkurrenten könnten schnell unlauteren Wettbewerb vermuten und dagegen vorgehen.

einfachISO

Erstzertifizierungs-audit

Bei diesem Audit prüft ein unabhängiger Auditor Ihres Zertifizierungsdienstleisters, ob Ihr Unternehmen die Anforderungen der ISO 27001 erfüllt.

Das Audit dauert meist einige Tage, da der Auditor alle relevanten Dokumente und Prozesse im Unternehmen prüfen und Gespräche mit Ihren Mitarbeitern führen muss.

Das Audit gliedert sich in zwei Teile:

- **Stufe 1**: In diesem Teil liegt der Fokus vor allem auf der Dokumentation.
- **Stufe 2**: In diesem Teil geht es darum, ob das Unternehmen die eigenen Regeln zur Informationssicherheit einhält und ob die technischen Maßnahmen umgesetzt sind und funktionieren.

Mehr über den genauen Ablauf des Erstzertifizierungsaudits erfahren Sie in diesem Blogbeitrag auf unserer Website.

Überwachungs-audits

Nach erfolgreicher Zertifizierung ist Ihr Unternehmen verpflichtet, in regelmäßigen Abständen Überwachungsaudits durchzuführen, um sicherzustellen, dass die Informationssicherheitsmaßnahmen immer noch auf dem neuesten Stand sind und weiterhin den Anforderungen der Norm entsprechen.

Es finden zwei Überwachungsaudits statt, ein Jahr bzw. zwei Jahre nach dem Erstzertifizierungsaudit.

Dabei handelt es sich nicht um gleichrangige Prüfungen, sondern um „Stichproben“ in bestimmten Fachbereichen.

Sie sind daher auch von wesentlich kürzerer Dauer.

einfachISO

Rezertifizierung

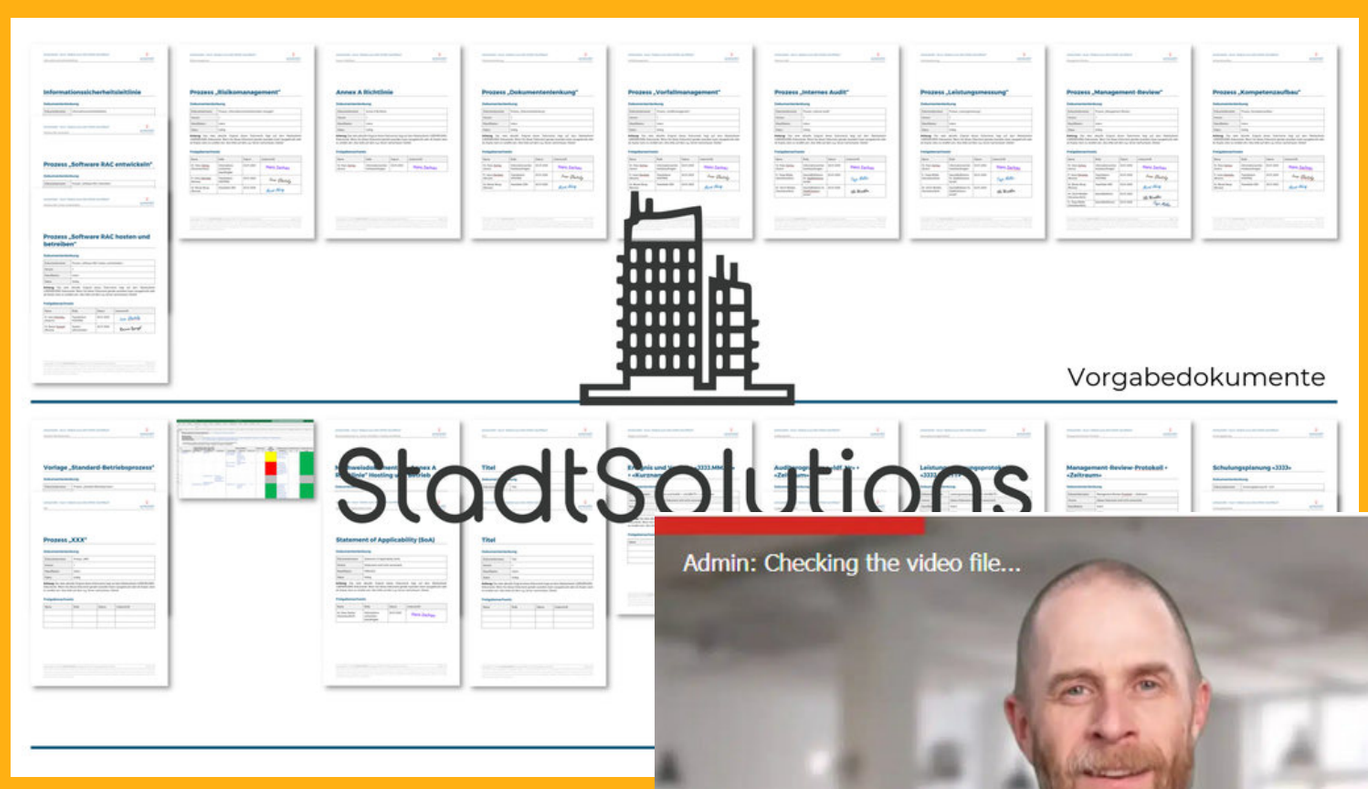
Ein Jahr nach dem zweiten Überwachungsaudit (also 3 Jahre nach der Erstzertifizierung) folgt das Rezertifizierungsaudit.

Durch dieses Audit wird bestätigt, dass Ihr Unternehmen weiterhin die Anforderungen des Standards erfüllt und ein angemessenes Maß an Informationssicherheit gewährleistet ist. Es entspricht vom Umfang dem Erstzertifizierungsaudit.

Nach dem Rezertifizierungsaudit beginnt der Zyklus von neuem, d. h. es folgen zwei weitere Überwachungsaudits, gefolgt vom nächsten Rezertifizierungsaudit usw.

einfachISO

Starten Sie noch heute kostenlos!



- **Vorlagen für alle erforderlichen Dokumente für Ihr ISO 27001-konformes ISMS**
- **> 60 Vorlagen insgesamt**
- **Video-Tutorial, das Sie durch die Anpassung der Vorlagen an Ihr Unternehmen führt**
- **über 20 Stunden Videos!**
- **Schritt für Schritt praktische Anleitung**
- **Praktisch und unterhaltsam.**

https://einfachiso.de/27001-isms

Wir helfen gerne!

Eine Expedition auf eigene Faust zu starten, kann eine Herausforderung sein. Gerne begleiten wir Sie auf dieser Reise!

einfachISO

https://einfachiso.de
info@einfachiso.de