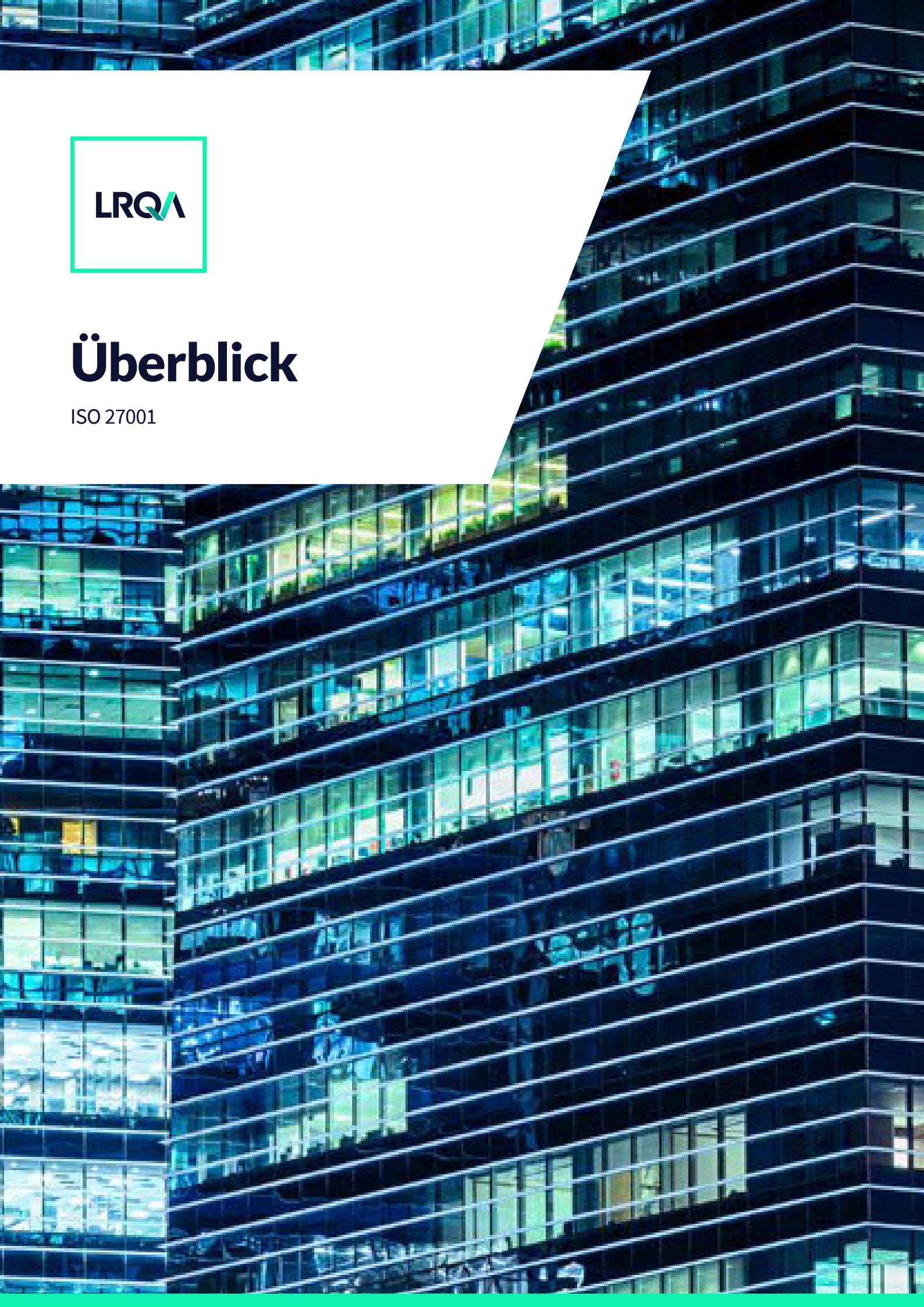

Überblick

ISO 27001

Wie Ihr Unternehmen von der Zertifizierung nach ISO 27001 profitieren kann

Wenn Sie interne Informations-managementsysteme verwalten, für die Informationssicherheit verantwortlich sind oder IT-Produkte und -Dienste für Ihre Kunden entwickeln: Effektive Informationssicherheits-managementsysteme (ISMS) sind immer unerlässlich.

Sie unterstützen Sie dabei, die richtigen Kontrollen, Systeme und Produkte zu entwickeln, um die ständig steigenden und anspruchsvollen Anforderungen Ihrer Kunden und Partner zu erfüllen.

ISO 27001 (Informationstechnologie – Sicherheitstechniken – Management-systeme für Informationssicherheit – Anforderungen) soll sicherstellen, dass angemessene Kontrollen im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen bestehen, um die Informationen von „interessierten Parteien“ zu schützen. Dies umfasst Ihre Kunden, Mitarbeiter, Lieferanten und die Bedürfnisse der Gesellschaft im Allgemeinen. Das Verständnis ihrer Anforderungen ist bei der Implementierung Ihres Managementsystems von entscheidender Bedeutung.

Wenn Sie interne Informationsmanagementsysteme verwalten, für die Informationssicherheit verantwortlich sind oder IT-Produkte und -Dienste für Ihre Kunden entwickeln: Effektive Informationssicherheits-Managementsysteme (ISMS) sind immer unerlässlich.

Ein ISMS gemäß ISO 27001 kann Sie dabei unterstützen, sowohl Lieferanten als auch Kunden zu zeigen, dass Sie Informationssicherheit ernst nehmen.

Die akkreditierte Zertifizierung nach ISO 27001 ist ein wirkungsvoller Beleg für die Verpflichtung Ihres Unternehmens, Informationssicherheit effektiv zu verwalten.

Dieser Überblick bietet einige praktische Anleitungen und Empfehlungen, um die Implementierung Ihres zertifizierten ISMS zu unterstützen.

Einführung in die Implementierung eines ISMS

Neben der gewöhnlichen wirtschaftlichen Notwendigkeit, vertrauliche Informationen – wie geistiges Eigentum und Preisinformationen – zu schützen, werden durch aktuelle Ereignisse in den Bereichen Vorschriften und Corporate Governance anspruchsvollere Anforderungen an die Integrität von Informationen denn je gestellt. Durch die Implementierung eines ISMS wird sichergestellt, dass Sicherheitsprobleme gemäß der besten Praxis behandelt werden.

Ein ISMS gemäß ISO 27001, das von LRQA zertifiziert ist, bietet Ihnen eine unabhängige und unvoreingenommene Sicht auf die Angemessenheit und Wirksamkeit Ihres ISMS. Dies unterstützt Sie dabei, Ihre Fähigkeiten gegenüber der Außenwelt unter Beweis zu stellen.

Anwendung bester Praktiken

In den vergangenen Jahren wurden mehrere Leitlinien eingeführt, um für die Risiken für Informationssysteme und Netzwerke zu sensibilisieren. Diese sind zwar vielfältig, die zugrunde liegenden Richtlinien, Praktiken, Maßnahmen und Verfahren erleichtern jedoch, beste Praktiken hervorzuheben, die das Risikomanagement und letztlich die Sicherheit von Informationssystemen und Netzwerken verbessern.

ISO 27001 bietet einen ISMS-Rahmen für die Implementierung von besten Praktiken und Prinzipien unter Verwendung des PDCAZyklus (Plan Do Check Act) und von Managementsystemprozessen:

- **Bewusstsein:** Die Teilnehmer sollten sich der Notwendigkeit der Sicherheit von Informationssystemen und Netzwerken bewusst sein und wissen, was sie tun können, um die Sicherheit zu erhöhen.
- **Verantwortung:** Alle Teilnehmer sind für die Sicherheit von Informationssystemen und Netzwerken verantwortlich.
- **Reaktion:** Die Teilnehmer sollten rechtzeitig und kooperativ handeln, um Sicherheitsvorfälle zu verhindern, zu erkennen und darauf zu reagieren.
- **Risikobewertung:** Die Teilnehmer sollten Risikobewertungen durchführen.
- **Design und Implementierung von Sicherheit:** Die Teilnehmer sollten die Sicherheit als ein wesentliches Element von Informationssystemen und Netzwerken integrieren.
- **Sicherheitsmanagement:** Die Teilnehmer sollten einen umfassenden Ansatz für das Sicherheitsmanagement übernehmen.
- **Neubewertung:** Die Teilnehmer sollten die Sicherheit von Informationssystemen und Netzwerken überprüfen und neu bewerten sowie geeignete Änderungen an Sicherheitsrichtlinien, -praktiken, -maßnahmen und -verfahren vornehmen.

Angepasst nach den OECD-Leitlinien zum Risikomanagement für digitale Sicherheit

Erste Schritte

Unabhängig vom aktuellen Status Ihres Unternehmens besteht der Ausgangspunkt für die Implementierung eines ISMS darin, Verpflichtung und Unterstützung durch das Management zu erlangen.

Motivation und Ausrichtung müssen jetzt vom leitenden Management ausgehen. Es muss aktiv daran beteiligt sein, die Ausrichtung des ISMS und dessen Vereinbarkeit mit der Strategie Ihres Unternehmens sicherzustellen und Eigentümer wichtiger Aspekte wie der Richtlinie und der Ziele zu sein.

Der Erfolg stellt sich ein, wenn das Management die Gründe für die Implementierung eines ISMS versteht und dessen Design und Betrieb voll unterstützt.

Planen für den Erfolg

Wie bei jedem Projekt, das Sie übernehmen, ist der Erfolg wahrscheinlicher, wenn Sie einen sinn- und bedeutungsvollen und realistischen Plan entwickeln, die Leistung auf der Grundlage des Plans messen und bereit sind, ihn im Fall unvorhergesehener Umstände zu ändern.

Der Plan sollte anerkennen, dass die Entwicklung eines Managementsystems Zeit und Aufwand erfordert, und das leitende Management sollte angemessene Ressourcen bereitstellen.

Die Gesamtverantwortung für die Informationssicherheit liegt beim leitenden Management und häufig bei der IT-Abteilung. Informationssicherheit hat jedoch breitere Auswirkungen als nur auf IT-Systeme, einschließlich Personal, Sicherheit, physischer Sicherheit und Einhaltung gesetzlicher Vorschriften.

ISO 27001 ist auf ISO 9001:2015 abgestimmt. Wenn Sie bereits über ein zertifiziertes Qualitätsmanagementsystem verfügen, bietet dies daher eine starke Grundlage für Ihr ISMS.

Wir empfehlen dringend, an einer Schulung von LRQA teilzunehmen, in der Sie Fragen der Informationssicherheit mit anderen Teilnehmern und Ihrem Tutor besprechen können.

Die Norm verstehen

Es ist wichtig, sich mit der Norm vertraut zu machen, einschließlich des Verständnisses der zu erfüllenden Kriterien und der Struktur. Letztendlich wirkt sich dies auf die allgemeine Struktur Ihres ISMS und der zugehörigen Dokumentation aus.

Die Norm besteht aus zwei Teilen:

- ISO 27002 ist selbst keine Norm, sondern ein Praxiskodex, der Sicherheitsziele und -kontrollen darlegt, die ausgewählt und implementiert werden können, um spezifische Risiken für die Informationssicherheit zu verwalten.
- ISO 27001 ist die Spezifikation des Managementsystems, die die Anforderungen definiert, die Sie erfüllen müssen, um ein ISMS zu implementieren, und in Bezug auf die Ihre Zertifizierungsstelle Sie während der Zertifizierungsbewertung auditiert.

Die Spezifikation umfasst die gemeinsamen Elemente aller Managementsysteme: Richtlinie, Führung, Planung, Betrieb, Überprüfung durch das Management und Verbesserung. Sie enthält ebenfalls einen Abschnitt, der speziell auf die Ermittlung von Risiken für Ihre Informationen und die Auswahl geeigneter Kontrollen und Überprüfungen ausgerichtet ist (Anhang A).

Was folgt danach?

Ein ISMS verfügt über zwei Hauptelemente, die als zwei verschiedene Aktivitäten angegangen werden können. ISO 27001 erfordert die Einrichtung eines ISMS, um die für Ihr Unternehmen spezifischen Sicherheitsanforderungen zu ermitteln und zu dokumentieren.

Die Norm verlangt auch, dass Managementprozesse definiert werden, um die Verpflichtung, die Verantwortung und die Kontrolle des Managements zu belegen, d. h. Führung, Kontext, Überprüfung durch das Management und Verbesserung.

Managementprozesse

Diese Prozesse sind entscheidend für die effektive Implementierung eines ISMS. Wenn Ihr Unternehmen bereits ein Managementsystem nach ISO 9001:2015 betreibt, sind Ihnen diese Prozesse vertraut.

Wenn dies der Fall ist, besteht der effizienteste Weg häufig in der Integration der Informationssicherheitsanforderungen in Ihr vorhandenes Managementsystem, um sicherzustellen, dass das entsprechende Know-how in der Informationssicherheit zur Verfügung steht, wann und wo es benötigt wird.

Wenn Sie diese Prozesse zum ersten Mal implementieren, sollten Sie den Gesamtzweck dieser Managementanforderungen berücksichtigen. Das leitende Management ist letztlich für die Effektivität des Managementsystems verantwortlich – seine Akzeptanz zu erlangen, ist entscheidend.

Für die Entwicklung, Implementierung und Überwachung des ISMS sollten angemessene Ressourcen (Personal, Anlagen, Zeit und Geld) bereitgestellt werden.

Interne Audits ermitteln Verbesserungsmöglichkeiten und überprüfen, ob das Managementsystem wie beabsichtigt funktioniert. Die Überprüfung durch das Manage ment bietet dem leitenden Management die Möglichkeit zu bewerten und zu verstehen, wie gut das Managementsystem funktioniert und die Geschäftstätigkeit unterstützt.

Sie halten es unter Umständen für nützlich, diese Managementprozesse mit den Kontrollzielen in Anhang A zu verknüpfen, da viele der Kontrollen die Managementanforderungen von ISO 27001 ergänzen.

Definieren des Umfangs

Es ist wichtig, den logischen und geografischen Umfang des ISMS genau zu definieren, damit die Grenzen Ihres ISMS und die Sicherheitsverantwortung ermittelt werden können. Der Umfang sollte die Personen, Orte und Informationen angeben, die vom ISMS abgedeckt werden.

Sobald Sie den Umfang definiert und dokumentiert haben, können die vom Umfang abgedeckten Informationsressourcen sowie deren Wert und Eigentümer ermittelt werden.

ISMS-Richtlinie

Die Anforderungen an die IMS-Richtlinie werden sowohl in ISO 27001 (5.2) als auch in ISO 27002 behandelt. Verweise auf die Richtlinie gibt es ebenfalls in anderen Anforderungen von ISO 27001 und in Anhang A, in dem angegeben ist, was die Richtlinie enthalten sollte. Beispielsweise müssen die ISMS-Ziele mit der ISMS-Richtlinie übereinstimmen. Um bestimmte Kontrollziele zu erreichen, sind weitere Richtlinien erforderlich.

Risikobewertung und Risikomanagement

Risikobewertung ist die Grundlage, auf der ein ISMS aufgebaut ist. Sie bietet den Fokus für die Implementierung von Sicherheitskontrollen und stellt sicher, dass diese dort angewendet werden, wo sie am dringendsten benötigt werden, kostengünstig sind und, ebenso wichtig, nicht dort angewendet werden, wo sie am wenigsten effektiv sind. Die Risikobewertung erleichtert, die Frage „Wie viel Sicherheit benötigen wir?“ zu beantworten.

Einer der wichtigsten Aspekte des Risikomanagements besteht in der Notwendigkeit, das Risiko positiv und negativ zu betrachten. Risiko wird als Auswirkung von Unsicherheit auf Ziele betrachtet. Daher ist es für das Risikomanagement von entscheidender Bedeutung, Ihre Möglichkeiten, daraus Nutzen zu ziehen, ebenfalls zu berücksichtigen.

An der Risikobewertung sind alle Eigentümer von Informationsressourcen beteiligt. Es ist unwahrscheinlich, dass Sie eine effektive Risikobewertung ohne sie durchführen können.

Der erste Schritt besteht darin, eine Methode der Risikobewertung auszuwählen und zu dokumentieren. Es stehen proprietäre Methoden zur Verfügung, die in der Regel computerbasiert sind, wie z. B. CRAMM (CCTA Risk Analysis and Management Method).

Darüber hinaus kann ISO 31000, der internationale Standard für das Risikomanagement, genutzt werden, um eine für das Unternehmen spezifischere Methode im Hinblick auf die Komplexität von Informationssystemen zu entwickeln.

Der Risikobewertungsprozess beinhaltet die Ermittlung und Bewertung von Informationsressourcen. Diese Bewertung ist nicht nur finanziell. Sie berücksichtigt ebenfalls andere Faktoren, wie z. B. Rufschädigung oder beeinträchtigte Einhaltung gesetzlicher Vorschriften. Hier hat Ihr Kontext wichtige Auswirkungen.

Der Prozess sollte die Bedrohungen und Sicherheitsrisiken sowie alle mit den Ressourcen und deren Ausnutzung verbundenen Möglichkeiten berücksichtigen. Schließlich müssen Sie das Risikoniveau bestimmen und die zum Management dieser Risiken zu implementierenden Kontrollen ermitteln.

Bei der Ermittlung von Bedrohungen, Sicherheitsrisiken und deren Auswirkungen muss die Sicherheitsumgebung berücksichtigt werden. Zum Beispiel ist die Gefahr der Verweigerung des physischen Zugangs zu den Räumlichkeiten für ein Unternehmen in einem Industriegebiet neben einer petrochemischen Anlage größer als für ein Büro in einem kleinen städtischen Büropark.

Ebenso ist die Gefahr des Diebstahls von Kreditkartendaten größer als des Diebstahls der täglichen Produktionsdaten eines kleinen Maschinenbauunternehmens.

Risikobehandlung

Die Risikobewertung ermittelt Risikoniveaus, die mit dem akzeptablen Risikoniveau verglichen werden, das durch die Sicherheitsrichtlinie des Unternehmens bestimmt wird. Es werden geeignete Maßnahmen getroffen, um Risiken zu verwalten, die über dem Akzeptanzniveau liegen, wobei folgende Maßnahmen möglich sind:

- Implementierung von Sicherheitskontrollen, die aus Anhang A ausgewählt wurden, um das Risiko auf ein akzeptables Niveau zu reduzieren. Das Risikoniveau sollte neu berechnet werden, um zu bestätigen, dass das Restrisiko unter dem Akzeptanzniveau liegt. Die ausgewählten Kontrollen werden in der Erklärung zum Geltungsbereich verzeichnet, die die Begründung für die Aufnahme oder den Ausschluss der einzelnen Kontrollen, den Status und die Rückverfolgbarkeit der Risikobewertung enthalten sollte.
- Akzeptanz des Risikos gemäß der Richtlinie des Managements und den Kriterien für die Risikoakzeptanz. Es kann Fälle geben, in denen das Restrisiko nach einer getroffenen Maßnahme über dem Akzeptanzniveau liegt. In diesem Fall sollte das Restrisiko ebenfalls dem Risikoakzeptanzprozess unterliegen. Es sollten Aufzeichnungen zur Risikoakzeptanz des Managements geführt werden.
- Beseitigung des Risikos durch Änderung der Sicherheitsumgebung. Zum Beispiel Installation sicherer Anwendungen, wenn Sicherheitsrisiken in Datenverarbeitungsanwendungen festgestellt wurden, oder Umsetzen physischer Ressourcen in ein höheres Stockwerk, wenn Überschwemmungsgefahr besteht. Bei diesen Entscheidungen müssen geschäftliche und finanzielle Erwägungen berücksichtigt werden. Auch hier sollte das Restrisiko nach Maßnahmen zur Risikobeseitigung neu berechnet werden.
- Übertragung des Risikos durch den Abschluss einer entsprechenden Versicherung oder Outsourcing der Verwaltung von physischen Vermögenswerten oder Geschäftsprozessen. Das Unternehmen, das das Risiko akzeptiert, sollte sich seiner Verpflichtungen bewusst sein und deren Annahme vereinbaren. Verträge mit Outsourcing-Unternehmen sollten die entsprechenden Sicherheitsanforderungen enthalten.

Der Risikobehandlungsplan wird zum Risikomanagement verwendet, indem die getroffenen und geplanten Maßnahmen sowie der Zeitrahmen für die Durchführung ausstehender Maßnahmen angegeben werden. Der Plan sollte die Maßnahmen priorisieren und die Verantwortlichkeiten und ausführliche Maßnahmenpläne enthalten.

Unsere Audit- und Trainings-dienstleistungen für ISO 27001

Unser Angebot an Audit- und Schulungsdienstleistungen eignet sich für Unternehmen aller Größen und Standorte und kann Sie dabei unterstützen, die Normen optimal zu nutzen.

Schulung

LRQA bietet maßgeschneiderte und gebündelte Schulungsdienstleistungen, die Ihr Unternehmen auf dem Weg zur Zertifizierung nach ISO 27001 unterstützen.

Gap-Analyse

Diese von Auditoren durchgeführte Tätigkeit bietet die Möglichkeit, sich auf kritische, risikoreiche oder schwache Bereiche in Ihrem System zu konzentrieren, um ein zertifizierbares System zu schaffen.

Wo auch immer Sie sich im Zertifizierungsprozess befinden: Der Umfang kann von Ihnen festgelegt werden.

Zertifizierung

Dies ist in der Regel ein zweiphasiger Prozess, der aus einer Beurteilung des Systems und einer Bewertung der Umsetzung in der Praxis besteht. Die Dauer ist von der Größe und Art Ihres Unternehmens abhängig.

Überwachung

Nachdem wir Ihr ISMS erfolgreich zertifziert haben, führen wir regelmäßige Überwachungsbesuche durch, um die laufende Effektivität Ihres Systems sicherzustellen Dadurch können Sie und Ihr Management sicher sein, dass Ihr ISMS auf Kurs ist und sich kontinuierlich verbessert.

Bewertung integrierter Managementsysteme

Wenn Sie das ISMS Ihres Unternehmens mit einem bestehenden Managementsystem (z. B. Qualität) kombinieren möchten, könnten Sie von einem koordinierten Auditierungs- und Betreuungsprogramm profitieren.

Warum mit LRQA zusammenarbeiten?

Zusammen mit unserem preisgekrönten Geschäftsbereich Cybersicherheit (Nettitude) bietet LRQA eine 360-Grad-Suite von Informations- und Cybersicherheitsprodukten.

Wir verstehen, dass die Mitarbeiter das Herz eines erfolgreichen Unternehmens sind. Alle Ihre Kunden, Lieferanten und Mitarbeiter übergeben ihre Informationen in Ihre Hände und erwarten von Ihnen, dass Sie alles in Ihrer Macht Stehende tun, um sie zu schützen.

Deshalb gehen wir über Compliance hinaus und tauchen tiefer in Ihr Unternehmen ein, um sinn- und bedeutungsvolle Einblicke und intelligentere Lösungen zu erzielen.

Unsere Auditoren und Trainer sind Branchenexperten, die mit Ihnen zusammenarbeiten, um zu verstehen, was Ihr Unternehmen dabei unterstützt, auf optimalem Niveau zu arbeiten. Sie schaffen durch Zusammenarbeit einen langfristigen Wert, der sich positiv auf Ihr Unternehmen, Ihre Mitarbeiter und Ihre Kunden auswirkt.

Die Unternehmen, mit denen wir zusammenarbeiten, sagen uns, dass wir uns dadurch von unseren Konkurrenten abheben.

Ein 360-Grad-Ansatz für Informationsund Cybersicherheit

Risikobasierte Lösungen

ISO 27001: Das Fundament Ihrer Informationssicherheits-strategie

ISO 27001 steht im Mittelpunkt unseres Informationssicherheitsangebots.

Unabhängig von der Größe Ihres Unternehmens oder der Branche, in der Sie tätig sind, bietet ISO 27001 einen Rahmen für die beste Praxis, um Kontrollen zur Verwaltung von Informationssicherheitsrisiken und zum Schutz geschäftskritischer Daten zu ermitteln, zu analysieren und zu implementieren. Die unabhängige Zertifizierung nach ISO 27001 zeigt, dass Ihr Unternehmen Informationssicherheit ernst nimmt, und bietet einen Wettbewerbsvorteil, um neue Geschäfte zu gewinnen und bestehende Kunden zu binden.

Verstärkung Ihres ISMS

Effektive Informationssicherheit hört mit der Zertifizierung nach ISO 27001 nicht auf. Wir bieten Dienstleistungen für eine Reihe anderer spezialisierter, branchenspezifischer Standards an, die Ihr ISMS ergänzen und stärken. Abhängig von Ihrem Risikoprofil können wir eine maßgeschneiderte Kombination von Produkten anbieten, die Ihr System und Ihre Erfahrung optimieren, sodass Ihr Unternehmen von Kosten-, Zeit- und Verwaltungseffizienz profitieren kann.

Cybersicherheit ist keine Einheitsgröße

Ihre Bedrohungslandschaft ist so einzigartig wie Ihr Unternehmen. Ihr Risikoprofil erleichtert Ihnen, die erforderlichen Schritte zu ermitteln, um Ihre Vermögenswerte, Ressourcen und Daten zu schützen. Umgebungen mit hohem Risiko erfordern effektiven Schutz, Erkennung, Reaktion und Wiederherstellung bei Cyberbedrohungen.

Unser Bereich Nettitude bietet eine breite Palette an erweiterten Cybersicherheitsdienstleistungen, die auf die Anforderungen Ihrer einzigartigen Betriebsumgebung zugeschnitten sind, einschließlich Penetrationstests, Sicherheitsrisikoanalysen, 24/7-Dienstleistungen für Ihre Sicherheit, Dienstleistungen für die Unterstützung bei Reaktionen auf Vorfälle, PCI-Compliance-Bewertungen und mehr.

Nettitude bietet den Kunden Cybersicherheitsdienstleistungen und zu den Kunden gehören Zentralbanken, Börsen, Behörden und führende globale Unternehmen in verschiedenen Branchen. Die Tester und Berater von Nettitude verfügen über die höchsten verfügbaren technischen Qualifikationen und Nettitude ist stolz darauf, eines von wenigen Unternehmen weltweit zu sein, die von CREST für verschiedene Dienstleistungen zertifiziert sind, und das weltweit erste, für Security-Operations-Center-Dienstleistungen (SOC) zertifizierte Unternehmen zu sein. Nettitude ist außerdem leitender Auditor für PCI ASV, PCI QSA, P2PE QSA und PA QSA und zugelassener Anbieter von Testdienstleistungen für Simulated Target Attack and Response (STAR).

LRQA bietet eine breite Palette von Dienstleistungen für die weltweit führenden Standards für Informationssicherheit und beste Praktiken

- Schulung ✓
- Gap-Analyse ✓
- Zertifizierung ✓
- Integrierte Bewertungen ✓
- Penetrationstests ✓
- Dienstleistungen für Sicherheit ✓
- Reaktion auf Vorfälle ✓

YOUR FUTURE. OUR FOCUS.

Über LRQA

Durch die Bündelung von konkurrenzlosem Fachwissen in den Bereichen Zertifizierung, kundenspezifischer Assurance, Cybersicherheit, Inspektion und Schulungen haben wir uns zu einem weltweit führenden Anbieter von Assurance entwickelt.

Wir sind stolz auf unser Erbe – aber was wirklich zählt, ist, wer wir heute sind, denn das bestimmt, wie wir morgen mit unseren Kunden zusammenarbeiten. Durch die Kombination von starken Werten, jahrzehntelanger Erfahrung im Risikomanagement und in der Risikominderung sowie einem starken Fokus auf die Zukunft unterstützen wir unsere Kunden beim Aufbau sicherer und nachhaltiger Unternehmen.

Vom Auditing als unabhängige Dritten, Zertifizierung und Schulungen über Beratungsdienstleistungene bis hin zu Echtzeit-Assurance-Technologie und datengestützter Transformation der Lieferkette – unsere innovativen End-to-End-Lösungen helfen unseren Kunden, sich in einer sich schnell verändernden Risikolandschaft zurechtzufinden. So stellen wir sicher, dass sie ihre eigene Zukunft gestalten, anstatt sich von ihr gestalten zu lassen.

Kontaktieren Sie uns

Besuchen Sie **www.lrqa.com/de** für weitere Informationen, rufen uns an: +49 (0)221 9675 7700 oder schreiben Sie uns per E-Mail an **info.de@lr.org.**

Lloyd's Register Deutschland GmbH
Butzweilerhofallee 3
50829 Köln
Deutschland