TOPCERTIFIER
www.topcertifier.com

SERVICE-METHODE ISO 27001:2013

INFORMATION SICHERHEITSMANAGEMENT SYSTEM (ISMS)

TOPCERTIFIER
www.topcertifier.com

EINFÜHRUNG IN ISO 27001:2013

ISO 27001:2013 ermöglicht es einer Organisation, Informationssicherheitsrisiken zu identifizieren. Berücksichtigung von Bedrohungen, Schwachstellen, Auswirkungen und Schutz der Organisation ohne die CIA (Confidentiality Integrity Availability) von Informationen durch die Übernahme zu gefährden ordnungsgemäßes Informationssicherheits managementsystem Die allgemeine Agenda von ISO 27001:2013 besteht darin, decken die folgenden Aspekte ab.

- Bereitstellung eines Modells für die Einrichtung, Implementierung, den Betrieb, die Überwachung, die Überprüfung und die Wartung und Verbesserung eines Information-ssicherheits-Managementsystems mit physischen und technischen Kontrollen.

- Stellen Sie sicher, dass das ISMS in die Geschäftsprozesse des Unternehmens integriert ist.

- Schaffen Sie eine Organisationskultur, die die aktive Beteiligung der Mitarbeiter fördert Informationssicherheits-Managementsystem.

BEGINNEN

Das Kickoff-Meeting ist ein wesentliches Instrument zur Kommunikation und Planung der Projektdurchführung mit minimaler Behinderung und um das Projekt innerhalb der geplanten Zeit und Kosten abzuschließen.Die Tagesordnung für das Kick-off-Meeting lautet:

- Diskussion des Projektplans: Dazu gehört auch die Diskussion über Rechenschaftspflicht und Verantwortung des Anteils Inhaber. Meilensteine und Ergebnisse im Projekt

- Leistungsumfang und Zertifizierungsumfang

- Gesetzliche und behördliche Anforderungen

BILDUNG DES KERNTEAMS

- Ernennung eines CISO
- Ernennung eines Informationssicherheits-Managementausschusses
- Ernennung interner Prüfer
- BCP-Manager
- Ernennung eines ISO-Leiters

TOPCERTIFIER
www.topcertifier.com

GAP-ANALYSE

In dieser Phase führen wir eine Lückenanalyse durch, um zu überprüfen, wie viele Ihrer aktuellen Praxen in der Lage sind den Standardanforderungen entsprechen. Praktiken werden anhand dieser vier Referenzkriterien überprüft

- Anforderungen der Norm ISO 27001:2013
- SOA
- Gesetzliche, gesetzliche und behördliche Anforderungen
- Kundenanforderungen
- Interne Richtlinien und Verfahren

Die Ergebnisse dieser Analyse werden in Form eines Gap-Analyseberichts dargestellt. Dieser Bericht gilt als Liste der Aktionselemente für die Erinnerung an das Projekt.

ISMS-Bewusstseinsschulung

Für die Mitarbeiter Ihrer Organisation wird eine ISMS-Sensibilisierungsschulung durchgeführt. Die Ausbildung Ziel dieser Sitzung ist es, den Mitarbeitern dabei zu helfen, Wissen zu erwerben, die Konzepte von ISO 27001:2013 zu verstehen, und Prozesse und Praktiken so auszurichten, dass ein sicheres und bedrohungsfreies Arbeitsumfeld geschaffen wird. Wenn das Personal geschult wurde, kann es denken und handeln und zur Erreichung des Ziels beitragen Ziele.

RISIKOREGISTER & SOA

Ein Risikomanagementverfahren muss dokumentiert und als Referenz für die Verwaltung verwendet werden identifizierte Risiken in Absprache mit allen Prozessverantwortlichen und Funktionsleitern. Wir verwenden ISO 31000 & ISO 27005 Risikomanagement -Standardtechniken zur Identifizierung, Analyse, Bewertung, Dokumentation, Priorisieren, behandeln und quantifizieren Sie die identifizierten Risiken. Dieser Schritt erstellt ein Risikoregister. Geeignetes Risiko Behandlungspläne werden auf der Grundlage der Risikobereitschaft und des CIA-Faktors des Unternehmens ermittelt. Die Ergebnisse solcher Maßnahmen werden berechnet, aufgezeichnet, bewertet und dokumentiert. Der Die Erklärung zur Anwendbarkeit (Statement of Applicabilit y, SOA) definiert und identifiziert die physischen und technischen Kontrollen auf Ihr Unternehmen anwendbar, basierend auf Ihren Geschäftsprozessen und Anforderungen.

TOPCERTIFIER
www.topcertifier.com

VERMÖGENSVERWALTUNG

Wir helfen bei der Entwicklung von Richtlinien und Verfahren zur Vermögensverwaltung durch die Abstimmung mit dem funktionale Köpfe und Verständnis für den Prozess. Das Hauptziel des Vermögens Management ist:

- Um organisatorische Vermögenswerte zu identifizieren und entsprechende Schutzverantwortlichkeiten zu definieren

- Um die unbefugte Offenlegung, Änderung, Entfernung oder Zerstörung der gespeicherten Informationen zu verhindern auf Medien

- Um sicherzustellen, dass die Informationen gemäß ihrer Bestimmung ein angemessenes Schutzniveau erhalten Bedeutung für die Organisation

NETZWERK-/KOMMUNIKATIONSSICHERHEIT:

Wir helfen bei der Entwicklung von Netzwerksicherheitsmanagementrichtlinien und -verfahren durch Koordinierung mit den Funktionsleitern und dem Verständnis für den Prozess. Das Hauptziel der Netzwerksicherheit ist:

- Gewährleistung des Schutzes von Informationen in Netzwerken und der unterstützenden Informationsverarbeitung Einrichtungen

- Um die Sicherheit der innerhalb einer Organisation und mit anderen übertragenen Informationen aufrechtzuerhalten jede externe Entität

VORFALLMANAGEMENT

Wir helfen bei der Entwicklung von Richtlinien und Verfahren für das Vorfallmanagement, indem wir uns mit dem koordinieren funktionale Köpfe und Verständnis für den Prozess. Das Hauptziel des Vorfalls Management ist:

- Gewährleistung eines konsistenten und effektiven Ansatzes für das Management der Informationssicherheit Vorfälle, einschließlich der Kommunikation zu Sicherheitsereignissen und Schwachstellen

ISO 27001:2013
SERVICE-METHODE

TOPCERTIFIER
www.topcertifier.com

GESCHÄFTSKONTINUITÄTSMANAGEMENT

Wir unterstützen Sie bei der Entwicklung von Richtlinien und Verfahren für das Business-Continuity-Management Koordination mit den Funktionsleitern und Verständnis für den Prozess. Das Hauptziel Das Geschäftskontinuitätsmanagement sieht wie folgt aus:

- Um sicherzustellen, dass die Kontinuität der Informationssicherheit im Geschäftsbetrieb der Organisation verankert ist Kontinuitätsmanagementsysteme

- Sicherstellung der Verfügbarkeit von Informationsverarbeitungseinrichtungen

PHYSIKALISCHE SICHERHEIT:

Wir helfen bei der Entwicklung von Richtlinien und Verfahren zur physischen Sicherheit, indem wir uns mit dem koordinieren funktionale Köpfe und Verständnis für den Prozess. Das Hauptziel von Physical Sicherheit ist:

- Um unbefugten physischen Zugriff sowie Schäden und Eingriffe in die Organisation zu verhindern Informations- und Informationsverarbeitungseinrichtungen

- Um Verlust, Beschädigung, Diebstahl oder Gefährdung von Vermögenswerten sowie Unterbrechungen im Betrieb der Organisation zu verhindern Operationen

PERSONALSICHERHEIT:

Wir helfen bei der Entwicklung von HR-Richtlinien und -Verfahren durch Abstimmung mit den Funktionsleitern und Verständnis für den Prozess. Das Hauptziel der Personalsicherheit ist:

- Um sicherzustellen, dass Mitarbeiter und Auftragnehmer ihre Verantwortlichkeiten verstehen und dafür geeignet sind welche Rollen sie in Betracht ziehen

- Um die Interessen der Organisation im Rahmen des Änderungs- oder Beendigungsprozesses zu schützen Anstellung

- Sicherzustellen, dass alle Mitarbeiter und Lieferanten angemessen geschult wurden Respekt vor der Informationssicherheit

TOPCERTIFIER
www.topcertifier.com

DOKUMENTATION

Unsere Experten listen die Richtlinien, Prozesse, SOPs, anwendbaren SOA und Aufzeichnungen auf, die vorhanden sein müssen werden gemäß den Anforderungen der ISO 27001:2013 definiert und dokumentiert, indem mit jedem besprochen wird Als Abteilungs- und Funktionsleiter unterstützen wir Sie bei der Erstellung der notwendigen Dokumentation.

Etablieren Sie ISMS-Kontrollen

Sobald die Richtlinien, Prozesse, Statement of Applicability (SOA), seine Kontrollen und SOPs vorliegen wurden dokumentiert und eine Liste der zu sammelnden Aufzeichnungen sowie das Personal wurden aufgelistet Identifiziert und für solche Aktivitäten geschult, besteht die Notwendigkeit, die zu bedienen, zu überwachen und zu überprüfen Effizienzen solcher Prozesse.

INTERNE AUDITOREN-SCHULUNG

Für das identifizierte Personal wird eine Schulung zum internen Auditor (IA) nach ISO 27001:2013 angeboten. Durch diese Schulung wird dieses Personal in die Lage versetzt, den Bedarf an Folgenabschätzungen zu analysieren, Folgenabschätzungen zu planen und einzuplanen und sich vorzubereiten Audit-Checklisten zu erstellen, eine Folgenabschätzung durchzuführen und ihre Beobachtungen zu dokumentieren und der Unternehmensleitung mitzuteilen Management.

INTERNE AUDIT

Unsere Experten überwachen die Durchführung der internen Revision durch Ihr internes Revisionsteam. Durch dieses interne Audit werden noch bestehende Lücken im System identifiziert und deren Ausmaß nachgewiesen Vorbereitung auf das Zertifizierungsaudit. Dieses Audit gibt der Organisation die Chance dazu Identifizieren und beheben Sie alle Nichtkonformitäten, bevor Sie mit dem Zertifizierungsaudit fortfahren. Die SpitzeDas Management wird über die Ergebnisse der internen Revision informiert.

TOPCERTIFIER
www.topcertifier.com

ROOT-CAUSE-ANALYSE (RCA) UND KORREKTURMASSNAHMEN

Alle Nichtkonformitäten, die während des internen Audits, der Kunden- oder Drittaudits oder von festgestellt wurden Risikobewertung und Risikobehandlungsmethodik, Risikoregister, Vorfallregister, Schwachstelle Bewertungs- und Penetrationstest-Bericht (VAPT), Malware-Angriffe, Ausfallzeitregister, Netzwerk Probleme, Zugangskontrollen, Vermögensregister, Risikobewertungsberichte Dritter, CIA-Informationen Klassifizierung, interne und externe Angriffe sowie sonstige Quellen müssen aufgeführt werden. RCA zu sein durchgeführt mit Techniken wie Brainstorming und Fish-Bone-Methoden. Das optimale Korrektiv Aktionen werden umgesetzt. Die Wirksamkeit solcher Maßnahmen wird dokumentiert und überprüft durch a Korrekturmaßnahmenbericht (CAR).

Management-Review-Sitzung (MRM)

Das MRM ist eine Gelegenheit für alle ISMS-Stakeholder, sich in geplanten Abständen zu treffen, um zu überprüfen, Besprechen und planen Sie Maßnahmen zu den folgenden Tagesordnungspunkten.

- Wirksamkeit des aktuellen Managementsystems in Bezug auf ISMS
- Pläne und Aufzeichnungen zur Risikobewertung und Risikobehandlung
- Ergebnisse zur CIA (Vertraulichkeit, Integrität und Verfügbarkeit) der Informationen
- Prüfungsfeststellungen und Nichtkonformitäten aus allen Quellen
- Korrekturmaßnahmenplan zur Lösung aller offenen Punkte
- Kontinuierliche Verbesserungen am System
- Erforderliche Ressourcen und Schulungen
- Gesetzliche und Compliance-Aspekte

ZERTIFIZIERUNGSAUDIT: STUFE 1

Wenn der Vorbereitungsgrad ein angemessenes Niveau erreicht hat, beginnt der Zertifizierungsprozess beginnt. Ein von der Zertifizierungsstelle (CB) ernannter Auditor überprüft den Standard Anforderungen durch ein Stufe-1-Audit. Dabei überprüft der Prüfer die Richtlinien, Prozesse, SOPs, SOA, kritische Betriebsaufzeichnungen, IA- und MRM-Aufzeichnungen. Alle größeren Abweichungen von den CBs Die Erwartungen werden an dieser Stelle benachrichtigt, damit die erforderlichen Korrekturen vorgenommen werden können. Dies reduziert die Wahrscheinlichkeit schwerwiegender Abweichungen während des Zertifizierungsaudits. Der TOP-Zertifizierer wird die Verbindung herstellen mit allen Beteiligten und überwacht den reibungslosen Abschluss des Audits.

TOPCERTIFIER
www.topcertifier.com

ZERTIFIZIERUNGSAUDIT: STUFE 2

Nach erfolgreichem Abschluss des Audits der Stufe 1 konzentriert sich der Auditor auf eine detaillierte Prüfung des Berichts und Dokumentation des Informationssicherheits-Managementsystems der Organisation. TOPCertifier hätte Ihr Personal sicher in die Audit-Anforderungen eingewiesen vor der Prüfung stehen. Unsere Experten stehen Ihnen mit allen für den reibungslosen Ablauf erforderlichen Maßnahmen zur Seite Funktionsweise der Prüfung. TOPCertifier unterstützt Ihr Team bei der Beseitigung etwaiger Nichtkonformitäten während des Audits identifiziert. Nach erfolgreichem Abschluss des Zertifizierungsaudits erhält TOPCertifier wird mit allen Beteiligten zusammenarbeiten, um das endgültige Zertifikat zu entwerfen, zu genehmigen und freizugeben.

FORTSETZUNG DER COMPLIANCE

TOPCertifier wird Teil der Compliance-Reise Ihres Unternehmens sein und Sie regelmäßig unterstützen Intervalle mit notwendigen Schulungen, Systemsupport und -updates, internen und externen Audits und regelmäßige Erneuerung Ihrer Zertifizierung.

ISO 27001:2013
SERVICE-METHODE