TOPCERTIFIER
www.topcertifier.com

サービス方法論
ISO 27001:2013
情報
セキュリティ管理
システム（ISMS）

TOPCERTIFIER
www.topcertifier.com

ISO 27001:2013 の概要

ISO 27001:2013 により、組織は情報セキュリティ リスクを特定できます。
脅威、脆弱性、影響を考慮し、組織を保護する
を採用することで、情報の CIA (機密性・完全性・可用性) を損なうことなく、
適切な情報 セキュリティ管理システム ISO 27001:2013 の全体的な課題は次のとおりです。
以下の側面をカバーします。

- 確立、実装、運用、監視、レビュー、維持のためのモデルを提供する
物理的および技術的制御による情報セキュリティ管理システムの改善。

- ISMS が組織のビジネス プロセスに統合されていることを確認します。

- 従業員の積極的な参加を奨励する組織文化を構築します。
情報セキュリティマネジメントシステム。

キックオフ

キックオフ ミーティングは、プロジェクトの実行に向けたコミュニケーションと計画を立てる-
ための重要なツールです 障害を最小限に抑え、計画された時間とコスト内でプロジェクトを-
完了します。キックオフミーティングの議題は次のとおりです。

- プロジェクト計画のディスカッション: これには、説明責任と利害関係者の責任に関するディ-
スカッションが含まれます。 ホルダー。プロジェクトのマイルストーンと成果物

- サービスの範囲と認証の範囲

- 法的および規制上の要件

コアチームの創設

- CISOの任命
- 情報セキュリティ管理委員会の設置
- 内部監査人の任命
- BCPマネージャー
- ISOリーダーの任命

TOPCERTIFIER
www.topcertifier.com

ギャップ分析

このフェーズでは、ギャップ分析を実施して、現在の実践がどれだけ当てはまるかを確認します。標準要件に沿っています。実践はこれら 4 つの参照基準に照らして検証されます

- ISO 27001:2013 標準要件
- SOA
- 法律、法定、規制上の要件
- クライアントの要件
- 内部ポリシーと手順

この分析の結果は、ギャップ分析レポートの形式で表示されます。このレポートは機能しますプロジェクトのリマインダーのアクション アイテムのリストとして。

ISMS啓発研修

貴社の従業員を対象にISMS啓発研修を実施します。トレーニング このセッションは、従-業員が知識を獲得し、ISO 27001:2013 の概念を理解できるように支援することを目的と-しています。 安全で脅威のない作業環境の実現に向けてプロセスと実践を調整します。スタッフがトレーニングを受けると、考えて行動し、目標の達成に貢献できるようになります。目標。

リスクレジスターとSOA

リスク管理手順は文書化され、リスク管理の参考として使用されます。 すべてのプロセス所-有者および部門責任者と協議してリスクを特定します。 ISO31000を使用しております& ISO 27005 リスク管理標準技術を特定、分析、評価、文書化、 特定されたリスクに優先-順位を付け、対処し、定量化します。このステップでは、リスク登録を作成します。適切なリスク治療計画は、企業のリスク選好レベルと CIA 係数に基づいて特定されます。 このようなア-クションの結果は計算され、記録され、評価され、文書化されます。の 適用ステートメント(SOA) は物理的および技術的管理を定義および特定します ビジネスプロセスと要件に基づ-いて組織に適用できます。

TOPCERTIFIER
www.topcertifier.com

資産運用管理

私たちは、資産管理のポリシーと手順の策定を支援します。
機能的な頭とプロセスについての理解。資産の主な目的
管理は:

- 組織資産を特定し、適切な保護責任を定義する。
- 保存されている情報の不正な開示、変更、削除、または破壊を防止するため
  メディア上で
- 情報がその規定に従って適切なレベルの保護を受けられるようにするため。
組織にとっての重要性

ネットワーク/通信セキュリティ:

ネットワークセキュリティ管理ポリシーと手順の策定を調整して支援します。
機能的な責任者とプロセスについての理解を深めます。
ネットワーク セキュリティの主な目的は次のとおりです。

- ネットワーク内の情報とそれをサポートする情報処理を確実に保護するため
設備
- 組織内および組織内で転送される情報のセキュリティを維持するため。
任意の外部エンティティ

インシデント管理

私たちは、インシデント管理のポリシーと手順の策定を支援します。
機能的な頭とプロセスについての理解。事件の主な目的
管理は:

- 情報セキュリティ管理に対する一貫した効果的なアプローチを確保するため
インシデント (セキュリティ イベントと弱点に関するコミュニケーションを含む)

TOPCERTIFIER
www.topcertifier.com

事業継続管理

私たちは、次のような方法で事業継続管理ポリシーと手順の開発を支援します。
部門責任者と調整し、プロセスを理解する。主な目的
事業継続マネジメントの内容は以下の通りです。

- 情報セキュリティの継続性を組織のビジネスに組み込むことを保証するため
継続管理システム

- 情報処理施設の可用性を確保するため

身体的セキュリティ:

私たちは、物理的セキュリティのポリシーと手順の開発を支援します。
機能的な頭とプロセスについての理解。フィジカルの主な目的
セキュリティは:

- 組織への不正な物理的アクセス、損傷、干渉を防止するため。
情報および情報処理施設

- 資産の紛失、損傷、盗難、侵害、および組織の活動の中断を防ぐため。
オペレーション

人的資源の安全:

部門責任者と連携して、人事ポリシーと手順の策定を支援します。
そしてプロセスについての理解。人事セキュリティの主な目的は次のとおりです。

- 従業員と請負業者が自らの責任を理解し、適切な業務に適していることを確認する。
考慮される役割

- 変更または終了のプロセスの一環として組織の利益を保護するため
雇用

- すべての従業員とベンダーに適切なトレーニングが確実に受けられるようにする。
情報セキュリティに関して

ISO 27001:2013
サービス方法論

TOPCERTIFIER
www.topcertifier.com

文書化

当社の専門家が、ポリシー、プロセス、SOP、適用可能な SOA、および必要な記録をリストします。
ISO 27001:2013 要件に従って、各担当者と話し合って定義および文書化されます。
部門や部門の責任者が必要な文書の作成を支援します。

ISMS管理の確立

ポリシー、プロセス、適用ステートメント (SOA) のコントロールと SOP が確立されると、
文書化され、収集される記録のリストがリスト化され、担当者が
そのような活動を特定し、訓練した後、必要となるのは、
そうしたプロセスの効率化。

内部監査員研修

ISO 27001:2013 内部監査人 (IA) トレーニングは、特定された担当者に提供されます。
このトレーニングでは、そのような担当者が IA の必要性を分析し、IA を計画およびスケ-
ジュールし、準備を行うことができるようになります。チェックリストを監査し、IAを実施し、-
観察結果を文書化して上層部に報告する 管理。

内部監査

当社の専門家が、御社の内部監査チームによる内部監査の実施を監督します。
この内部監査は、システム内にまだ存在するギャップを特定し、システムのレベルを実証します。
認証監査に直面する準備ができています。この監査は組織に次の機会を与えます。
認証監査に進む前に、すべての不適合を特定して修正してください。頂上
経営陣は内部監査の結果を知らされています。

TOPCERTIFIER
www.topcertifier.com

根本原因分析 (RCA) と是正措置

内部監査、顧客または第三者の監査中に特定されたすべての不適合、または
リスク評価とリスク処理方法論、リスク登録インシデント登録、脆弱性
評価および侵入テスト (VAPT) レポート、マルウェア攻撃、ダウンタイム
レジスタ、ネットワーク 問題、アクセス制御、資産登録、第三者リスク評価レポート、CIA 情報
分類、内部および外部攻撃、その他のソースをリストする必要があります。
RCAになる ブレーンストーミングやフィッシュボーン手法などの手法を使用して実行されます。
最適な矯正 アクションが実装されます。このようなアクションの有効性は文書化され、-
次の方法でレビューされます。 是正措置報告書 (CAR)。

経営検討会議 (MRM)

MRM は、すべての ISMS 関係者が予定された間隔で集まり、レビューを行う機会です。
以下の議題について話し合い、行動を計画します。

- ISMS に関する現在の管理システムの有効性
- リスク評価とリスク治療計画と記録
- 情報の CIA (機密性の完全性と可用性) に関する結果
- あらゆる情報源からの監査結果と不適合
- 未解決の項目を解決するための是正措置計画
- システムに対する継続的な改善
- リソースとトレーニングが必要
- 法定およびコンプライアンスの側面

認定審査: ステージ 1

準備レベルが適切なレベルに達すると、認定プロセスが開始されます。
が始まります。認証機関 (CB) から任命された監査人が基準を検証します。
ステージ 1 監査を通じて要件を満たします。これには、監査人がポリシー、プロセス、
SOP、SOA、重要な運用記録、IA、MRM 記録。CB からの大きな逸脱
必要な修正をもたらすために、この時点で期待が通知されます。これにより、
認証監査中に重大な不適合が発生する可能性。TOP 認証者が連絡します
すべての利害関係者と連携し、監査がスムーズに完了するよう監督します。

TOPCERTIFIER
www.topcertifier.com

認定審査: ステージ 2

ステージ 1 監査が正常に完了すると、監査人はレポートとレポートの詳細な監査に焦-
点を当てます。組織の情報セキュリティ管理システムの文書化。TOPCertifier
は、監査要件について、自信を持って従業員を訓練しているでしょう。監査に直面している。
当社の専門家が、スムーズな手続きのために必要なあらゆる手段を支援します。
監査の機能。TOPCertifier は、チームが不適合を解決できるよう支援します。
監査中に特定されました。 認証監査が正常に完了すると、TOPCertifier
すべての関係者と連携して、最終証明書の草案、承認、発行を行います。

コンプライアンスの継続

TOPCertifier は、組織のコンプライアンスへの取り組みの一部となり、定期的なコンプライア-
ンスの遵守を支援します。必要なトレーニング、システムのサポートと更新、内部および-
外部の監査の間隔 そして定期的に認定を更新します。