情報セキュリティ管理システム

ISO 27001:2022
チェックリスト

LRQA のチェックリストを使用することで、認証取得に向けた準備が十分にできているかどうかをご確認いただけます。

当てはまる項目にチェックを付けて、すでに満たしている ISO 27001:2022 の要求事項と、さらに注意が必要となりうる要求事項を明確に示した概要を確認します。チェックリストは ISO 27001:2022 の要求事項に従って構成されており、以下の主要分野をカバーしています。

- 組織の状況
- 利害関係者のニーズと期待
- リーダーシップと取り組み
- リスクと機会
- リスク対応

このチェックリストを活用すると、各要求事項に対する回答の選択とコメントの記入が簡単にでき、ISMS の全ての側面を包括的に理解する上で役立ちます。

セクション 01
組織の状況

附属書 SL に基づいて発行された ISO 27001:2022 は、ISMS を設計し導入する前に、組織の状況を徹底的に分析することの重要性を強調しています。この分析は、組織の特定のニーズと要求事項を判断し、最終的に ISMS の有効性を確保する上で重要です。事業が運営されている状況を十分に理解するために時間をかけることで、独自のリスクと機会に対処する、適合性の高い効果的な ISMS を作成できます。

チェックリストをご活用いただくことで、完了した要求事項を確認し、関連するコメントを追加できます。

- [ ] ISMS と望ましい結果を達成する能力に影響を与える可能性のある外部要因を特定している。

ここにコメントを入力

- [ ] ISMS と望ましい結果を達成する能力に影響を与える可能性のある内部要因を特定している。

ここにコメントを入力

- [ ] 適用範囲を定義して文書化する時、また ISMS を計画するときに、状況の要因（内部および外部）を考慮している。

ここにコメントを入力

- [ ] 状況上の要因の変化は、マネジメントレビュー中に定期的に見直されている。

ここにコメントを入力

セクション 02
利害関係者のニーズと期待

ISO 27001:2022 では、ISMS は、利害関係者のニーズと期待に加え、それらが望ましい結果にどのように影響するかを考慮しなければなりません。これは、運用から戦略までのシステムの適用範囲を決定し、組織のビジネス目標と整合させる上で不可欠です。組織は、管理下にある全ての関係者の理解と期待を評価し、システムの効果的な運用に関与させる必要があります。

- [ ] 他の利害関係者を含む、組織の管理下にある全ての人々のニーズと期待を特定し、これらのうちどれが法的要求事項とみなされるかを特定した。

ここにコメントを入力

- [ ] ISMS を計画し、適用範囲を定義して文書化する際に、利害関係者のニーズと期待を考慮した。

ここにコメントを入力

- [ ] 組織の管理下にある者に対して、利害関係者のニーズと期待を決定する際に相談し、そのニーズと期待をマネジメントが定期的に見直している。

ここにコメントを入力

- [ ] 組織の管理下にある者に加えて、ISMS や望ましい成果を達成する能力に影響を及ぼしうる利害関係者を特定した。

ここにコメントを入力

セクション 03
リーダーシップと取り組み

ISO 27001:2022 には、ISMS においてトップマネジメントがリーダーシップを発揮する方法と、従業員の役割に関する具体的な要求事項が含まれています。シニアマネジャーは、最終的な責任を負いながら、特定のタスクを割り当てることができます。その活発かつ積極的な参加は、ISMS を企業のビジネスと整合させ、情報セキュリティ方針、ビジネス目標、企業戦略の間の一貫性を確保するのに役立ちます。

- [ ] シニアマネジャーは、システムを遵守することの重要性を周知させ、組織の機能を支援することで ISMS の推進に直接関与しており、システムの有効性に貢献している。

ここにコメントを入力

- [ ] 情報セキュリティ方針には、情報セキュリティの要求事項を満たし、ISMS を継続的に改善するという取り組みと、情報セキュリティの目的（またはそれらを設定するためのフレームワーク）が含まれている。

ここにコメントを入力

- [ ] ISMS 内の関連する役割の権限と責任を定義し、周知させ、文書化した。

ここにコメントを入力

セクション 04
リスクと機会

ISO 27001:2022 は、システムの適用範囲内で、組織の状況と利害関係者に関連するリスクと機会の両方に効果的に対処できるよう ISMS を設計することを義務付けています。これは、マネジメントシステムがその目標と目的を達成できるかどうかという観点から、組織がリスクと機会を評価しなければならないことを意味します。この評価は、単に情報セキュリティ上の脅威やデータ保護規則の遵守にとどまらず、許容できないリスクを管理し、特定された機会を活用する計画に結びつかなければなりません。これらの措置の有効性は定期的に見直される必要があります。

☐ ISMS の期待される成果に関連するリスクと機会を決定した。

ここにコメントを入力

☐ リスクと機会を特定する際に、組織の全体的なビジネス戦略と目的、内部および外部の状況要因、利害関係者のニーズと期待、組織内の情報のライフサイクル、ISMS の適用範囲を考慮した。

ここにコメントを入力

☐ リスクと機会を、情報セキュリティの目的の定義、マネジメントシステムの計画、監視・測定のニーズの決定、マネジメントレビューの状況内で考慮した。

ここにコメントを入力

セクション 05
リスク対応

ISO 27001:2022 は、組織がリスク対応計画を確立し、実施することを要求しています。この計画は、適切な対応方法を選択し、その有効性を監視する上で効果的である必要があります。管理策の適切な選択を確保するために、ISO 27001:2022 の附属書 A に概説されているベストプラクティスと比較しなければなりません。リスク対応計画は、特定されたリスクオーナーによって承認され、受理される必要があります。

- [ ] 適切なリスク対応の選択肢を選ぶプロセスを導入した。

ここにコメントを入力

- [ ] 対応の選択肢を実施するために必要な組織、人材、物理的、技術的の管理策を決定するプロセスを導入している。

ここにコメントを入力

- [ ] 管理策を附属書 A と比較し、管理策が欠落していないことを検証した。

ここにコメントを入力

- [ ] 管理策の包含と除外の根拠を示す適用宣言書を作成した。

ここにコメントを入力

- [ ] リスクマネジメント計画についてリスクオーナーの許可を得ている。

ここにコメントを入力

ISO 27001:2022 教育研修および審査サービス

教育研修

ISO 27001:2022 に関する知識を深めるために、様々な学習スタイルで提供される各種コースを経験レベルに合わせて設計しています。

ギャップ分析

移行審査の前に、システムの重要な領域、リスクの高い領域、または脆弱な領域の特定に向けて、専門の審査員が支援するサービスです。

認定された認証

独立した 2 段階のプロセスにより、クライアントの能力を明確に示し、新たなビジネスの獲得と利害関係者との信頼構築を支援します。

統合審査

複数のマネジメントシステムを導入している場合、より効率的でコスト効率に優れた、統合審査 / 定期審査プログラムを活用できます。

コースを表示 →

LRQA を選ぶ理由

ローカル & グローバル

クライアントがどこにいても、LRQA がサポートします。世界中に 300 人以上の有能な審査員と 250 人以上の専任のサイバーセキュリティ専門家を擁する LRQA は、グローバルに一貫して卓越性を追求するとともに、ローカルにサービスを提供できます。LRQA の社員は、情報およびサイバーセキュリティのリスク、課題、規格、規制、フレームワークに関する詳細な知識を持つ技術の専門家です。

柔軟な提供

ほとんどの場合、ISO 27001 教育研修および認証サービスは、安全で安心な技術を使用してオンサイトまたはリモートで提供できます。LRQA のリモートサービスを選択すると、オンサイトと同じ高品質のサービスに加えて、柔軟性、迅速な配信、グローバルな専門知識へのアクセスなど複数のメリットを享受できます。

世界初の UKAS 認定機関

LRQA は世界初の UKAS の認定を受け、世界中の様々な規格の認証サービスを提供しています。LRQA は様々なセクターにわたり、各種の具体的な規格やフレームワークの開発に貢献し続けています。

コンプライアンスのその先へ

表彰歴のあるサイバーセキュリティ事業 Nettitude と共に、あらゆる脅威や脆弱性に対して第一線で防御・対応を提供する先進的なサービスにより、高度なサイバー脅威の一歩先を行くお手伝いをします。

サイバーセキュリティのあらゆる側面を、クライアントと一緒に取り組む

保証に関する LRQA の深い経験と、受賞歴のあるサイバーセキュリティサービス、脅威主導のインテリジェンスを組み合わせることで、クライアントのビジネスが直面する独自の脅威に対する洞察と防御を提供することができます。今日、明日、さらに将来のサイバーリスクに先手を打つことができます。

LRQA は世界の主要な国際的規格・スキームに準拠した審査、教育研修、認証サービスを展開するとともに、LRQA のスペシャリストである Nettitude を通じて、幅広い高度なサイバーセキュリティサービスを提供しています。クライアントのビジネスと協力して、直面している具体的な脅威を特定し、それらを軽減する戦略を構築する支援をします。LRQA がクライアントと協力してシステムを認証し、脆弱性を特定し、ブランド・インテグリティ（整合性）、財務、業務に影響を与えうる攻撃やインシデントの防止を支援します。

情報セキュリティ

LRQA の認証サービスが、ビジネスに不可欠な情報の保護と、国際的に認められたベストプラクティスの実証を支援します。

ISO 27001、ISO 27701、
ISO 27017、ISO 27018、
CSA STAR

詳細情報 >

オペレーショナル・レジリエンス

認証、教育研修、ガバナンス、リスク、コンプライアンスのサービスにより、混乱の予防、対応、復旧のために備えます。

ISO 22301、ISO 20000-1、
Cyber Essentials 認証

詳細情報 >

サイバー脅威からの保護

あらゆる種類のサイバー攻撃に対して第一線の防御と対応を提供するカスタマイズされたソリューションにより、サイバー脅威に先手を打つことができます。

セキュリティ保証テスト、
マネージドセキュリティサービス、
脅威インテリジェンス、
インシデント対応

詳細情報 >

YOUR FUTURE. OUR FOCUS.

LRQA について

認証・サイバーセキュリティ・検査・教育研修分野の比類なき専門知識を結集することにより、当社は世界的な認証のリーディングプロバイダーの地位を確保しています。

その伝統は誇るべきものですが、顧客との今後のパートナー関係を構築する上で、本当に重要なのは現在の当社の姿です。揺るぎない価値・リスク管理、軽減における数十年の経験・未来への的確なフォーカスを組み合わせることで、より安心・安全・持続可能なビジネス構築に向けてお客様をいつでも支援します。

独立した審査・認証・教育研修から、リアルタイムの認証技術・データによるサプライチェーン改革まで、当社の革新的なエンドツーエンドのソリューションが、変化の速いリスク環境に積極的に対処できるようお客様をサポートします。つまり、未来の状況を成り行きに任せるのではなく、お客様が自ら構築できるようになるのです。

お問い合わせ

詳細については、https://www.lrqa.com/ja-jp/ をご覧ください。

LRQA リミテッド
〒 220-6010
横浜市西区みなとみらい 2-3-1
クイーンズタワー A10 階