ISO 27001審査プロセス

CLIENT INFORMATION NOTE

はじめに

この「お客様へのお知らせ」(Client information note)は、LRQAの情報セキュリティマネジメントシステム審査プロセスにおける主要なステージについて説明するものです。審査プロセスには、通常、認証が推奨される前に2回の訪問審査があります。その2回の訪問審査は以下の通りです。

- ステージ1（文書審査と実地審査の計画立案）
- ステージ2（実地審査）

いったん登録証が発行されますと、認証の維持のために定期審査(Surveillance)が行われます。
LRQA審査員によるアプローチは、全てのステージを通してオープンで協力的な態度、且つマネジメントシステム認証への実際的なアプローチを採用することにより、審査に付加価値を与えるものとなっています。
審査日程（審査期間、審査開始及び終了時刻を含む）、審査チーム、審査対象部署については、審査が行われる前に貴組織と調整し、決定します。

ステージ1 – 文書審査並びに実地審査計画立案

審査の目的
この審査の目的は以下のとおりです。

- 有意義な実地審査(ステージ2)が行えるように、規格で要求されるマネジメントシステムプロセスや文書類が存在し、運用されていることを確認します。
- ビジネス目標とISMSとの関係を経営陣によるコミットメントにて確認します。
- 審査スコープ、審査チームに対する要求事項及び実地審査(ステージ2)の時期を確認します。
- リスクを識別していることを確認します。また有効なリスク対応方法と情報セキュリティ管理策の適用を確認します。
- 実地審査(ステージ2)の計画立案ができるように、貴組織の業務プロセスや業務活動についての情報を収集します。
- LRQAの提供するサービスについての質問を受けます。

審査の実施

審査(通常2日間)は、オープニングミーティングで始まります。ここで審査員はLRQAの審査方法を説明し、貴組織からは組織概要を説明していただくことになります。なおステージ1審査計画は事前に貴組織の合意を得ます。ステージ1審査計画には、マネジメントシステム全体の責任を有する‘トップマネジメント’へのインタビューが含まれます。

審査は以下の確認を含みます。

- ビジネス目的とマネジメントシステムとの関係性を確認するために、トップマネジメントにビジネスの戦略的な方向性とマネジメントシステムへの期待に関して確認させていただきます。
- リスクアセスメントとリスク対応プロセスの評価、そして選択した管理策の有効性を確認します。
- 審査規格に対するマネジメントシステム文書類、および予定している審査スコープを経営陣とのディスカッションを通して確認します。
- 管理目的の達成を確実にするために、予定している管理策についても評価します。
- 必要に応じて現場の視察を行います。
- ステージ2(実地審査)のための詳細な審査計画書を作成します。
- ステージ2審査までに貴組織に注意を払っていただきたい問題点だけではなく、良い面があればその審査所見も記載した報告書を作成します。なお報告書には、これらの指摘事項に相当するグレードを記述します。

審査員が通常、確認させていただく事項は下記の通りです。

- ビジネスの環境と戦略的な方向性
- 情報セキュリティ基本方針及び目的
- ISMS適用範囲
- リスクアセスメントとセキュリティ管理策の選択
- ISMSに関する主要な役割と責任
- コミュニケーション計画
- 法令要求事項
- リスク対応計画と計画の実施状況
- 監視測定と分析の計画
- 内部監査とマネジメントレビューの記録

審査はクロージングミーティングで終了しますが、その際ステージ1の審査報告書の内容を説明すると共に、ステージ2審査に関する安全・衛生およびセキュリティ上の注意事項や宿泊・交通等の事務的な事項を含む審査方法を確認します。

ステージ2 – 実地審査

審査の目的

この審査を通して審査員は貴組織のマネジメントシステムの実施状況に焦点をあてます。ステージ2審査の目的は、次の事項を確認することです。

- 基本方針、目的、管理策、手順が効果的に実施されていること
- 計画されたシステマティックな改善に対するアプローチが存在する
- 情報セキュリティプロセスがマネジメントシステムの中で管理されていること
- マネジメントシステムが審査規格の要求事項にすべて適合していること

審査の実施
審査はステージ1で準備されたプログラムに従って行います。審査チームのメンバーは、審査に立会う（審査所見を一緒に確認する）ことで審査を円滑に進めることができるガイドと供に審査部門を訪問します。ステージ2審査では、マネジメントシステム全体の責任を有する‘トップマネジメント’との面談が含まれます。（ステージ1審査で行われなかった場合のみ）

LRQAの審査チームは少なくとも，以下に関連する審査所見を報告します。

- ステージ1審査における指摘事項のフォローアップ
- 合意された審査スコープにおいて特定された事業活動やサービス
- 継続的改善と顧客満足を含む基本方針の達成に関するマネジメントシステムの有効性
- サービスマネジメントプロセスによる管理の実施状況
- マネジメントプログラムによる目標の遂行状況
- マネジメントシステムで要求されているシステムの運用と適切な記録の維持の状況
- マネジメントシステムのパフォーマンスと管理目的及び管理策の達成度に関する監視･測定の実施状況
- マネジメントシステムに対するトップマネジメントの関与とコミットメント
- 内部監査，是正・予防処置システム及びマネジメントレビューの有効性

審査での指摘事項を確認するためにデイリーミーティングを開催します。指摘事項を確認し、了承していただくためには、同ミーティングへの適切な方の出席が必要です。指摘事項の定義については、「審査報告」の項をご参照下さい。ただし、いかなる指摘事項のグレードも審査終了までは暫定的なものです。

指摘事項のまとめをクロージングミーティングで行い、次回審査工程の同意を得て審査は終了します。完成した報告書は貴組織の管理責任者に提出します。「Major NC」（重大な不適合）が発行されない場合、かつ「Minor NC」（軽微な不適合）に対する是正処置計画を提示していただいた場合には、認証を推奨することになりますが、LRQAオフィスのテクニカルレビューで問題がないことが条件となります。ただし「Major NC」（重大な不適合）が出された場合は、認証は延期され、「不適合に対して採られた是正処置」のレビューのためにフォローアップ審査が必要となります。その場合、LRQAのチームリーダーは貴組織と合意したうえでこのフォローアップ審査の計画を作成します。

定期審査(サーベイランス)

審査の目的
マネジメントシステムが認証されますと、LRQAは定期審査(Routine Surveillance)のプログラムの運用を開始しますが、これは通常6か月間隔で設定されます。定期審査の目的は、認証されたマネジメントシステムが引き続き、以下の通りであることを確認することにあります。

- 維持されていること
- 運用されていること、そして
- 継続的改善が行われていること

貴組織の事業活動、製品およびサービスの変更等の結果としてもたらされるマネジメントシステムの変更についても確認させていただきます。規格要求事項への適合が継続していることも確認させていただきます。

審査の実施
審査は、その直前の審査（ステージ2審査あるいは定期審査）で合意された定期審査プログラムにしたがって実施しますが、詳細はそのオープニングミーティングで決定します。
定期審査での一般的な確認項目は下記の通りです。

- 内部監査とマネジメントレビュープロセス
- インシデント報告とその管理状況
- セキュリティ管理目的に合致した管理策の実施状況
- 是正及び予防処置プロセス
- システム変更がリスクマメジメントへ与える影響、およびリスク対応策の有効性
- 主要スタッフの責任と権限の関係する変更

前回審査での指摘事項のレビューも行います。

定期審査が 6 か月毎に行われる場合、審査で出された「Minor NC」（軽微な不適合）のレビューは、通常次回の審査で行われます。
ただし定期審査において「Major NC」（重大な不適合）が発行された場合は、通常その発行日から 3 か月以内に、是正処置のフォローアップのための特別審査が行われます。「Major NC」（重大な不適合）の発行は、LRQAの認証プロセスにおいて保留そして取消への第一段階となります。
したがって、クロージングミーティングにおいて、LRQA審査員は審査結果を報告し、次回の審査プログラムの了解をとりますが、もし「Major NC」（重大な不適合）が発行された場合には審査員は是正処置のフォローアップのための特別審査を計画します。

更新審査

更新審査の計画
更新審査は3年に一度実施しますが、その直前の定期審査時に更新審査計画を作成し、確認していただきます。更新審査計画のプロセスには、以下のレビュー・プレビュー・プランニングの3ステップが含まれます。
レビュー
このステップには、過去のパフォーマンスのレビューが含まれます。

- 苦情その他のパフォーマンス指標に関する傾向の情報
- システム文書の改善
- 継続的改善事項の進捗（継続的改善ログ）
- 審査結果からのフィードバック
- 指摘事項のトレンド

これら過去のパフォーマンスのレビューに基づき、審査員は戦略及び目標の達成に関するマネジメントシステムにおける潜在的なリスクを特定します。

プレビュー
プレビューの目的は、審査を貴組織の戦略・目標に整合させることです。審査員はシニアマネジメントとコミュニケーションにより、貴組織の長期展望、例えばビジネスリスクを含む企業戦略、他社との競合、内外の環境の変化等を理解し、これらの展望、目標、戦略がマネジメントシステムもしくは利害関係者にどの様なインパクトを与えるかを確認します。
またプレビューは、更新審査後の3年間のサイクルに適応する将来的なテーマを特定する機会にもなります。

プランニング
次のステップは、更新審査計画の作成です。このプロセスにおいて審査員は以下を実施します。

- 過去の定期審査サイクル中に適切に取り上げられなかったシステムの側面を明確にし、この側面をどのように審査するかを計画します。
- 「レビュー」（上記参照）、「プレビュー」（上記参照）のステップにおいて得られた情報を活用します。
- （継続的改善ログを含む）特定されたテーマについても配慮します。
- 審査の対象とする場所、部署、プロセスそして活動を特定します。
- それぞれの審査対象のリスクに見合う審査時間を貴組織と合意します。
- 人的資源の有効活用をめざし、重複がないように計画します。
- 審査レポートの作成および貴組織への説明のために必要な時間を計画のなかに追加します。
- 上記の情報を審査計画にまとめます。

審査員は、すべての関係する部署の記録をレビューし、すべての関係するマネジャーとの話し合いの時間を設定します。

更新審査の実施

LRQAは、初回審査のステージ2と同じように、更新審査を実施します。加えて、以下の項目を確実にするため、貴組織のシステム文書類のレビューも行います。

- 文書類が引き続いて、貴組織にとって適切であること。
- 継続的改善も含めて、認証登録のための要求事項および認証範囲に適合していること。

認証変更

登録証上の記載項目の追加、変更もしくは削除がありましたら、いずれの場合も、登録変更に関する正式な申請書のご提出をお願いします。LRQAは、以下の項目を考慮するために、申請内容をレビューします。

- 審査員（チーム）に対する要求の追加、もしくは変更があるか。
- 審査工数の追加もしくは削減があるか。

貴組織に対しては、いずれの変更に対しても変更契約書によって連絡します。

もし当該の登録変更申請が貴組織の文書システムにおける大きな変更もしくは追加を必要としていると判断した場合、LRQAは別途、文書審査（ステージ1）を実施します。

事前に登録変更のための審査計画が作成されていない場合、登録変更審査は、ステージ2審査のプロセスに準じて実施します。もし、別途文書審査（ステージ1）を実施しない場合、あらかじめ計画された審査訪問（定期審査もしくは更新審査）の審査期間中にチームリーダーが関連の文書類をレビューし、かつ追加要素を審査する審査計画の変更に合意いただくことになります。

このように登録変更審査は、あらかじめ計画された審査訪問（定期審査もしくは更新審査）と複合して実施するか、もしくは別途単独の審査訪問として実施することも可能です。

LRQAは記載内容が変更された登録証を、現行の登録証と同じ有効期限を記載して発行します。

審査報告書

ステージ1、ステージ2、定期審査、更新審査等の報告書作成手順は概ね同じです。LRQAは、審査所見、決められた審査計画に対する進捗、良い点へのコメント、そして審査内容の説明を記録した審査報告書を作成します。審査所見は、「Major Nonconformity」（重大な不適合）もしくは「Minor Nonconformity」（軽微な不適合）として特定し、審査指摘事項ログに記録します、以下に、これらの格付けについて定義します。

Major Nonconformity（重大な不適合）：マネジメントシステムの1つ以上の要素が完全に欠落しているか、実施・維持ができていない、または客観的な証拠に基づき、マネジメントによる以下の達成が疑わしいと判断される状況。

- 組織の方針、目標または公式のコミットメント
- 適用される規制要求事項への適合
- 適用される顧客要求事項への適合
- 適用される審査基準（規格等）への適合

一般的に、Major NC（重大な不適合）は以下のシステムの欠陥を表します。

- システムの有効性もしくは成果物に既に影響を与えている
- マネジメントシステムの能力にリスクが発生している
- 直ちに「封じ込め」が必要である
- 直ちに根本原因の分析および是正処置が必要である

注）「封じ込め」とは、不適合が他に影響することを管理・軽減し、顧客先が運用するシステムへの流出を防止する行動。不適合状態がさらに悪化しないようにするための暫定処置および、すみやかなる是正処置と関係者への連絡・確認を含む。

審査チームリーダーは、フォローアップ審査のための手続きの調整を行います。

Minor Nonconformity（軽微な不適合）：実施・維持されているマネジメントシステムの弱点を示唆しているが、マネジメントシステムの実現能力に大きな影響を及ぼさない、またはシステムの成果物にリスクをもたらさないと考えられる所見を意味します。ただし、将来のマネジメントシステムの実現能力を確実にするために対応が必要です。

一般的に、軽微な不適合は内部のプロセスもしくは手順上の弱点、もしくは、いかなる種類であれ、さらに管理状態が悪くなり、システムの有効性を損なう可能性があると合理的に考えられる場合の所見です。不適合の根本原因の特定と是正処置が必要です。

登録証が発行される審査で軽微な不適合が挙げられた場合、担当審査員は、貴組織に対して是正処置計画を提出を求めます。この是正処置計画は、登録証を発行する審査の場合は、LRQAの事務所における認証決定のためのレビューの要件のひとつになります。軽微な不適合が6 ヵ月ごとの定期審査時に挙げられた場合は、貴組織において、審査後の適切な期間内に是正処置を実施する必要がありますが、通常、次回審査まで是正処置の詳細を提供していただく必要はありません。次回の審査で確認します。

いずれの場合も、次回の審査時に審査員は、審査指摘事項ログの是正処置の所見欄に貴組織が実施した是正処置をレビューした結果を記入します。

LRQAの審査報告書のコピーは、3年間は保管してください。例外的には、それ以前の審査報告書のご提示をお願いする場合もあります。

次回審査において審査員が不適合として指摘する可能性が見込まれ、貴組織がそれを避けるために対応していただきたい事象についても、審査報告書上の関連箇所に記録します。

既に適合しているマネジメントシステムであっても、実施対象のプロセスの有効性を改善する提案を記述することがあります。その場合は審査報告書中の以下のどちらかに記録します。

- 戦略的な改善提案は「エクゼクティブサマリー」
- 特定の部署/プロセスに関連する改善提案は、報告書本文中の「評価及び審査結論」

サンプリング

ここで留意していただきたい重要な点は、組織の活動のいかなる領域においても「不適合事項」が発見されないということが、必ずしも問題がないということを意味しないということです。なぜなら、審査はサンプリング技法に基づいているため、統計的には審査中に特定できない問題点が残っている可能性が常にあります。このことは貴組織において、自らのマネジメントシステムの内部監査を行う際にも常に覚えておいていただきたいことです。

守秘義務

LRQAは、貴組織から収集したいかなる情報（審査報告書の内容を含みます）も、貴組織の許可なしに第三者もしくは他の組織に開示することはしません（ただし認定機関から要求がある場合は、この限りではありません）。

その他の情報

貴組織のビジネスが各事業分野での要求事項を満たし、他社との競争力を維持するために、LRQAがどのようにお役にたてるのかを、より詳細にご理解いただくためには、LRQAジャパンのホームページwww.lrqa.com/jpをご参照ください。ここでは、私たちの審査サービスおよびその他関連のサービスについて、より多くの情報を提供させていただいています。

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

本書に示すすべての情報が正確かつ最新であるように、LRQA リミテッドでは細心の注意を払っています。ただし、情報の不正確さや変更について当社は一切の責任を負いません。
LRQA は、LRQA Group Limited およびその子会社の商号です。詳細については www.lrqa.com/entities をご参照ください。© LRQA Group Limited 2022

Your Risk Management Advantage