情報セキュリティ ISO 27001

規格概要ガイド

あなたが社内の情報マネジメントシステムを管理する情報セキュリティの責任者であっても、顧客のためにIT製品やサービスを開発する場合であっても、効果的な情報セキュリティマネジメントシステム（ISMS）を欠かすことはできません。ISMSは、厳しさを増し続ける顧客や提携先の要求事項を満たすための適切な管理策とシステムや製品の開発を確実なものにしてくれるでしょう。

組織がISO 27001認証のメリットを享受するには

ISO 27001：2013 （情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）は、‘利害関係者’の情報を保護するための（機密性、完全性及び可用性に対処した）適切な管理策が確実に整うようにすることを意図しています。これらには、顧客、従業員、取引先、一般的な社会のニーズが含まれます。マネジメントシステムを実際に運用するには、利害関係者の要求事項を理解することが必須です。

あなたが社内の情報マネジメントシステムを管理する情報セキュリティの責任者であっても、顧客のためにIT製品やサービスを開発する場合であっても、効果的な情報セキュリティマネジメントシステム（ISMS）を欠かすことはできません。

ISO 27001に適合したISMSは、取引先に対しても顧客に対しても、貴社が情報セキュリティを重要視していることの実証に役立ちます。

認定されたISO 27001の認証は、情報セキュリティマネジメントへの組織の取組みの強力な証明になります。

この規格概要ガイドは、自己の組織のためにISMS認証取得の職務を課された人々のための実務手引と助言を示すものです。

この規格概要ガイドは、LRQAのISO 27001主任監査員であるジョナサン・アルソップ（Jonathan Alsop）とLRQA ICTの技術部長であるロブ・アッカー（Rob Acker）によって改訂されたものです。

ISMS 実施にあたって

契約情報や価格情報、知的財産権などの機密情報を保護するための通常の商業的ニーズに加えて、近年、規制やコーポレートガバナンスの分野で新たな動きがあり［（サーベンス・オクスリー法（Sarbanes-Oxley）、コビット（Cobit）など）］、企業財務情報の完全性を求める声がかつてないほど強くなっています。情報セキュリティマネジメントシステム（ISMS）を導入することで、現在認められているベストプラクティスに従ってセキュリティ問題が対処されていることを示すことになります。

LRQAなどの第三者認証機関の審査を受け、ISO 27001のマネジメントシステム認証をもつことで、貴社のISMSの適切性と有効性に対する独立かつ公平な見解が得られ、外部に向けた貴社の対応能力の実証につながります。

ISO 27001は、Plan - Do - Check - Act（PDCA）サイクルとマネジメントシステムプロセスを活用して、ISMSの枠組みを示しています。

- **認識**：参加者は、情報システム・ネットワークの必要性に加えて、セキュリティを高めるためには何ができるかを認識すべきです。
- **責任**：参加者全員が、情報システム・ネットワークの責任を担います。
- **対応**：参加者は、適時に協力して、セキュリティ事象を防止し、発見し、それに対応すべきです。
- **リスクアセスメント**：参加者は、リスクアセスメントを実施すべきです。
- **セキュリティの設計と実現**：参加者は、情報システム・ネットワークの基本要素としてセキュリティを具現化すべきです。
- **セキュリティマネジメント**：参加者は、セキュリティマネジメントに総合的なアプローチを採用すべきです。
- **再評価**：参加者は、情報システム・ネットワークのセキュリティについてレビューを行い、再評価を実施することに加えて、適宜、セキュリティ方針、実務、対策及び手順に修正を加えるべきです。

まずはじめに

組織の現状がどのようなものであれ、ISMS導入の第一歩は、経営陣の取組みと支援を得ることです。

トップマネジメントがモチベーションと方向性を示すという要求事項があり、トップマネジメントは積極的に関与してISMSの方向付けを確実にし、それが組織の戦略と両立するだけでなく、方針と目標のような重要な側面を確立することが必要です。

経営陣がISMS導入の理由を理解し、その設計と運用を完全に支援することが成功につながります。

成功への計画立案

企図するどのようなプロジェクトでもそうであるように、成功への道は、有意義で現実に即した計画を立て、その計画に沿ってパフォーマンスを測定し、予期しない事態が発生したときに変更できる体制を整えておくことが重要です。

計画段階で、マネジメントシステムの開発には時間と労力が必要であることを認識しておくべきであり、トップマネジメントは適切な資源を提供すべきです。

情報セキュリティの全般的責任はトップマネジメントが、またしばしば IT 部門が担うべきものですが、情報セキュリティの影響は IT システムだけにとどまらず、要員やセキュリティ、物理的セキュリティ、そして法令順守などにまで波及します。

ISO 27001 は ISO 9001:2015 に準拠しています。そのため、認定済みの品質マネジメントシステムをすでに導入している場合、これが ISMS の強固な基盤となります。そこで強くおすすめしたいのが、LRQA 教育・訓練コースの受講です。このコースでは、情報セキュリティの問題について他の受講者や講師と議論する機会もあります。

規格の理解

はじめの第一歩は規格を熟知して、満たさなければならない基準や規格の構成、それにご自身のISMSの構成と関連文書を理解することです。

この規格は二つのパートで構成されています。

- ISO 27002では、情報セキュリティリスクに対する個別のリスクを管理するために選択して実施できる、セキュリティ目標と管理策について記述しています。
- ISO 27001はマネジメントシステムの仕様書であり、ISMSを導入するために対処する必要のある、認証機関が認証評価の過程で監査基準とする要求事項について規定しています。

この仕様書には、全てのマネジメントシステムに共通の要素である、方針、リーダーシップ、計画、運用、マネジメントレビュー、改善が盛り込まれています。この仕様書はまた、具体的に情報リスクの特定にねらいを定めた箇条と、標準的な項目別に適切な管理策の選択を取り上げた部分（附属書A）も含まれています。

次は何か

ISMSには二つの主要な要素があり、それぞれをはっきりと異なる活動として取り扱うことができます。ISO 27001は、貴社に固有のセキュリティ要求事項を特定し、文書化するための、ISMSの構築を要求しています。

規格はまた、経営陣のコミットメント、責任、定めるべき管理策の実証に必要なマネジメントプロセス、すなわち、リーダーシップ、状況、マネジメントレビュー及び改善も要求しています。

マネジメントプロセス

このプロセスはISMSの効果的な導入にとって不可欠のものです。組織がすでにISO9001： 2015を運用しているのであれば、このプロセスはおなじみのものでしょう。

ISO 9001をすでに導入しているのであれば、情報セキュリティ要求事項を既存のマネジメントシステムに統合することが、しばしば最も効率的な方法であり、必要なときに必要な場所で、情報セキュリティの専門知識を確実に活用できるようになります。

このようなプロセスを初めて導入するのであれば、これらマネジメント要求事項の全ての含意を検討します。マネジメントシステムを効果的なものにするためには、トップマネジメントの影響と責任がとても重要であり、またISMSはトップマネジメントが推進すべきものですから、トップマネジメントの同意を得ることを確実にします。

ISMSの開発、導入及びモニタリングには、適切な資源（人、機材、時間及び資金）を割り当てるべきです。

内部監査では、マネジメントシステムが意図したとおりに運用されていて、改善の機会が特定されるかを検証します。

マネジメントレビューは、トップマネジメントに、マネジメントシステムがいかにうまく運用されていて、事業を支援しているかを評価し、理解する機会を与えるものです。

管理策の多くはISO 27001のマネジメント要求事項を補完するものですから、これらのマネジメントプロセスを附属書Aの管理目的に関連付けることができれば有益となるでしょう。

適用範囲の定義

ISMSの論理的及び地理的適用範囲を正確に定義して、情報セキュリティシステムとセキュリティ責任の境界を識別できるようにすることが不可欠です。適用範囲では、ISMSの対象となる人、場所及び情報を明確にすべきです。

適用範囲を定義して文書化したら、適用範囲の対象となる情報資産を、その価値と所有者とを合わせて特定することができます。

ISMS方針

ISMS方針に関連する要求事項は、ISO27001（5.2）とISO 27002の両方で取り上げられています。方針に関しては、ISO27001の他の要求事項と、方針に含めるべきものを示している附属書Aでも言及されています。例えば、ISMSの目的は、ISMS方針と整合するものでなければならない（6.2）などです。ある種の管理目的を達成するためには、別の方針が必要となるでしょう。

リスクアセスメント及びリスクマネジメント

リスクアセスメントはISMSを構築するための基礎です。リスクアセスメントではセキュリティ管理策の実施に焦点を合わせ、それらが最も必要なところに適用され、費用対効率が高く、そして、これもまた重要なことですが、効果の低いところには適用されないことを確実にします。リスクアセスメントは“どれほどにセキュティが必要か?”という問いへの解を得ることに役立ちます。

リスクマネジメントの重要な考慮事項の一つは、リスクをその好影響と悪影響の両面で検討する必要があるという点です。リスクとは不確かさが目的に及ぼす影響とみなされるもので、リスクマネジメントでは、うまく生かせる機会についても検討することが重要です。

リスクマネジメントは、情報資産の全ての所有者に関わる問題です。彼らなしに、効果的なリスクアセスメントを実施することはできないでしょう。

第一歩は、リスクアセスメントの方法を決め、次にそれを文書化することです。これには独特な、通常はコンピュータを使用するCRAMMのような方法があります。組織独自の構成と情報システムの複雑さに適した方法の選択や開発については、ISO31000に詳細が示されています。

リスクアセスメントプロセスは、情報資産の特定と価値評価を伴います。価値評価には金銭的価値以外のものがあり得ますので、風評被害や法令順守の困難さのようなものも考慮します（これには組織の置かれた状況が大きく影響します）。

このプロセスでは、脅威と脆弱性、それに資産とその活用の影響に付随する機会を検討すべきです。そして最後にリスクレベルを決定し、そのリスクを管理するために実施すべき管理策を明確にしなければなりません。

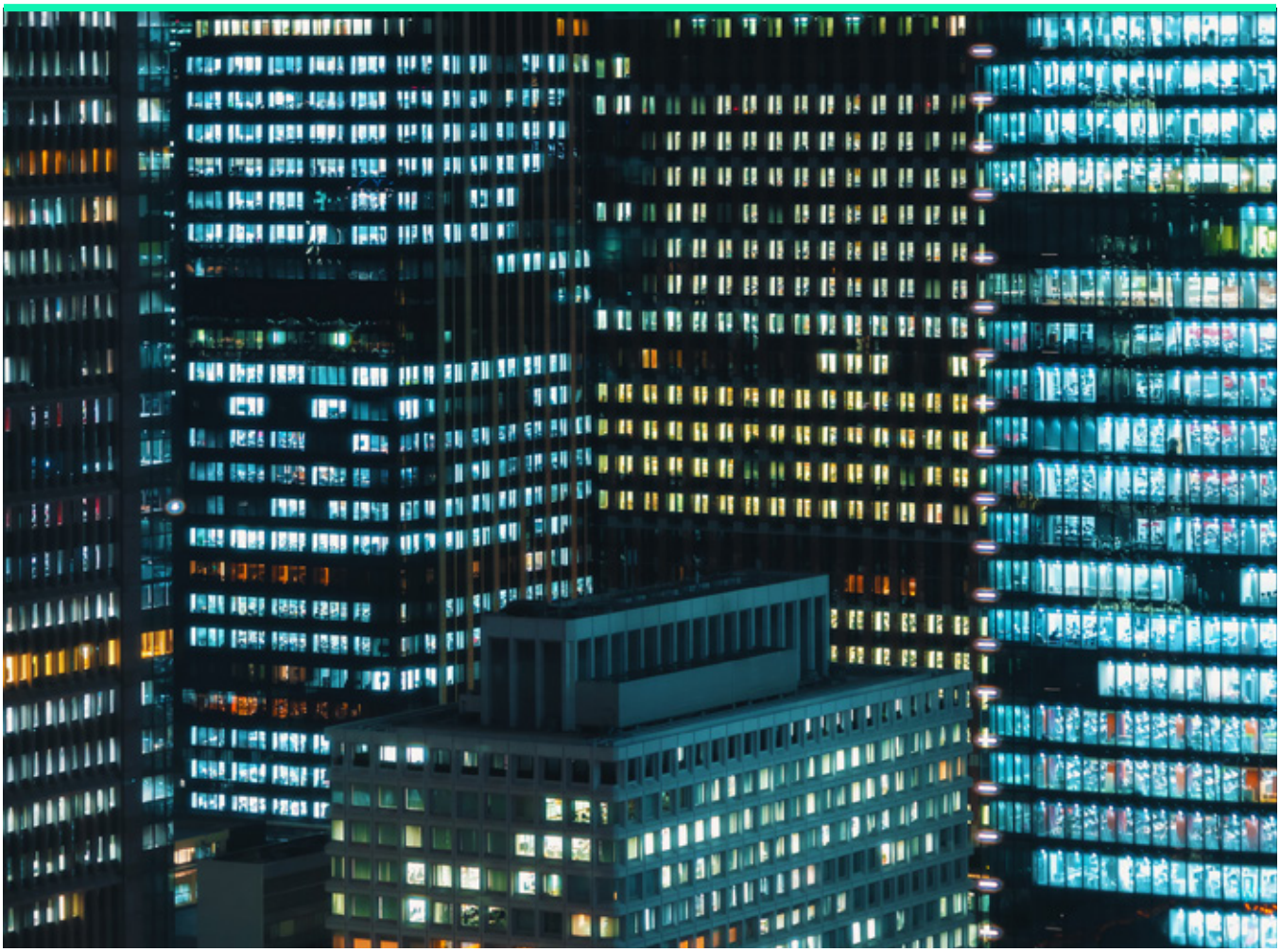
脅威、脆弱性、そしてそれらの影響の特定では、セキュリティ環境を考慮に入れなければなりません。例えば、施設内への物理的アクセスの拒否の脅威は、石油化学プラントに隣接する工業団地に拠点を置く組織のほうが、小さな都市のオフィス街にある事務所の場合よりも大きくなります。

同様に、クレジットカードデータ漏洩の脅威のほうが、小規模工務店の日々の生産データ漏洩の脅威よりも大きくなります。

リスク対応

リスクアセスメントでリスクレベルを特定し、次にそれを組織のセキュリティ方針で定められた許容リスクレベルと比較します。適切な処置をとって、許容レベルを超えたリスクを管理しますが、次のような処置が考えられます。

- 附属書Aから選択したセキュリティ管理策を実施して、リスクを許容レベルまで下げます。リスクレベルは再計算して、残留リスクが許容レベルを下回っていることを確認すべきです。選択した管理策を適用宣言書に記録しますが、これには、各管理策を含めた又は含めなかった正当性の根拠と状況を記載し、リスクアセスメントまでのトレーサビリティを示すべきです。
- マネジメントの方針とリスク許容の基準に従って、リスクを受容します。処置をとった後に、残留リスクが許容レベルを超えている場合があり得ますが、その場合は、残留リスクをリスク許容プロセスで検討すべきです。マネジメントのリスク許容記録を維持すべきです。
- セキュリティ環境を変更してリスクを排除します。例えば、データ処理アプリケーションに脆弱性が確認された場合にセキュリティの高いアプリケーションをインストールしたり、あるいは洪水のリスクがある場合に物理的資産をより高い階に移動したりというようなことです。このような決定には、事業と財務面を考慮に入れることが必要です。この場合もやはり、リスク除去処置の後に、残留リスクについて再計算すべきです。
- 適切な保険を掛けたり、又は物理的資産若しくは事業プロセスを外部委託したりすることによって、リスクを移転します。そのリスクを受容する組織は、自己の義務を認識した上で、そのリスクを受容することに合意すべきです。外部委託先組織との契約では、適切なセキュリティ要求事項を取り上げるべきです。リスク対応計画では、採用し計画した処置に加えて、未処理の処置の完了日程を明確にして、リスクを管理するために活用します。計画では処置の優先順位を定め、責任者と詳細な処置計画を含めるべきです。



LRQAの情報セキュリティ審査と教育研修サービス

広範囲にわたるオンラインと対面評価サービスは、あらゆる規模と場所の組織に適したもので、規格を最大限に活用できるようにお手伝いします。

教育研修

LRQAでは、お客様のマネジメントシステムおよび人材育成に向け、変化と改善をもたらすことを目的に研修を提供しています。

現在、以下のコースのほか、様々な研修を提供しています。

- 情報セキュリティ
  ISO/IEC 27001：2013 規格解説
- 情報セキュリティ
  ISO/IEC 27001：2013 内部監査員養成
- 個人情報保護
  JIS Q 15001：2017 規格解説
- クラウドサービス情報セキュリティ
  ISO/IEC 27017：2015 規格解説

ギャップ分析

審査員がこの作業を実施することで、認証の取得が可能なシステムを構築できるように、システムの重要な領域やリスクの高い領域、または弱い領域に焦点を合わせる機会がもたらされます。認証手続き中かどうかに関係なく、対象範囲はお客様が定義できます。

認証

通常はシステム評価と登録審査で構成される2段階のプロセスです。期間は組織の規模と種類によって異なります。LRQAのサービスをご利用いただく組織は、多くの場合、安全で信頼できるテクノロジーを用いたリモート方式での審査を選ぶことができます。このオプションにおいても、柔軟性や迅速な提供、査察に関するグローバルな専門知識へのアクセスなど、いくつものメリットが加わった、同じ高品質のサービスを受けることができます。

ISMS認証後、システムの継続的な有効性を確認するために定期審査が実施されます。これにより、ISMSが順調に運用され継続的に改善されていることが、お客様とお客様のトップマネジメントに保証されます。

ビジネス課題重点審査（FABIK）

Focused **A**ssessment **B**usiness **I**ssues and **K**aizen

これまでの定期審査をより進化させたのが、ビジネス課題重点審査「FABIK」です。 組織が真に重要と捉えていることに焦点を当て、組織のマネジメントシステムの適合性のみならず有効性も判断し、顧客のビジネスをより確かにすることを支援する審査です。効果的な審査及び組織のマネジメントシステムの審査登録を通じて、組織がマネジメントシステムを使用し、ビジネスを向上させることを支援するというLRQAのミッションに基づき、組織が真に重要と捉えていることに焦点を当て、組織のマネジメントシステムの適合性のみならず有効性も判断し、顧客のビジネスをより確かにすることを支援する審査です。経営層の方との話し合いで組織が抱えているマネジメントシステム上の課題を抽出して、課題解決の該当業務システムだけに焦点を当てて審査いたします。そのため、経営者の方が考える重要な課題を解決でき、より具体的な改善効果、メリットを得ていただくことが出来ます。

統合マネジメントシステムの評価

お客様がISMSと既存のマネジメントシステム（品質マネジメントシステムなど）との連携を検討している場合、評価や査察のプログラムを連携して調整することができます。

LRQAのサービスがもたらす利点

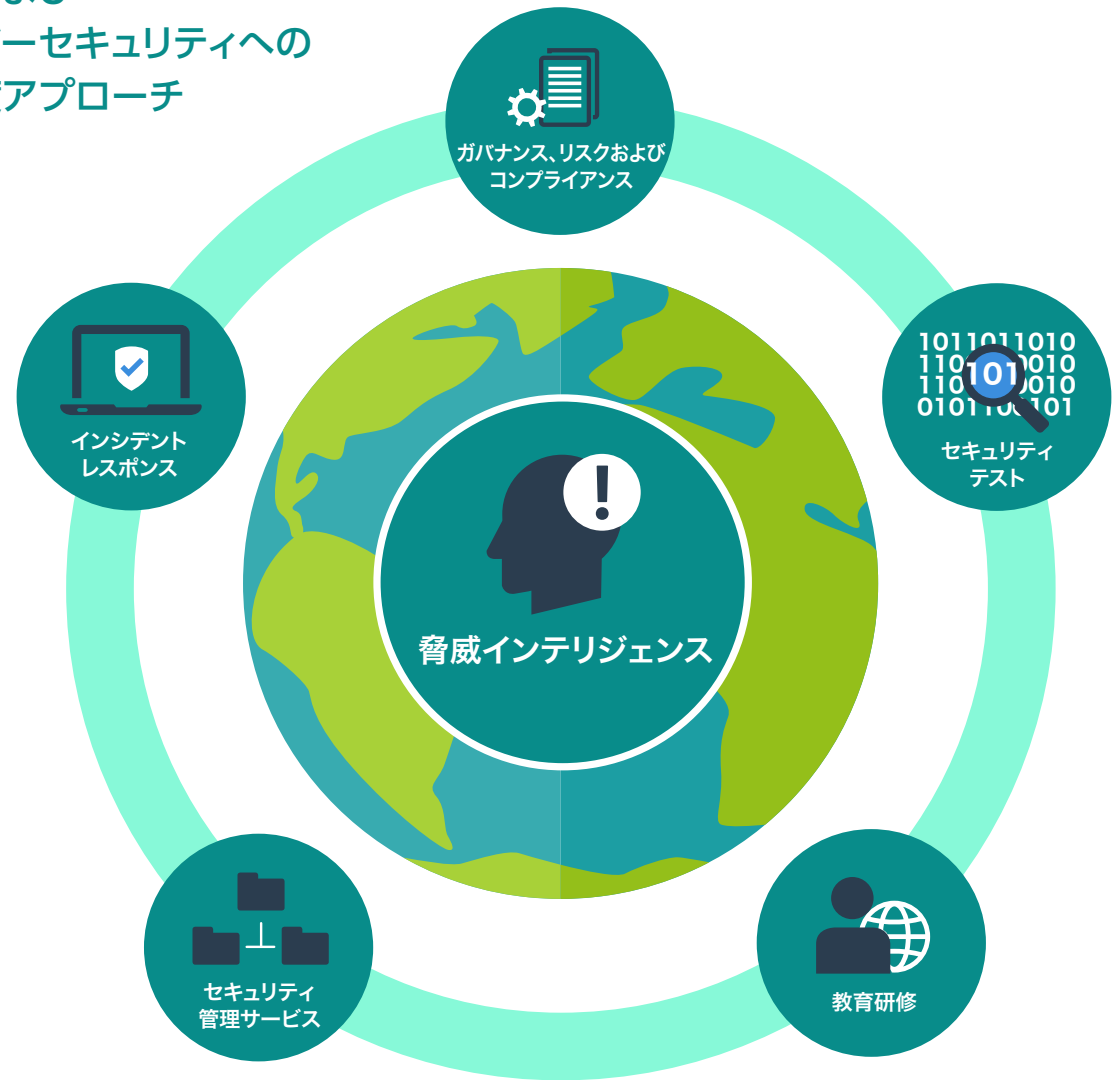
サイバーセキュリティのスペシャリストであるNettitudeと共に、LRQAは情報およびサイバーセキュリティへの360度アプローチを提供します。

顧客やサプライヤーそして、従業員が皆、貴社が情報を保護するために力を尽くすことを期待しています。

そこで、LRQAではお客様のビジネスをより深く掘り下げ、深い洞察とよりスマートなソリューションを提供します。

LRQAの審査員と教育研修講師は業界の専門家であり、ビジネスの運営に役立つよう、お客様と共に取り組むことを心掛けています。互いに協力し取り組むことで、長期的な価値を生み出し、ビジネス、従業員、顧客により大きな影響を与えます。

情報およびサイバーセキュリティへの360度アプローチ



NETTITUDE
A LLOYD'S REGISTER COMPANY

リスクベース ソリューション

ISO 27001：
情報セキュリティ戦略の基盤

ISO 27001は、情報セキュリティマネジメントシステムの中心に位置する規格です。ISO 27001は、ビジネスの規模や業界等関係なく、ビジネスに不可欠なデータを保護するための情報セキュリティリスクを特定、分析し、マネジメントシステムを実装するためのベストプラクティスフレームワークを提供します。

ISO 27001の第三者認証は、新規事業の獲得と既存顧客維持にむけ、組織が情報セキュリティを非常に重視している姿を示すことになります。

貴社のISMSを強化

効果的な情報セキュリティは、ISO 27001認証だけでは終わりません。

私たちは、お客様のISMSを補完強化につながるセクター固有の規格に関するサービスも提供しており、貴社の事業改善に向けて貴社のリスクプロファイルに応じ、様々なサービスを組み合わせてご提供することも可能です。

サイバーセキュリティだけでは、
十分とは言えません

脅威の状況は、ビジネスと同じくらい独特です。貴社の資産、リソース、およびデータ保護に必要な手順を決定する上で、リスクプロファイルが役立ちます。

LRQAは2018年3月、顧客とそのサービスの利用者の安全性のために、サイバーセキュリティのスペシャリストであるNettitude社を取得しました。

同社は顧客がサイバー脅威を特定、保護、検出し、それに対応して、そこから復旧できるように手助けするために、複数のセクターや地域に適用できるサイバーセキュリティの構築支援サービスを提供しています。

Nettitude社は、ペネトレーションテスト、脆弱性アセスメント、24時間年中無休のマネージドセキュリティサービス、インシデントレスポンスサービス、PCIコンプライアンスアセスメントなど、貴社の動作環境ニーズに合った幅広い高度なサイバーセキュリティサービスを提供します。

Nettitude社は、中央銀行や証券取引所、政府機関、そしてさまざまな業界の主要なグローバル企業などをクライアントに持ち、サイバーセキュリティサービスを提供しています。

同社のチームは、最高の技術力と資格を保持しており、世界初の認定を受けたセキュリティオペレーションセンターサービスの他、多くのサービスについてCRESTより認定を受けた世界でも数少ない企業の1つです。また、PCI ASV、PCI QSA、P2PE QSA、PA QSAの主任監査員もおり、SimulatedTarget Attack and Response (STAR) テストサービスの認定プロバイダーでもあります。

LRQAは、世界を牽引する様々な情報セキュリティ規格とベストプラクティスを提供します。

教育研修 ✓

ギャップ分析 ✓

認証サービス ✓

統合審査 ✓

YOUR FUTURE. OUR FOCUS.

LRQAについて

検査、認証、ブランド認証、サイバーセキュリティ、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、当社は世界的な保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。揺るぎない価値観、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。

独立した検証・認証・審査から、教育研修と技術アドバイザリーサービス、リアルタイムの保証技術、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

Email : japan-tech@lr.org
URL : https://www.lrqa.com/jp

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