JIS Q 27001:2014 FAQ

その２

注意事項：

① 本書に示した回答は、一般的な事例です。考え方の一つとして参考にする程度が望まれます。

② 各規格項番及び附属書 A. の各管理策は、それぞれが単独で存在するのではなく、全てがオーバーラップする構造になっています。したがって、同じ事例が本書での説明で使用する管理策と、他で発信される情報で使用される管理策と相違する場合があります。それは、中心をどこに置いて考えるかで変わってきます。そのような要素を持っていると認識することが重要です。

No.	項番	質問	回答
1	9.1 a)	Q1. 2006 年版であった管理策の有効性測定は無くなったのですか？	A1. 9.1 a）項にあります。2014 年版では、監視・測定の対象を決めて取り組むことを要求しています。あわせて、管理策だけでなく本文も考慮することを要求しています。
2	全般	Q2. JIS Q 27001:2014 の良い解説本をご紹介いただけませんか？	A2. 規格は画一的な構造や文書化を求めていません。 規格を活用する観点で、解説本に限らずセミナーなどで情報収集され、自組織にあったものを利用することをお勧めします。
3	7.5.1 0.1	Q3.「情報セキュリティマニュアル」、「リスクアセスメントマニュアル」など手順書類の改訂は必要ですか？	A3. マニュアルや手順書は、規格項番に合わせて作る必要はありませんが、規格要求事項を満足する必要があります。 特に文書化を要求している手順や記録がどこに反映されているかが特定できるかどうかで判断して下さい。
4	全般	Q4. 移行に向けて行った活動の記録は、どこまで残す必要がありますか？	A4. たとえば、2014 年対応でリスクアセスメントの手順を改訂した場合は、改訂したリスクアセスメント手順で実施する計画と、手順に従って実施したことが分かる程度に残すことが必要です。
5	全般	Q5. 移行は、文書を改訂するだけでいいのか？	A5. 文書の改訂後運用し、内部監査で確認し、マネジメントレビュー等で評価をする必要があります。

No.	項番	質問	回答
6	6.1.2	Q6. c)“情報セキュリティリスクを特定”、d)“情報セキュリティリスクを分析”に関して、2006 年版では附属書 A を割り当ててから行っていました。 2014 年版では、自分たちで行うとしていますが、やり方で良い方法はありませんか？	A6. JIPDEC の ISMS ユーザーズガイドの付録 2 では、情報セキュリティリスクアセスメントの 4 つの手法、留意事項が紹介されていますのでこれらを参考にするとよいでしょう。 例えば、4 つの手法の一つ「非形式的アプローチ」として、関係する複数の人でブレーンストーミングの手法を活用し、多角的な視点からリスクを特定したり、リスク分析することも、方法の一つと考えられます。 特に当事者を含めてブレーンストーミングを行うと、自らリスクに気づき、改善につながる効果が期待できます。
7	6.2	Q7. “関連する部門及び階層において、情報セキュリティ目的を確立”とありますが、どの程度まで要求されているのですか？	A7. 5.2　方針　b)の“情報セキュリティ目的の設定のための枠組みを示す”で設定した枠組みに対応した部門及び階層に整合させます。
8	7.2	Q8. 力量の c)　“とった処置の有効性を評価する”とは、具体的にどこまで要求されますか？	A8. 以下の要素を考慮して行います。 (ア) 必要な知識・技能は習得できているか (イ)OJT で行った成果物に問題は無かったか
9	7.2 7.3	Q9. “力量”と“認識”の項番が分かれました。同じでは？	A9. 必要な力量の要素に認識も含まれるかも知れませんが、当該の情報処理や業務上で必要とされる、最低限の知識と技能及びそれを適用する能力を意図しています。 認識は、規定を守らなかった場合に、どのような問題につながるかなどを理解し、行動するようになることを意図しています。
10	7.5	Q10. 文書と記録の識別が無くなりました。どのように理解すると良いですか？	A10. “プロセス”や“手順”の表記後の文書化は手順を規定した文書と理解し、“結果”や“証拠”の表記後の文書化は記録と理解すればよいでしょう。 その他の表現は“情報セキュリティ方針”や“適用範囲”など、掲示物や手順の中に文言として反映を期待している文書があります。
11	9.3	Q11. マネジメントレビューの要求事項が簡素化されました。重要性が変わったのでしょうか？	A11. マネジメントシステムを運営管理する上でマネジメントレビューの重要性に変更はありません。 項番が一つにまとまっただけと判断するとよいでしょう。

No.	項番	質問	回答
12	附属書 A.16.1.4	Q12. “情報セキュリティインシデントに分類するか否か”とは、どのようなことを行うことを要求しているのですか？	A12. ISMS の構築はインシデントの未然防止にあります。従って、懸念事項を出来るだけ多く収集し、活用することを期待しています。 収集した懸念事項を評価し、インシデント懸念の項目に未然防止を図ること、時機を逸しない対応を行うことを期待しています。
13	附属書 A.6.1.5	Q13. プロジェクトマネジメントの対象を教えてください。 (1) 顧客から受注した案件 (2) 社内業務システムのための開発案件	A13. “プロジェクト”とは、開始日と終了日がある特定の期間実施される活動であり、A.6.1.5 は、通常とは異なるリスクが“特定期間”に発生することが想定される場合や、プロジェクトによってリスクが変化する場合において、問題が発生しないように管理する管理策となります。従って、質問にあるいずれもが関係することが考えられます。他の管理策も有効活用する観点で検討することが重要です。 (1) 顧客からの受注案件については、製品･サービスの提供が特定の期間のみであれば、その期間中に特有のリスクを特定し、期間中、管理策を適用し、管理することが必要になるでしょう。また、新規製品･サービスメニューが追加されるような期間が限定されないような案件では、その製品･サービス提供に関わるリスクを特定し、管理策を決定、既存のプロセスに統合するまで(ISMS に組み込まれるまで)がプロジェクトマネジメントの対象になる可能性があります。 (2) 社内業務システム開発では、システムに組み込むべきセキュリティ条件の設定、組み込み、評価がプロジェクトマネジメントの対象となるでしょう。また、新規開発・導入に伴って、旧システムの廃棄、工事や設備の導入・移設を伴う場合は、通常とは異なる特有のリスクがプロジェクトの期間に存在するかもしれませんから、そうしたリスクへの対応、その対応状況の管理も対象になる可能性があります。

No.	項番	質問	回答
14	4.1 4.2	Q14. 新規格には、あらたな追加要求として、 4.1 組織及びその状況の理解、4.2 利害関係者のニーズ及び期待、がありますが、ここは、文書化は要求されていません。 従って、審査では、どのように審査するかを教えてもらいたいです。	A14. 4.3　“情報セキュリティマネジメントシステムの適用範囲の決定”で、ISMS の適用範囲は文書化が要求されています。 従って、文書化された適用範囲を審査する際に、適用範囲を決定するプロセス及び根拠として 4.1、4.2 を確認することになります。 6.1.2　情報セキュリティリスクアセスメント及び 6.1.3　情報セキュリティリスク対応ではプロセスの文書化を求めています。 このベースとして 6.1.1 項があり、この項目で 4.1 及び 4.2 とのつながりを要求しています。 従って、構築されたリスクアセスメントを審査する上で、4.1 項、4.2 項を確認することになります。 「ＩＳＭＳ ユーザーズガイド-JIS Q 27001 JIS Q 27001 :2014 (ISO/IEC 27001:2013)」を参照
15	10.2	Q15. 継続的改善は審査ではどのようなことを確認するのですか？	A15. “継続的改善”として単独で確認するのではなく、情報セキュリティ目的、内部監査、マネジメントレビュー、是正処置など ISMS の運営が効果的に行われ、継続的改善につなげているかが確認ポイントになります。