4.6.2.4　組織は、監査基準及び監査範囲を明確にする。[27001-9.2ｄ)]
　監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。
・監査の基準（以下の内容も含む。）
　―目的、権限と責任
　―独立性、客観性と職業倫理
　―専門能力
　―業務上の義務
　―品質管理
　―監査の実施方法
　―監査報告書の形式
・監査の範囲
・監査の頻度又は時期
・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）
4.6.2.5　組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2ｅ)]
　監査人の選定においては監査基準に従い、以下の点を考慮する。
・外観上の独立性
・精神上の独立性
・職業倫理と誠実性
　なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。
4.6.2.6　組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2ｆ)]
4.6.2.7　組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。[27001-9.2ｇ)]
　監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。
・監査の計画・実施に関する責任及び要求事項
・結果報告・記録維持に関する責任と要求事項
　要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。
4.6.3　マネジメントレビュー［27001-9.3］
4.6.3.1　トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。[27001-9.3]
　あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。
・マネジメントレビュー基本計画
・マネジメントレビュー実施計画
・マネジメントレビューのための実施報告
　基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。
4.6.3.2　トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3]
・前回までのマネジメントレビューの結果とった処置の状況
・情報セキュリティマネジメントに関連する外部及び内部の課題の変化
・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック
　―不適合及び是正処置
　―監視及び測定の結果
　―監査結果
　―情報セキュリティ目的の達成
・利害関係者からのフィードバック
・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況
・継続的改善の機会
　また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。
4.6.3.3　マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。[27001-9.3]
　マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。
・情報セキュリティマネジメントの有効性の改善
・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新
・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正
・必要となる経営資源の特定
・パフォーマンス測定方法の改善
　なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。
4.6.3.4　組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。[27001-9.3]
　マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。
4.7　情報セキュリティマネジメントの維持及び改善［27001-10］
4.7.1　是正処置［27001-10.1］
4.7.1.1　組織は、不適合が発生した場合、不適合の是正のための処置を取る。[27001-10.1ａ)]
ａ）是正措置を取る際は、以下を実施する。
・その不適合を管理し、是正するための処置
・その不適合によって起こった結果への対処
・是正処置を手順どおりに実施するために、以下について文書化する。
　―不適合の再発防止を確実にするために選択した処置の必要性の評価
　―必要な是正処置の決定
　―必要な是正処置の実施
　―実施した処置の記録
　―実施した是正処置のレビュー