4.5.2.2　組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。[27001-7.2ａ)]

情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。

・役職名
・業務内容
・担当者の責任範囲
・業務に必要な知識
・業務に必要な資格
・業務に必要な経験

知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。

4.5.2.3　組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。[27001-7.2ｂ)]

適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。

4.5.2.4　組織は、必要な力量を身につけるための処置をとり、とった処置の有効性を評価する。[27001-7.2ｃ)]

必要な力量を身につけるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクや、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。

教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するための取組を実施する。取組の例を以下に示す。

・知識の確認テスト
・スキルの実習テスト
・チェックリストなどによるベンチマーク

実施結果については記録し、要員選択の客観性を確保する。

4.5.2.5　組織は、力量の証拠として、適切な文書化した情報を保持する。[27001-7.2ｄ)]

教育、訓練については以下の例示を参考に検討し、定期的に実施する。

・教育・訓練基本計画
・教育・訓練実施計画
・確認テスト又は評価報告

教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。

4.5.2.6　組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3ａ)]

情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについて関係者の理解を深める。

4.5.2.7　組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3ｂ)]

以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。

・情報セキュリティマネジメントにおけるそれぞれの役割
・役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。）
・これらが記載された文書の所在

4.5.2.8　組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3ｃ)]

4.5.3　コミュニケーション［27001-7.4］

4.5.3.1　組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4]

ａ）内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。

・コミュニケーションの内容
・コミュニケーションの実施時期
・コミュニケーションの対象者
・コミュニケーションの方法

ｂ）内部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、適宜及び定期的なコミュニケーションを実施する。

・トップマネジメント
・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者
・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者
・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者
・組織内の従業員

ｃ）外部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、必要に応じて、コミュニケーションを実施する。

・取引先、パートナー、サプライチェーン上の関係者
・親会社、グループ会社
・当該組織のセキュリティを監督する省庁、政府機関
・所属するセキュリティ団体、協会

4.5.4　情報セキュリティマネジメントの運用の計画策定及び管理［27001-8.1］

4.5.4.1　組織は、次に示す事項の実施によって情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1]

・プロセスに関する基準の設定
・その基準に従った、プロセスの管理の実施