また、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ために、以下のような責任・権限を割り当てていることを確認する。

・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限
・リスクアセスメントにおいて、リスクを運用管理する責任・権限
・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限
・セキュリティ要求事項を満たしているか監査する責任・権限
・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限
・各プロセスの結果及び効果を組織内に周知する責任・権限

4.4.1.3　トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。[27001-5.1h)]

管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。

4.4.2　組織及びその状況の理解［27001-4.1］

4.4.2.1　組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。[27001-4.1]

・外部の課題
・内部の課題

これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。

a）外部状況
・国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術、経済、自然並びに競争の環境
・組織の目的に影響を与える主要な原動力及び傾向
・外部利害関係者との関係並びに外部利害関係者の関係及び価値観

b）内部状況
・統治、組織体制、役割及び責任
・方針、目的及びこれらを達成するために策定された戦略
・資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）
・内部利害関係者との関係並びに内部利害関係者の認知及び価値観
・組織の文化
・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
・組織が採択した規格、指針及びモデル
・契約関係の形態及び範囲

4.4.3　利害関係者のニーズ及び期待の理解［27001-4.2］

4.4.3.1　組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。[27001-4.2]

・情報セキュリティマネジメントに関連する利害関係者
・利害関係者の情報セキュリティに関連する要求事項

利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。

・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。
　―情報セキュリティに関する方針等を策定する人又は組織（トップマネジメント等）
　―セキュリティ管理策を全組織に徹底させる人又は組織（総務部、情報システム部等）
　―情報セキュリティ監査を行う人又は組織（監査室等）
　―組織内の情報セキュリティ専門家
・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

4.4.4　適用範囲の決定［27001-4.3］

情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。

4.4.4.1　組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。[27001-4.3]

a）組織は以下の点を考慮して適用範囲及び境界を定義する。
・自らの事業
・体制
・所在地
・資産
・技術の特徴
・外部及び内部の課題
・利害関係者の情報セキュリティに関連する要求事項
・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

b）情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。

c）情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。
・外部状況には、以下のようなものが含まれる。
　―国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術、経済、自然並びに競争の環境
　―組織の目的に影響を与える主要な原動力及び傾向
　―外部利害関係者との関係並びに外部利害関係者の関係及び価値観
・内部状況には、以下のようなものが含まれる。
　―統治、組織体制、役割及び責任
　―方針、目的及びこれらを達成するために策定された戦略
　―資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）
　―内部利害関係者との関係並びに内部利害関係者の認知及び価値観
　―組織の文化
　―情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
　―組織が採択した規格、指針及びモデル
　―契約関係の形態及び範囲