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、以下に例示するものが含まれ得る。

ａ）外部状況

・国外、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
・組織の目的に影響を与える主要な原動力及び傾向
・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観

ｂ）内部状況

・統治、組織体制、役割及びアカウンタビリティ
・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見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術）
・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。）
・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
・組織文化
・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
・利害関係者に関連する要求事項
・要求事項のうち、情報セキュリティマネジメントを通じて取り組むもの

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る場合もあるが、利害関係者には、以下に例示する人又は組織が含まれ得る。

・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・権限をもつ人又は組織。以下にその例を示す。
　―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、以下に例示するものが含まれ得る。
　―国外、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
　―組織の目的に影響を与える主要な原動力及び傾向
　―外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観
・内部状況には、以下に例示するものが含まれ得る。
　―統治、組織体制、役割及びアカウンタビリティ
　―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見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術）
　―情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。）
　―内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
　―組織文化
　―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

4.4.5　方針の確立［27001-5.2／6.2／5.1］

4.4.5.1　トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。［27001-5.2］

・組織の目的に対して適切であること。
・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組
・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。
・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。

また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。

4.4.5.2　組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。［27001-6.2］

ａ）情報セキュリティ目的は、以下を満たすこととする。

・情報セキュリティ方針と整合していること。
・（実行可能な場合）測定可能であること。
・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。