d）ソフトウェアの開発及び本番システムの管理
e）アプリケーションの使用及び管理
f）アプリケーションの使用及びデータベースの管理
g）情報セキュリティ管理策の設計、監査及び保証

5a-5.3.2　分離の管理策の設計においては、共謀のおそれを考慮する。
（5a-5.3.2参考）　小さな組織では、職務の分離を実現するのは難しい場合がある。しかし、この原則は、実施可能な限り適用することが望ましい。
5a-5.3.3　分離が困難である場合には、活動の監視、監査証跡、管理層による監督等の他の管理策を考慮する。
5a-5.3.4　役割に基づくアクセス制御システムを使用する場合に、一人の個人に対して、相反する複数の役割を許可しないことを確実にするように注意する。
5a-5.3.5　多数の役割がある場合、組織は、相反する役割を特定し、その除去を容易にするために自動化ツールの使用を考慮する。
5a-5.3.6　役割を除去又は再割当てする場合のアクセスの問題を最小限にするために、役割は慎重に定義し、付与する。

5a-5.4　管理層の責任

管理策：管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。
目的：　管理層が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。
詳細管理策

5a-5.4.1　管理層は、情報セキュリティ方針、トピック固有の方針、手順及び情報セキュリティ管理策に対する支援を実証する。
5a-5.4.2　管理層の責任には、要員について、次の事項を確実にすることを含む。
a）組織の情報及びその他の関連資産へのアクセスを許可する前に、情報セキュリティの役割及び責任について、要点を適切に伝える。
b）組織内で、情報セキュリティについて要員に期待する役割を示す指針を提供する。
c）組織の情報セキュリティ方針及びトピック固有の方針に従うことを指示する。
d）組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成させる。
e）組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件、契約又は合意を順守させる。
f）継続的な専門教育を通じて、情報セキュリティに関する適切な技能及び資格を維持させる。
g）実行可能な場合、情報セキュリティ方針、トピック固有の方針又は情報セキュリティのための手順への違反を報告するための、匿名の報告経路を提供する。これによって、匿名の報告を可能にする、又は報告者のアイデンティティに関する知識をその報告を扱う必要のある人だけが知ることを確実にする備えをもつことを可能にする。
h）組織のセキュリティ関連のプロセス及び管理策を実施するための、適切な資源及びプロジェクトを計画する時間を提供する。

5a-5.5　関係当局との連絡

管理策：組織は、関係当局との連絡体制を確立し、維持する。
目的：　組織と、関係する法務、規制及び監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。
詳細管理策

5a-5.5.1　組織は、いつ、誰が関係当局に連絡するか、及び特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。
5a-5.5.2　関係当局との連絡は、これらの関係当局の現在及び今後の期待についての理解を促進するためにも用いる。

5a-5.6　専門組織との連絡

管理策：組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持する。
目的：　情報セキュリティに関して適切な情報流通が行われることを確実にするため。
詳細管理策

5a-5.6.1　次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。
a）最適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。
b）情報セキュリティ環境の理解が最新であることを確実にする。
c）攻撃及びぜい弱性に関する早期警戒警報、勧告及びパッチを受理する。
d）専門家から情報セキュリティの助言を得る。
e）新しい技術、製品、サービス、脅威又はぜい弱性に関する情報を共有し、交換する。
f）情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する。

5a-5.7　脅威インテリジェンス

管理策：情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築する。
目的：　適切なリスク低減処置を講じることが可能となるように、組織の脅威環境についての認識をもつため。
詳細管理策

5a-5.7.1　既存の又は新たな脅威に関する情報を、次の目的で収集し、分析する。
a）脅威が組織に危害を及ぼすことを防止するために、十分な情報に基づく活動を支援する。
b）脅威の影響を減らす。
5a-5.7.2　脅威インテリジェンスを構成する次の３層全てを考慮する。
a）戦略的脅威インテリジェンス：脅威の動向に関する大局的な情報の交換
b）戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び技術に関する情報の交換
c）運用上の脅威インテリジェンス：技術的特徴を含む特定の攻撃に関する詳細