b）供給者が組織に提供するＩＣＴサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するようＩＣＴサービスの供給者に要求する。
c）ＩＣＴ製品に関して､その製品に他の供給者又は他のエンティティから購入又は取得した構成要素が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するようＩＣＴ製品の供給者に要求する。
d）ＩＣＴ製品の供給者に、製品で使用しているソフトウェア構成要素を記載した情報を提供するよう要求する。
e）ＩＣＴ製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した運用に必要な構成を説明する情報を提供するよう要求する。
f）提供されたＩＣＴ製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するための、監視プロセス及び許容可能な監視方法を実施する。このような供給者レビュー方法の例に、侵入テスト、及び供給者の情報セキュリティ運用に関する第三者立証の検証又は妥当性確認がある。
g）製品又はサービスの機能を維持するために重要な構成要素を特定し、文書化するプロセスを実施する。重要な構成要素に対しては、組織の外で作られる場合に必要とされる注意、精査及び更なるフォローアップの強化が求められる（特に、供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合。）。
h）重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。
i）提供されるＩＣＴ製品が期待どおりに機能し、予期しない又は好ましくない特性をもたないという保証を得る。
j）供給者からの構成要素が真正のものであり、その仕様から変更されていないことを確実にするためのプロセスを実施する。対策の例に、改ざん防止ラベル、暗号ハッシュ検証又はディジタル署名がある。仕様外の動作を監視することが、改ざん又は偽造を見つける手掛りとなる可能性がある。改ざんの防止及び検知は、設計、開発、統合、運用及び保守を含むシステム開発ライフサイクルの複数の段階で実施する。
k）ＩＣＴ製品が、例えば、正式な認証又は共通基準承認アレンジメント
（Common Criteria Recognition Arrangement）などの評価体系を通じて、必要なセキュリティレベルを達成していることの保証を得る。
l）サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定める。
m）ＩＣＴ構成要素のライフサイクル及び継続的な使用、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施する。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含まれる。代替供給者の特定、並びにソフトウェア及び力量を代替供給者に移転するプロセスを検討する。

5d-5.22　供給者のサービス提供の監視、レビュー及び変更管理
管理策：組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビューし、評価し、変更を管理する。
目的：　供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。
詳細管理策
5d-5.22.1　供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。
a）合意における情報セキュリティの条件の順守
b）情報セキュリティのインシデント及び問題の適切な管理
c）供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと
5d-5.22.2　供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。
a）合意の順守を検証するために、サービスのパフォーマンスレベルを監視する。
b）次の事項を含む供給者による変更を監視する。
1）現在提供されているサービスの強化
2）新しいアプリケーション及びシステムの開発
3）組織の諸方針及び諸手順の、変更又は更新
4）情報セキュリティインシデントの解決及び情報セキュリティの改善のための、新たな又は変更した管理策
c）次の事項を含む供給者サービスの変更を監視する。
1）ネットワークの変更及び強化
2）新技術の利用
3）新製品又は新しい版若しくはリリースの採用
4）新たな開発ツール及び開発環境
5）サービス設備の物理的設置場所の変更
6）下請負供給者の変更
7）他の供給者への下請負契約
d）供給者の作成したサービスの報告をレビューし、合意で求めている定期的な進捗会議を設定する。
e）独立した監査人の報告書が入手できれば、これのレビューと併せて供給者及び下請負供給者の監査を実施し、特定された問題の追跡調査を行う。
f）合意書並びに全ての附属の指針及び手順書の要求に従い、情報セキュリティインシデントの情報を提供し、その情報をレビューする。
g）供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する事業の中断・阻害の記録をレビューする。