14.2.4.3　パッケージソフトウェアの変更が必要な場合は、業者の同意を取得する。
14.2.4.4　パッケージソフトウェアの変更が必要な場合は、標準的なプログラム更新として、業者から必要とする変更が得られる可能性について確認を行う。
14.2.4.5　パッケージソフトウェアの変更が必要な場合は、変更の結果として、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。
14.2.4.6　パッケージソフトウェアの変更が必要な場合は、用いている他のソフトウェアとの互換性について確認を行う。
14.2.4.7　パッケージソフトウェアの変更が必要な場合、原本のソフトウェアは保管し、指定された複製に対して変更を適用する。
14.2.4.8　全ての認可されたソフトウェアに対して最新の承認したパッチ及びアプリケーションの更新を導入していることを確実にするために、ソフトウェアの更新管理手続を実施する。
14.2.4.9　将来のソフトウェア更新において、パッケージソフトウェアの変更を再び適用できるように、全ての変更は、十分に試験し、文書化する。
14.2.4.10　パッケージソフトウェアの変更が必要な場合には、変更は、独立した評価機関による試験を受け、正当性を証明する。
14.2.5　セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。
14.2.5.1　セキュリティに配慮したシステム構築の原則に基づき、情報システムの構築手順を確立し、文書化し、組織の情報システム構築活動に適用する。
14.2.5.2　セキュリティは、情報セキュリティの必要性とアクセス性の必要性との均衡を保ちながら、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。
14.2.5.3　新技術は、セキュリティ上のリスクについて分析し、その設計を既知の攻撃パターンに照らしてレビューする。
14.2.5.4　セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。
14.2.5.5　セキュリティに配慮したシステム構築の原則及び手順が、新規の潜在的な脅威に対抗するという点で最新であり続けていること、及び適用される技術及びソリューションの進展に適用可能であり続けていることを確実にするために、定期的にレビューする。
14.2.5.6　セキュリティに配慮したシステム構築の原則は、組織と組織が外部委託した供給者との間の、契約及び拘束力をもつその他の合意を通じて、外部委託した情報システムにも適用する。
14.2.5.7　組織は、供給者の設計のセキュリティに関する原則が、自身の原則と同様に厳密なものであることを確認する。
14.2.6　組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。
14.2.6.1　セキュリティに配慮した開発環境には、システムの開発及び統合に関連する要員、プロセス及び技術を含める。
14.2.6.2　組織は、個々のシステム開発業務に伴うリスクを評価し、システムによって処理、保管及び伝送されるデータの取扱いに慎重を要する度合いを考慮して、セキュリティに配慮した開発環境を確立する。
14.2.6.3　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、適用される外部及び内部の要求事項（例えば、規制又は方針によるもの）を定める。
14.2.6.4　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、組織によって既に実施されており、システム開発を支えるようなセキュリティ管理策を定める。
14.2.6.5　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、その環境で作業する要員の信頼性を考慮して要員を決定する。
14.2.6.6　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、システム開発に関連した外部委託の程度を考慮して委託先を決定する。
14.2.6.7　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、異なる開発環境の分離の必要性を考慮して環境を構築する。
14.2.6.8　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境へのアクセスの制御を実施する。
14.2.6.9　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境の変更及びそこに保管されたコードに対する変更を監視する。
14.2.6.10　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、セキュリティに配慮した遠隔地でのバックアップを保管する。
14.2.6.11　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境からの、及び開発環境への、データの移動を管理する。
14.2.6.12　特定の開発環境の保護レベルを決定した後、組織は、セキュリティに配慮した開発手順の中の該当するプロセスを文書化し、必要とする全ての要員にこれらを提供する。
14.2.7　組織は、外部委託したシステム開発活動を監督し、監視する。
14.2.7.1　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部委託した内容に関連する使用許諾に関する取決め、コードの所有権及び知的財産権に関わる事項を契約に含める。
14.2.7.2　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティに配慮した設計、コーディング及び試験の実施についての要求事項を契約に含める。
14.2.7.3　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部の開発者への、承認済みの脅威モデルの提供を契約に含める。
14.2.7.4　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の質及び正確さに関する受入れ試験を契約に含める。
14.2.7.5　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティ及びプライバシーについて、容認可能な最低限のレベルを定めるためにセキュリティしきい（閾）値を用いていることを示す証拠の提出を契約に含める。
14.2.7.6　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、引渡しに当たって、悪意のある内容（意図的なもの及び意図しないもの）が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。