5g-5.36.4　管理者及びサービス、製品又は情報の管理責任者が実施した情報セキュリティのレビュー及び是正処置の結果を記録し、また、その記録を維持管理する。

5g-5.36.5　管理者の責任範囲に対して、情報セキュリティの独立したレビューが実施されるときは、管理者は、独立したレビュー実施者に対して、その結果を報告する。

5g-5.36.6　情報セキュリティ要求事項の不順守に対する是正処置は、リスクに対して適切に、時機を失せずに完了する。

5g-5.36.7　次に予定している情報セキュリティのレビューまでに完了しない場合、そのレビュー時に少なくとも進捗状況を取り上げる。

5g-5.37　操作手順書

管理策：情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にする。

目的：　情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。

詳細管理策

5g-5.37.1　次の場合には、情報セキュリティに関連する組織の操作活動の手順書を作成する。

a）多くの人が同じ活動を行う必要がある場合
b）まれにしか行わない活動で、次に実行するときに手順を忘れている可能性が高い場合
c）新たな活動で、正しく実行しないとリスクが生じる場合
d）新しい要員に活動を引き継ぐ前

5g-5.37.2　情報処理設備の操作手順には、次の事項を明記する。

a）責任者
b）システムのセキュリティに配慮した導入及び構成
c）情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。）
d）バックアップ及びレジリエンス
e）スケジュールに関する要求事項。これには、他のシステムとの依存関係を含む。
f）作業中に発生し得る、誤り又はその他の例外状況の処理についての指示
g）操作上又は技術上の不測の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及びエスカレーション用の連絡先
h）記憶媒体の取扱いに関する指示
i）システムが故障した場合の再起動及び回復の手順
j）監査証跡及びシステムログ情報並びにビデオ監視システムの管理
k）容量・能力、パフォーマンス及びセキュリティなどの監視手順
l）保守手順

5g-5.37.3　情報処理設備の操作手順書は必要に応じてレビューし、更新する。

5g-5.37.4　情報処理設備の操作手順書の変更は認可のもとで行う。

5g-5.37.5　技術的に可能であれば、情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う。

6　人的管理策

6a　人的管理

6a-6.1　選考

管理策：要員になる全ての候補者についての経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加わる前に、及びその後継続的に行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。

目的：　全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。

詳細管理策

6a-6.1.1　選考プロセスは、フルタイム、パートタイム及び臨時スタッフを含む全ての要員に対して実行する。

6a-6.1.2　サービス供給者を通じて選考される個人に関して契約をする場合には、選考の要求事項を組織と供給者との間の合意に含める。

6a-6.1.3　組織内である職位に付けることを検討している全ての候補者についての情報は、当該法域での適切な法令を考慮して収集し、扱う。

（6a-6.1.3参考）　法域によっては、選考活動について、組織が候補者に事前に通知することが法的に必要な場合がある。

6a-6.1.4　要員になる候補者の確認は、関連があるプライバシー、ＰＩＩ保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。

a）満足のいく推薦状の入手の可否
b）応募者の履歴書の確認（完全であるか及び正確であるかの確認）
c）提示された学術上及び職業上の資格の確認
d）公的証明書の確認
e）候補者が重要な役割を担う場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認

6a-6.1.5　情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。

a）候補者が、情報セキュリティに関するその役割を果たすために必要な力量を備えている。
b）特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物である。

6a-6.1.6　最初の発令で就く業務であるか、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報を扱っているときには、組織は、より詳細な確認も検討する。

6a-6.1.7　選考手順には、要員になる候補者の確認のためのレビューの基準及び制約を定める。

6a-6.1.8　時機を失せずに要員になる候補者の確認を完了できない状況では、レビューが終了するまで、例えば、次のようなリスク低減のための管理策を実施する。

a）実務研修の開始時期を遅らせる。
b）企業資産の利用を遅らせる。
c）アクセスを限定した実務研修を実施する。
d）雇用を終了する。

6a-6.1.9　個人の役割の重要性に応じて、要員が適切であり続けることを確実にするための確認を定期的に繰り返す。