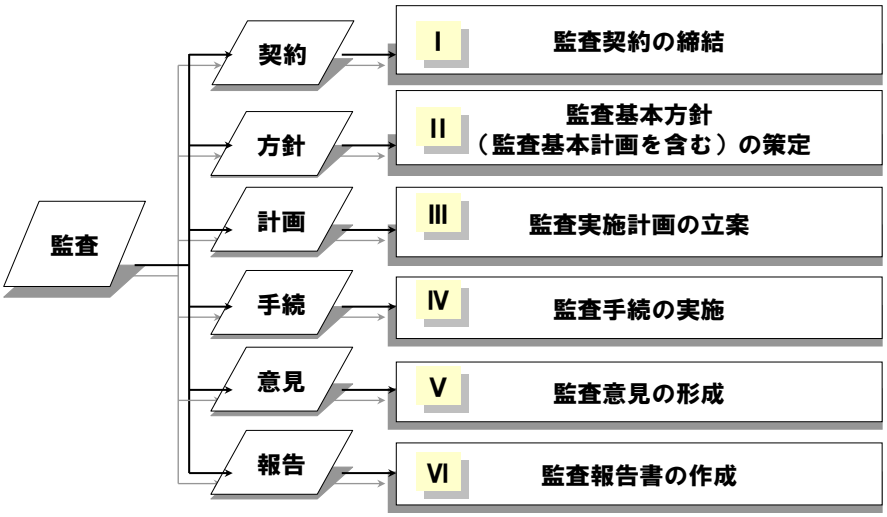
監査経験確認試験　【模範解答】

【例題】

現行の情報セキュリティ監査制度をふまえて、以下の問いに答えなさい。
なお、問題毎に指定された字数の範囲内で記述すること。

【問１】

助言型情報セキュリティ監査の全体プロセス（下図参照）のうち、「監査契約の締結」フェーズで行うことを説明しなさい。
（４００字以内）



【問１模範解答】

監査契約を締結する際には、監査組織は監査依頼者が提示している監査仕様書の内容を確認した上で適任と考えられる監査責任者の決定を行う。また、資格要件や独立性などの形式的要件及び、監査を実施する能力があるかなどの実質的要件を満たしているかも検討する。要件を満たしている場合は監査依頼者が要求している監査の目的・監査対象・使用する管理基準・監査対象期間などの確認を行う。監査仕様書にこれらの内容の記載がない場合は、監査依頼者に確認することも監査契約を締結する上では重要なことである。

監査に係わる契約リスクを評価するために、監査対象の業務内容などを確認することも必要である。監査を実施するのに必要な、監査対象の業種に特有の業務の知識が十分にあるかどうか、また期間内に監査を行えるかどうかなど、監査契約する際には、監査責任者が契約リスクを評価し確認しなければならない。

【問２】

情報セキュリティ監査の精度を向上させるため、監査技法をどのように組み合わせて情報セキュリティ監査を実施しますか。

これまでの情報セキュリティ関連業務あるいは他の監査業務での経験をふまえて、あなたの考えを１，２００字以内で述べなさい。

【問２模範解答】

私が監査を実施する場合は、三つ以上の監査技法を組み合わせて監査することが多い。
具体的な例を上げると、「情報資産を重要度に応じたラベル付けを行うこと」という規定に対して監査対象部門を監査する場合には、この規定がどのように社内で公開されているかを「閲覧」の技法を用いて確認する。規定文書として社内に保管しているケースもあるし、社内ポータルサイトに掲示されているケースもある。当然文書があるかないかだけではなく、発行日付が最新版であることも確認する。
次に「質問」の技法を用いて監査対象部門の複数の人に対して、ラベル付けの規定が周知されている事を確認する。確認するのは、規定に定められているラベル付けの基準をどのように解釈しているか、文書もしくは電子データの場合に、どこにラベル付けを記すのか、また、ラベル付けをどのタイミングで行うのかも確認する。
その後、ラベル付けが実際に行われている事を「視察」の技法を用いて確認する。社内文書の保管場所であるキャビネット、電子データであれば保管場所として決められたストレージなどを対象に実際の文書・電子データにラベル付けが行われている事を、自分の目で確認する。
この視察の時に私が気を付けているのは、ラベルを付ける場所によっては、社内文書の内容が目に触れる場合があるので、必要以上には内容を見ないようにする点と、監査証拠として文書名などを記録することを被監査人に了承を得ることである。
この例の場合は、「閲覧」「質問」「視察」だけだが、監査内容によっては「再実施」を加える場合もある。たとえばICカードによる入退室管理を執務室などの一般エリアとサーバ室などの機密エリアで、従業員によって入室制限が適切に行われているかを監査する場合は、「再実施」を行う。一般エリアしか入室が許されないICカードを機密エリアのカードリーダにかざし、入室できないことを確認する。
このようにアクセス制御されているかどうかを、確認する場合には「再実施」の監査技法を使うことが多い。「再実施」の技法を使用する場合には、エラーログなどが履歴に残ることがあるので、事前にシステム管理者にどのシステムに対していつ監査を行うかを連絡するようにする。
このように、規定が存在しているかを規定類の文書を「閲覧」して確認を行う。また、その規定が周知されているかを被監査人に「質問」して確認する。実際の運用がされているかは、「視察」と「再実施」で運用状況を確認する。このように三つ以上の監査技法を組み合わせて監査の精度を上げるようにしている。