

問 12 内部統制の整備状況の評価に関する次の記述を読んで、設問 1～4 に答えよ。

M 社は、株式上場している電子機器メーカーである。M 社では、金融商品取引法の内部統制報告制度に対応するために、内部統制の整備を行ってきた。この度、整備が一段落したので、監査部でその整備状況の評価することにした。監査部の N 君は、受注から代金回収までのプロセスの整備状況の評価を担当することになった。

[内部統制の整備状況の評価手順]

N 君が計画した内部統制の整備状況の評価手順は、次のとおりである。

- (1) フローチャート、職務記述書、リスクコントロールマトリックスなどの文書をレビューして、コントロールを理解し、予備の評価を実施する。その際、リスクを識別するに当たっては、不正や誤^び謬^うが発生した場合に、、網羅性、権利と義務の帰属、評価の妥当性、期間配分の適切性、表示の妥当性といった適切な財務情報を作成するための要件のうち、どの要件に影響を及ぼすかについて理解する。また、入力情報の完全性・正確性・正当性等を確保する統制、などの IT 業務処理統制の観点からも確認する。
- (2) 今回評価の対象にする取引を選定し、必要な証^ひ憑^{よう}を入手する。
- (3) 現場の視察や関係者に対するヒアリングなどを実施する。取引の発生時点から手作業や情報システムによる処理を経由して最終的に財務報告に反映されるまでのプロセスを追跡することで文書化の内容を検証して、コントロールの不備を把握する。
- (4) コントロールの改善や文書の修正を行う。必要に応じて情報システムも改善する。
- (5) 内部統制の整備状況の評価結果を文書化する。

[文書のレビュー]

まず、N 君は、フローチャート、職務記述書、リスクコントロールマトリックスなどの文書をレビューした。そのうちの受注プロセスのリスクコントロールマトリックスの抜粋は、表のとおりである。

表 受注プロセスのリスクコントロールマトリックス (抜粋)

想定されるリスク	番号	コントロール
不適切な顧客情報の登録	1	新規顧客と取引を開始する際には、業務課で財務状況などを調査する。経理課長が与信限度額を決定する。経理課担当者は、与信限度額を顧客マスタのほかの項目と併せて情報システムに入力する。経理課長は、入力内容を確認して承認する。
受注入力 の漏れ、誤り	2	受注入力は業務課の専従の受注担当者が行う。顧客からの注文はファックスで受け付ける。受注担当者は、受け付けたファックスに連番を振って情報システムに受注入力する。業務課長は、情報システムの入力内容をファックスと照合して承認する。
	3	入力データは、顧客マスタ及び商品マスタとチェックされ、各マスタに存在しないデータは入力できない。
ユーザ ID の不正使用	4	情報システムへのアクセスは、担当者のユーザ ID とパスワードで制御されている。業務課、経理課では必要な人だけがユーザ ID をもつことができ、ユーザ ID の登録・削除には、それぞれの上長の承認が必要である。
	5	管理課の担当者は、四半期ごとにユーザ ID とアクセス権の棚卸しを行い、不要なユーザ ID や間違ったアクセス権があれば、業務課や経理課に問い合わせ、ユーザ ID の削除やアクセス権の変更を行う。管理課長がその結果を承認すると、削除・変更が有効になる。
与信限度額を超えた受注	6	顧客の与信限度額を超える受注入力はできない。与信限度額を超える場合は、業務課長の承認後、経理課長の最終承認によって、当該受注案件に限って入力することができる。
	7	経理課では、与信限度額を年に一度、定期的に見直し、変更がある場合には、経理課長の承認を得た上で、情報システムに反映させる。

次に N 君は、関連部署にヒアリングを行った。

〔業務課へのヒアリング〕

- (1) 新規の顧客と取引を開始する際には、業務課が必要事項を調査し、その結果を経理課に提出する。与信限度額の決定や顧客マスタの入力は経理課で行われている。
- (2) 受注入力は、業務課の専従の受注担当者が行っている。顧客からの注文は、ファックスで受け付ける。受注担当者は、二重登録を避けるために、受け付けたファックスに連番を振る。受注担当者がファックスの内容を情報システムに入力した後、業務課長は、入力内容がファックスの内容と合っているかを確認して承認する。商品マスタ及び顧客マスタに存在しないデータは、情報システムに入力できない仕組みになっている。

- (3) ユーザ ID の登録・削除は、上長の承認を得て、管理課に提出する。
- (4) 受注担当者が不在や外出のときには、あらかじめ用意していた共有のユーザ ID を使って受注入力する。
- (5) 与信限度額を超えて受注入力できない場合は、業務課長の承認をもらって、該当顧客の限度額の変更依頼書を経理課に提出する。変更依頼書が承認されると、それ以降は変更後の与信限度額まで入力できる。

[経理課へのヒアリング]

- (1) ユーザ ID の登録・削除は、上長の承認を得て、管理課に提出する。
- (2) 新規の顧客と取引を開始するときは、業務課からの依頼に基づき、経理課長が与信限度額を決定する。
- (3) 経理課担当者は、与信限度額を含めた顧客情報を顧客マスタに登録する。経理課長は、入力された顧客情報を確認して承認する。
- (4) 業務課から与信限度額の変更依頼書を受領したら、経理課担当者は、不備がないかどうかを確認する。経理課長は、財務情報などと併せて内容を最終確認した上で、承認する。
- (5) 経理課担当者は、年に一度与信限度額の見直しを行う。変更した与信限度額も含め、更に変更が必要な場合には、経理課長の承認を得て、与信限度額を変更する。

[管理課へのヒアリング]

- (1) 管理課担当者は、四半期に一度、ユーザ ID とアクセス権の棚卸しを実施する。管理課だけがユーザ ID とアクセス権の変更権限をもっていて、間違いがあれば、担当者がユーザ ID の削除やアクセス権の変更を行う。その結果を管理課長が承認する。管理課長が承認した時点で、削除や変更の内容が初めて有効になる。承認時に内容の不備を発見したときには、管理課長が修正入力と承認をしている。

N 君は、ヒアリングの結果を受けて、リスクコントロールマトリックスの不備やコントロールそのものの欠如などの問題点を幾つか発見した。

設問1 本文中の a , b に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

- | | |
|---------------|-------------------|
| ア 資産の保全 | イ システム開発, 保守に係る管理 |
| ウ 実在性 | エ 統制環境 |
| オ 独立性 | カ 法令遵守 |
| キ マスタデータの維持管理 | ク モニタリング |
| ケ リスクの評価と対応 | |

設問2 N君が行った, [内部統制の整備状況の評価手順] の下線部の特徴がある, システム開発時のレビューなどでも使われる評価手法の名称を答えよ。また, この手法の留意点として不適切なものを解答群の中から選び, 記号で答えよ。

解答群

- ア コントロールごとに進めていくと話が飛びやすく混乱が生じやすいので, フローチャートの順序に従って話を進めるのが望ましい。
- イ 事前に質問事項や依頼文書のリストを参加者に伝えておくこと効率よく進められる。
- ウ 日ごろから業務にかかわっている担当者は, 潜在しているリスクや統制の弱点を見逃しがちである。
- エ 評価の対象とする取引数は, 作業負荷などを考慮した上で, できるだけ多く選択することが望ましい。
- オ プロセス全体や関連する情報システムに詳しい人員を参加させるべきである。

設問3 ヒアリング結果から, ユーザ ID 管理に関する問題点を二つ挙げ, それぞれ 40 字以内で述べよ。

設問4 ユーザ ID 管理以外で, リスクコントロールマトリックスどおりに実施されていないコントロールの番号を答えよ。また, それによって発生する問題は何か。30 字以内で述べよ。