演習１２　監査計画の策定

Sサービス株式会社の内部監査中期計画及び年度計画は以下のようになっています。

■中期計画

今年度は「ISMSの運用の確認を行う」となっている。

■年度計画

・開発部及び総務部の内部監査は５月に実施

・営業部の内部監査は７月に実施

今回、営業部においてISMSを導入する目的（テストケース参照）の③のうち、運用が適切に行われているかどうかを、内部監査で確認しようとしています。判断は、ISMSの運用がJIS Q 27001:2006の附属書Aに適合しているかどうかで行うことにしました。

演習１２－１．　内部監査計画書（営業部の内部監査の個別計画）を作成します。内部監査計画書の空欄を埋めてみてください。

監査計画書

（１）目的

演習12-1-1.　内部監査の目的をどうするか、書いてください。

　受託内容および受託データ、契約上の要求事項および個人情報保護を含む法規制上の要求事項を守るため、営業部においてISMSを導入する目的である仕組みの構築、運用、見直し、改善のうち、運用が適切に行われているかどうかを確認する。

（２）基準

演習12-1-2.　内部監査の基準をどうするか、書いてください。

・情報セキュリティ基本方針及び社内ルール

・JIS Q 27001:2006附属書A

（３）対象部署

演習12-1-3.　内部監査の対象となる部署をどこにするか、課のレベルで書いてください。

営業部 宣伝課

営業部 IT構築サポート課

(４)監査項目

演習12-1-4.　 “（１）目的”、“（３）対象部署”を考慮した上で、“（２）基準”で決定した基準から、どの項目を内部監査でチェックすればよいか、書いてください。

　　　　　　　　その際、教材の「個別計画の例(1/2)」の「監査範囲」の記述例を参考にして書いてください。

|  |  |  |
| --- | --- | --- |
| 基準項目 | 対象となる部署 | |
|  |  |
| ISMS文書管理手順書に従った文書の適切な管理  情報セキュリティ基本方針及び社内ルール | 営業部 | 宣伝課  IT構築サポート課 |
| 情報システムのマニュアルなどの文書は誰でも利用できるように、情報システムのそばに設置されている。  JIS Q 27001:2006附属書A  A.10.1.1 操作手順書 | 営業部 | 宣伝課  IT構築サポート課 |
| 持ち出し可能な記憶媒体の持ち出しルール  JIS Q 27001:2006附属書A  A.9.2.7 資産の移動 | 営業部 | 宣伝課  IT構築サポート課 |
| 社内で「極秘」「秘密」社外と「公開」以外に担当する情報やソフトウェアの授受を行う場合には所定の管理シートに記録、管理する。  JIS Q 27001:2006附属書A  A.9.2.7 資産の移動 | 営業部 | 宣伝課  IT構築サポート課 |
| 不要となったPCや記録媒体の廃棄ルール  JIS Q 27001:2006附属書A  A.10.7.2 媒体の処分 | 営業部 | 宣伝課 IT構築サポート課 |
| リモートアクセス及びテレワーキング  JIS Q 27001:2006附属書A  A.11.7.1 モバイルコンピューティング及び通信  A.11.7.2 テレワーキング | 営業部 | 宣伝課 IT構築サポート課 |
| ノートPCを社外に持ち出す際の運用  JIS Q 27001:2006附属書A  A.11.7.1 モバイルコンピューティング及び通信 | 営業部 | 宣伝課 IT構築サポート課 |
| 情報システムを利用できる時間は午前6時から午後11時までに限定  JIS Q 27001:2006附属書A  A11.5.6 接続時間の制限 | 営業部 | 宣伝課 IT構築サポート課 |
| アカウントの定期的な見直しに関する運用  JIS Q 27001:2006附属書A  A.8.3.3 アクセス権の削除 | 営業部 | 宣伝課 IT構築サポート課 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |