ICTマネージメント人材育成PBL教育プログラム

授業計画書

平成20年3月

KDDI株式会社

1

目次

1. コース概要及び目標・・・・・・・・・・・・・・・・P.3
2. コース構成　　・・・・・・・・・・・・・・・・P.4
3. 進行計画　　・・・・・・・・・・・・・・・・P.5
4. コース各段階の研修内容の概要と学習目標・・・P.6～P.7
5. 学習成果物　　・・・・・・・・・・・・・・・・P.8
6. 講師の必要要件（要求スキルを含む）・・・・・P.9
7. 講師の必要人数　　・・・・・・・・・・・・P.10
8. 学習者に求められるスキル　　・・・・・・P.11～P.12
9. 使用する資料、施設及び設備　　・・・・・P.13

1．コース概要及び目標

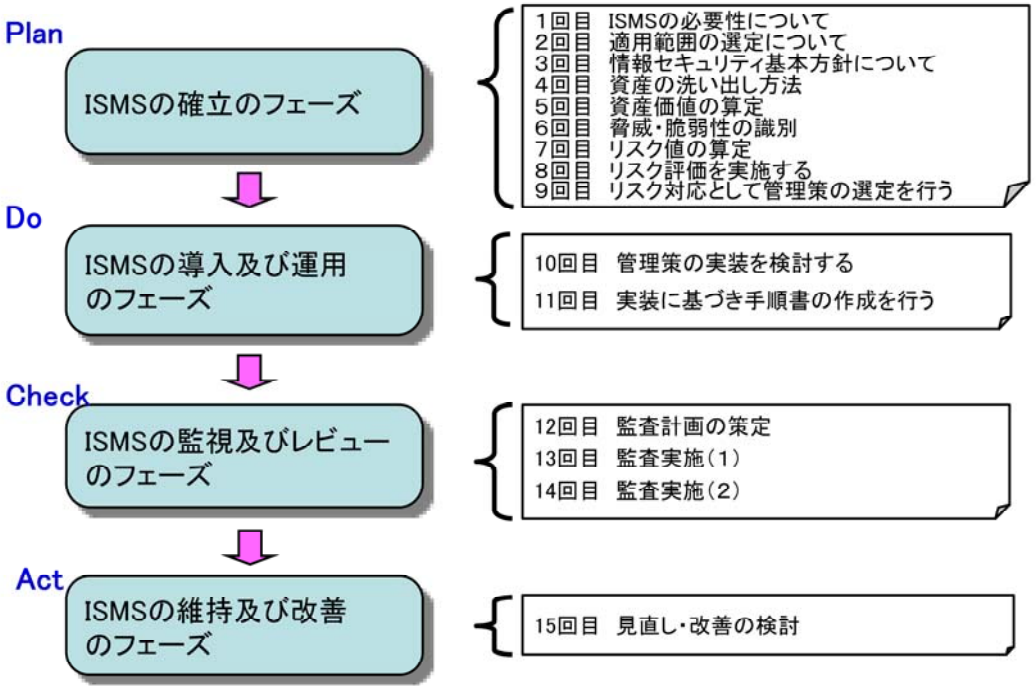
＜概要＞

- 情報セキュリティマネージメントシステムのPDCAに必要な一連の作業を、一貫した同一のテストケースを用いた、演習（一部ロールプレイ）形式で経験する。

＜目標＞

- 演習を通して情報セキュリティマネージメントプロセスに必要な経験を積むことで、情報セキュリティマネージメントシステム構築・導入・運用・評価・改善ができるスキルを習得する。

2. コース構成


Plan
ISMSの確立のフェーズ
Do
ISMSの導入及び運用のフェーズ
Check
ISMSの監視及びレビューのフェーズ
Act
ISMSの維持及び改善のフェーズ
1回目 ISMSの必要性について
2回目 適用範囲の選定について
3回目 情報セキュリティ基本方針について
4回目 資産の洗い出し方法
5回目 資産価値の算定
6回目 脅威・脆弱性の識別
7回目 リスク値の算定
8回目 リスク評価を実施する
9回目 リスク対応として管理策の選定を行う
10回目 管理策の実装を検討する
11回目 実装に基づき手順書の作成を行う
12回目 監査計画の策定
13回目 監査実施（1）
14回目 監査実施（2）
15回目 見直し・改善の検討

3. 進行計画

ISMSのPDCA	単元		所要時間
Plan（確立のフェーズ）	1回目	ISMSの必要性について	90分
	2回目	適用範囲の選定について	90分
	3回目	情報セキュリティ基本方針について	90分
	4回目	資産の洗い出し方法	90分
	5回目	資産価値の算定	90分
	6回目	脅威・脆弱性の識別	90分
	7回目	リスク値の算定	90分
	8回目	リスク評価を実施する	90分
	9回目	リスク対応として管理策の選定を行う	90分
Do（導入及び運用のフェーズ）	10回目	管理策の実装を検討する	90分
	11回目	実装に基づき手順書の作成を行う	90分
Check（監視及びレビューのフェーズ）	12回目	監査計画の策定	90分
	13回目	監査実施（1）	90分
	14回目	監査実施（2）	90分
Act（維持及び改善のフェーズ）	15回目	見直し・改善の検討	90分

4. コース各段階の研修内容の概要と学習目標(1/2)

単元		概要	学習目標
1回目	ISMSの必要性について	・情報セキュリティ事件・事故の例を用いた問題点の解説 ・上記テーマを用いた損失計算の演習	情報セキュリティマネジメントの重要性・必要性を理解する
2回目	適用範囲の選定について	・適用範囲のポイントについての解説 ・適用範囲定義書の作成演習	適用範囲定義書の作成のポイントを理解する
3回目	情報セキュリティ基本方針について	・情報セキュリティ基本方針の章立て及び各章の内容の解説 ・情報セキュリティ基本方針の作成演習	情報セキュリティ基本方針の作成のポイントを理解する
4回目	資産の洗い出し方法	・資産目録に記載すべき内容の解説 ・資産目録の作成演習	保護すべき重要な資産の資産目録の作成のポイントを理解する
5回目	資産価値の算定	・資産価値の算定のポイントの解説 ・資産価値算定の演習	資産価値の算定のポイントを理解する
6回目	脅威・脆弱性の識別	・資産と脅威、脆弱性の紐付けについての解説 ・脅威、脆弱性の識別の演習	脅威、脆弱性の識別のポイントを理解する
7回目	リスク値の算定	・リスク値の算定例についての解説 ・リスク値の算定演習	代表的なリスクアセスメント手法のポイントを理解する

7回目:リスク分析を指導要項に記載する

4. コース各段階の研修内容の概要と学習目標(2/2)

単元		概要	学習目標
8回目	リスク評価を実施する	・リスク受容水準の解説 ・リスク評価の演習	リスク評価のポイントを理解する
9回目	リスク対応として管理策の選定を行う	・適切な管理策の選択のポイントの解説 ・管理策選択の演習	適切な管理策の選択のポイントを理解する
10回目	管理策の実装を検討する	・管理策の具体化のポイントの解説 ・リスク対応計画の作成演習	リスク対応計画書の作成のポイントを理解する
11回目	実装に基づき手順書の作成を行う	・具体化した管理策を手順書化する演習	手順書の作成のポイントを理解する
12回目	監査計画の策定	・監査実施計画のポイントの解説 ・監査計画書の作成演習	監査計画書の作成のポイントを理解する
13回目	監査実施（1）	・テストケースを用いた監査ロールプレイ	不適合報告書の作成のポイントを理解する
14回目	監査実施（2）	・監査報告書の作成演習	監査報告書の作成のポイントを理解する
15回目	見直し・改善の検討	・監査結果に基づく改善検討の演習	改善計画立案のポイントを理解する

5. 学習成果物

単元		学習成果物
1回目	ISMSの必要性について	ー
2回目	適用範囲の選定について	適用範囲定義書
3回目	情報セキュリティ基本方針について	情報セキュリティ基本方針
4回目	資産の洗い出し方法	資産目録
5回目	資産価値の算定	
6回目	脅威・脆弱性の識別	リスク算定シート
7回目	リスク値の算定	
8回目	リスク評価を実施する	
9回目	リスク対応として管理策の選定を行う	
10回目	管理策の実装を検討する	リスク対応計画書
11回目	実装に基づき手順書の作成を行う	手順書
12回目	監査計画の策定	監査計画書
13回目	監査実施（1）	不適合報告書
14回目	監査実施（2）	監査報告書
15回目	見直し・改善の検討	リスク対応計画書

6. 講師の必要要件（要求スキルを含む）

- ISMS審査員補以上の資格保有者、若しくは、以下に相当する条件を満たすこと。

パラメータ	条件
情報セキュリティの知識	・情報セキュリティ基本方針を見て、内容を説明できる ・マネージメントサイクルの各フェーズ（PDCA）について説明できる ・ISMSの基本的な用語（資産、機密性、完全性、可用性、脅威、脆弱性、リスク、管理策等）について説明できる ・管理策（特にJIS Q 27001の附属書A）を説明できる ・リスク対応の選択肢（最適化、回避、移転、保有）を説明できる ・管理策の4つの側面（技術、物理、管理、人）を説明できる ・管理策の4つの段階（予防、検知、極小化、復旧）を説明できる
情報セキュリティ業務経験合計	・2年以上
マネジメント分野の業務経験合計	・2年以上
講師経験合計	・4回かつ20日以上の講師経験

7. 講師の必要人数

- 学習者の人数は、8名以上20名以下とする
- 学習者は原則毎回出席するものとする
- 講師が1名で対応
- 講師の役割は以下の通りである
  - ✓ 講義の実施
  - ✓ 演習問題の説明
  - ✓ 演習の進捗のモニタリング及び管理
  - ✓ 演習解答の解説

8. 学習者に求められるスキル(1/2)

- 必要なスキルと、スキルが必要な単元は以下の通り

単元		必要なスキル
1回目	ISMSの必要性について	ー
2回目	適用範囲の選定について	専門用語(資産、ルータ、FireWall、HUB)を理解している
3回目	情報セキュリティ基本方針について	情報セキュリティ基本方針の内容を説明できる マネージメントサイクルの各フェーズ(PDCA)を説明できる
4回目	資産の洗い出し方法	専門用語(リスクマネジメント)を理解している
5回目	資産価値の算定	専門用語(機密性、完全性、可用性)を理解している
6回目	脅威・脆弱性の識別	専門用語(脅威、脆弱性、リスクアセスメント)を理解している
7回目	リスク値の算定	リスクについての説明ができる
8回目	リスク評価を実施する	ー

8. 学習者に求められるスキル(2/2)

- 必要なスキルと、スキルが必要な単元は以下の通り

単元		必要なスキル
9回目	リスク対応として管理策の選定を行う	専門用語（管理策、リスク対応の選択肢[リスク最適化、リスク移転、リスク回避、リスク保有]）を理解している
10回目	管理策の実装を検討する	専門用語（管理策の4つの側面[技術、物理、管理、人] を理解している
11回目	実装に基づき手順書の作成を行う	―
12回目	監査計画の策定	JIS Q 27001:2006の附属書Aの要求内容について理解している
13回目	監査実施（1）	―
14回目	監査実施（2）	―
15回目	見直し・改善の検討	―

9. 使用する資料、施設及び設備

＜講師資料＞
- 講義用の教材
  講義用教材、演習問題、演習解答解説の資料
- 演習用テストケース
- 指導要項
- JIS Q 27001:2006

＜学習者資料＞
- 講義用の教材
  講義用教材、演習問題、演習解答解説の資料
- 演習用テストケース
- JIS Q 27001:2006

＜施設及び設備＞
- 研修室
  テキスト等を参照しながら4～5名でのグループ討議ができる環境である事
- PC1台
  Microsoft® Office PowerPoint® 2003 SP2がインストールされている事
  Microsoft® Office Word® 2003 SP2がインストールされている事（PCで解答例を説明する場合）
- プロジェクタ1台
  普通紙が投影できる事が望ましい（ディスカッションした結果をチーム毎に発表するため）
- 解答作成・発表をPCで行う場合は、必要台数のPC
  解答作成に必要なアプリケーションがインストールされていること