

ISO27001:2005 認証取得 コンサルティング

あどばる経営研究所／A.V.MANAGEMENT
<http://www.addval.jp>

1. あどばる経営研究所のISO27001認証取得コンサルティングの特長

(1) お客様の認証取得目的に沿ったコンサルティングを致します。

- ① ISO27001認証取得だけが目的なのか／認証取得以外の経営目的は何なのか・・・総合判断して対処します
- ② 他のISO規格取得済み／未取得の企業様の各々のシステム構築負荷は異なります・・・各企業に見合ったコンサルを致します

(2) 総合力でコンサルティング致します。・・・ISO+アルファの付加価値を提供致します

- ① あどばる経営研究所は総合コンサルティングファームの機能を有しています。
- ② 以下の規格の認証取得コンサル及び内部監査員研修で多くの企業様のご支援をさせていただいています。
ISO9001(品質)/JISQ9100(航空・宇宙)/ISO13485(医療機器)/TS16949(自動車)/ISO14001(環境)
ISO22000(食品安全)/ISO27001(情報)/OHSAS18001(安全・衛生)等のリスクマネジメント
ISO17025(検査・試験所)/JISQ15001(個人情報保護)/ISO39001(道路交通安全)等

- ③ コストダウンコンサルティング、品質向上コンサルティング、省エネコンサルティング、内部統制(J-SOX)コンサルティング
事業リスクマネジメントに係るコンサルティングなど経営改善コンサルティングで多面的・柔軟なご支援を致します。

(3) ISO27001情報セキュリティマネジメントシステム(ISMS)は、経営資源の中で重要な位置付けにある情報資産のセキュリティを確保するだけでなく、セキュリティ対策全般の企業の信頼性評価の基本として、重要視されています。経営に貢献する仕組みとして構築致します。

(4) 認証取得プロジェクトの作業分担、役割の明確化と全員参加のタイミングに配慮します。

(5) プロジェクトの進捗管理により期限内取得が確実にできるようにプロジェクト管理を徹底します。

(6) 作成する文書のシンプル化につとめます。

- ① 他のマネジメントシステムなどで作成済みの文書との融合及び重複の排除
- ② 統合マネジメントシステムへの移行が円滑に行えるよう配慮します。・・・ISO9001+ISO14001+ISO27001+・・・等の統合化
- ③ ISOの全ての規格は2013～2015年の間にHLS(ハイベルストラクチャー)の考え方で見直しが行われ、統合化が容易になりますが、ISO27001は2013年中にHLS構造として改訂される予定であり、これらを配慮して、既存のISO規格を活かしながら統合化がし易いように文書化指導致します。

(7) 文書作成が簡単に行えるようにご支援します。

- ① 文書事例及び記録様式の雛形をテキストデータ(Word等)でお渡しし、文書作成に役立てていただきます。
- ② メール添削により、訪問指導日以外でも、いつでも何回でも丁寧にご指導します。・・・実質的に1.5倍相当のコンサル提供

(8) 内部監査員養成研修、模擬監査による実践指導、審査前の審査対策Q&Aを、コンサルの重要事項としてご指導致します。

(9) ISO27001の審査機関を選定する際、将来必須になると思われる統合マネジメントシステムを構築することを配慮すると、どの審査機関でも良いと言うことにはなりません。・・・審査機関選定とご紹介の支援を致します。

(10) コンサル支援のスタイルとして3つのパターンがあり、要望によりいずれの対応も致します。(Bが標準)

A: コンサル依存型 B: 導入企業のスタッフとコンサルが共同で作り上げる C: 導入企業主体でコンサルは支援する

2. ISO27001 認証取得タイムスケジュール

資料1: 詳細タイムスケジュール

経過月	フェイズ	実施内容
1ヶ月	準備・体制づくり	導入前自己診断／認証取得推進体制の構築（各企業様で事前検討） 推進委員会メンバー及びワーキングGRリーダー教育 ISO認証取得PJオリエンテーション／PJ実行計画作成 ISO27001規格解釈／説明 既存文書・記録の統合化検討／現状把握
2～4ヶ月	システム構築	文書・記録様式作成計画 ISMSマニュアル草案作成～添削・手直し～完成～制定（他の規格との統合マニュアルも可能） 必要な2次文書及び3次文書の草案作成～添削・手直し～完成～制定 既存2次文書等の改訂 新規作成すべき記録様式・改訂すべき記録様式の作成 ISMS方針・目標の設定 リスクアセスメントの仕組み構築／情報資産の棚卸し・リスク評価 管理策の選定及び策定／リスク対応計画書作成／適用宣言書作成
5～8ヶ月	システム運用・評価	新ISMSの従業員教育 資格認定対象者など教育訓練計画作成～実施 内部監査員養成研修 新ISMS試行～見直し～文書改訂 不適合発見～是正処置～ISMSの改善 ISMS模擬審査によるシステム運用面の実践的仕上げ 内部監査計画作成～内部監査実施（内部監査員実践指導含む）～是正処置 ISMS方針・目標のレビュー指導／セキュリティ対策改善指導 マネジメントレビュー実施（実践指導含む）
6～8ヶ月	認証審査	審査前対策指導 文書審査～第一段階審査～第二段階審査（企業様で対応）

3. コンサルタントの訪問による指導方法等

システム構築までは月2回の訪問指導、運用開始後は月2～1日の訪問指導、

新規に取得する企業は、コンサル期間中の訪問指導回数は15日を標準とします。

他の規格を取得済みの場合、訪問指導回数は標準回数より少なくなる可能性があります。

(個別見積の際、企業様に事情確認の上、配慮します)

***いずれも内部監査員研修は別途2日必要**

- ISO27001 認証取得PJで、作業として最も大変な時期はシステム構築までの期間です。
- システム構築までは、月2回訪問指導で1回当たり4時間のご指導を行います。
イメージとしては、
第1週の○曜日 13:00～17:00(4時間)
* テーマによっては、ご相談の上、臨時的に宿泊も検討します
同様に、第3週の○曜日 13:00～17:00(4時間)
- 実際の研修日は、前月の研修日に都合の良い日程を確認し、都度設定します。
- システムが落ち着いた以降は、ISMSの運用段階ですので、月1回～2回の指導になります。
- 内部監査員研修及び模擬監査は、密度を濃く実施しますので研修当該月に別途研修時間を設定します。

4. 文書作成支援・・・必要な文書類事例及び記録様式事例をご提供します

代表的な文書事例	ISO27001要求事項
ISMSマニュアル	全章が対象
文書・記録管理規定	4.3 文書化に関する要求事項
リスクアセスメント管理規定	4.2.1 ISMSの確立
管理策選定及び適用宣言書管理規定	4.2.1 ISMSの確立
教育訓練規定	5.2.2 教育・訓練、意識向上及び力量
内部監査規定	6. ISMS内部監査
マネジメントレビュー管理規定	7. ISMSのマネジメントレビュー
是正処置・予防処置管理規定	8. ISMSの改善
セキュリティインシデント対応手順	4.2.2h. セキュリティインシデントに対応できるための手順
社内システム管理手順	4.2.2f.g. ISMSの運用管理／経営資源の管理
施設セキュリティ管理手順	同上

文書完成までのステップ

St1:文書作成スケジュール作成

* 作成予定文書別に担当者設定

* 文書別の作成スケジュール設定

St2:雛形事例を参照して草案作成

* テキストデータ(word)に加筆

St3:メール添削、訪問コンサルで指導

St4:担当者が手直し～再添削指導

St5:完成・制定

* ISO規格取得済みの企業は既存文書をベースに改訂します。

* ISMSマニュアル主体で二次文書を作成しないシステムでも対応いたします。

* 各文書事例に関連の記録様式事例が添付されています

* 上記文書以外で提供出来る文書事例

情報セキュリティ基本方針

情報資産台帳

適用宣言書

リスク対応計画書

事業継続リスクアセスメント

事業継続計画書

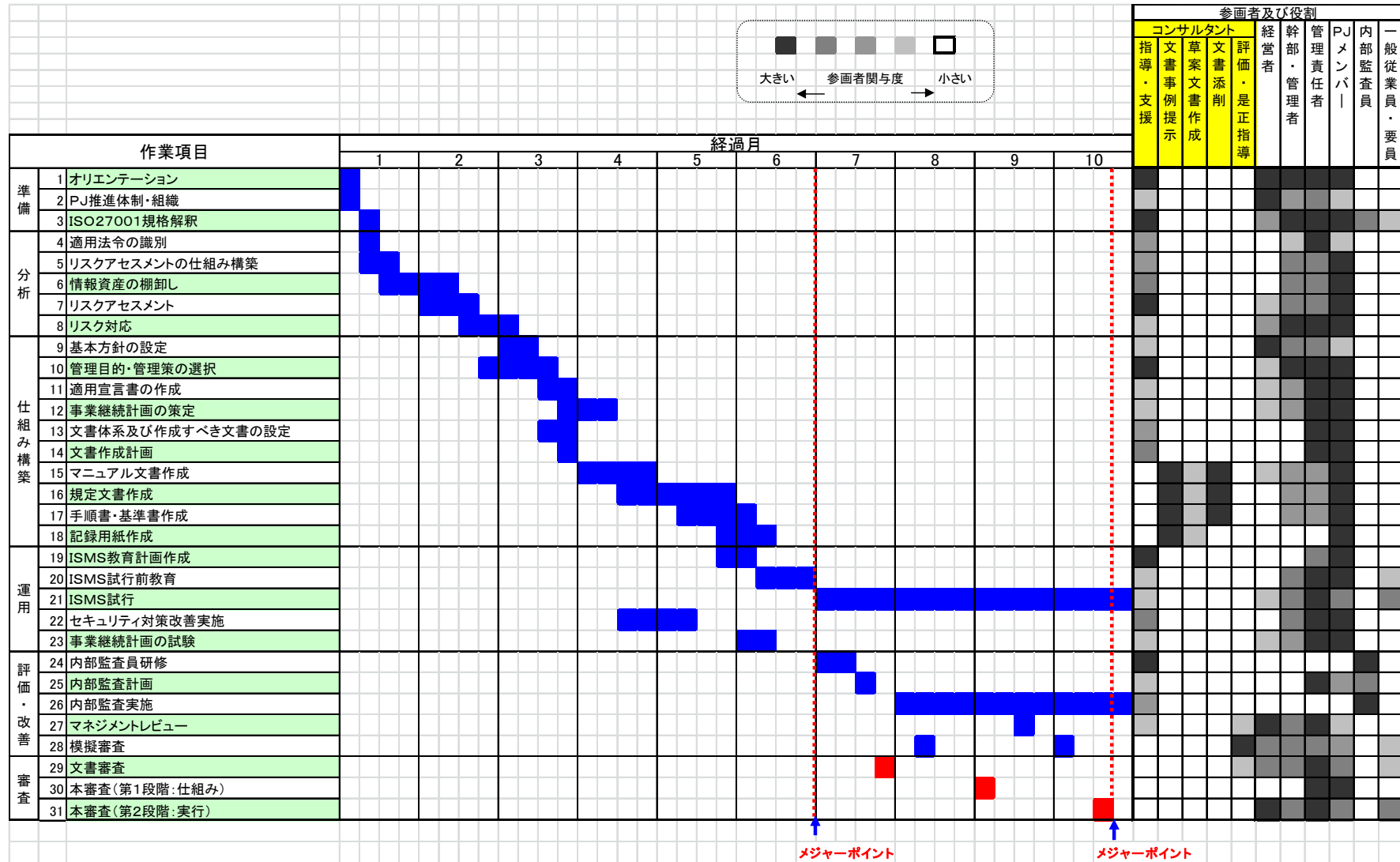
管理策有効性測定記録

5. 内部監査員研修・・・企業内研修で進めます

研修内容	使用テキスト
研修オリエンテーション	
ISO27001要求項目解説／講義	ISO27001要求項目／規格の解釈 ISO27001要求項目(一覧タイプ)
内部監査の基本知識／講義 内部監査とPDCA／講義 内部監査員の養成／講義	ISMS内部監査の進め方
内部監査の進め方／講義	ISMS内部監査の進め方
リスクアセスメント	リスクアセスメント
ケーススタディ(1) 監査証拠の想定 ケーススタディ(2) 想定問答チェックリスト作成	ケーススタディ: 想定問答チェックリスト作成
ケーススタディ(3) 不適合判定	ケーススタディ: 不適合判定
不適合判定ケーススタディ発表会	
ケーススタディ(4) 監査後会議準備 ケーススタディ(5) 監査後会議ロープレ	ISMS内部監査の進め方
理解度テスト&自己採点	理解度テスト
研修まとめ／Q&A	

- ◆2日研修で実施します
(9:00～16:00)
- *1日研修も企画致します。
- *休日等の活用で実施することも出来ます。
- ◆企業内研修として、貴社の会議室等を会場に致します。
- ◆MAX15名まで同時に研修可能です。
- ◆修了証を発行します。
- ◆必要に応じて理解度テストも実施します。
- ◆単なる知識研修ではなく、ケーススタディを通じて、実践スキルのある監査員を養成するのが、特長です。

6. ISO27001 認証取得プロジェクト／タイムスケジュール及び作業項目



7. オプション／ISO27001 認証取得プロジェクト／構築支援コンサル・運用自力活動型

* 費用は通常コンサルの約6割で済みます。

経過月	フェイズ	実施内容
1ヶ月	準備・体制づくり (コンサル支援)	導入前自己診断／認証取得推進体制の構築（各企業様で事前検討） 推進委員会メンバー及びワーキングGRリーダー教育 ISO認証取得PJオリエンテーション／PJ実行計画作成 ISO27001規格解釈／説明 既存文書・記録の統合化検討／現状把握
2～4ヶ月	システム構築 (コンサル支援)	文書・記録様式作成計画 ISMSマニュアル草案作成～添削・手直し～完成～制定（他の規格との統合マニュアルも可能） 必要な2次文書及び3次文書の草案作成～添削・手直し～完成～制定 既存2次文書等の改訂 新規作成すべき記録様式・改訂すべき記録様式の作成 ISMS方針・目標の設定 リスクアセスメントの仕組み構築／情報資産の棚卸し・リスク評価 管理策の選定及び策定／リスク対応計画書作成／適用宣言書作成 新ISMS運用のための実行計画作成（作業項目、役割担当、スケジュールを具体化します）
5～8ヶ月	システム運用・評価 (自力活動)	企業の皆さんで自力活動していただきます。／以下の項目はオプション選択で支援可能 オプション①: 新ISMSの従業員教育計画作成／資格認定対象者など教育訓練計画作成 オプション②: 内部監査員養成研修／内部監査計画作成 オプション③: ISMS模擬審査によるシステム運用面の実践的仕上げ オプション④: ISMS方針・目標のレビュー／セキュリティ対策改善指導 オプション⑤: マネジメントレビュー実施（実践指導） オプション⑥: 審査前直前対策
6～8ヶ月	認証審査	審査前対策指導 文書審査～第一段階審査～第二段階審査（企業様で対応）