情報セキュリティマネジメント・セミナー2023

「ISMS内部監査」どうやってますか？

2023年12月18日

日本ISMSユーザグループ インプリメンテーション研究会
尾崎 幸彦 (株式会社Speee)

自己紹介

尾崎 幸彦 (おざきゆきひこ)

- 株式会社 Speee セキュリティ推進室
  - ISMS/ISMS-CLS主任審査員 (JRCA)
  - 日本ISMSユーザグループ インプリメンテーション研究会 副主査

略歴	
2006年頃 ～2018年	NECソフトウェア中部 →[全国7社合併]→ NECソリューションイノベータ株式会社 • 情報セキュリティ部門マネージャ • 2015年の合併時、既存13個(計1.5万人)のISMS認証を1年間で1個に統合
2019年4月 ～2021年10月	株式会社 日本環境認証機構 (JACO) • ISMS/BCMS 審査員
2021年11月～	株式会社 Speee • セキュリティ推進室 -情報セキュリティマネジメント担当

本テーマの狙い

以下のような思いを抱いている方、いませんか？

少なくとも、私自身が事務局当時はそうでした。

- **前任者から引き継いだ仕組みを続けている、大きな問題はない(つもり)**
- **審査で指摘事項はないけれど、要改善点が無いとは思えない**
- **今の方法が自組織にとって良いやり方なのか、判断する知見・基準が無い**
- **他の組織がどのようなやり方をしているのか知る機会が欲しい**

今回は内部監査を題材に、研究会メンバーでの実態や知見を集めてみました。

構成

Part.1 研究会参加者と組織のプロファイル紹介

Part.2 2013年の発表「ISMS推進各社が抱える諸課題の対応策」での『内部監査のマンネリ化』を振り返ります

Part.3 「9.2 内部監査」要素ごとの、各組織での対応状況など

Part.4 「監査所見の定義」の比較

Part.5 改善事例の紹介

Part.1
研究会参加者と組織のプロファイル紹介

質問項目 (研究会参加者と組織のプロファイル紹介)

【回答者個人について】

Q1.回答内容の時期

- 現役を離れている方には、過去の状況を答えていただきました

Q2.回答内容当時の立場

【回答対象組織について】

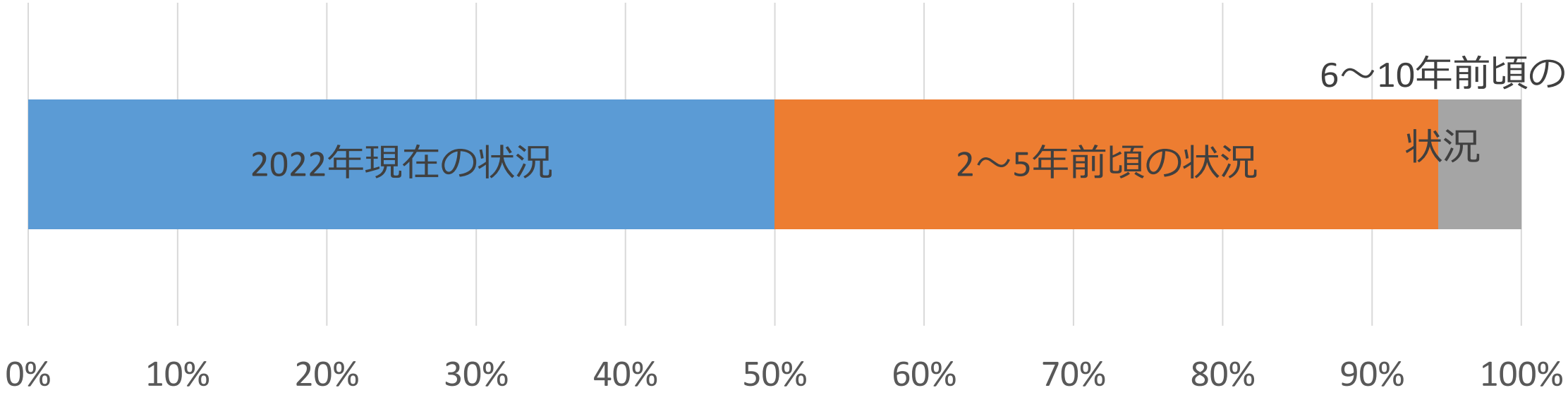
Q3.適用範囲の人数

Q4.適用範囲サイト数

Q5.ISMS認証の有無

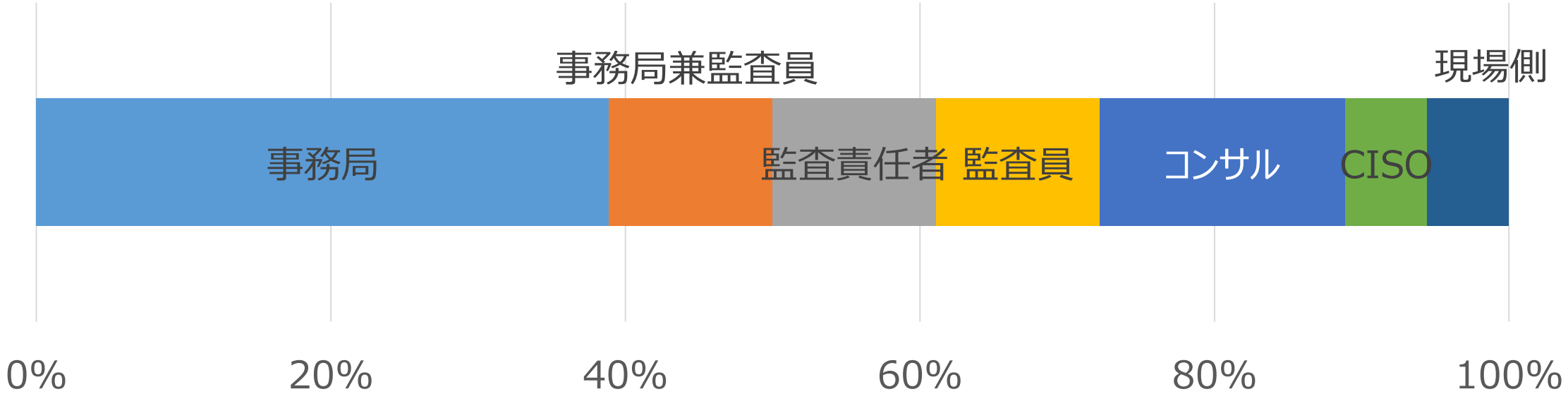
Q1.回答内容の時期

半数が現在(2022～23年)の状況に基づいた回答で、九割以上が5年以内の情報となっています。



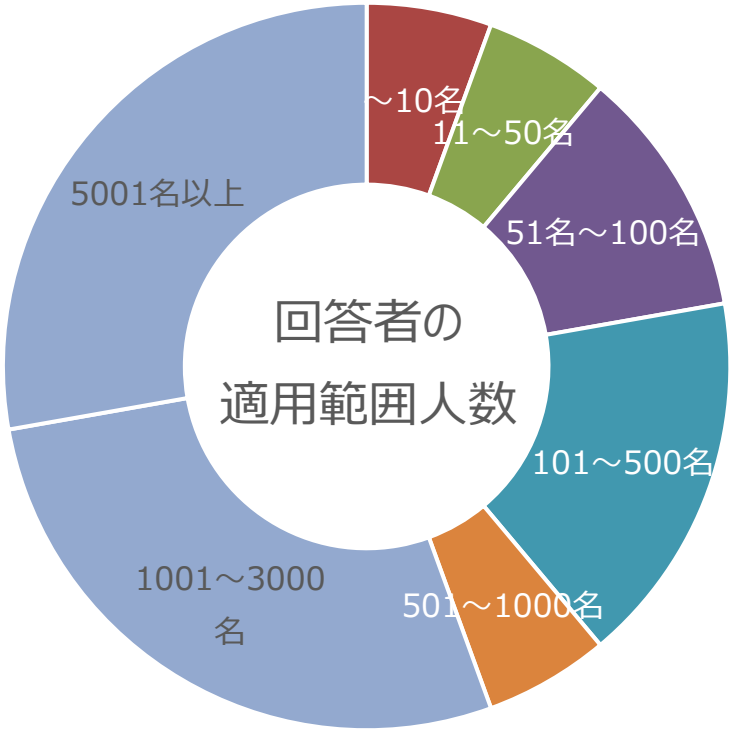
Q2.回答内容当時の立場

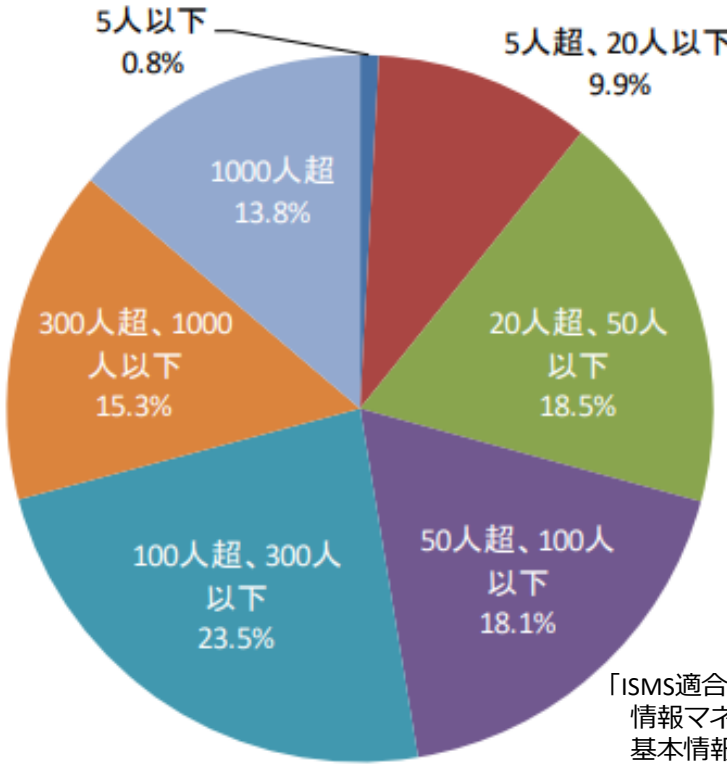
半数が事務局要員(兼監査員)、二割が監査員側の立場での経験に基づく回答でした。



Q3.適用範囲の人数

研究会メンバーは大企業での経験が多いことが、JIPDECのアンケート結果との比較で読み取れます。

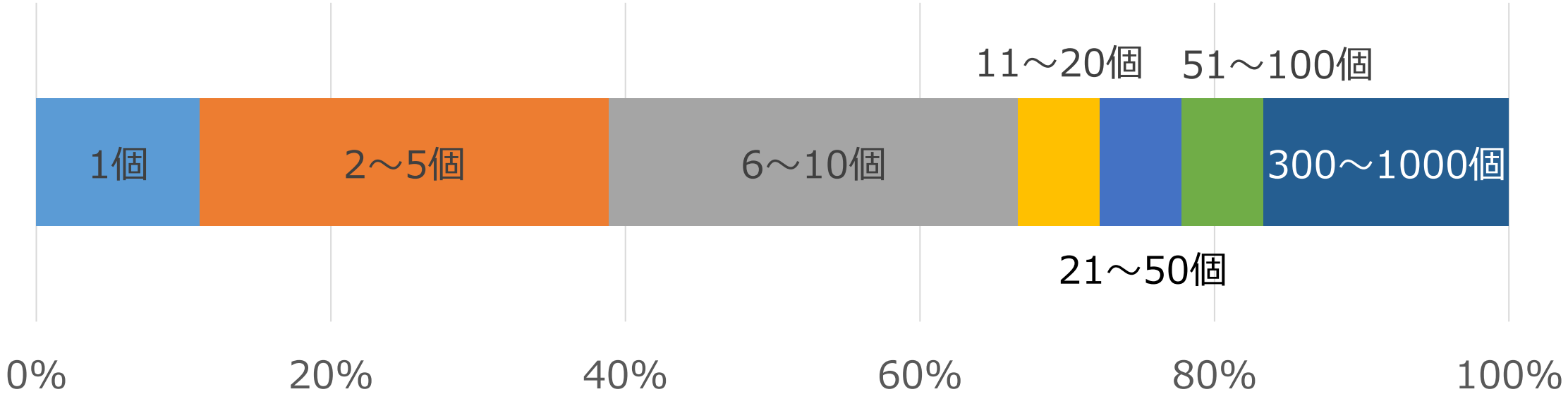




「ISMS適合性評価制度に関する調査報告書」2018年3月
情報マネジメントシステム認定センター(ISMS-AC)
基本情報について 質問3 従業員数 より引用

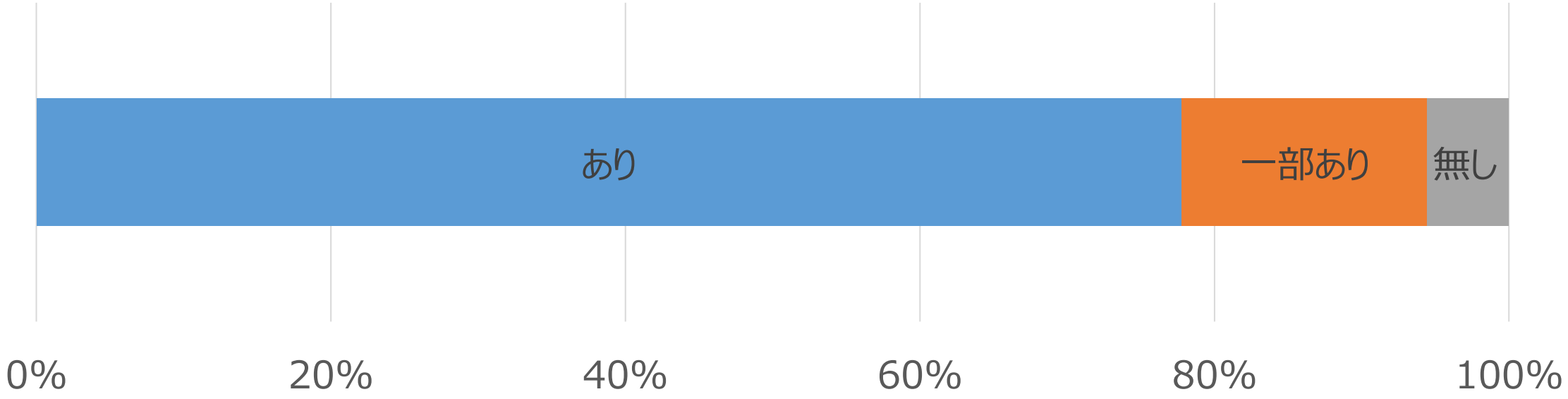
Q4.適用範囲のサイト数

適用範囲規模が大きい事からの必然として、サイト数が多い組織の比率が高い事が特徴的でした。



Q5.ISMS認証の有無

認証未取得な組織の方も、研究会に参加いただいています！



Part.2
2013年の「ISMS推進各社が抱える諸課題の対応策」での『内部監査のマンネリ化』を振り返ります

2013年の発表内容

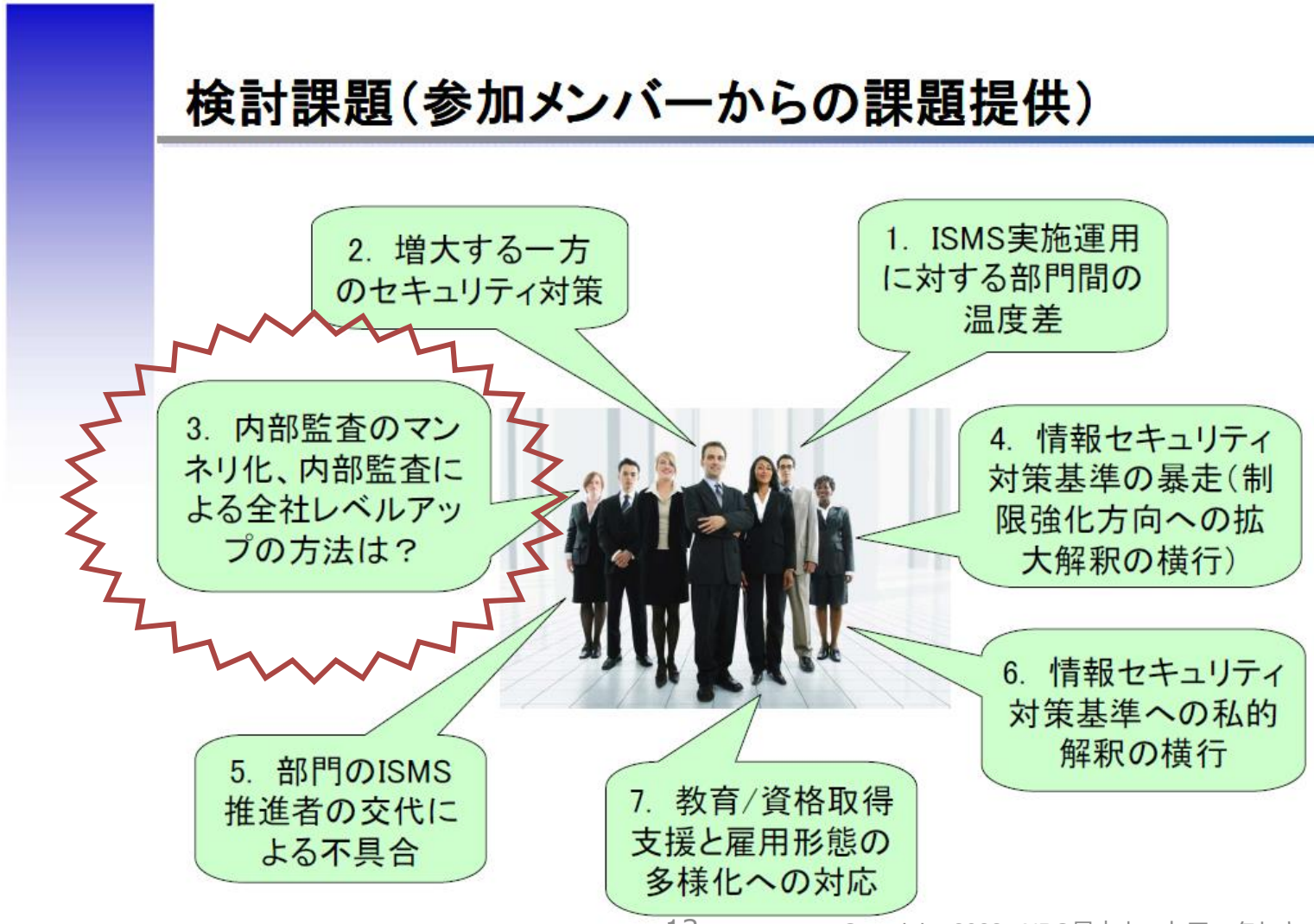
テーマ1：
ISMS推進各社が抱える諸課題の対応策

日本ISMSユーザグループ
インプリメンテーション研究会

2013年12月20日

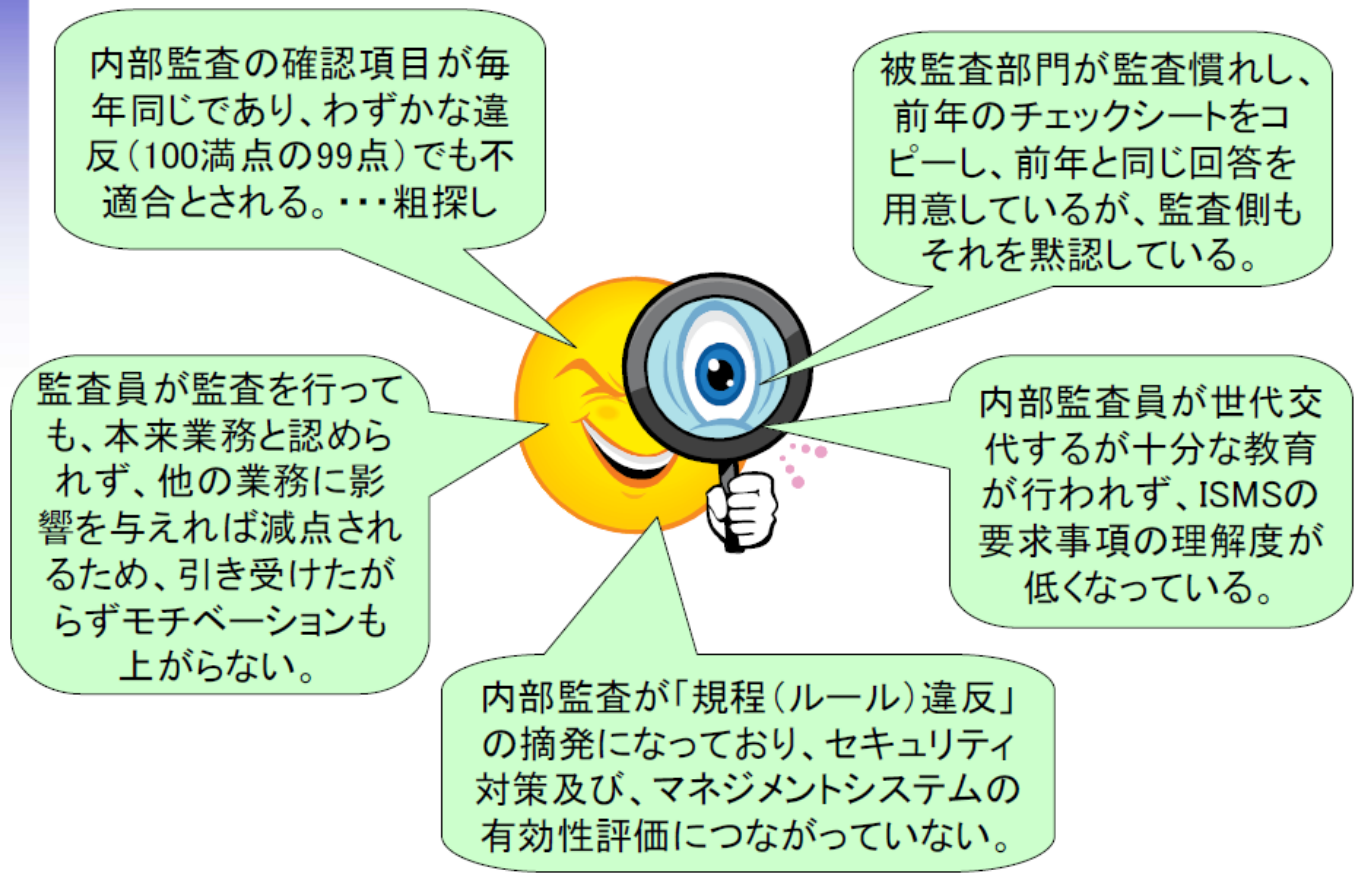
主査　羽田　卓郎
リコージャパン㈱

2013年の発表内容

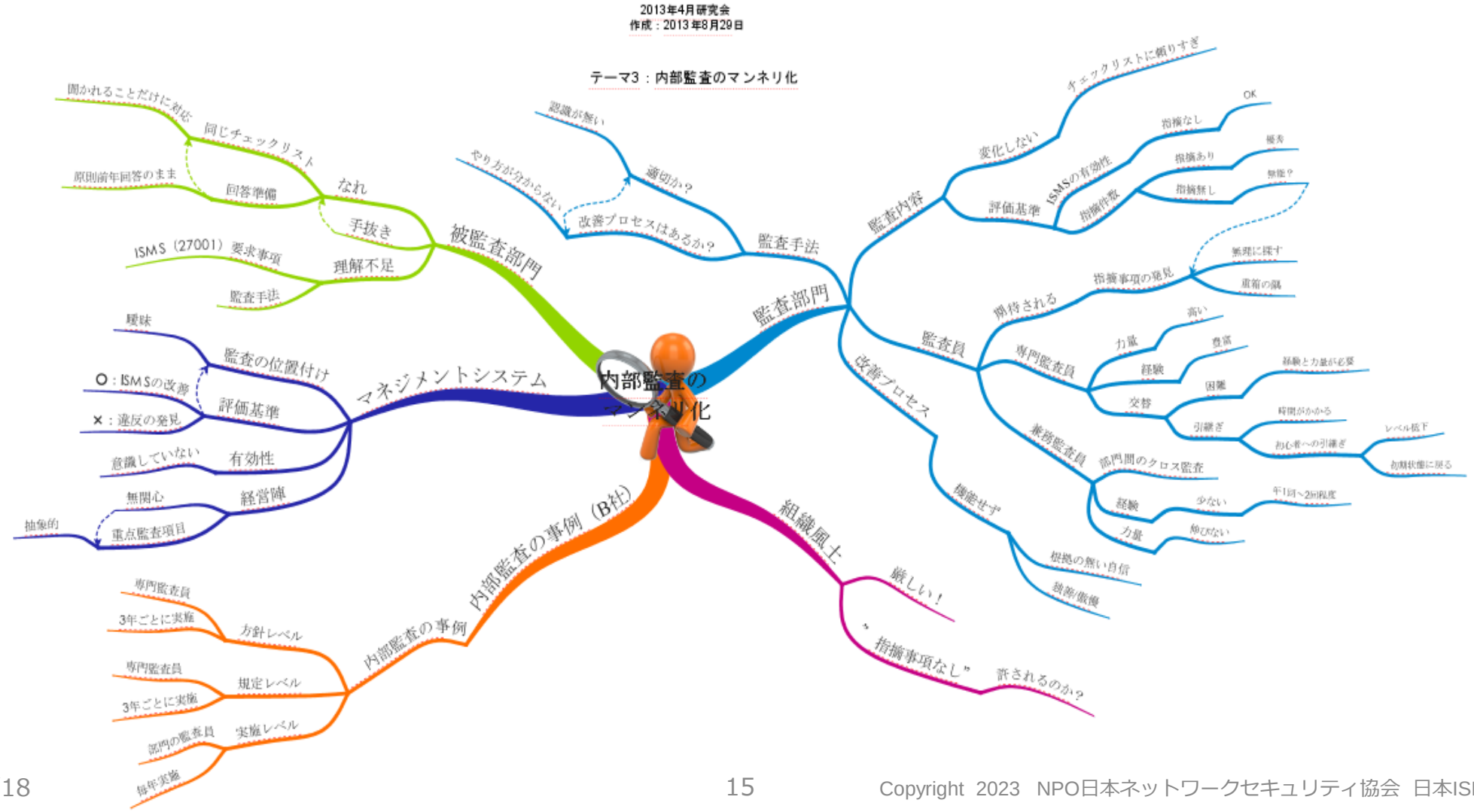


2013年の発表内容

検討課題3. 内部監査のマンネリ化、内部監査による全社レベルアップの方法は？



2013年の発表内容



ところで・・・

研究会で、ここまで振り返った時点で

「内部監査のマンネリ化」ってそもそも何？

という疑問がメンバーから湧きました。

ところで・・・

「マンネリ」の定義 (広辞苑より引用)

マンネリズムの略。
マンネリズム【mannerism】

マンネリズム【mannerism】
一定の技法や形式を反復慣用し、固定した型にはまって独創性や新鮮さを失うようになる傾向。マナリズム。→マニエリスム

ところで・・・

「内部監査のマンネリ化」を感じる事象としては、以下が挙げられました

① ISMSとPMSの認証取得が、①自社の事業化と、②入札・取引条件に対応するものであったことから、本来の情報セキュリティの維持が目的とされていなかったため、導入時のみ全社プロジェクト体制にて組織的に取り組んだが、認証以降は、事務局による維持に必要な最低限の稼働となっている。

② 内部監査チームは二人一組で事務局から指定された被監査部門に対するクロス監査を実施するが、職位や入社年等の暗黙の力学が一名のみで形式的な監査を実施する。

③ 被監査部門の監査対応者は、部門長と定めれているが、部門長は任意の対応者に対応を指示し監督しない。

④ 上記2.3項の結果、前回監査の指摘事項が2年連続して是正されていないことが検出され、部門長は監督していないため、そのままマネジメントレビューに報告される。

⑤ しかしながら経営者も関心がないため、是正していない部門の部門長が咎められることがなく、フォローアップ監査も指示されない。

ところで・・・

定義を確認した上での「内部監査のマンネリ化」に対するメンバーからの意見感想は、以下のようなものでした。

ただし、結論や合意には至っていません。

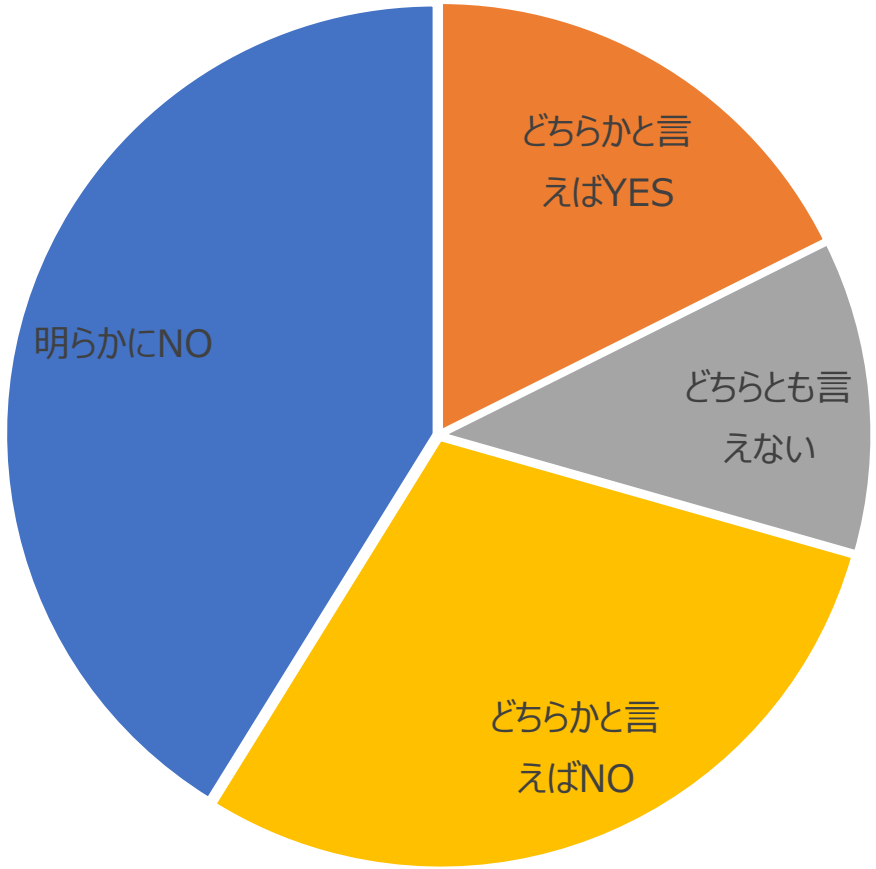
- 規格条文に準拠した事項を繰り返すのは当たり前
  - ただし、変化に合わせて見直しをするのかを個々に判断していく必要がある
  - 形だけまねしているのはマンネリ、リスクの変化・脅威の分析をして考えたのかが重要
- 例えば経理で「支払伝票処理のマンネリ化」とは言わないよね
- 「やらされ感」という意味が混ざっているかも
- マンネリというより「上っ面の監査」に問題があるのではないかと考えます。

現在の状況アンケート

2023年の今、「内部監査のマンネリ」に関するキーワードで、参加者各位に質問してみました。

① 監査で「指摘事項がゼロ件」が許されない雰囲気はあるか
② 経営陣は情報セキュリティ内部監査を重要視していたか
③ 設問は毎年最適化・最新化されていたか
④ 監査の指摘内容には、改善への示唆や手順が含まれていたか
⑤ チェックリスト内容そのままだけではなく、派生した質問まで踏み込めていたか

①監査で「指摘事項がゼロ件」が許されない雰囲気はあるか



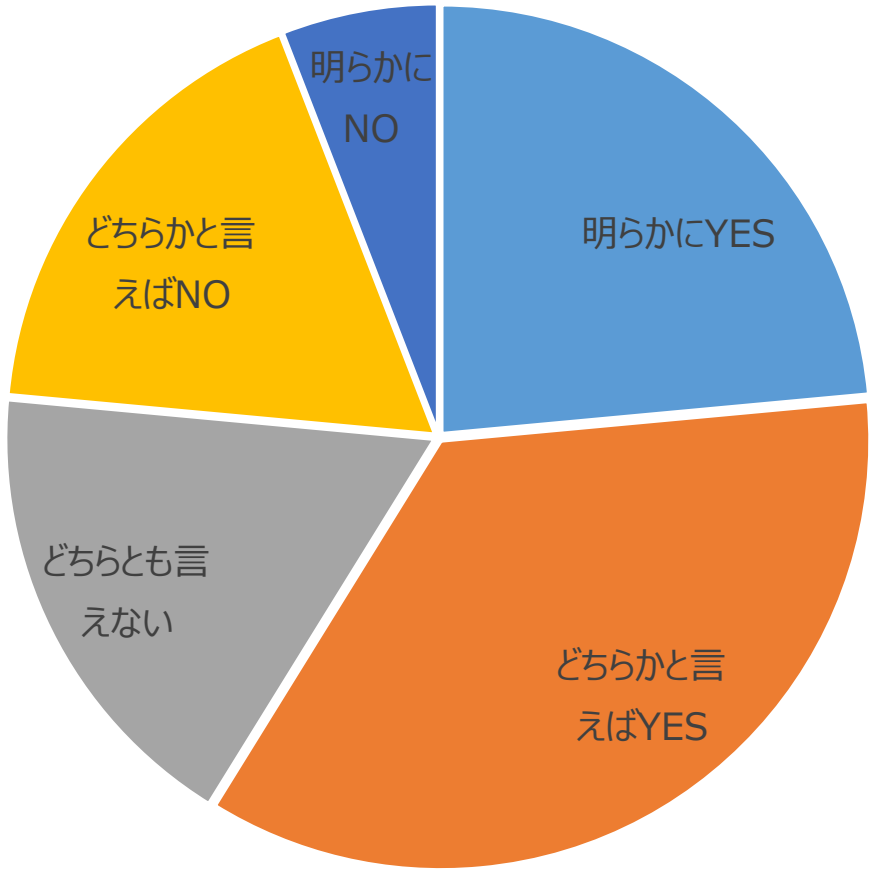
【各種意見】

- 「改善のために指摘を出し、組織のセキュリティを向上させること」が目的であることを事前に伝えてあります
- 「指摘事項がゼロ件」がNGというよりは、せめてGoodPointは出そうという感じです
- 許されてはいましたが、大抵は何かしら指摘、もしくはグッドポイントなど記載している監査員が多数だったように思うので、そのように解釈していた人はいたのだと思っています
- 完璧に対策が実行できている会社ではないので、「指摘事項がゼロ件」のはずがない
- 「指摘事項がゼロ件」は、監査を実施していないのと同じという雰囲気になるため、何かしら指摘があった

【改善提案】

- 内部監査を外注している場合、ゼロ件だと仕事をしていない様に見える。ゼロ件であることの意味を、監査結果の報告対象(トップマネジメント、経営層)に理解してもらうことが重要だと思う

②経営陣は情報セキュリティ内部監査を重要視していたか



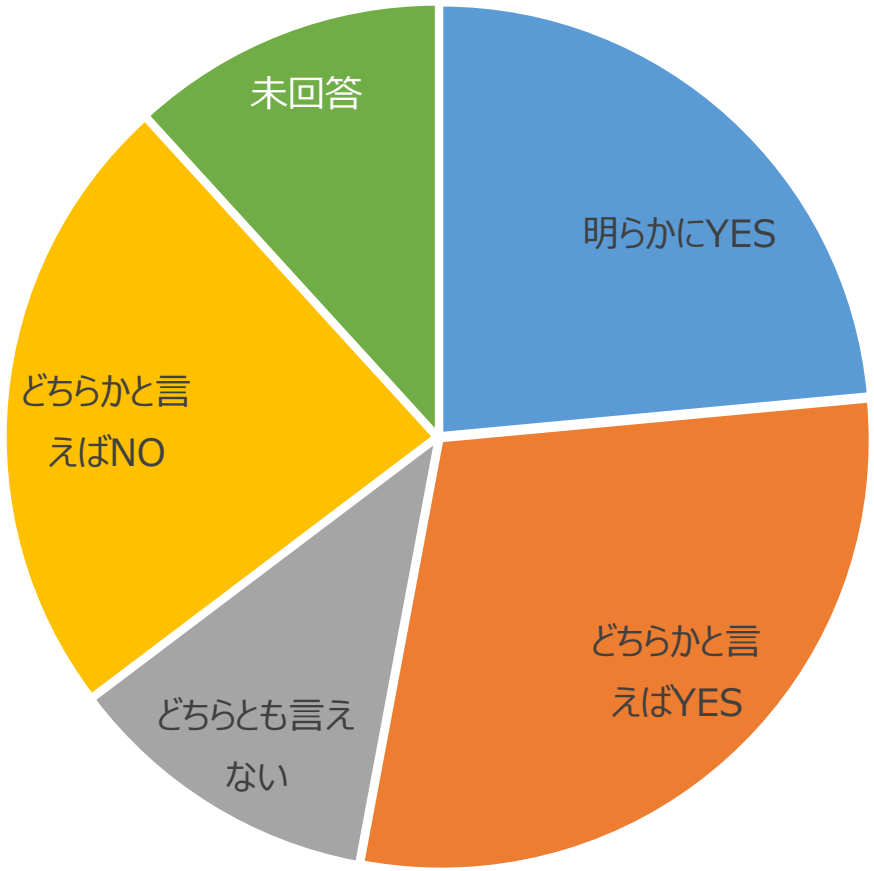
【各種意見】

- 内部監査での指摘事項について、マネジメントレビューで対応・改善の指示があった
- 経営会議で監査結果が報告され、経営陣から指示等が出されている
- 経営陣は、内部監査を実施することで、従業員の意識レベルが上がることを期待しているが、事務局側が内部監査の準備で大変になると、他の仕事に影響があるため、どちらとも言えないとしている
- ISMS認証が通ればいいという空気感を感じています

【改善提案】

- 内部監査の結果をもとに、経営リスクやERMにどのような影響があるのかについて、内部監査責任者が報告できることが必要だと思う

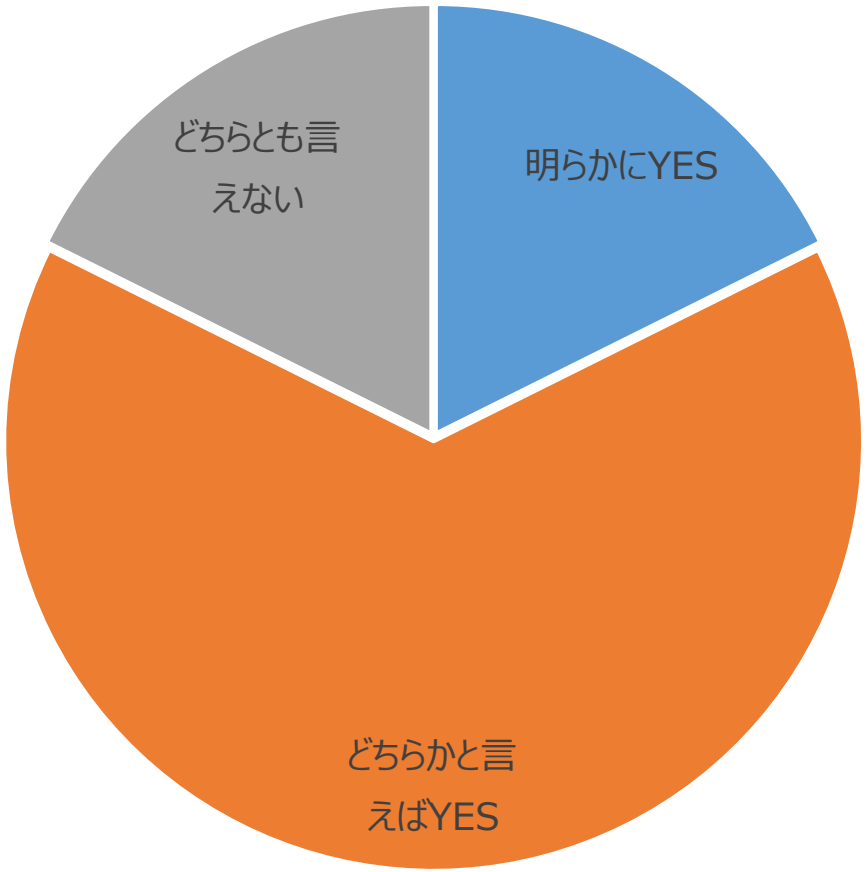
③設問は毎年最適化・最新化されていたか



【各種意見】

- 規程の改定や大きな組織変更ない限り大幅な変更はなかった。事務局主査が元ネタとなるチェックシートから当該年度の重点監査項目に合った項目を複数選択しチェックシートを作成していた
- 必要最低限の設問になっていたと思っています
- 毎年、見直しが必要かを確認し、審査・承認を得ている
- 毎年、3割は設問を更新していた

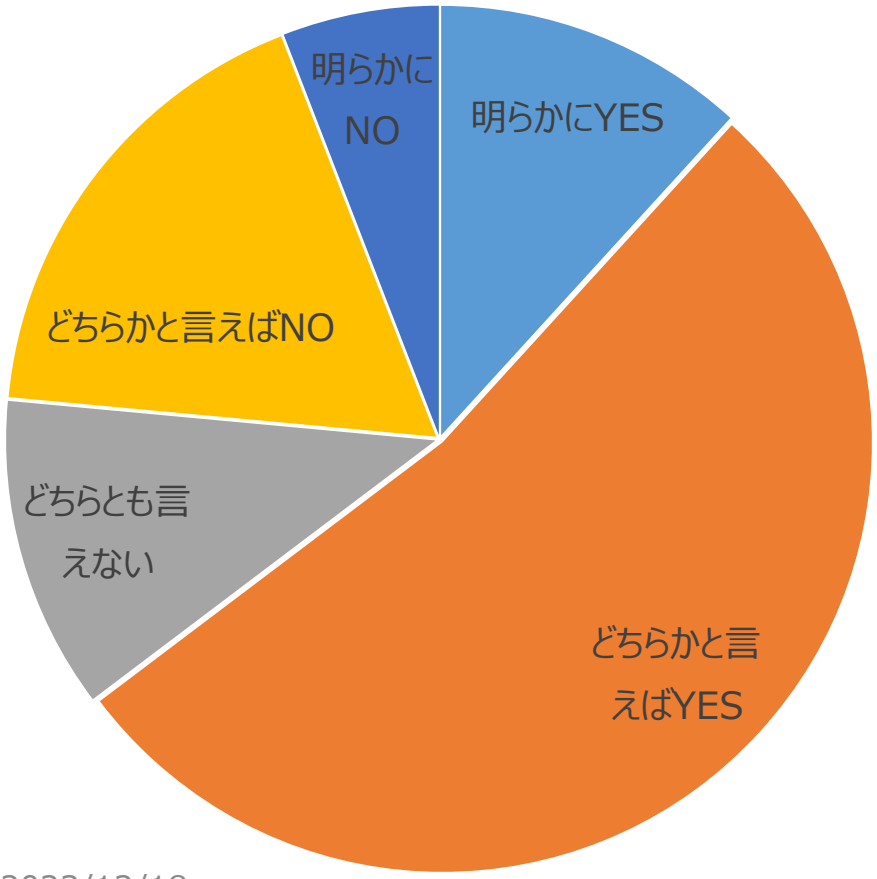
④監査の指摘内容には、改善への示唆や手順が含まれていたか



【各種意見】

- 被監査部門を回答者とする、監査員評価アンケートと結果のフィードバックがある
- 現地監査のクロージングの際に相談に乗る場合、その場で改善に関する示唆・手順の相談を受けて回答はしているが、指摘内容の通知と是正依頼の際に改善の対応について示唆はされていない
- 個別の部署の書類やデバイスなどの保管や持ち出しについては、改善指摘はしやすいですが、やラベリングやバックアップ、ログの保管など、改善指摘が含めなかった
- 指摘内容によってはその場で改善させてその旨報告書へ記載していました

⑤チェックリスト内容そのままだけではなく、派生した質問まで踏み込めていたか



【各種意見】

- 監査人によってまちまち。たまに、形式的な監査実施結果を残すためだけの活動に収支指定折るケースが見られた
- 監査員の力量による部分で、個人差がでていると感じます
- 時間の制約の中で、監査員の力量の範疇で、必要と判断した場合、派生の質問に踏み込んでいます
- 時間制限があるので、派生できないが、内部監査は話し合いの機会にして欲しいとしていたので、他の方は、派生していたかもしれません
- コンサルタントに同席している事務局員が気になったことは都度追加質問していた

Part.3
「9.2 内部監査」箇条要素ごとの、各組織での対応状況など

JIS Q 27001:2014　9.2 内部監査

9.2　内部監査

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

a)　次の事項に適合している。

　1)　ISMS に関して，組織自体が規定した要求事項

　2)　この規格の要求事項

b)　有効に実施され，維持されている。

組織は，次に示す事項を行わなければならない。

c)　頻度，方法，責任及び計画に関する要求事項及び報告を含む，監査プログラムの計画，確立，実施及び維持。監査プログラムは，関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない。

d)　各監査について，監査基準及び監査範囲を明確にする。

e)　監査プロセスの客観性及び公平性を確保する監査員を選定し，監査を実施する。

f)　監査の結果を関連する管理層に報告することを確実にする。

g)　監査プログラム及び監査結果の証拠として，文書化した情報を保持する。

JIS Q 27001:2023　9.2 内部監査

9.2　内部監査

9.2.1　一般

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

a)　次の事項に適合している。

1)　ISMS に関して，組織自体が規定した要求事項

2)　この規格の要求事項

b)　有効に実施され，維持されている。

9.2.2　内部監査プログラム

組織は，監査プログラムを計画し，確立し，実施し，維持しなければならない。これには，その頻度，方法，責任，計画策定の要求事項及び報告を含める。

それ（れら）の内部監査プログラムを確立するとき，組織は，関連するプロセスの重要性及び前回までの監査の結果を考慮しなければならない。

組織は，次に示す事項を行わなければならない。

a)　各監査について，監査基準及び監査範囲を明確にする。

b)　監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。

c)　監査の結果を関連する管理層に報告することを確実にする。

組織は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にしなければならない。

JIS Q 27001:2023　9.2 内部監査

2014→2023の変化点 (変更点は実質無し)

9.2　内部監査

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

a)　次の事項に適合している。

1)　ISMS に関して，組織自体が規定した要求事項

2)　この規格の要求事項

b)　有効に実施され，維持されている。

組織は，次に示す事項を行わなければならない。

c)　頻度，方法，責任及び計画に関する要求事項及び報告を含む，監査プログラムの計画，確立，実施及び維持。監査プログラムは，関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない。

d)　各監査について，監査基準及び監査範囲を明確にする。

e)　監査プロセスの客観性及び公平性を確保する監査員を選定し，監査を実施する。

f)　監査の結果を関連する管理層に報告することを確実にする。

g)　監査プログラム及び監査結果の証拠として，文書化した情報を保持する。

9.2　内部監査

9.2.1　一般

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

a)　次の事項に適合している。

1)　ISMS に関して，組織自体が規定した要求事項

2)　この規格の要求事項

b)　有効に実施され，維持されている。

9.2.2　内部監査プログラム

組織は，監査プログラムを計画し，確立し，実施し，維持しなければならない。これには，その頻度，方法，責任，計画策定の要求事項及び報告を含める。

それ（れら）の内部監査プログラムを確立するとき，組織は，関連するプロセスの重要性及び前回までの監査の結果を考慮しなければならない。

組織は，次に示す事項を行わなければならない。

a)　各監査について，監査基準及び監査範囲を明確にする。

b)　監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。

c)　監査の結果を関連する管理層に報告することを確実にする。

組織は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にしなければならない。

JIS Q 27001:2023　9.2 内部監査

9.2　内部監査

9.2.1　一般

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

a)　次の事項に適合している。

1)　ISMS に関して，組織自体が規定した要求事項

2)　この規格の要求事項

b)　有効に実施され，維持されている。

9.2.2　内部監査プログラム

組織は，監査プログラムを計画し，確立し，実施し，維持しなければならない。これには，その頻度，方法，責任，計画策定の要求事項及び報告を含める。

それ（れら）の内部監査プログラムを確立するとき，組織は，関連するプロセスの重要性及び前回までの監査の結果を考慮しなければならない。

組織は，次に示す事項を行わなければならない。

a)　各監査について，監査基準及び監査範囲を明確にする。

b)　監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。

c)　監査の結果を関連する管理層に報告することを確実にする。

組織は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にしなければならない。

JIS Q 27001:2023　9.2 内部監査

9.2　内部監査

9.2.1　一般

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

①適合性

a)　次の事項に適合している。

1)　ISMS に関して，組織自体が規定した要求事項

2)　この規格の要求事項

②有効性

b)　有効に実施され，維持されている。

9.2.2　内部監査プログラム

組織は，監査プログラムを計画し，確立し，実施し，維持しなければならない。これには，その頻度，方法，責任，計画策定の要求事項及び報告を含める。

それ（れら）の内部監査プログラムを確立するとき，組織は，関連するプロセスの重要性及び前回までの監査の結果を考慮しなければならない。

組織は，次に示す事項を行わなければならない。

③監査員の選定

a)　各監査について，監査基準及び監査範囲を明確にする。

b)　監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。

c)　監査の結果を関連する管理層に報告することを確実にする。

組織は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にしなければならない。

①適合性

9.2.1　一般

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

a)　次の事項に適合している。

1)　ISMS に関して，組織自体が規定した要求事項

2)　この規格の要求事項

9.2.1 a)項では、以下について調査しました。

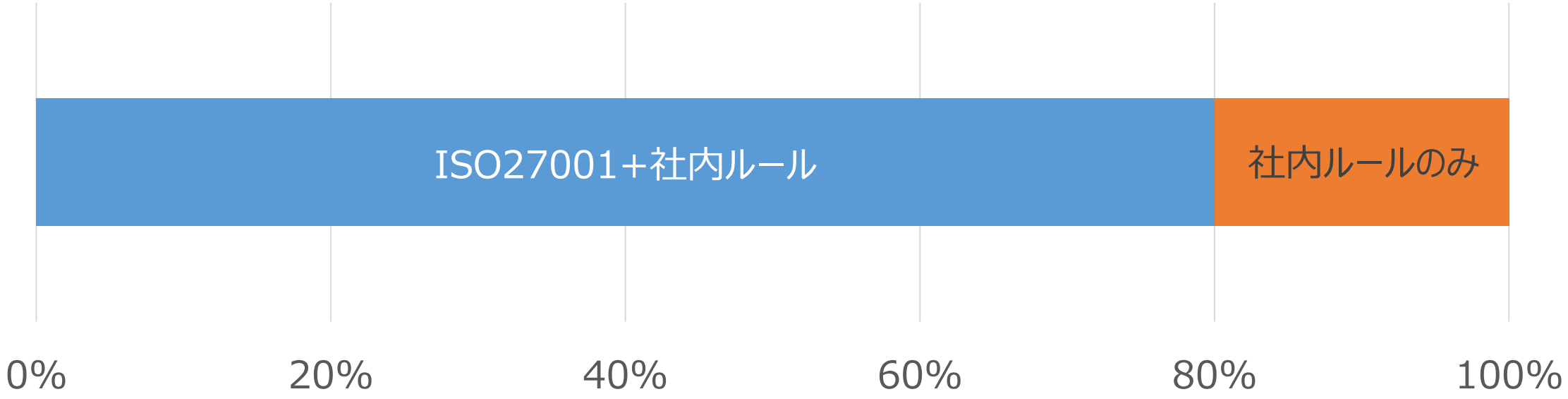
① 内部監査では、何に対する適合性を測っていますか？

② 内部監査の設問の更新頻度は？

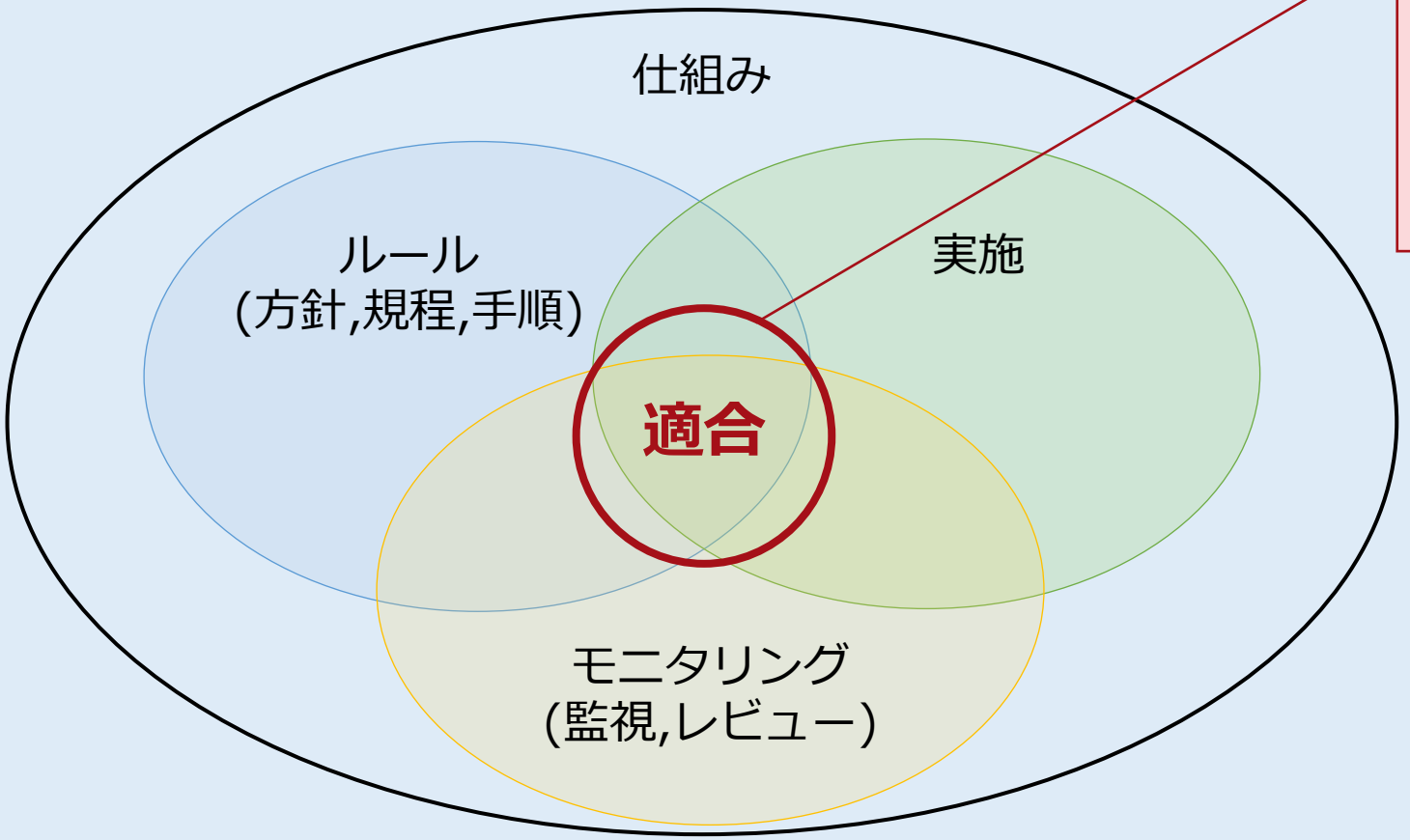
③ 内部監査の設問の作成者は誰ですか？

①内部監査では、何に対する適合性を測っていますか？

「社内ルールのみ」との回答もありましたが、そのルールは27001に準拠しているはずなので、実質全件同じかと思います。



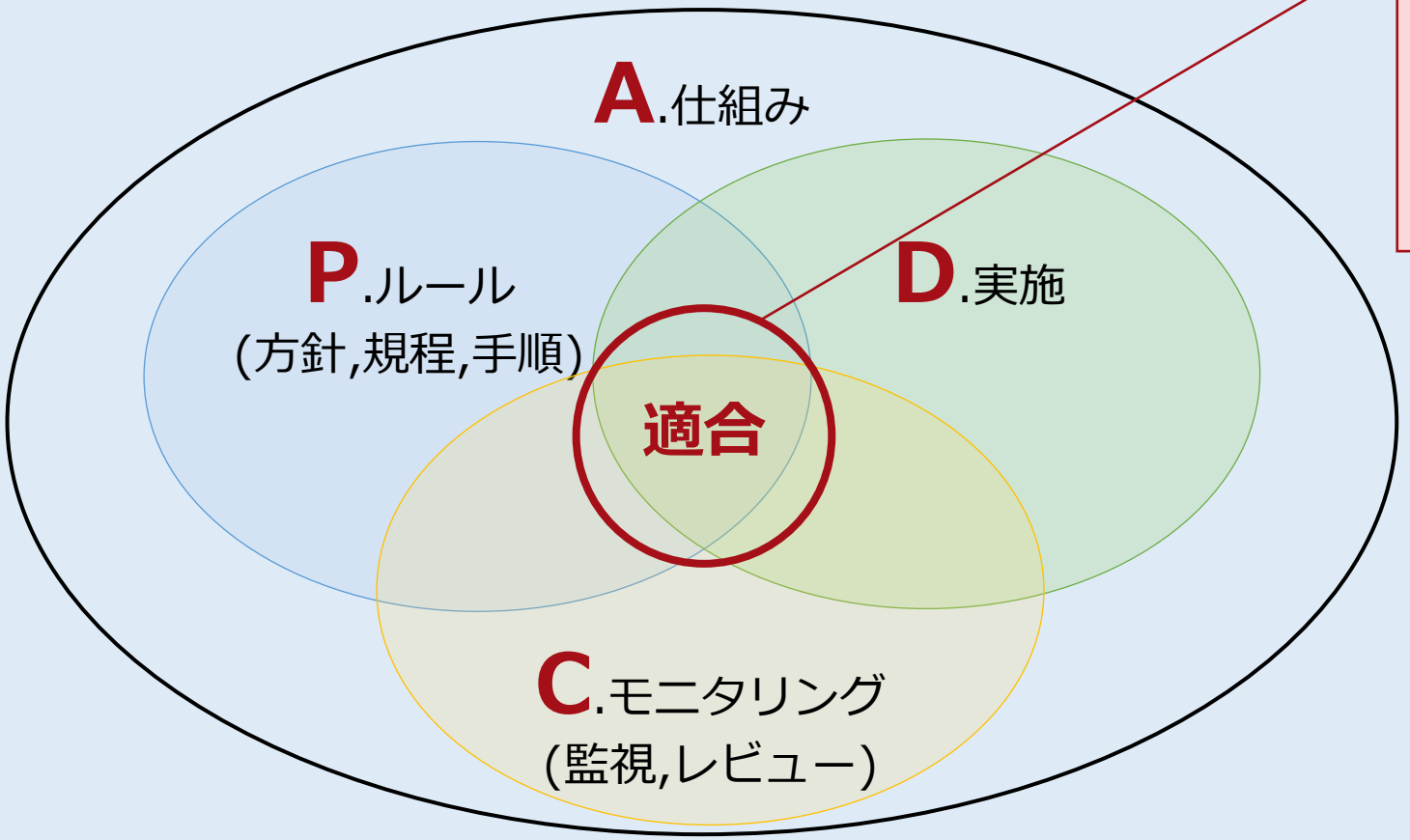
適合性確認の視点



この要素が揃っていることが、適合を確認するうえで重要

(という事を、監査員が理解している！)

適合性確認の視点



この要素が揃っていることが、適合を確認するうえで重要

(という事を、監査員が理解している！)

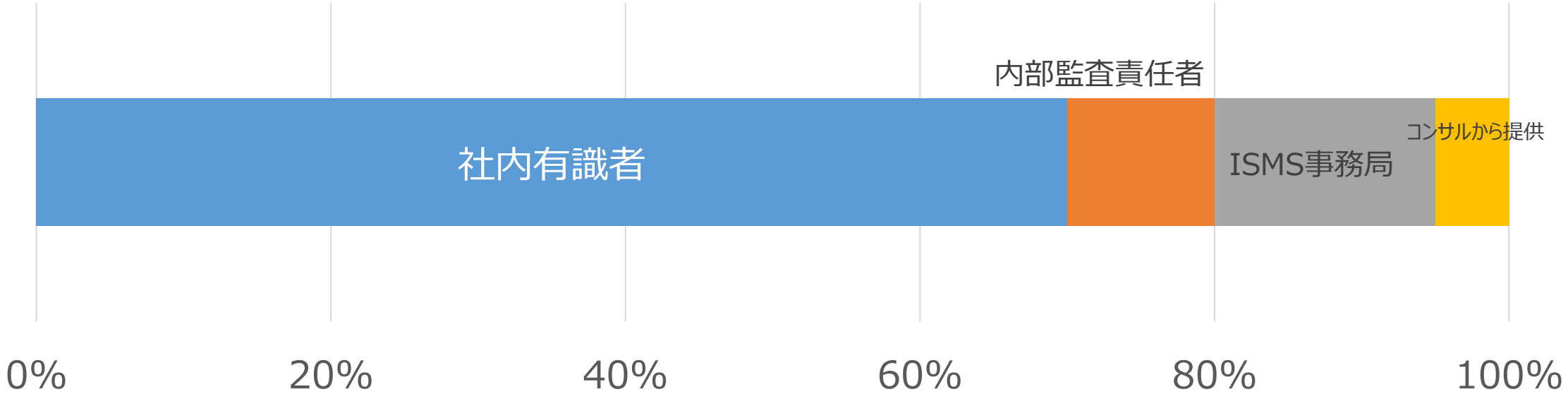
②内部監査の設問の更新頻度

見直すポイントとしては・・・

- 発生した事故の再発防止策実施状況の確認
- 前回監査での指摘事項、規程の変更、内外の環境の変化、など

③内部監査の設問の作成者

業務内容が分かる人でISMSの知識経験がある方を「社内有識者」と呼称するようですが、『同じ人がずーっと担当している』例も少なくないようです。



②有効性

9.2.1　一般

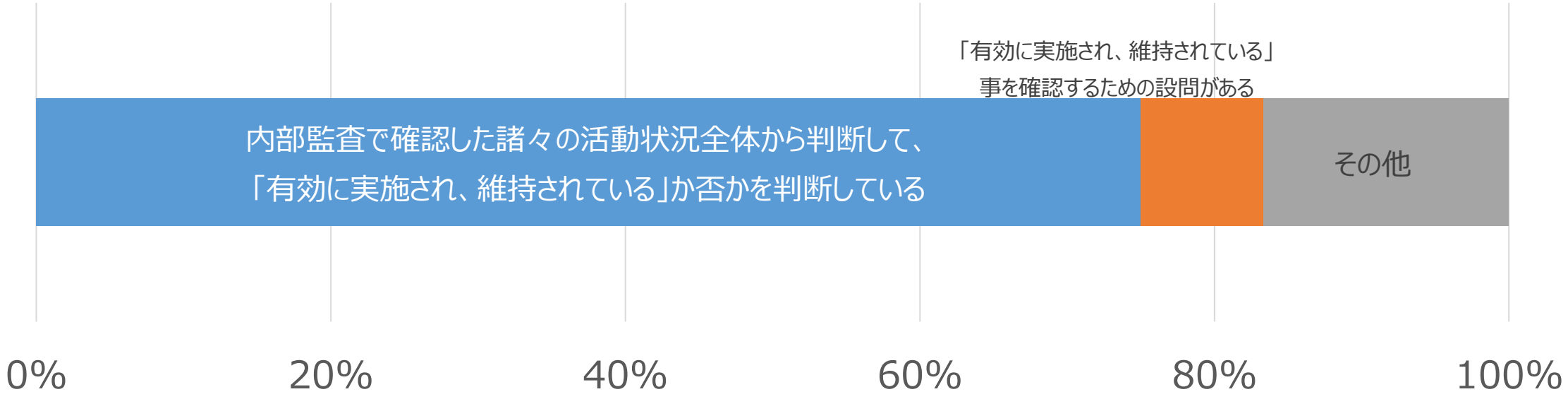
組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。

b)　有効に実施され，維持されている。

9.2.1 b)項では、以下について調査しました。
①　「有効性」をどのように判断していますか？

①「有効性」をどのように判断していますか？

「諸所の活動状況全体から判断」が大勢でしたが、
実は『2つの異なる(有効性の)解釈』が存在することがわかりました。



②箇条9.2「有効に実施され」の解釈

有効性判断の要素としている「**諸処の活動**」には、どんなものがありますか？

ISMSが有効に実施されているか派

- セキュリティルールの順守状況、運用タスクの実施状況など
- ビジネスの目的に沿ったセキュリティ目標が設定していて、それのガバナンス状況をみて総合的に判断
- ヒヤリハット等をインシデントの兆候と捉え、組織内の事象の共有と、潜在的なリスク源に係る討議を踏まえた安全管理措置の見直しと是正を行う能動的な活動
- 情報セキュリティ目的を達成させるための各対策・活動について、効果が見込まれること、無理なく行えること、確実に行えていること、確実に行える仕組み(再現性)を備えていることなどを内部監査員が総合的に判断している。
- セキュリティの順守状況と、ISMS運用のイベントの実施状況(教育等)

内部監査が有効に実施されているか派

- 監査責任者・監査担当者向け個別監査毎の報告会&年次報告会、経営者向け報告会
- 内部監査の年間計画やプログラム、チェックリスト、報告書を指します。
- 内部監査を担当するコンサルより提出される「監査報告書」。
- 内部監査報告書は取り合えず内部監査責任者に報告され、その時点で内部監査結果、内部監査手法に関するチェックが入ります。それらの内部監査結果を再度レビューすることで、内部監査担当者、内部監査責任者の独断にはなっていない→従って有効である という論調で進めました。

③その他の「有効性」の解釈

その他の、有効性判断の手法

「(ISMSが)有効に実施され、維持されている」の確認は、いわゆる有効性に関する監査だと考えており、

不適合	**適合性に関する監査の指摘**
改善の機会	**有効性に関する監査の指摘**

と整理しています。

すなわち、改善の機会の内容をもとに、有効に実施され維持されているかどうかを確認しています

③監査員の選定

9.2.2　内部監査プログラム

組織は，次に示す事項を行わなければならない。

b)　監査プロセスの客観性及び公平性を確保するために，監査員を選定し，監査を実施する。

9.2.2 b)項では、以下について調査しました。

① 体制

② 監査員の育成

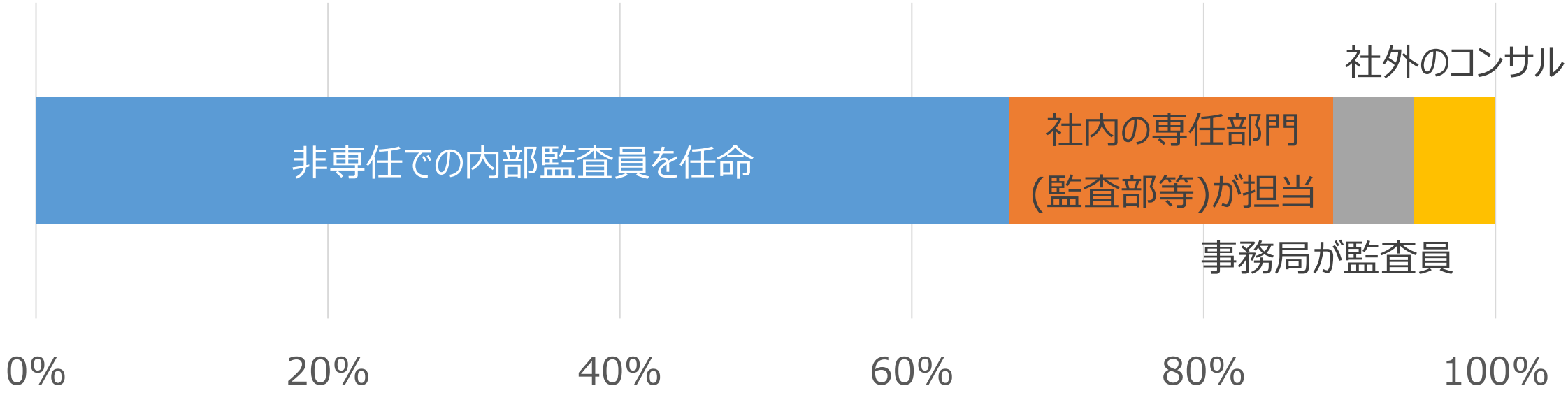
③ 事務局が被監査部門での監査員

④ 監査員の工数や出張費用の負担

①内部監査の体制

非専任の監査員を横断的に選出しているパターンが大勢でした。

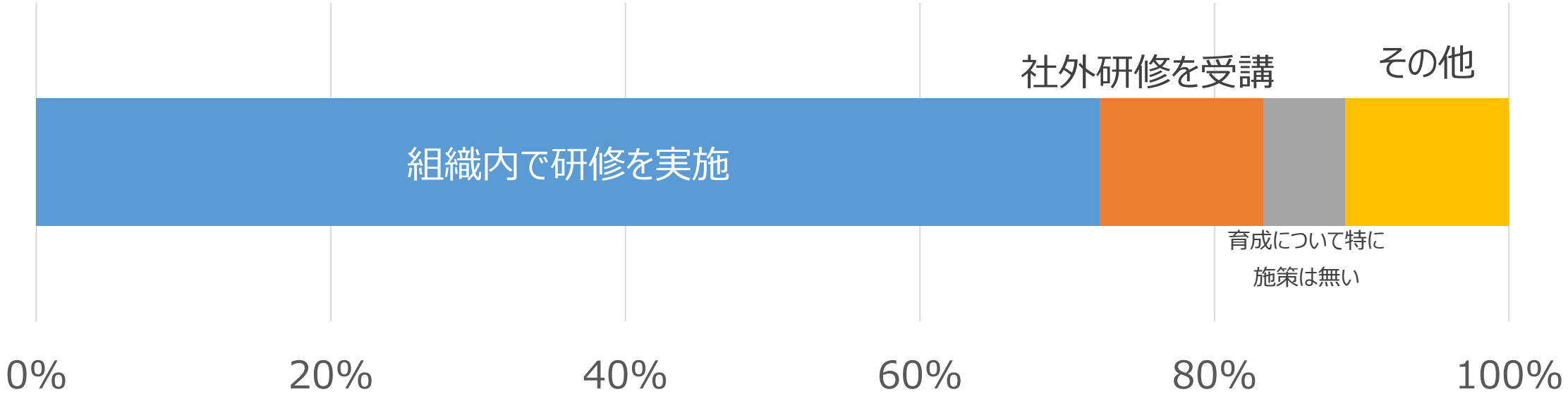
その方々が情報セキュリティ知識や監査テクニックの力量を予め備えているわけではないため、育成の施策が必要となりますが。。。



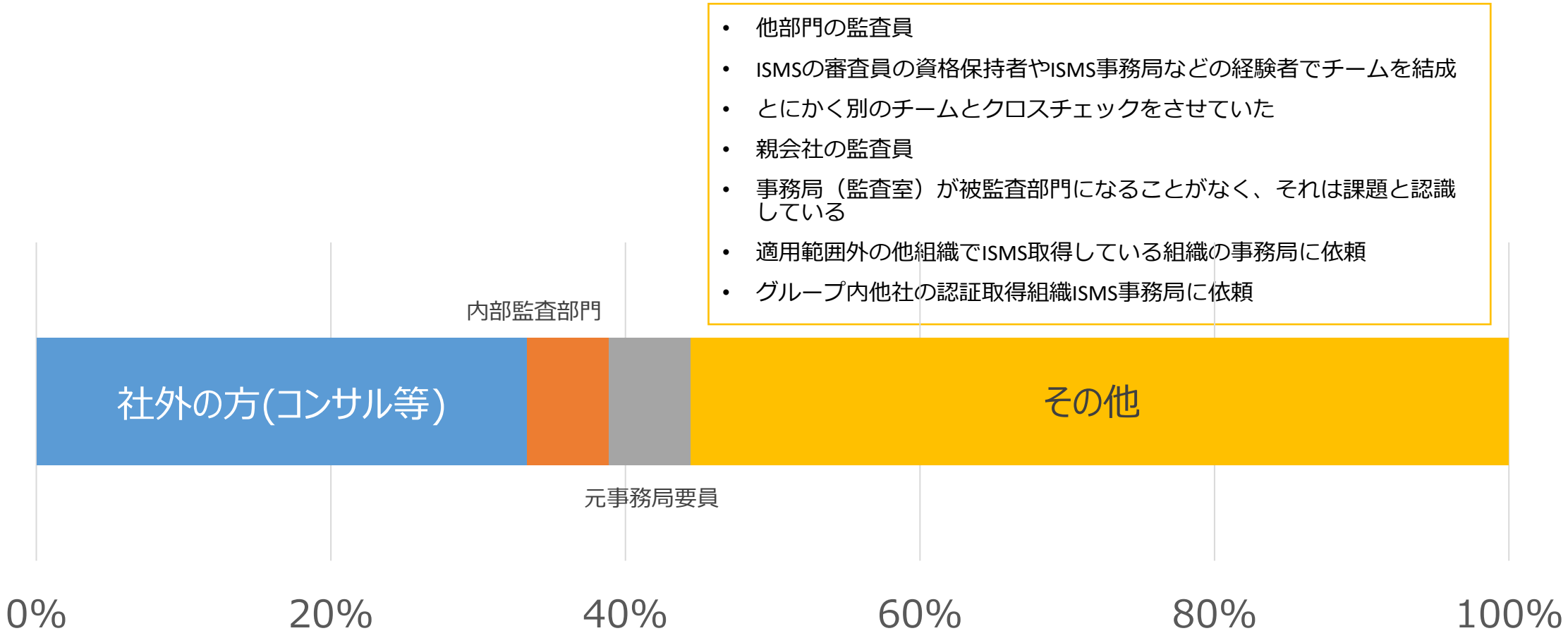
②監査員の育成

育成は社内で実施している場合が大勢でした。

監査員の力量としては、監査基準の理解把握に加えてヒアリングテクニックといったものも必要のため、皆さん苦労されているようです。



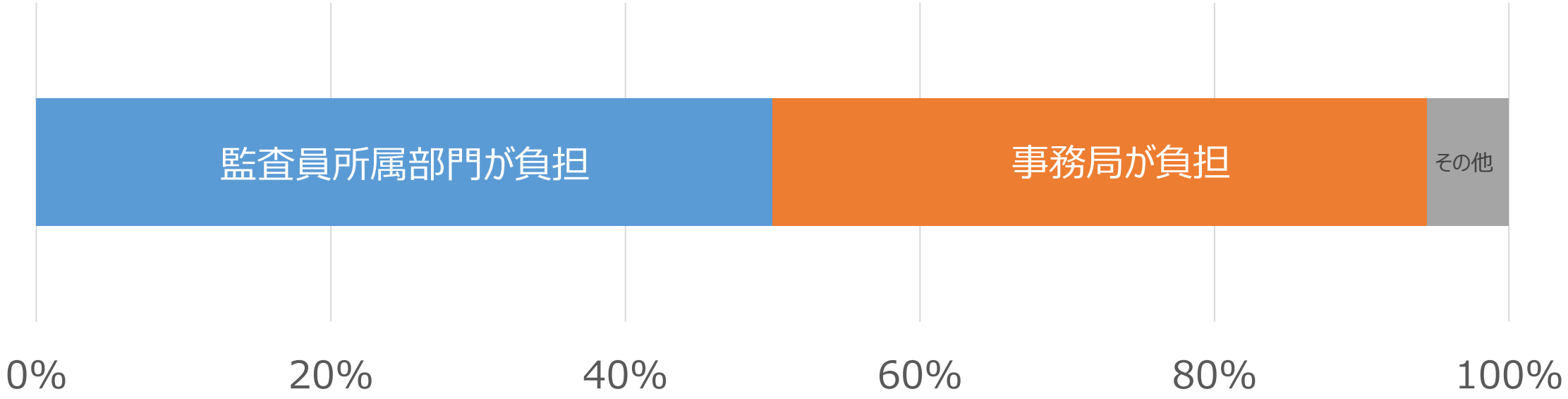
③事務局が被監査部門での監査員



- 他部門の監査員
- ISMSの審査員の資格保持者やISMS事務局などの経験者でチームを結成
- とにかく別のチームとクロスチェックをさせていた
- 親会社の監査員
- 事務局（監査室）が被監査部門になることがなく、それは課題と認識している
- 適用範囲外の他組織でISMS取得している組織の事務局に依頼
- グループ内他社の認証取得組織ISMS事務局に依頼

④監査員の工数や出張費用の負担部門

本質的な話ではないのですが、大企業では特にこういった話が挙がりがちかと思い興味本位で調べてみました。



⑤監査プロセスの客観性及び公平性を確保する監査員を選定

課題・悩みなど

- 毎年特定の担当者に監査作業が集中しており、スケジュール調整が非常に煩雑なため、上質な監査員の人数を増やす必要がある。
- 研修等は行うものの、内部監査員の力量の差がどうしても発生してしまう。
  そのため、同様の事象だったとしても不適合となる被監査部門もあれば、スルーされることもあるなど、審査内容にムラが発生してしまう。
- コンサルに依頼している都合上、自社特有の事情についての確認は同席している事務局員の力量次第になってしまう。
- 限られた時間で監査を行うため、重要な業務プロセスを特定しサンプリングによる監査を行っているが、この特定方法が属人化している。
  また、正しくサンプリングされている保証が難しい。

Part.4
「監査所見の定義」の比較

「監査所見の定義」とは

下記を指しています。

【例】

区分	評価基準	修正および是正措置
適合	要求事項を満たしている。	
重大な不適合	要求事項を満たしていない。（規格要求事項及び法令・規制、各種マニュアル及び要領の要求事項を満たしていない場合。） • 規格の重要要件の完全欠落。 • PDCAサイクルが全く機能していない。 • 遵法違反・重要要件が全く実施されていない。 • 同類の軽微な不適合が多数確認された。 • 重要人物が無視、知らず。 • 軽微な不適合が是正されていない。等	• 監査員と組織が合意した期日までに修正及び是正処置をレビューし、有効性の検証を行う。
軽微な不適合	要求事項に不適合で、不適合の程度が軽微な場合 • 要求事項の一部が欠けている。 • 一部の部門で実施されていない。 • 実施しているが、十分な成果が期待できない。 • 手順書と作業が不一致。等	• 組織がコミットした期日までに修正及び是正処置の計画をレビューし、有効性の検証は次回監査で確認する。
観察事項	要求事項に適しているが、改善すべきことがある場合 • 誤解を招く記述、表現が曖昧。 • 一部の部門の軽微な抜け。 • 実施するも、有効性が若干疑問である。 • 証拠（記録）がない。等	• 次回監査で改善状況を確認する場合がある。
グッドポイント	要求事項を満たしていることに加え、特筆すべきことがある場合。 • 組織の期待以上に情報セキュリティの維持に努めている。 • 組織の施策に加え、システム化等によってさらなる改善を行っている。等	

各社の基準

各組織で基準の項目は多様ですが、類似を集約すると以下の通りです。

	A社	B社	C社	D社	E社	F社	G社	H社	I社	J社	K社	L社	M社	N社
不適合	不適合重大	不適合 (指摘事項)	不適合	重大な不適合	メジャー	重大な不適合	重度の不適合	重度の不適合	重大な不適合	指摘	重大な不適合	不適合	不適合	緊急
	不適合軽微			軽微な不適合	マイナー	軽微な不適合	軽度の不適合	軽度の不適合	軽微な不適合		軽微な不適合	一部不適合		至急
														一般
適合	改善の機会	改善の機会 (観察事項、 意見・提案)	観察事項	観察事項	提案	提案事項	改善の機会 (観察事項)	改善の機会	観察事項	改善事項	観察事項	改善の機会	改善の機会	
				推奨事項						提言	意見			
	グッドポイント	GoodPoint	グットポイント			グッドポイント	ストロング ポイント				グッドポイント	GOOD POINT		
	ストロングポイント													

規格での不適合の定義 (重大/軽微)

JIS Q 17021-1:2015 適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項－第1部:要求事項より引用

不適合：要求事項を満たしていないこと	重大な不適合	意図した結果を達成するマネジメントシステムの能力に影響を与える不適合。 注記 次の事項は，重大な不適合に分類される可能性がある。 • 効果的なプロセス管理が行われているか，又は製品若しくはサービスが規定要求事項を満たしているかについて，重大な疑いがある。 • 同一の要求事項又は問題に関連する軽微な不適合が幾つかあり，それらがシステムの欠陥であることが実証され，その結果重大な不適合となるもの。
	軽微な不適合	意図した結果を達成するマネジメントシステムの能力に影響を与えない不適合。

重大な不適合

基準の表現例

1	社内ルール及び法令・規制、各種マニュアル及び要領の社内ルールを「全く」満たしていない
2	意図するかしないかに関わらず、部門内全体でルール通り実施していない
3	監査基準に監査証拠が適合していない
4	当該監査項目に係るプロセスまたはコントロールが完全に欠落している、完全に機能していない
5	規程類、ガイドライン等のルールを逸脱しており、インシデントにつながる恐れがある
6	明らかに情報漏えい、改ざん、紛失が発生している又はそれらの兆候が認められる
7	明らかに目的外の(編注:個人情報の)作成・取得・利用・保管・提供が発生している

重大な不適合

修正・是正措置

「期日までに修正及び是正処置をレビューし、有効性の検証を実施」は共通ですが、その期限設定にはバラエティがありました。

1	監査員と組織が合意した期日までに
2	監査員の指定した期日までに
3	直ちに是正しなければならない。速報を発行すると共に是正計画書を作成し、完了報告書にて完了を報告
4	監査人からの報告後１週間を目途に是正計画（是正時期、内容等）を記載
5	監査日より原則14日以内に修正および是正処置の計画をレビュー
6	３ヶ月以内を目途に是正

軽微な不適合

基準の表現例

1	規格または社内ルールに一部不適合
2	監査証拠は十分ではないが、法令・規程・実施手順等に違反している可能性が疑われる
3	実態としてルールを順守、または対応はしているものの、記録として残されていないなど、資料に不備がある
4	多少運用に欠陥は認められるが、マネジメントシステムの欠陥とはいえない
5	当該監査項目に係るプロセスまたはコントロールの一部が欠落
6	複数回の作業の内、実施漏れ、実施時期の遅れなど、やる気はあるけどやれていない物

軽微な不適合

修正・是正措置

「期日までに修正及び是正処置の計画をレビュー」は共通ですが、やはり期限設定にはバラエティがありました。

1	組織がコミットした期日まで
2	監査員の指定した期日まで
3	事務局が指定した期日まで
4	2週間以内に是正の必要性を検討

不適合(N社の基準)

不適合	緊急	発見した不適合は、組織に重大な影響を及ぼす可能性があるため最優先で対処すべきと判断した場合。
	至急	発見した不適合は、組織に影響を及ぼす可能性のあるため、社内手続きに従って速やかに対処すべきと判断した場合。
	一般	発見した不適合が直ちに組織に影響を及ぼすことは無いが、社内手続きに従って対処すべきと判断した場合。

「修正」と「是正措置」の違い①

JIS Q 27000:2019より引用

修正（correction）

検出された不適合を除去するための処置。

是正処置（corrective action）

不適合の原因を除去し，再発を防止するための処置。

「修正」と「是正措置」の違い②

JIS Q 27001:2023より引用

修正

是正措置

10.2　不適合及び是正処置

不適合が発生した場合，組織は，次の事項を行わなければならない。

a)　その不適合に対処し，該当する場合には，必ず，次の事項を行う。

　1)　その不適合を管理し，修正するための処置を講じる。

　2)　その不適合によって起こった結果に対処する。

b)　その不適合が再発又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置を講じる必要性を評価する。

　1)　その不適合をレビューする。

　2)　その不適合の原因を明確にする。

　3)　類似の不適合の有無，又はそれが発生する可能性を明確にする。

c)　必要な処置を実施する。

d)　講じた全ての是正処置の有効性をレビューする。

e)　必要な場合には，ISMS の変更を行う。

是正処置は，検出された不適合のもつ影響に応じたものでなければならない。

組織は，次に示す事項の証拠として，文書化した情報を利用可能な状態にしなければならない。

f)　不適合の性質及びそれに対して講じたあらゆる処置

g)　是正処置の結果

改善の機会/観察事項

基準の表現例は各組織特徴があり面白かったため、要約を一覧で掲載します。

	基準	詳細
1	社内ルールに適しているが、改善すべきことがある場合	• 誤解を招く記述、表現が曖昧。 • 一部の部門の軽微な抜け。 • 実施するも、有効性が若干疑問である。 • 記録の記載に不備がある
2	監査基準に監査証拠が適合しているが、改善したほうが望ましい状態	
3	不適合と同様の事象が発生しているが、その内容が一部に留まる場合。（法的な要求事項に適合していない場合を除く）	• 放置すると不適合になり得る事柄 • 追跡を要する疑わしい事柄 • より効率的な運用のために改善の余地がある
4	監査証拠が十分ではなく、法令・規程・実施手順等では明示されていないものの、管理策の有効性が損なわれている可能性が考えられる	• 被監査部門において、現時点での運用実態を確認し、組織として認識されている管理策を特定し、再リスクアセスメントが必要と考えられる • リスクアセスメントの結果、リスク受容したうえで、現時点での管理策を文書化することを条件に継続することはあり得る
5	監査対応した担当は規定通りに実施内容の説明とエビデンスの提示ができるが、現場（職場や現場）でヒアリングしたときに担当者の回答があやふやなことがある。	
6	現時点では規定違反には該当しないが、このまま行けば「軽微な不適合」になる可能性の高い事象	

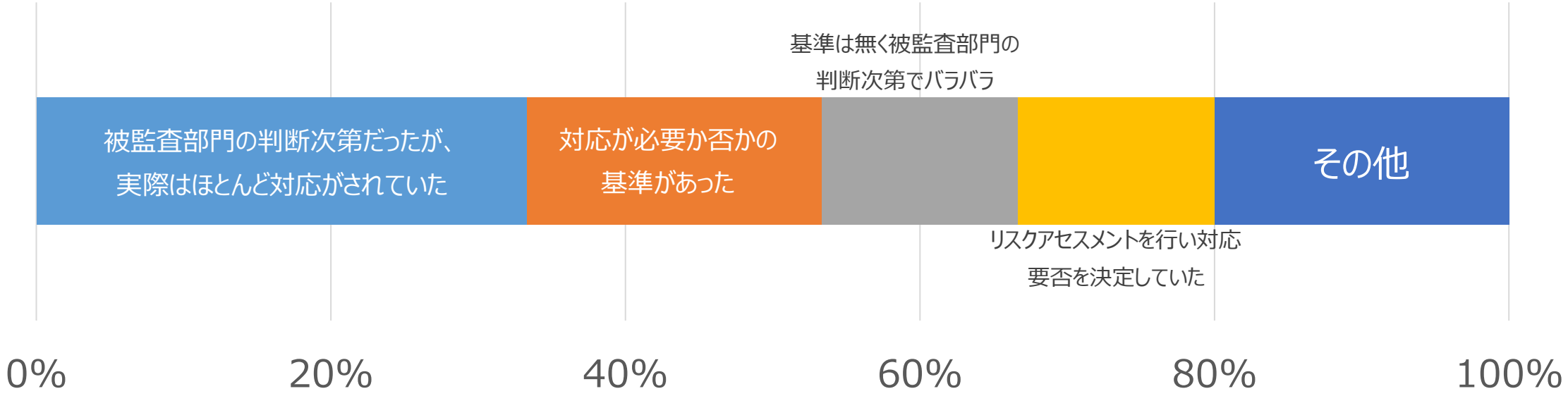
改善の機会/観察事項

基準の表現例は各組織特徴があり面白かったため、要約を一覧で紹介します。

	基準	詳細
7	現時点では「不適合」ではないが、今後「不適合」になる可能性がある。 現時点では「不適合」の判定はできないが、今後「不適合」となる可能性がある。	
8	形式的には適合しているが、放置すると不適合になる可能性がある。 対応はされているが適切性、妥当性、有効性に問題がある。	

改善の機会/観察事項

改善の機会への対応状況



その他

- 原則、改善の機会を出すまえで監査担当と被監査部門の間で協議され、被監査部門においてリスク評価し、対策を行うべき、と判断したものだけを改善の機会として取り上げることとしています。そのため、改善の機会は、不適合と同様に原則、是正する、ことになります。ただし、進捗管理の対象ではないので、３ヶ月毎の進捗管理は行われず、被監査部門の裁量において対応を行うことになります。但し、１年経過後に対応していない場合、是正対象になる懸念があります。
- 被監査部門の判断次第で、対応される傾向にはある認識です。対応しない場合でも、不要であるという理由を明記する運用になっています。
- 基本は対応する。対応しない場合、理由を記載し、監査人、事務局納得でOK。

グッドポイント/ストロングポイント

基準の表現例

1	社内ルールを満たす活動の中で、創意工夫等で特に優れた良事例であり、他部門での取り入れを検討すべき事項
2	規程に定められているルールより更にレベルの高い取り組みを行っている場合や、ルールを守るために独自のアイデアで運用上の工夫を行っている場合
3	法令・規程・実施手順等に基づき、組織の特徴に応じて管理策が工夫され、文書化され、継続的に改善されている
4	社内共有を図るべき優れた活動内容

グッドポイント/ストロングポイント

JIS Q 19011:2019より引用

3.10 監査所見

収集された監査証拠を、監査基準に対して評価した結果。 注記1 監査所見は、適合又は不適合を示す。

注記2

監査所見は、リスク若しくは改善の機会の特定、又は**優れた実践事例の記録を導き得る。**

注記3

監査基準が法令要求事項又は規制要求事項から選択される場合、監査所見は“順守”又は“不順守”と呼ばれる。

Part.5
改善事例の紹介

①内部監査での主任審査員の育成

Before

- 内部監査員にISMS審査員補資格保持者がいるが、従来の活動では主任昇格要件を満たすことが出来なかった
- 事務局要員(内部監査員)キャリアパス選択肢の一つである、審査員への道を開きたい

After

◆ ISMS認証取得企業5社間でのクロス監査の仕組みを構築

◆ グループ内の主任審査員に、育成指導を依頼

◆ 数年計画での、主任昇格要件を満たす監査プログラムを策定実行

②有識者による報告書所見の添削

Before	After
• 内部監査員の力量による、監査報告書のレベル差があった • 記述の曖昧さや不統一により事象の具体的且つ正確な把握が困難な指摘が散見された • 指摘された事象について改善が求められる根拠と明示したルールが整合しないことが散見された • 同一事象に対して明示された根拠がバラバラであった • 同一事象に対して判定がまちまちであった • 事象の問題点に対して提示する改善案の根拠の明示がない又は不十分であった	◆ 所見の記述で、事実と該当するルールが明確に把握できるようになった ◆ 検出された事象の記述及び事象に対する指摘レベル(不適合/観察事項)の均一化が実現した ◆ 事象、結果、影響、原因及び再発防止策について一貫性が保たれる。 ✓ 標準化された用語集からの択一により、厳密には異なる事象や組織や業務等の事情について把握されず潜在リスクが残されていることが懸念される（マンネリ化が発生する温床となることが考えられる）

③当事者部門によるストロングポイント事例発表

Before	After
• 他部門(事業部)での活動(活躍)が、他からは見えづらい • 資料のみで良事例が紹介されても、伝わりづらい	◆ 従来の「グッドポイント」に加えて、他部門に紹介すべき「ストロングポイント」を設定 ◆ ストロングポイントの所見を、情報セキュリティ委員会で、当該部門自身より事例発表 ◆ 当事者自らが事例紹介する事により、思いが伝わり良事例の社内共有が強化された ◆ 別部門から、当事者部門に直接コミュニケーションをとるきっかけにも

④監査員研修の内製化

Before

- 研修を外注していたため、費用が発生していた
- 出来合いのコースのため、内容が毎年ほとんど変わらない研修内容だった
- 研修内容と当社の内部監査の内容や手順に乖離があった

After

◆ 座学とOJTを組み合わせた研修が出来るようになった
◆ 会社業務の特性に合わせた内容にカスタマイズしたことにより、監査員力量の大幅アップと、監査の質的向上が実現した。
◆ 前回の内部監査の成功例や失敗例を研修に取り入れることができるようになり、改善につながりやすい

✓ 研修資料等の作成等にリソースがかかる
✓ 外からの視点が無いため、自己流になっていないか不安(コンサル等からのフィードバックも必要？)

まとめとフォロー

まとめとフォロー

「マンネリの打破」を含めた継続的改善を各組織で行っている
- 監査員の育成や指摘事項定義の見直しなど

適合性判断の基準は明確に
- 不適合指摘は是正活動が発生するので、曖昧な基準・判断は避ける
- 基準に沿った適合性判断が出来る監査員の育成が重要

グッドポイント/ストロングポイント
- 良事例の横展開に有効
- 被監査部門での継続的改善への動機づけ

部門ごとの指摘事項数比較は止めた方が良い
- 指摘を忌避する強い動機となりうる
- やるなら「管理策ごと指摘件数」などで

聴講いただき、ありがとうございました。
皆さんの活動の一助になれば幸いです。

研究会へのお誘い

月イチの研究会では、発表には載せられないような興味深い「ここだけの話」なども交えた討議や情報交換、あるいは困りごと相談なども活発に行っています。

ぜひ、ご参加を検討ください！