CISM®試験問題
作成ガイド

（注）本書はガイドの翻訳であり試験問題は英語で作成することが必要です。

2012年11月改訂

ISACA
Trust in, and value from, information systems

CISM試験問題作成ガイド

日本語訳に際しての謝辞

ISACAの各資格認定の試験問題は、世界の会員からの応募により作成されています。しかし、残念ながら、日本語を母国語とする会員からの問題応募は、過去は特定のケースに限られていました。東京支部は、「問題応募を会員にとってもっと身近なもの」とするため本文書の日本語訳を企画し、支部会員の有志の方々に協力をお願いしました。また、CISA版をテキストとした「試験問題開発ワークショップ」を実施しています。これらの活動は、全て参加メンバーの専門家としてのボランティア活動に支えられています。ここに、翻訳者並びに協力頂いた会員の指名を列記し、深く感謝の意を表する次第です。

翻訳　東京支部副会長兼理事　坂本 正徳 CISM, CISA, CGEIT, CRISC

ISACA東京支部
2012-2013 会長兼理事　柴田　昭

Quality Statement:
This Work is translated into Japanese from the English language version of CISM Item Development Guide-2012 by the ISACA Tokyo Chapter with the permission of ISACA. The ISACA Tokyo Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.
品質について
本書は「CISM Item Development Guide-2012」を、ISACAの許可を得て東京支部が英語から日本語に翻訳したものです。翻訳の正確性および忠実性はISACA東京支部が責任を担います。

CISM試験問題作成ガイド

目　　次

CISM試験問題作成ガイド

CISM試験問題作成ガイドの目的

CISM試験問題作成ガイド（以下、「本ガイド」という）の目的は、CISM試験の品質を向上させる上で、試験問題作成者への支援を提供するものです。本ガイドでCISM試験問題の構成を十分説明することで、作成者が問題を作成・見直しにより習熟するよう支援を行ないます。

本ガイドを通じて試験問題作成の原則に留意して下さい。当該原則を適用することで、作成・提出した問題が承認される機会が増えることとなるでしょう。

CISM試験の構成

ISACAおよびCISM認定委員会では、情報セキュリティマネージャーにとって最新で必要なタスクおよび知識を決定するため、CISMの職務領域の分析を定期的に実施しています。当該分析の結果は、CISM試験の青写真として提供されます。試験問題は、CISMの職務領域分析による確立されたプロセスと定義された内容の知識を、受験者に問うよう記述されていなければなりません。

試験問題作成の品質

問題を作成する際に最初に考えなければならないのは、対象者あるいはCISMの受験者です。試験問題は、望ましいCISMの受験者に求められる適切な経験レベル（3-5年の情報セキュリティ管理の実務経験）に応じて作成されなければなりません。

情報セキュリティ管理はグローバルに展開されている職業であり、グローバルな位置や環境を反映していないような個人の見識や経験といったものでないかどうか、試験問題を作成する際には、考慮しなければいけません。試験およびCISM試験問題は、国際的な情報セキュリティ管理のコミュニティのために策定されなければならず、試験問題もグローバルで受け入れられている手法に柔軟に対応する必要があります。

CISM試験問題作成ガイド

複数選択肢問題

CISM試験問題は、複数の選択肢から構成されます。複数の選択肢は最も一般的に使用される認定試験のテスト設問のタイプです。

複数選択肢問題は1つの設問と4つの選択肢で構成されます。

設問:
設問は、評価しようとする知識に関連する状況あるいは背景を記述した導入の文章あるいは質問です。設問は、質問型であったり不完全な文章として記述されます。

選択肢:
回答の選択肢は導入の文章を完結させるもの、あるいは質問へ回答する形であり、1つの正答(Key)と3つの不正解あるいは誤答で構成されます。

正答:
正答は最新の実務を反映するものでなければいけません。正答は明示的に唯一、正しいものとして記述する場合と、相対的に提供された選択肢のなかで「最もそうであると思われる」ものを記述する場合があります。

誤答:
誤答は不正解な選択肢であるが、妥当で充分な知識を持っていない受験者が選択してしまうような内容とすべきものです。

試験問題作成の手順

手順1　CISM職務領域の中からトピックを選択します。試験問題は特定のタスクを実行するのに必要な知識を試すように記述されている必要があります。試験問題は、単一のトピックあるいは知識項目に焦点を当てるべきです。知識項目から記述された試験問題はより高い品質になると共に、実務に基づいた設問となる可能性が高いものです。Appendix AのCISM職務領域にあるタスクと知識の記述を参照して下さい。

トピックを選択した後は、以下の手順に従います。試験問題を作成する際には、ガイドラインとして試験問題作成の原則を参照し、AppendixBの試験問題作成チェックリストでレビューを行って下さい。

手順2　問題の設問と(選択肢Aに)正答を記述します。

手順3　もっともらしく見える誤答を作成します。誤答は単語や語句だけの記述をすべきではありません。誤答は経験が乏しい専門家にとっては正しい選択肢のように見えるようなものであるべきでしょう。試験問題作成のなかで、作者にとってよい誤答を作ることが最も難しい作業となります。当該作成に際して困難な場合は、経験者に相談すると良いでしょう。また経験の乏しいIT専門家が正しい回答と考えがちなものが何かを考えてみましょう。これらの経験の乏しい専門化は最良の誤答を生むことでしょう。

手順4　正答となる選択肢が何故正しく、各誤答が何故誤りであるかの説明を記入します。誤答が単に誤りだから、という書き方ではいけません。

手順5　参照したリソースを記入します。該当する参照先はISACAのウェブサイトにあります。– http://www.isaca.org/knowledge-center.

手順6　AppendixBの試験問題作成チェックリストを用いてレビューを行います。

手順7　作成した試験問題を仲間や同僚にレビュー、批評してもらいましょう。

試験問題作成に際しての一般原則

しなければならないこと:

1. 肯定的な文脈の試験問題を作成すること。否定的な文章は、それだけで書き直しが要求され、自動的に返却となる。
2. 各試験問題は、ひとつのコンセプトあるいは知識についてのみ問うこと。知識項目は当該目的で策定されている。対象となる知識項目はAppendixAの実務領域を参照のこと。
3. 設問および選択肢は共に関連性があること。例えば「最良の統制となりうるのは次のうちどれか」という設問であれば、全ての選択肢は統制についての記述とならねばならない。
4. 不要な文章や専門用語の使用を避け、可能な限り設問および選択肢は短くすること。設問に答える前の受験生に過大な情報を提供してコンセプトや理論を教えることがないようにしなければならない。これは試験であり授業ではない。
5. 正答や誤答ではなく、設問には一般的な単語あるいは語句を使用すること。
6. 全ての選択肢はだいたい同じ長さおよび形式に揃えて記述する。ITの知識や経験が乏しくとも上手な受験者は、最も短いあるいは選択肢の文を選んだり、正しいと思われる回答を選ぶことで正答を導くことになる。
7. 選択肢を作成する際には、問題の設問と文法的に一貫性を持たせて並列な文法形式とする。例えば正答が動詞で始まり「ing」で終わるのであれば、全ての誤答も動詞で始まり「ing」で終わるように作らなければならない。
8. 設問および選択肢には専門的に認められた言葉、あるいは専門用語を用いること。

してはいけないこと:

1. 試験問題の正答な単語あるいは語句を設問に入れないこと。経験豊富な受験者は、このような正答が設問にないかを探し回るからである。
2. 試験問題には、「frequently」「often」「common」「rarely」といった用語は、試験問題に主観的な概念をもたらすので使用してはならない。問題が主観的であると正答以外の選択肢も正答になってしまう可能性がある。試験問題が主観的であることは最も一般的な作成者への返却理由であり、試験において試されるものではない。
3. 設問には、「always」「never」あるいは「all」といった可能性を狭めて受験生に誤答の発見を容易にするような用語は使用してはならない。
4. 「least」「not」あるいは「except」といった用語は否定的であり、受験生に正解や望ましい選択を求めずに不正解や最低限の選択を求める。否定的な語句のテスト設問は良いものではなく、用いてはならない。

5. 「he」「she」「his」あるいは「her」といった性別の代名詞を使用しない。
6 各設問に複数のコンポーネントがある、あるいはひとつの選択肢の部分がその他の選択肢の内容を含むようなことはさける。これらは「複合、複合選択肢」と考えられ、試験としては良くない。各選択肢は各々独立しているべきである。
7. 選択肢に「all of the above」あるいは「none of the above」がある試験問題は作成者に返却される。受験生はこのような選択肢正解であることが非常に稀であることを周知しており、よい誤答とはらない。
8. ISACAはいかなるベンダー製品も支持するものではなく、ベンダー固有の製品に関する知識を問う設問は作成者に返却される。
9. 特定の標準やフレームワーク、マニュアル（例、COBIT, ISO）を個々に掲載するような試験問題は承認されない。しかしながら、最良の実践に関する知識を問うことは、全く承認および奨励されることである。
10. 以下のような主観的なコンセプトを試すことは避ける。
    a. 特定の国際的あるいは各国の法規制
    b. グローバルあるいは全ての業界では適用されない文化や業界の問題に特化した情報
    c. 組織に特化した役割や責任

    CISM試験はグローバルで全ての業界で運営されていること、試されるコンセプトはグローバルおよび全ての業界で承認され認識された実務であることを忘れてはならない。

試験問題の実例(EXAMPLES)

試験問題には、質問型、不完全文章型、あるいはシナリオ型があり、以下に記されています。
当該問題はサンプルとして問題作成用に作られたものであり、試験に出るものではありません。

質問型:

設問(Stem): Which of the following will **BEST** tie information security to business objectives?

選択肢(Options):
A. Value analysis
B. Security metrics
C. Deliverables list
D. Process improvement model

注）設問は質問型である。

不完全型:

設問(Stem): The **PRIMARY** goal of a post-incident review is to:

選択肢(Options):

A. identify ways to improve the response process.
B. gather evidence for subsequent legal action.
C. identify individuals who failed to take appropriate action.
D. make a determination as to the identity of the attacker.

注）当該設問への対応は以下の語句を伴い始まり、文章を完結させるように続き、回答は設問で始まる文を各々完成させるものである。

シナリオ型

シナリオの作成は、特定の主題あるいはコンセプトに背景を加えることになります。それは、以下に続く設問のための導入情報（あるいはシナリオ）から構成します。
シナリオ型の設問を作成する際には多くの考慮が必要となります。

- o導入情報に関連して2問から5問の設問を設定します。
- o題材は特定の領域によるもので、関連および実践なければならず、受験生に仮定を強要することなく正答を導ける必要な情報を全て含まなければいけません。
- o関係する設問は順序立てて設定されているべきで、論理的な進行に従います。
- o各設問は他の設問とは独立して作成されているべきであり、ひとつ誤答したことが他の問題の回答に影響を及ぼしてはいけません。注意を払うのは、ひとつの設問が他の設問の正答を導くようになってはいけないことです。
- o新しい情報が関連する設問のなかにあってはいけません。設問への回答に必要な全ての情報はシナリオあるいは導入情報のなかに存在すべきものです。
- oシナリオの文章に複数の事実を掲載あるいは記載する必要があれば、箇条書きにすることで、読者にとって明確かつ理解し易い最良の方法となる。

最良のシナリオは、経験に基づき業務上で生じた実際の状況が記述されたものです。加えてシナリオを作成することは、CISM職務領域内で見られる、より主観的なコンセプトを試すのに効果的な方法です。例えば、法規制や役割と責任について問う場合、法規制や組織の報告構造といった特定の要件を、導入情報の項目で説明することができます。

シナリオ型の試験問題が返却される一般的な理由としては、作成された設問が「一般的すぎる」というもので、シナリオを読まなかったとしても回答できるようなものです。また、たとえ読むことが課題であったとしても、シナリオの記述のなかに正答が直接的に検出できるような場合も、当該シナリオ型の試験問題は返却となります。シナリオ型の試験問題は、受験生に知識と経験に基づいて回答を考えさせるようにすべきであり、記述の中で答えを見つけ出させるべきではありません。されます。提出する前にシナリオを仲間や同僚にレビュー、批評してもらうのは良い考えです。

CISM試験問題作成ガイド

試験問題を作成する際に避けなければならないこと

以下は、試験問題を作成する際に避けなければいけないと記載されているものです。これらの設問は、CISM試験のプールにあるものではなく、いかなる試験でも使用されません。あくまで試験問題作成の練習目的のサンプルとして作られたものです。

例1:

設問(Stem):An intrusion prevention system does which of the following?

選択肢(Options):

A. Prevents any attacks that occur from affecting the target system
B. Stops all network traffic that is part of an attack before it can get to the intended victim
C. Constantly modifies operating systems to make them a moving target
D. Launches attacks against attacking systems to bring them down or disable them

正答(Key):A

注）正解となる単語が設問に「prevention」と記されており、「prevent」が正答であることを導いています。正解が非常に明確になってしまうので、重要な類似語を設問および回答で使うことは避けて下さい。また、選択肢Bでの「all」や、選択肢Cの「constantly」といった絶対的な言葉が使われていることで、容易にこれらが誤答であることが判ってしまいます。選択肢には絶対的あるいは主観的な単語は使用しないようにして下さい。

例2:

設問(Stem): Which of the following is **MOST** important to writing good information security policies?

選択肢(Options):

A. Ensure that they are easy to read and understand
B. Ensure that they allow for flexible interpretation
C. Ensure that they describe technical vulnerability
D. Ensure that they change when ever operating systems are upgraded

正答(Key):A

注）最初の3つの単語が各々繰り返されています。この問題では、より試験問題を簡潔に作り変えることが可能です。これらの3つの単語は設問の最後に、以下に続くものとして含めましょう。

新しい設問(New Stem): Which of the following is **MOST** important to writing good information security policies? Ensure the policies:

新しい選択肢(New Options):

A. are easy to read and understand.
B. allow for flexible interpretation.
C. describe technical vulnerability.
D. change when ever operating systems are upgraded.

設問は、文章を完成させるような選択肢を伴う不完全型となります。

例3:

設問(Stem): When building support for an information security program, which of the following should be performed **FIRST**?

選択肢(Options):

A. Identification of existing vulnerabilities
B. Cost-benefit analysis
C. Business impact analysis
D. Formal risk assessment

正答(Key):A

この試験問題はタイミングの質問の例であり、主観に基づいてしまいます。選択肢CおよびDは、組織内の状況によっては正しい回答となり得ます。プロセスの中で「最初の」段階を明確化しない限り、「最初に」すべきことは何か、という問いは良い問題ではありません。しかし、「最初の」段階を明確化すれば、設問としては簡単過ぎてしまいます。

例4:

設問(Stem): Security awareness programs should be:

選択肢(Options):

A. standardized throughout the organization.
B. customized depending on the target audiences.
C. avoided since key security vulnerabilities may be disclosed.
D. limited to IS personnel.

正答(Key):A

例4は、主観的な試験問題のもうひとつの実例です。組織のいくつかでは、セキュリティ啓蒙プログラムは標準化されたものとして義務付けられますが、一方ではプログラムをカスタマイズすることがより良い場合もあります。回答は組織のセキュリティニーズとプログラムによって変わるものです。

何がセキュリティ啓蒙プログラムとして良いのか、とか、役割と責任を試すといった、本来的に主観的になりがちな領域の設問を作成する際には、全ての状況において唯一の正答が存在するものかを注意深く確認することが必要です。全ての状況において適用される回答に自信がないものであれば、設問に更なる状況を付加したり、主観性を取り除くシナリオ型の設問にするようにしましょう。例えば、組織の構成を記載できれば、経験ある情報セキュリティマネージャーは、どの型のセキュリティ啓蒙プログラムが実施するのに最良であるかが明確になります。

例5:

設問(Stem): Record retention policies generally are driven by:

選択肢(Options):

A. legal and regulatory requirements.
B. risk levels acceptable to the organization.
C. business goals and objectives.
D. audit and assurance requirements.

正答(Key):A

当該設問は、誤答が脆弱なために正答が明確すぎる場合を描いています。法規制の要件といった回答は、受験生を正答から誤答へ導く他の強力な選択肢の余地がないことから、設問を貧弱にしてしまいます。

前の例は、試験問題が何故承認されなかったか、という最も一般的な理由を示すものです。その他に試験問題が返却される理由としては、技術的あるいは定型過ぎるといったものがあります。技術的な本質の試験問題を作成する際には、内容は情報セキュリティマネージャーの経験した知識を試す必要があること、技術者を試すものではないことを忘れないで下さい。また、CISM試験は、個人の情報セキュリティ管理の知識の応用を試す実務的な試験です。もし定型過ぎるという理由で返却される場合は、受験生に対して知識あるいはコンセプトをいかに応用するかということに反して、技術あるいはセキュリティ用語の定義を知っているかどうかを尋ねるだけの単純な試験問題である、ということが多いものです。

CISM試験問題作成ガイド

CISM職務領域とは

CISMの職務領域とは、セキュリティ、リスクおよび統制の領域で業務を遂行するIT専門家に関連するタスクと、これらのタスクを実行するのに必要知識を記載したものです。これらのタスクと知識はCISM試験の設問の基礎となるものです。CISM試験の目的は、タスクを実行するのに必要な知識を試すため、実務に基づいた設問を行うことです。CISM職務領域は、AppendixAに掲載されています。設問を作成する際には、ひとつの知識あるいは試験コンセプトのみ問うようにすることを忘れないで下さい。

種別化

全ての試験問題は領域が種別化されなければなりません。種別は、CISMのどのタスクおよび知識項目に最も関連しているかを示します。各種別では、2-3桁のタスクの番号および同様の知識の記述の番号が記載されます。種別はタスクと知識項目の前に記されます。試験問題を種別化する際には、AppendixAの「CISM職務領域」を参照して下さい。

試験問題の提出およびレビュープロセス

試験問題は、CISMitems@isaca.org に提出しなければなりません。全ての試験問題は、AppendixC – Item Construction Formの様式を使用し、英語で記載して提出する必要があります。しなければなりません。Item Construction Form内は、全項目に記載が必要です。空欄があればレビューされることなく返却されます。

*www.isaca.org/itemwriter*にある*CISM Item Writing Application*を作成した首題の専門家は、CISM認定委員会が要請したCISM職務領域内の特定の重点領域（タスク項目）を連絡する電子メール（試験問題作成キャンペーン）を受け取ることになります。試験問題作成キャンペーンには、試験問題の提出締切日も含まれます。

一次審査は、ISACAの事務局が、記載の完全性や「試験問題作成に際しての原則」への準拠について確認を行います。何か重大な欠陥があると判断された場合は、適切かつ建設的なフィードバックを付記して作成者へ返却されます。一次審査を通過した試験問題はCISM試験問題評価委員会(CISM Test Enhancement Subcommittee – TES)へ送られて試験問題プールに入れるべきかどうかの審査を行います。

評価委員会でレビューされた問題は、承認されるか返却されることになります。問題が作成者に返却される場合は、適切かつ建設的なフィードバックが付記されます。承認された場合には、当該試験問題はISACAが所有権を有するものとなり、作成者には2CPEの付与と共に謝礼金が支払われます。$100の謝礼金が重点領域で承認された各試験問題に授与され、重点領域以外で承認された各試験問題には$50が授与されます。

AppendixA

CISM職務領域

ドメイン1 – 情報セキュリティガバナンス: 情報セキュリティガバナンスのフレームワークと支持プロセスを確立し維持して、確実に情報セキュリティ戦略が組織の目標と目的と調和し、情報リスクが適切に管理され、プログラム・リソースが責任を持って管理されるようにする。

タスク

1.1 情報セキュリティ戦略を組織の目標と目的と調和するよう確立し維持して、情報セキュリティプログラムの確立と継続的管理を指導すること。
1.2 情報セキュリティガバナンスのフレームワークを確立し維持して、情報セキュリティ戦略を支援する活動を指導すること。
1.3 情報セキュリティガバナンスを企業ガバナンスに組み込んで、組織の目標と目的が情報セキュリティプログラムによって確実に支援されるようにすること。
1.4 情報セキュリティ方針を確立し維持して、経営陣の指示を伝達し、基準、手順、およびガイドラインの策定を指導すること。
1.5 情報セキュリティへの投資を支援するビジネスケースを開発すること。
1.6 組織に対する内部的および外部的影響(技術、ビジネス環境、リスク許容度、所在地、法令や規制の要件など)を把握して、これらの要素が確実に情報セキュリティ戦略の対象項目になるようにすること。
1.7 経営陣上層部のコミットメントおよび利害関係者からの支援を得て、情報セキュリティ戦略の実施に成功する可能性を最大限に高めること。
1.8 情報セキュリティの役割と責任を規定し、組織全体に伝達して、明確な説明責任と権限のラインを確立すること。
1.9 測定基準(重要目標達成指標[KGI]、重要業績評価指標[KPI]、重要リスク評価指標[KRI]など)の確立、監視、評価、および報告を行って、情報セキュリティ戦略の有効性に関する正確な情報を経営陣に提供すること。

知識項目

1.1 情報セキュリティ戦略を策定する方法に関する知識
1.2 情報セキュリティと事業の目標、目的、機能、プロセス、および実務の間の関係に関する知識
1.3 情報セキュリティガバナンスのフレームワークを実現する方法に関する知識
1.4 ガバナンスの基本的概念、およびそれらの概念と情報セキュリティとの関係に関する知識
1.5 情報セキュリティガバナンスを企業ガバナンスに組み込む方法に関する知識
1.6 情報セキュリティのガバナンスと戦略策定に関連して、国際的に認知された標準、フレームワーク、およびベストプラクティスに関する知識
1.7 情報セキュリティ方針を策定する方法に関する知識
1.8 ビジネスケースを開発する方法に関する知識
1.9 戦略的予算計画および報告方法に関する知識
1.10 組織に対する内部的および外部的影響(技術、ビジネス環境、リスク許容度、所在地、法令や規制の要件など)、およびこれらが情報セキュリティ戦略に影響を及ぼす方法に関する知識
1.11 情報セキュリティについて経営陣上層部のコミットメントおよび利害関係者からの支援

を得る方法に関する知識
1.12 情報セキュリティ管理の役割と責任に関する知識
1.13 組織構造と権限のラインに関する知識
1.14 報告と伝達の経路を組織全体に新規に確立するか既存の経路を活用する方法に関する知識
1.15 測定基準(重要目標達成指標[KGI]、重要業績評価指標[KPI]、重要リスク評価指標[KRI]など)の選択、実施、および解釈を行う方法に関する知識

ドメイン2 - 情報リスクの管理とコンプライアンス: 情報リスクを許容できるレベルまで管理して、組織の事業要件とコンプライアンス要件を満たす。

タスク

2.1 情報資産のランク付けのプロセスを確立し維持して、資産保護の手段が事業価値に確実に比例するようにすること。
2.2 法令、規制、組織、およびその他の該当する要件を把握して、不遵守のリスクを許容できるレベルまで管理すること。
2.3 リスク評価、脆弱性評価、および脅威分析が確実に定期的かつ一貫して実行されて、組織の情報に対するリスクを把握できるようにすること。
2.4 適切なリスク対応オプションを判断して、リスクを許容できるレベルまで管理すること。
2.5 情報セキュリティコントロールを評価して、それらが適切でありリスクを許容できるレベルにまで効果的に低減するかどうかを判断すること。
2.6 現在のリスクレベルと目標レベルとのギャップを把握して、リスクを許容できるレベルまで管理すること。
2.7 情報リスク管理を事業とITの各プロセス(開発、調達、プロジェクト管理、合併・買収など)に組み込んで、一貫性があり包括的な情報リスク管理プロセスを組織全体に推進すること。
2.8 既存のリスクを監視して、変化を確実に把握し適切に管理すること。
2.9 情報リスクにおける不遵守やその他の変化について該当する経営陣に報告して、リスク管理の意思決定プロセスを支援すること。

知識項目

2.1 事業目的に一致する情報資産のランク付けモデルを確立するための方法に関する知識
2.2 情報の資産とリスクの責任と所有権を割り当てるために使用される方法に関する知識
2.3 有害な事象がビジネスに及ぼす影響を評価するための方法に関する知識
2.4 情報資産の評価方法に関する知識
2.5 情報セキュリティに関連する法令、規制、組織、およびその他の要件に関する知識
2.6 新たな情報セキュリティ上の脅威と脆弱性に関する、評判が良く、信頼できる時宜にかなった情報源に関する知識
2.7 リスクの再評価および情報セキュリティ・プログラム要素の変更が必要になる可能性のある事象に関する知識
2.8 情報の脅威、脆弱性、および発現度とそれらの進展性に関する知識
2.9 リスクの評価と分析の方法論に関する知識
2.10 リスクの優先度設定に使用される方法に関する知識
2.11 リスクの報告要件(頻度、対象読者、項目など)に関する知識
2.12 リスクの監視に使用される方法に関する知識
2.13 リスク対応戦略とその適用方法に関する知識
2.14 コントロール・ベースラインモデリング、およびリスクを基準とする評価と同モデリングとの関係に関する知識
2.15 情報セキュリティのコントロールと対策、およびそれらの有効性と効率の分析方法に関する知識

2.16 情報セキュリティに関連するギャップ分析法に関する知識
2.17 リスク管理を事業とITプロセスに組み込むための手法に関する知識
2.18 コンプライアンス報告のプロセスと要件に関する知識
2.19 リスク対応オプションを評価するための費用対効果分析に関する知識

ドメイン3 – 情報セキュリティプログラムの開発と管理: 情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し管理する。

タスク

3.1 情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し維持すること。
3.2 情報セキュリティプログラムとその他のビジネス機能(人事[HR]、経理、調達、ITなど)との間で整合性を確実に取って、ビジネスプロセスへの組み込みを支援すること。
3.3 内部と外部のリソースの要件の把握、取得、管理、および定義を行って、情報セキュリティプログラムを実行すること。
3.4 情報セキュリティアーキテクチャ(人材、プロセス、技術)を確立し維持して、情報セキュリティプログラムを実行すること。
3.5 組織の情報セキュリティの基準、手順、ガイドライン、および他の文書の確立、伝達、および維持を行って、情報セキュリティ方針の遵守を支援し指導すること。
3.6 情報セキュリティの周知と研修のためのプログラムを確立し維持して、セキュリティで保護された環境と効果的なセキュリティ文化を推進すること。
3.7 情報セキュリティ要件を組織の各種プロセス(変更コントロール、合併および買収、開発、事業継続、災害復旧など)に組み込んで、組織のセキュリティベースラインを維持すること。
3.8 情報セキュリティ要件をサードパーティ(合弁会社、委託業者、ビジネス・パートナー、顧客など)の契約と活動に組み込んで、組織のセキュリティベースラインを維持すること。
3.9 プログラムの管理と運用上の測定基準の確立、監視、および定期的な報告を行って、情報セキュリティプログラムの有効性と効率を評価すること。3.1 情報システムの調達、開発、保守、及びその後の廃棄への提案された投資が、ビジネス目標に合致しているかどうかを判断するために、そのビジネスケースを評価すること。

知識項目

3.1 情報セキュリティプログラムの要件と他のビジネス機能の要件を合致させる方法に関する知識
3.2 内部と外部のリソースの要件の把握、取得、管理、および定義を行うための方法に関する知識
3.3 情報セキュリティ技術、最近の動向(クラウンドコンピューティング、モバイルコンピューティングなど)、および根底にある概念に関する知識
3.4 情報セキュリティコントロールを設計する方法に関する知識
3.5 情報セキュリティアークテクチャー(人材、プロセス、技術)およびそれらを適用する方法に関する知識
3.6 情報セキュリティの基準、手順、およびガイドラインを策定する方法に関する知識
3.7 情報セキュリティの方針、基準、手順、およびガイドラインを実施し伝達する方法に関する知識
3.8 効果的な情報セキュリティの周知と研修のプログラムを確立し維持するための方法に関する知識
3.9 情報セキュリティ要件を組織の各種プロセスに組み込む方法に関する知識

3.10 情報セキュリティ要件を契約およびサードパーティ管理プロセスに組み込むための方法に関する知識
3.11 情報セキュリティの運用上の測定基準の設計、実施、および報告を行うための方法に関する知識
3.12 情報セキュリティコントロールの有効性および適用性をテストする方法に関する知識

ドメイン4 - 情報セキュリティのインシデントの管理: 情報セキュリティのインシデントの検知、調査、対応、および復旧を行う能力の計画、確立、および管理を行って、ビジネスへの影響を最小限にとどめる。

タスク

4.1 情報セキュリティのインシデントの組織内定義と重大度の序列を確立し維持して、インシデントを正確に把握し対応できるようにすること。
4.2 インシデント対応計画を確立し維持して、情報セキュリティのインシデントに効果的かつ即座に対応できるようにすること。
4.3 各種プロセスを開発し実施して、情報セキュリティのインシデントを即座に把握できるようにすること。
4.4 情報セキュリティのインシデントを調査し記録するためのプロセスを確立し維持して、法令、規制、および組織の要件に準拠しながら、適切に対応し原因を究明できるようにすること。
4.5 インシデントのエスカレーションと通知のプロセスを確立し維持して、該当する利害関係者がインシデント対応管理に確実に参加できるようにすること。
4.6 情報セキュリティインシデントに即座に効果的に対応するチームの編成、訓練、および準備を行うこと。
4.7 インシデント対応計画を定期的にテストし見直して、情報セキュリティインシデントに効果的に対応し、対応能力を向上できるようにすること。
4.8 コミュニケーションの計画とプロセスを確立し維持して、内部および外部の主体とのコミュニケーションを管理すること。
4.9 事後レビューを実施して、情報セキュリティのインシデントの根本原因を特定し、是正処置を策定し、リスクを再評価し、対応の有効性を評価し、適切な対策を実施すること。
4.10 インシデント対応計画、災害復旧計画、および事業継続計画の間の統合を確立し維持すること。

知識項目

4.1 インシデント対応計画の要素に関する知識
4.2 インシデント管理の概念と実務に関する知識
4.3 事業継続性計画(BCP)と災害復旧計画(DRP)、およびそれらとインシデント対応計画との関係に関する知識
4.4 インシデント分類法に関する知識
4.5 損害抑制法に関する知識
4.6 通知とエスカレーションのプロセスに関する知識
4.7 情報セキュリティインシデントの特定および管理における役割と責任に関する知識
4.8 インシデント対応チームで十分に備えておく必要があるツールや機器の種類または供給源に関する知識
4.9 証拠の収集、保存、および提出のためのフォレンジックの要件と能力(証拠の許容性、品質、完全性、分析過程の管理など)に関する知識
4.10 内部と外部のインシデント報告の要件と手順に関する知識
4.11 根本原因の特定と是正処置の決定を行うための事後レビュー実務および調査方法に関する知識

4.12 情報セキュリティインシデントによって生じる損害、費用、および他のビジネスへの影響を定量化する技術に関する知識
4.13 情報セキュリティイベントの検知、ログ作成、および分析を行う技術とプロセスに関する知識
4.14 情報セキュリティのインシデントの調査に使用できる内部と外部のリソースに関する知識

AppendixB

試験問題作成チェックリスト

試験問題を提出する前に、以下の全ての質問に「はい」と答えられなければいけません。

1. 試験問題は、CISMのコンセプトを、適切な経験レベル（3-5年の情報システム監査）で、受験者を試そうとしていますか。

2 当該試験問題は、CISMに関するひとつのコンセプトだけを試していますか。

3. 試験問題は明確ですか。

4. 設問には、ひとつの正しい回答を導く十分な情報がありますか。
受験生は、設問に情報が欠けていることにより、誤答を正しいものと推測するような解釈ができないように作られていますか。

5. いかなる状況や組織あるいは文化においても、設問に対するひとつの正答がありますか。設問に対応しない状況に基づき、ひとつ以上の正答がある場合に、試験問題の多くは状況によるという理由で、返却されています。

6. 設問および選択肢は相互に関連性がありますか。例えば「統制のうちどれが…」という設問であれば、全ての選択肢は統制に関するものであることが必要です。

7. 試験問題には妥当な誤答があり、ひとつだけの正答がありますか。

8. 試験問題には、正答となるような単語あるいは語句が設問の中に表現されていませんか。

9. 設問あるいは選択肢に「frequently」「often」「common」といった主観的な用語を使わないようにしていますか。

10. 設問あるいは選択肢に「all」「never」「always」といった絶対的な用語を使わないようにしていますか。

11. 「least」「not」「except」といった用語を使わないようにしていますか。

AppendixC

ITEM CONSTRUCTION FORM

Item#
Name:
ISACA ID:

Assign one task statement and one knowledge statement (KS) from the CISM Job Practice to your item.
Task:
KS:

Testing Concept: (One sentence describing what is being tested):

Stem:

Options:
A. (Always make A the correct answer)
B.
C.
D.

Key:A

Justification:
A. (Why is A the correct answer)
B. (Why is B incorrect)
C. (Why is C incorrect)
D. (Why is D incorrect)

Reference(s): Provide references to enable independent review. Include the publication title, publication year, author and page.

ISACA Representative Review:
Accept:
Return:
Comment: