CISA® 試験問題
作成ガイド

2018 年 10 月改定

（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。

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。東京支部は、「問題応募を会員にとって身近なもの」とするため本文書の日本語訳を２０１２年に実施し、これをテキストとした「試験問題開発ワークショップ」を実施しています。今般、東京支部では5年ぶりに「CISA試験問題作成ガイド」について最新版を元に再度翻訳を行いました。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　東京支部理事（元会長）　坂本 正徳 CISA, CISM, CGEIT, CRISC, CISSP

協力　東京支部会長兼理事　田中 秀幸 CISA, CISM, CGEIT, CRISC

ISACA東京支部

2018-2019 会長兼理事　田中　秀幸

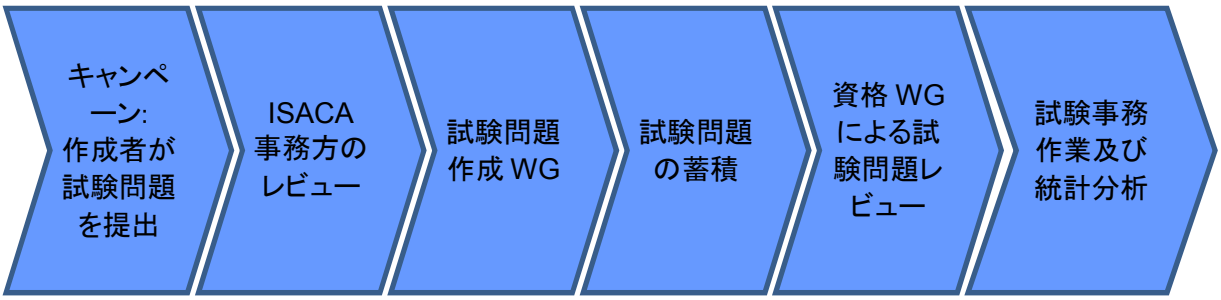
Quality Statement:
This Work is translated into Japanese from the English language version of CISA Item Development Guide-Oct. 2018 by the ISACA Tokyo Chapter with the permission of ISACA. The ISACA Tokyo Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.
品質について
本書は「CISA Item Development Guide-Oct. 2018」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。

CISA 試験問題作成ガイドの目的

CISA 試験問題作成ガイドの目的は、CISA 試験用の新しい問題を作る作成者を支援することです。本ガイドは作成者が問題作成プロセスに習熟するように、そして試験問題の品質を向上させるような新規の問題作成を支援する手段及び見識を提供します。

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、試験問題が CISA 試験に採用される機会が増えることとなるでしょう。

CISA 試験問題作成とレビュープロセス: 概要



ISACA は CISA 試験問題を貯蔵するために新しい試験問題を作成する試験問題作成キャンペーンを年複数回実施しています。キャンペーンへの参加を促す文書は、どのようにシステムを用いて新しい試験問題をレビューのために作成、提出するかの指示と共に、オンラインの試験問題作成システムから送付されます。資源及びガイドも各キャンペーンを通じて問題作成を支援できるようになります。

新しい試験問題を提出すると、ISACA の試験問題作成チームのメンバーは当該問題が ISACA の試験問題作成ガイドラインに準拠しているかをレビューします。ISACA スタッフのレビュー者は各領域の専門家ではありませんが、試験問題作成に関する専門家であり、当該試験問題が上手く受験者を試すものか、そうでないかといった観点を良く理解しています。ISACA スタッフのレビューは一般的には試験問題の内容そのものに焦点を当てるものではありませんが、文章の明確化を強化すべく選択的な用語の使い方への示唆を提供するものです。ISACA のガイドラインに合致すべく修正が必要な試験問題は、作成者にフィードバックを添えて返却されます。返却された試験問題は当該キャンペーンが終了するまでに再提出することも可能です。

ISACA スタッフが試験問題は次の段階へ進むべきものと判断した後、様々な業界および地域から成る CISA 専門家の審査会である CISA 試験問題作成評価ワーキンググループ（EIDWG）によるレビューへと進みます。ワーキンググループは、試される内容を考えた上で試験問題のレビューを実施する会合をキャンペーン終了後の数週間後に行います。ワーキンググループに承認された問題は ISACA の試験問題に直接的にプールされることとなり、作成者には作成問題毎に、報奨金が支払われ、CPE 時間が授与されます。

ワーキンググループに却下された試験問題は、会合後にグループからの詳細なフィードバックと共に、その旨が通知されます。

キャンペーン期間中に ISACA スタッフから初期段階のフィードバックが、キャンペーン期間中に随時行われますが、試験問題作成評価ワーキンググループ（EIDWG）からの最終結果は、普通はワーキンググループの会合後の週に行われます。これは、一旦キャンペーンが終了するとワーキンググループからのフィードバックには会合の日程にもよりますが、4～6週間を要する、ということになります。

新規作成者のトレーニング

新しく試験問題作成者となる者は、正規の CISA キャンペーンに参加する以前に、オンライントレーニングプログラムを終了することが義務付けられています。トレーニングプログラムに登録された試験問題作成者は、ISACA 試験問題作成チームのメンバーとして割り当てられますが、そこでは試験問題作成者が作成プロセス及び効果的な CISA 試験問題の作成に隠れた原則に馴染むよう、提出における詳細なフィードバックが提供されます。トレーニングプログラムが終了すると、試験問題作成者は正規の CISA 試験問題作成キャンペーンに参加する適格者となります。

試験問題作成の品質

ISACA および CISA 認定ワーキンググループでは、情報システム監査の専門家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、CISA 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、CISA 試験および CISA レビューマニュアルの青写真として提供されます。試験問題は、CISA の職務領域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。CISA 試験問題としてプールすべく承認される各々の新しい問題には、ガイドの巻末に含まれる領域に記されるトピックと支援タスクが作成者により割り当てられなければなりません。

CISA 試験問題を作成する際、対象者を考える必要があります。それは最低限 CISA の受験者にとって適切であるか、ということになります。試験問題は CISA 試験に合格することが期待される個人の、情報技術および業務システムの監査、統制、監視および精査に関する3－5年の経験があるという適切な経験レベルに応じて作成されなければなりません。

CISA 試験はグローバルに展開されるものであることを鑑みて、試験問題の内容及び用語は国際的な情報システム監査および統制コミュニティにとって適切かつ認められる必要があることも、考えておかなければなりません。

試験問題形式

CISA 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:
試験の設問は、完成したり解答すべく問いかける導入の文章を含むものです。設問には、試される知識に関連した状況や環境を説明する背景なども時として含みます。設問は、不完全な文章を読めるように改善すべく記述されることもありますが、通常は直接的な質問となります。

選択肢(選択可能性):
解答の選択肢は導入の文章を完結させるもの、あるいは設問へ解答する形であり、1つの正答(Key)と3つの誤答(distractors)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、効果的な誤答を作成することは、試験問題を作成する上で、最も難しい作業のひとつとなります。誤答は最も適切な解答ではないことが明確でなければいけませんが、それらしく見えて充分な知識を持っていない受験者は誤って選択してしまうような選択肢とすべきものです。

前述の通り、多数の CISA 試験問題の設問は、以下の例に見られるように、直接的な質問形式を用いています。(ガイド中の設問は実際の試験問題で使われるものではありませんので、ご注意下さい。)

設問(Stem): Which of the following concerns would **BEST** be addressed by the comparison of production application systems source code with an archive copy?

選択肢(Alternatives):

A. File maintenance errors
B. Unauthorized modifications
C. Software version currency
D. Documentation discrepancies

時として不完全な文章が試験問題では使われます。以下を参照下さい。

設問（Stem): The comparison of production application systems source code with an archive copy would **BEST** address:

選択肢（Alternatives):

A. file maintenance errors.
B. unauthorized modifications.
C. software version currency.
D. documentation discrepancies.

注）当該設問への対応は文章を完結させるように続き、解答は設問で始まる文を完成させるものです。

避けるべき試験問題のタイプ

以下の問題がある試験問題は、ISACA スタッフによる見直し段階でチェックされて作成者に返却されます。

1. 否定的な文脈の設問で問い掛ける試験問題 – これは例えば、選択肢のいずれが適切でないか、とか、選択肢のいずれが最も好ましくないか、といったものです。否定的な設問は受験者に伝統的な思考方式の逆展開を求めるもので、統計的に設問が機能しなくなります。
2. 正解/誤りを問う試験問題、あるいは選択肢のいずれが正しい記述であるかを問う試験問題。
3. 「多数−多数」形式での選択肢を伴う試験問題 – これは選択肢のいくつかの構成要素が他に含まれているものです。解答する選択肢をリスト化して用いることを許してしまうもので、要素がひとつの選択肢に含まれていなければ、その他の選択肢で繰り返すべきものです。
4. 「all of the above」「none of the above」あるいは「Both B and C」といった選択肢を含む試験問題 – 各選択肢は個々に独立するものです。（これらの流れに沿うと、「take no action」あるいは「ignore this issue」といった選択肢は、一般的に「none of the above」に余りに密接しています。そういった選択肢では貧弱な誤答を産むものであり、避けるべきものです。）
5. 穴埋め形式を用いる試験問題。
6. ベンダー固有の製品或いは地域固有の法規制の知識を試す試験問題。
7. 用語の意味を直接的に試す試験問題 – CISA 試験は経験に基づく試験であり、定義的な設問では、レビューマニュアルその他の関連文献をたまたま勉強してきたその他の経験に乏しい受験者でも答えうる可能性があります。つまり、そういった設問では、受験者に正しい解答を導くために備える専門的な経験を求められなくなります。

試験問題作成の手順

手順1　新規の試験問題のために CISA 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、一度に複数の概念を試そうとするより単一のトピックに焦点を当てるべきです。可能なトピックと支援タスクをリスト化するためには、ガイド巻末の CISA 職務領域を参照して下さい。

手順2　問題の設問と正答（正しい解答）を記述します。**試験問題をする際には、選択肢 A を常に正しい解答として作成して下さい。**

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。誤答を作成する際には、経験の乏しい IT 専門家にとって何を正しい解答と考えがちになるのかを考慮することが役立つかもしれません。あるいは同僚に経験の乏しい専門家がどのような誤りを犯すと想定されるかを相談するのも良いでしょう。

手順4　論理的根拠を記入する箇所には、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。これは、ISACA 本部のレビュー者および WG のメンバーがテストコンセプトで試したいことを理解するのに役立つものです。

手順5　作成した試験問題を支える参照したリソースを記入します。提出した試験問題には、少なくともひとつの参照項目を含まなければいけません。信頼性があればどのような参照先でも良く、最良の事例を導き、解答を支援するものです。該当する参照先については、以下のサイトをチェックして下さい。www.isaca.org/knowledge_center

手順6　試験問題作成チェックリストを用いて試験問題の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。

試験問題作成のための良い実践

1. 各試験問題は、ひとつのコンセプトのみを問うものであり選択したトピックと支援タスクの記述を反映していることを確認して下さい。一度に複数のコンセプトを問う試験問題は、不明確あるいは潜在的な混乱を誘うものとして、返却される典型的なケースです。
2. 試験問題が、3－5年の経験がある CISA の受験者に適切であることを確認して下さい。基礎的過ぎたり簡単過ぎたりすることがないように。また先進的過ぎたり難解過ぎたりすることがないようにして下さい。
3. 設問及び選択肢は簡潔で、不要な詳細や説明を含まないで下さい。受験者は試験において各問を読んで理解し、解答するためには短い時間しか与えられていないことにご留意下さい。
4. 試験問題は受験者に教育するものではないことを確認 – これは、設問或いは選択

肢の中においてコンセプトを明白に説明することを示しています。

5. 正答は、設問で付与された状況では常に正しい、或いは最も可能な解答であることを確認下さい。受験者が仮説を立てることなく正しい解答に到達するのに十分な背景を提供していなかった場合、正しい解答が組織やその環境に依存して様々でありうる場合、試験問題は時としてそのまま返却されます。
6. 試験問題が役割と責任を試すものである場合、正しい解答は組織の規模や構造、あるいは組織固有の要因などに依存しないものであることを確認ください。
7. 設問の用語は主観的な導入を行わないことを確認 - 「commonly」「frequently」或いは「rarely」といった用語は、解釈に依存するものであり、常に避けるべきものです。
8. 「all」「always」或いは「never」といった絶対的な用語を用いないことを確認 – 受験者は当該用語を伴う誤答を容易に排除できてしまいます。
9. 個人的あるいは性別の代名詞（you, your, she, he, her, his 等）は避けることを確認して下さい。「Company XYZ」のような即席の名前も同様です。
10. 重要な用語が設問と正答に記述するのであれば、少なくともひとつの誤答にも同様に記述して下さい。受験者に正しい解答へ辿りつく手掛かりを不注意に与えることがないようにするためです。
11. 選択肢が設問と適合していることを確認して下さい。例えば、もし質問が「Which of the following controls（=統制）…,」で始まるならば、全ての選択肢は統制(=controls)であるべきです。
12. 試験問題で推奨されるいかなる用語や実務は、グローバルに認められているもので、現在使用されているものであることを確認して下さい。
13. 選択肢が設問から明らかでないような新しい情報を導かないことを確認して下さい。受験者が複数の選択肢を吟味することなく正答を推測することを可能にしてしまいます。
14. 全ての選択肢は、ほぼ同様の長さで、かつ簡潔に構築されていることを確認して下さい。もし正答が「ing」で終わる動詞で始まるものであれば、誤答も同様な形式で始まるべきものです。これにより、選択肢が不要に目立つことを避けることになります。

試験問題作成チェックリスト

1. 試験問題には、「避けること」の章での試験問題の種類に例示されているような何らかの問題があるか。もしそうであれば、それらの問題は提出以前に対応しておかなければならない。
2. 試験問題は、試験問題作成ガイドの「試験問題作成」の章で良い事例として掲げられている事項を着実に実施しているか。
3. 試験問題は文法および綴りがチェックされているか。そして当該問題は一読して分かりやすいか。受験者が実際に試験を受ける際は設問と各選択肢の関係を補足説明するような解説文を参照できないことに注意せねばならない。もし試験問題文を目にしたものが、その内容と意味を理解するために問題作成者が用意した解説文を読まなければならないようであれば、さらに補足的な説明が必要と考えるべきであろう。
4. 試験問題のためのトピックと支援タスク話題は選択されているか。そして当該試験問題の試験概念はそれらに沿って作成されているか。
5. 設問及び選択肢には論理的根拠が組み込まれているか。

6．少なくとも1つの参照項目が試験問題には提供されているか。

試験問題の実例

さて、試験問題を策定する際に直面する可能性がある潜在的な問題を抱える例をいくつかを見てみましょう。

例1：

設問(Stem):
An IS auditor is reviewing an organization's disaster recovery plan. Which of the following areas should the auditor review?

選択肢(Alternatives):

A. Offsite data file storage
B. Firefighting equipment
C. Backup UPS for the computer center
D. Access to the data center by backup staff

正答(Key): A
設問には、ひとつの正しい答えを選択できる十分な情報がありません。情報システム監査人は災害復旧計画をレビューする際、これらの対象のいずれかあるいは全てを見るべき十分な理由があるでしょう。設問に「Best」あるいは「Most」といった限定詞を加えることで、このタイプの問題を解決することが時としてありますが、このケースではより多くの背景なしには監査人がレビューすべき最も重要な選択肢がいずれであるかを確実にすることを言明するのは難しいでしょう。それは組織や状況に依存するものですから。この試験問題は、記載が主観的過ぎることから返却されるべきものです。

例2：

設問(Stem): An IS auditor learns that a manager in the loan department of a financial institution changes the interest rates of several loans in the financial system. Which of the following is the auditor's **BEST** recommendation to address this situation?

選択肢(Alternatives):

A. Functional access controls should be strengthened.
B. Changes to loan information should be logged.
C. Senior management should supervise changes to loan information.
D. Change management controls should be implemented.

正答(Key): A
当該試験問題において、設問で職務の責任に関することを問うていると想定されるのが問題です。これらの変更を成すことでマネージャーが何か悪いことをしているというのは明確ではありません。いずれかの組織においては、マネージャーがこのタイプのアクセス権限を保持しているということも考えられます。役割と責任に関する実践は様々な異なる地理的な地域によっても様々です。役割と責任を試す効果的な試験問題を書く際には、いかな

る組織にも適用する最良のひとつの解答を選択できる十分な背景を、試験の実施者が持っていることを確実にするための多くの注意を払わなければいけません。

例3：

設問(Stem): An organization uses spreadsheets to calculate project cost estimates, and totals for each cost category are then keyed into the job costing system. Which of the following is the BEST control to ensure the accuracy of data entered into the job costing system?

選択肢(Alternatives):

A. Reconciliation of total amounts by project
B. Reasonableness of total amounts by project
C. Validity checks, preventing entry of character data
D. Display back of project detail after entry

正答(Key): A

当該試験問題では、情報システム監査における特定の背景が欠如しています。情報システム監査人が知る必要があるかもしれない財務的な懸念はある種存在しているかもしれませんが、CISA 主体の知識と職務領域と本試験問題の関連性は十分強いものではなく、CISA 試験に最終的に採用されるような試験問題とは程遠くなっています。時として監査の観点を強化するために試験問題を修正することも可能でしょう。当該方法を実施すべく監査人の視点から設問を再構成する、というのもひとつの良い方法となります。所与の状況においてレビューや助言すべき、最良或いは最も重要なものはなにか、といったものです。

NOTE: The new CISA Job Practice will not be in effect until June 2019. It is included in this guide to ensure new item submissions are mapped to the new content.

CISA JOB PRACTICE – EFFECTIVE JUNE 2019

Content Area 1: Information System Auditing Process	
A.	**Planning**
	1A1. IS Audit Standards, Guidelines, and Codes of Ethics
	1A2. Business Processes
	1A3. Types of Controls
	1A4. Risk-Based Audit Planning
	1A5. Types of Audits and Assessments
B.	**Execution Subtopics**
	1B1. Audit Project Management
	1B2. Sampling Methodology
	1B3. Audit Evidence Collection Techniques
	1B4. Data Analytics
	1B5. Reporting and Communication Techniques
	1B6. Quality Assurance and Improvement of Audit Process
Content Area 2: Governance and Management of IT	
A.	**IT Governance Subtopics**
	2A1. IT Governance and IT Strategy
	2A2. IT-Related Frameworks
	2A3. IT Standards, Policies, and Procedures
	2A4. Organizational Structure
	2A5. Enterprise Architecture
	2A6. Enterprise Risk Management
	2A7. Maturity Models
	2A8. Laws, Regulations, and Industry Standards affecting the Organization
B.	**IT Management**
	2B1. IT Resource Management
	2B2. IT Service Provider Acquisition and Management
	2B3. IT Performance Monitoring and Reporting
	2B4. Quality Assurance and Quality Management of IT

CISA JOB PRACTICE – EFFECTIVE JUNE 2019

Content Area 3: Information Systems Acquisition, Development, and Implementation	
A.	**Information Systems Acquisition and Development**
	3A1. Project Governance and Management
	3A2. Business Case and Feasibility Analysis
	3A3. System Development Methodologies
	3A4. Control Identification and Design
B.	**Information Systems Implementation**
	3B1. Testing Methodologies
	3B2. Configuration and Release Management
	3B3. System Migration, Infrastructure Deployment, and Data Conversion
	3B4. Post-Implementation Review
Content Area 4: Information Systems Operations and Business Resilience	
A.	**Information Systems Operations**
	4A1. Common Technology Components
	4A2. IT Asset Management
	4A3. Job Scheduling and Production Process Automation
	4A4. System Interfaces
	4A5. End-User Computing
	4A6. Data Governance
	4A7. Systems Performance Management
	4A8. Problem and Incident Management
	4A9. Change, Configuration, Release, and Patch Management
	4A10. IT Service Level Management
	4A11. Database Management
B.	**Business Resilience**
	4B1. Business Impact Analysis (BIA)
	4B2. System Resiliency
	4B3. Data Backup, Storage, and Restoration
	4B4. Business Continuity Plan (BCP)
	4B5. Disaster Recovery Plans (DRP)

CISA JOB PRACTICE – EFFECTIVE JUNE 2019

Content Area 5: Protection of Information Assets	
A.	**Information Asset Security and Control**
5A1.	Information Asset Security Frameworks, Standards, and Guidelines
5A2.	Privacy Principles
5A3.	Physical Access and Environmental Controls
5A4.	Identity and Access Management
5A5.	Network and End-Point Security
5A6.	Data Classification
5A7.	Data Encryption and Encryption-Related Techniques
5A8.	Public Key Infrastructure (PKI)
5A9.	Web-Based Communication Technologies
5A10.	Virtualized Environments
5A11.	Mobile, Wireless, and Internet-of-Things (IoT) Devices
B.	**Security Event Management**
5B1.	Security Awareness Training and Programs
5B2.	Information System Attack Methods and Techniques
5B3.	Security Testing Tools and Techniques
5B4.	Security Monitoring Tools and Techniques
5B5.	Incident Response Management
5B6.	Evidence Collection and Forensics

Supporting Tasks

1. Plan audit to determine whether information systems are protected, controlled, and provide value to the organization.
2. Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy.
3. Communicate audit progress, findings, results, and recommendations to stakeholders.
4. Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
5. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
6. Evaluate the effectiveness of IT governance structure and IT organizational structure.
7. Evaluate the organization's management of IT policies and practices.
8. Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements.
9. Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives.
10. Evaluate the organization's risk management policies and practices.
11. Evaluate IT management and monitoring of controls.
12. Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
13. Evaluate the organization's ability to continue business operations.
14. Evaluate whether the business case for proposed changes to information systems meet business objectives.
15. Evaluate whether IT supplier selection and contract management processes align with business requirements.
16. Evaluate the organization's project management policies and practices.
17. Evaluate controls at all stages of the information systems development lifecycle.
18. Evaluate the readiness of information systems for implementation and migration into production.
19. Conduct post-implementation review of systems to determine whether project deliverables, controls, and requirements are met.
20. Evaluate whether IT service management practices align with business requirements.
21. Conduct periodic review of information systems and enterprise architecture.
22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives.
23. Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives.
24. Evaluate database management practices.
25. Evaluate data governance policies and practices.
26. Evaluate problem and incident management policies and practices.

27. Evaluate change, configuration, release, and patch management policies and practices.
28. Evaluate end-user computing to determine whether the processes are effectively controlled.
29. Evaluate the organization's information security and privacy policies and practices.
30. Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.
31. Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
32. Evaluate data classification practices for alignment with the organization's policies and applicable external requirements.
33. Evaluate policies and practices related to asset lifecycle management.
34. Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.
35. Perform technical security testing to identify potential threats and vulnerabilities.
36. Utilize data analytics tools to streamline audit processes.
37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.
38. Identify opportunities for process improvement in the organization's IT policies and practices.
39. Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.