



# CERTIFIED INFORMATION SYSTEMS AUDITOR®

2012 CISA® 考生應試與認證指南

## 2012 年 CISA 考試 — 重要日期資訊

### 考試日期 — 2012 年 6 月 9 日

早期報名截止日期：	2012 年 2 月 8 日
最終報名截止日期：	2012 年 4 月 4 日
考試報名變更：	在 4 月 14 日至 20 日間收到的變更將收取美金 \$50 的費用，2012 年 4 月 20 日後即不接受變更。

退費：退費截止日期為 2012 年 4 月 13 日，將收取美金 \$100 的處理費，此日期之後即不接受退費。

延期：在 2012 年 4 月 20 日前收到的變更將收取美金 \$50 的處理費。在 2012 年 4 月 21 日到 5 月 24 日間收到的延期，將收取美金 \$100 的處理費。2012 年 5 月 24 日之後，即不允許延期。

### 考試日期 — 2012 年 12 月 8 日

早期報名截止日期：	2012 年 8 月 15 日
最終報名截止日期：	2012 年 10 月 3 日
考試報名變更：	在 10 月 6 日至 12 日間收到的變更將收取美金 \$50 的費用，2012 年 10 月 12 日後即不接受變更。

退費：退費截止日期為 2012 年 10 月 5 日，將收取美金 \$100 的處理費，此日期之後即不接受退費。

延期：在 2012 年 10 月 12 日前收到的變更將收取美金 \$50 的處理費。在 2012 年 10 月 13 日至 11 月 21 日間收到的變更，將收取美金 \$100 的處理費。2012 年 11 月 21 日之後，即不允許延期。

所有日期的截止時間都是美國伊利諾州芝加哥時間下午 5 點 (中部時間)

2012 CISA® 考生應試與認證指南  
在美國印製

## 目錄

概述.....	3
CISA 計劃獲得 ISO/IEC 17024:2003 標準的資格認定展期 ...	3
CISA 考試.....	3
準備 CISA 考試.....	3
舉辦 CISA 考試.....	4
CISA 考試的計分.....	6
CISA 考試的試題類型.....	6
申請 CISA 認證.....	6
初始國際電腦稽核師 (CISA) 認證的要求.....	6
維持國際電腦稽核師 (CISA) 認證的要求.....	7
國際電腦稽核協會職業道德準則.....	7
CISA 認證的撤消.....	7
CISA 任務和知識面描述.....	8

### ISACA®

國際電腦稽核協會 (ISACA®, 網址：[www.isaca.org](http://www.isaca.org)) 是資訊系統 (IS) 與安全、企業資訊技術治理與管理及資訊技術相關風險與知識、認證、社群、倡導與教育訓練，會員遍佈 160 個國家，總數 95,000 人。ISACA 是 1969 年成立的非營利獨立機構，ISACA 公開舉辦國際會議外，還發行《國際電腦稽核期刊》(ISACA® Journal)、制定國際資訊系統的稽核與監控標準，以協助會員確保對資訊系統的信賴，並從中獲得珍貴的價值。此外，ISACA 透過廣為放心推崇的國際電腦稽核師 [Certified Information Systems Auditor® (CISA®)] 業界國際認證服務，包括，國際資訊安全經理人 [Certified Information Security Manager® (CISM®)] 證照、國際企業資訊治理師 [Certified in the Governance of Enterprise IT® (CGEIT®)] 證照及國際資訊風險控制師 [Certified in Risk and Information Systems Control™ (CRISC™)] 證照，推動與證明其資訊技術技能與知識的實力。ISACA 同時也持續更新 COBIT®, 以協助資訊技術專業人員和企業領導人履行所轄資訊技術治理與管理責任，尤其專長於(認證、安全、風險和控管領域，以及提升業務價值等方面。

### 免責聲明

ISACA 和 CISA 認證委員會已編寫 2012 CISA® 考生應試與認證指南以作為想取得 CISA 資格證書者的指南。電腦稽核協會對本指南或有關協會出版品的使用不作任何保證，也不擔保考生能通過 CISA 考試。

### 保留權限

Copyright © 2011 ISACA。未獲得 ISACA 的書面許可之前，不得以任何形式複製或儲存本文件的任何部分以作為任何用途。本文件不另行授予其他權限或許可權。保留所有權利。

### ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
電話：+1.847.253.1545  
傳真：+1.847.253.1443  
電子信箱：[exam@isaca.org](mailto:exam@isaca.org)  
網站：[www.isaca.org](http://www.isaca.org)

## 概述

職業認證計劃的優異之處，在於賦予持證人的價值與認可。自 1978 年以來，由 ISACA 所舉辦的國際電腦稽核 (CISA) 計劃，已經成為電腦稽核、控管與安全等專業領域中全球公認的資格標準。

CISA 所推廣與評價的技術技能與實務，是在這個領域成功的基石。獲得 CISA 資格代表持證人對技能的精通程度，並且這也是其專業的測量基礎。由於對具備電腦稽核、控管和安全技能的專業人員的需求與日俱增，CISA 已成為全球個人與機構的首選認證計劃。CISA 資格證書代表持證人能夠在機構服務當中表現其卓越的敬業精神，以及優秀的專業才幹。

## CISA 計劃獲得 ISO/IEC 17024:2003 標準的資格認定展期

美國國家標準協會 (ANSI) 已經按照 ISO/IEC 17024:2003 標準對 CISA 認證計劃進行了資格鑒定和認可，上述標準是針對人員認證系統營運實體的總體要求。ANSI 是一個私營的非營利機構，它對其他機構進行鑒定認可，並擔當產品、系統和人員的第三方認證機構。

ISO/IEC 17024 標準規定了那些按照具體要求對個人進行認證的機構所要遵守的要求。ANSI 將 ISO/IEC 17024 描述為「預期在促進認證團體的全球標準化、增加跨國的人才流動、增加公共安全和保護消費者方面，將扮演卓越的角色。」

ANSI 鑒定認可的作用：

- 促進對 ISACA 認證所提供之特有資格和專業特長的宣傳
- 保護認證的信譽並提供法律辯護的證據
- 增進消費者和公眾對本認證和持證者的信心
- 便利跨國、跨行業的人才流動

得到 ANSI 的公認象徵著 ISACA 的認證程序滿足 ANSI 在公開程度、平衡、一致和正當程序方面的關鍵要求。有了這一認可，ISACA 預計 CISA 的持證人將面臨卓爾不凡的機遇，使他們得以繼續在全世界範圍內展示自己的實力。



ANSI Accredited Program  
PERSONNEL CERTIFICATION  
#0694  
ISO/IEC 17024

## CISA 考試

### CISA 考試的發展/描述

CISA 認證委員會負責監督考試的開發，並確保其內容的適切性。CISA 考試試題的開發，是透過能加強最高考試品質的全面性程序來完成。此程序包括與考題作者協力合作的試題提升子委員會 (Test Enhancement Subcommittee, TES) 開發及審查題目，然後再提交給 CISA 認證委員會進行審查。

工作實務是通過考試及獲得 CISA 資格證書之所需經驗的基礎。此工作實務定期更新，並且包含五個內容領域 (範圍)。該範圍及相應任務與知識面的描述，是多方面的研究結果與世界各地的課題事務專家所提供的意見。

任務及知識面描述說明的是 CISA 所從事的任務，以及執行這些任務所需的知識。考生將接受與執行這些任務相關之實際知識的測試。

更新的工作實務分析範圍及百分比分配如下：

- 電腦稽核程序 (14%)
- 資訊治理與管理 (14%)
- 資訊系統的取得、開發與建置 (19%)
- 資訊系統的營運、維護及支持 (23%)
- 資訊資產的保護 (30%)

註：列出範圍的百分率表明考試中每個範圍出現題目所占的比重和百分率。有關每個範圍的任務和知識面描述，請參考第 8-11 頁。

該考試有 200 多道選題，每年舉辦兩次，分別於六月及十二月舉行，考試時間為四個小時。考生可以選擇其中一種語言來應試。如需最新的語言清單，請造訪網站 [www.isaca.org/cisaterminology](http://www.isaca.org/cisaterminology)。

## 準備 CISA 考試

完整而系統的學習計劃可以幫助你通過 CISA 考試。為幫助考生制定成功的學習計劃，ISACA 為考生提供了一些學習輔導資料與複習課程。請造訪網站 [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide) 以查看能幫助您準備考試的 ISACA 學習輔導資料。請提早訂購，因根據地理位置和通關規定的不同，貨運時間可能為一至四個星期。若想查詢貨物目前的資訊，請造訪 [www.isaca.org/shipping](http://www.isaca.org/shipping)。

# CISA® 考生應試與認證指南



ISACA 也提供 CISA® 線上複習課程。該課程包括雙方互動的練習、個案研究、復習工具和實務性問題。請造訪網站 [www.isaca.org/elearning](http://www.isaca.org/elearning) 來查詢進一步資訊並預覽課程。

您可以在 2012 年 CISA 複習手冊中取得學習參考資料的完整清單。

您可以在網站 [www.isaca.org/cisaguide](http://www.isaca.org/cisaguide) 上找到進階學習的建議參考資料清單，以協助您準備考試。

為協助考生了解專有名詞，ISACA 的網站 ([www.isaca.org/cisaguide](http://www.isaca.org/cisaguide)) 上提供常用術語表，有英文與其他語言的對照翻譯。

ISACA 會維護術語詞彙以及各種認證的專用詞彙。這些詞彙可以在網站 [www.isaca.org/glossary](http://www.isaca.org/glossary) 上找到。

電腦稽核協會或 CISA 認證委員會對有關協會的出版物或課程不作任何保證，也不擔保考生通過考試。

## 舉辦 CISA 考試

ISACA 使用國際認可的專業考試機構來協助 CISA 考試的建構、舉辦和計分。

希望提出有關測試舉辦之任何意見的考生，請在測試最後填寫「測試舉辦問卷」，提報意見。「測試舉辦問卷」會印在考試小冊背面，而您應該要在答卷正面特別代碼區段的 P 到 S 方塊 (方格編號 4) 中填入問卷答案。

考生如對考試舉辦 (包括考場環境或考試內容) 有任何意見或疑慮，請以書信或電子郵件 ([exam@isaca.org](mailto:exam@isaca.org)) 聯絡 ISACA 國際總部。這些意見或疑慮應在考試日之後 2 週內送抵 ISACA。請於意見中包含下列資訊：考試 ID 編號、考場、考試日期，以及特定問題的相關細節。考試的最後計分程序只會將考試舉辦後 2 週內送抵 ISACA 的意見納入考量。

### 准考證

在 CISA 試前 2 到 3 週，考生會收到來自 ISACA 的准考證以及電子准考證。考生亦可到 [www.isaca.org](http://www.isaca.org) 網站，然後從網站的 MyISACA 頁面下載准考證。准考證上標明了考試的日期、入場登記時間與考試地點、當天日程安排以及參加 CISA 考試必須攜帶的材料。除非是關於聯絡資訊的變更，否則考生不得在准考證上書寫任何文字。

請注意：您必須支付所有費用之後才會收到准考證。准考證會同時以書面及電子郵件寄送至報考資料中最新的郵寄地址與電子郵件地址。只有具備准考證與政府簽發之護照的考生得以參加考試，並且准考證上的名字必須與護照上的名字相符。書面准考證或列印出的電子准考證均可用於參加考試。如果考生的郵寄地址和/或電子郵件地址有所變更，請至 ISACA 網站 ([www.isaca.org](http://www.isaca.org)) 更新考生資料或聯絡 [exam@isaca.org](mailto:exam@isaca.org)。

考生必須注意准考證上的確切登記入場時間與考試時間。在考試開始前約 30 分鐘，主考人開始宣讀說明，此時，任何考生均不得進入考場。任何在主考人宣讀說明開始之後到達的考生都不能進入考場，並且不予退還報名費。考生只能在准考證上指定的考場使用此准考證。考試舉辦期間會查驗身份證。

### 特別安排

接到申請後，ISACA 將根據出具的殘疾或宗教證明，在考試程序方面為應試者作出合理安排。應試人可以要求適當地改變考試形式、表述方式、考場內提供的飲食或調整考試時間，以顧及應試人由於殘疾或宗教要求而影響到考試狀態的因素。在考場內進食的要求必須有醫生的證明材料，否則不允許將食品和飲料帶入考場。應試人必須向 ISACA 國際總部提出書面申請和相應的證明文件，如果是參加 2012 年 6 月的考試，必須在 2012 年 4 月 4 日前提出申請，如果是參加 2012 年 12 月的考試，則必須在 2012 年 10 月 3 日前提出申請。

### 準時入場

每個考場將於准考證上所註明的時間開始開放入場。所有考生必須於主考人開始宣讀說明前進入考場教室。在考試開始前約 30 分鐘，主考人開始宣讀說明，此時，任何考生均不得進入考場。

### 記得攜帶准考證

考生只能在准考證 (無論是電子准考證或實體准考證) 上指定的考場使用此准考證。考生只有攜帶有效的准考證以及通用的身份證明才能進入考場。可接受的身份證形式必須是當前有效並由政府簽發的身份證原件，其中包含與准考證姓名相符的考生姓名，同時還應帶有考生相片。身份證上的資料不可以是手寫的。考生所提供的一件身份證必須顯示以上所有重要特徵。相關示例包括但不限於護照、駕駛執照、軍人身份證、州身份證、綠卡和國家身份證等。任何無法提供身份證明原件的考生都不會獲准進入考場，並且其報名費不予退還。

### 詳讀考場規則

# CISA® 考生應試與認證指南

- 開始宣讀說明之後，任何考生均不得進入考場。
- 考生應攜帶數支削尖的 2 號或 HB (軟芯) 鉛筆及好用的橡皮擦。考場不提供鉛筆及橡皮擦。由於考場眾多，我們會盡一切努力確保每個考場都能維持舒適的溫度。建議考生穿著舒適自在的衣服。
- 考生不得攜帶參考資料、白紙、便條本或字典進入考場。
- 考生不得攜帶計算機進入考場，也不可在考場內使用計算機。
- 考生不得攜帶任何類型的通訊裝置 (比如手機、PDA、黑莓手機) 進入考場。如果在考試舉辦期間發現考生攜帶任何此類物品，將取消其考試資格並要求其立刻離開考場。
- 訪客不得進入考場。
- 考生不得攜帶食物或飲料進入考場 (在未獲得 ISACA 事先許可的情況下)。

## 作弊行為

若發現考生有任何作弊行為，例如提供或接受幫助、使用字條、紙張或其他輔助工具、試圖替他人考試、在考試舉辦期間使用任何類型的通訊裝置 (包括手機)、或撕下考試卷、答案卷或附卷帶出考場教室，將取消考生考試資格並可能對其採取法律行動。考生在未經過監考人員許可或陪同的情況下離開考場，將無法返回考場教室並會取消其考試資格。考試機構將對 ISACA 的 CISA 認證委員會呈報這類違規行為。

請至網站 [www.isaca.org/cisabelongings](http://www.isaca.org/cisabelongings) 查詢完整的個人攜帶物品政策。ISACA 或其考試機構皆不對考生的個人所屬物品負任何保管責任。

## 填寫答卷時請小心

- 在考生開始考試前，考場的主考人將大聲宣讀有關在答卷上填寫身份資料的說明。考生必須正確填寫准考證上所表示的准考證號碼與其他所有必填資訊，以避免延遲計分或通知錯誤。
- 監考人會以各考場所用的主要語言來談話。如果考生想以不同於考場主要語言的其他語言來參加考試，監考人可能會不熟悉考生所選擇的語言。但是考生可以取得與考試語言相同的書面說明。
- 現場會先指導考生詳細閱讀並瞭解所有說明，然後再嘗試答題。略過指導或草率閱讀說明的考生，可能會遺漏重要資訊並喪失資格。
- 所有答案都要標示在答卷的正確圓圈內。考生必須小心作答，每道試題不可以標示一個以上的答案，並確認在正確的答案列回答試題。如果需要變更答案，請考生將錯誤的答案擦拭乾淨之後再標示新的答案。
- 所有試題都必須作答。答錯不扣分。評分只根據答案正確的試題數目來計分，因此請不要留下任何試題不作答。
- 考完之後，考生必須交出答卷和考試卷。

## 計算考試時間

- 整場考試的時間為四小時，每道試題僅允許花費一分多鐘。建議考生調整自己的答題速度以完成整場考試。考生平均每小時必須完成 50 道試題。
- 建議考生將答案立即記錄在答卷上。如果考生將答案標示在考試卷上，考試時間結束之後，將不會給予考生額外的時間謄寫或記錄答案。

## 適當管理自己的行為

- 為保護考試的安全並維護分數的有效性，我們要求考生在答卷上簽名。
- 考場中如發現考生有作弊行為或違反考試規則，比如提供或接受幫助、使用字條、紙張或其他輔助工具、試圖替他人考試或撕下考試卷、答卷或附卷帶出考場時，CISA 認證委員會有權取消任何考生考試的資格。考試機構將提供 CISA 認證委員會有關這類違規行為的記錄，以供他們進行審查並做出裁決。

## 驅離考場或取消考試資格的原因

- 沒有資格進入考場。
- 考生造成騷動或提供或接受幫助。
- 考生替他人考試。
- 考生試圖撕下考試卷、答卷或附卷帶出考場。
- 考生將不允許的東西帶入考場。
- 考生在考試舉辦期間攜帶任何通訊裝置 (比如手機、PDA、BlackBerry®)。
- 考生未經許可離開考場。

如果在考試舉辦期間發生考生攜帶任何通訊裝置 (比如手機、PDA、BlackBerry®)，將取消其考試資格，並要求其立刻離開考場。

## CISA 考試的計分

CISA 考試包含 200 道多選題。考生的成績按照比率分數來報告。比率分數是把考試的原始分數轉換為通用比例後所得的分數。ISACA 按照從 200 至 800 的通用比例來使用和報告分數。例如，比率分數 800 為滿分，表示答對所有試題；比率分數 200 為可能的最低分，表示只答對少數幾題。考生要達到 450 分或更高分才算通過考試。450 分代表由 CISA 認證委員會所制定的最低的統一知識標準。如果其他要求全部都達到，則考試分數及格的考生可以隨後提出認證申請。

CISA 考試中包含一些僅為研究和分析目的而被加入的考題。這些考題沒有被分別指明出來，並且不會用於計算最後的分數。

自考試之日起約八個星期後，考生將接到郵寄的正式考試成績通知。此外，如果考生在辦理報名時同意，我們會將含有考生及格/不及格狀態及分數的電子郵件寄給考生。這份電子郵件只在最初發佈考試成績時向考生資料中所列的電子郵件地址發送。為了對考試分數保密，考試成績將不採用電話或傳真的方式進行通知。為了防止電子郵件通知被發送到垃圾郵件的文件夾，請考生把 [exam@isaca.org](mailto:exam@isaca.org) 加入地址簿、白名單 (Whitelist) 或安全發件人名單。

考生將會收到含有各範圍領域子分數的成績單。成功通過考試的考生將隨成績單一起收到如何申請 CISA 認證的詳細資訊。未通過考試的考生將隨成績單一起收到一份新的 CISA 資訊公告。

未成功通過考試的考生可藉由子分數找出日後應該加強的領域，以再次參加考試。未成功通過考試的考生應該注意到，不能用計算單純的子分數或加權的平均分數來決定總比率分數。

收到不及格考試分數的考生可以請求對其答卷人工計分。此程序能確保沒有雜亂記號、多重反應或其他會干擾電腦計分的情況。但考生應該要瞭解，所有分數都經過數道品質控管檢查才會報告；因此，重新計分可能不會造成分數的改變。人工計分的請求必須在發佈考試成績之後 90 天之內，以書面向認證部提出。在截止日之後才提出的人工計分請求將不受理。所有請求都必須有考生的姓名、准考證號碼和郵遞地址。每項申請需繳納 \$75 美元費用。

## CISA 考試的試題類型

CISA 考試試題的發展，是以評估和測試對一般概念和標準的實際知識與應用為目的。所有試題都設計一個最佳解答。

每道 CISA 試題都有主幹 (試題) 和四個選項 (答案選擇)。考生被要求從選項中選擇正確或最佳解答。主幹可能是問題或不完整描述的形式。在某些情況下，可能還會加入情節。這些試題一般都會包含情況的描述，並要求考生根據所提供的資訊回答二至三道試題。考生要小心仔細閱讀每道試題。CISA 考試的試題可能會要求考生根據合格選項來選擇適當的答案，例如最有可能或最佳。無論哪一種情況，考生都必須仔細閱讀試題，刪除已知的錯誤答案，然後選出可能的最佳選項。考生可以在網站 [www.isaca.org/cisaassessment](http://www.isaca.org/cisaassessment) 上找到 CISA 考試試題的簡報。

## 申請 CISA 認證

通過考試不代表考生就是 CISA。一旦考生通過 CISA 考試，自考試日起，他/她有五年的時間可以申請認證。成功通過考試的考生必須完成認證申請，並且必須使用申請所附的適當表格來驗證工作經驗。在收到完整的申請及核准之前，考生未獲認證，並且不可以使用 CISA 資格。請注意，申請的裁定並非最終判決，還需經過認證申請拒絕的上訴程序才會定案。如果您有任何關於認證遭拒的問題，請將問題寄到 [certification@isaca.org](mailto:certification@isaca.org)。獲得認證後，新的 CISA 將會收到認證和 CISA 認證 PIN 碼。在申請時，個人也必須瞭解 ISACA 得保留權利，但沒有義務發佈或揭露其 CISA 狀態。申請 CISA 認證時，我們會向您酌收美金 \$50 的處理費。

## 初始國際電腦稽核師 (CISA) 認證的要求

認證最初是授予給成功完成 CISA 考試，並且符合下列工作經驗要求的個人。

認證要求至少要有五年的專業電腦稽核、控管、確認或安全工作的經驗。具有下列同等經驗者，可按規定申請抵減：

- 一年以下電腦經驗或一年非電腦稽核經驗可抵一年的經驗。
- 完成 60-120 大學學分 (相當於兩年或四年大學學位)，不受 10 年先前經驗的限制，可以相應抵減一年或兩年的經驗。即使獲得多個學位，最多只能抵減兩年。
- 在開設 ISACA 主辦模型課程 (Model Curriculum) 的大學中獲得學士或碩士學位可抵一年的經驗。若要查看這些學校的名單，請造訪 [www.isaca.org/modeluniversities](http://www.isaca.org/modeluniversities)。如果已經使用三年經驗抵減和教育豁免的規定，則不能使用本項規定。
- 獲得認可大學資訊安全或資訊技術碩士學位可抵一年的經驗。

例外：兩年相關領域( 計算機科學、會計、電腦稽核等) 內從事大學全職講師工作的經驗，可抵一年的經驗。

經驗必須在 CISA 認證申請日之前的十年內，或最初通過考試之日起的五年內獲得。如果在通過考試日的五年之內沒有提出 CISA 認證的完

整申請，則必須再次參加並通過考試。

請特別注意，許多人選擇在符合工作經驗的要求之前就參加 CISA 考試。我們接受並鼓勵這樣做，但在符合所有要求之前，將不會授予 CISA 資格。

## 維持國際電腦稽核師 (CISA) 認證的要求

CISA 必須符合下列要求才能維持資格證書：

- 每年至少要獲得並報告 20 個持續專業進修 (CPE) 時數，並在三年的報告期中，獲得並報告至少 120 個持續專業進修 (CPE) 時數。如需更多詳細資訊，請造訪網站 [www.isaca.org/cisacpepolicy](http://www.isaca.org/cisacpepolicy) 查看 CISA CPE 政策。
- 每年全額繳納持續專業進修 (CPE) 維持費給 ISACA 國際總部。
- 如果被選為年度稽核，需回應及提交所需的持續專業進修 (CPE) 活動的文件以支持所報告的時數。
- 遵守 ISACA 職業道德準則。

若未遵守這些一般要求，將導致個人的 CISA 資格被撤消。所有認證的所有權均屬於 ISACA。如果個人獲得核發認證後又遭到撤銷，則必須銷毀認證。

## 國際電腦稽核協會職業道德準則

ISACA 實施一「職業道德準則 (Code of Professional Ethics)」以作為協會會員和/或其認證持有人之專業人員和個人的行為準則。未遵守本職業道德準則將導致協會會員和/或認證持有人的行為遭到調查，並且最後可能會受到懲戒處分。您可至下列網站檢視 ISACA 職業道德準則：[www.isaca.org/ethics](http://www.isaca.org/ethics)。

## CISA 認證的撤消

CISA 認證委員會在經過正當及徹底的考慮之後，可根據下列任何原因撤消個人的 CISA 認證：

- 未遵守 CISA 持續專業進修 (CPE) 政策
- 違反 ISACA 職業道德準則的任何條款
- 偽造或故意不提供相關資訊
- 故意對重要事實作出不實陳述
- 任何時候從事或協助他人進行與 CISA 考試或認證過程有關的不誠實、未授權或不適當的行為

## CISA 工作實務領域說明 CISA 任務和知識面描述

<b>內容範疇 (領域)</b>	
<b>範圍 1：電腦稽核程序</b> —按照電腦稽核標準，提供稽核服務，以協助組織保護和控制資訊系統。	
<b>範圍 1：任務描述</b>	
T1.1	開發和建置符合以風險為基礎之電腦稽核策略以遵循電腦稽核標準，確保涵蓋關鍵領域。
T1.2	進行具體稽核計劃以確定資訊系統受到保護、控制與提供組織價值。
T1.3	按照資訊技術稽核標準進行稽核工作，以達成稽核計劃的目標。
T1.4	向利益關係人報告稽核發現項目並提供建議，並在必要時針對結果及影響進行溝通。
T1.5	處理後續追蹤或準備狀態報告，以確保管理階層即時採取適當行動。
<b>範圍 1：知識面描述</b>	
KS1.1	關於 ISACA 電腦稽核與保證標準、指引、工具和技術、職業道德標準及其他適用標準的知識
KS1.2	關於對稽核環境之風險評估概念、工具與技術的知識
KS1.3	與控制目標與資訊系統相關控制的知識
KS1.4	關於稽核計劃與稽核專案管理技術 (包括後續追蹤) 的知識
KS1.5	關於包括相關資訊技術在內之基本業務流程 (例如：採購、薪資、應付帳款、應收帳款) 的知識
KS1.6	關於受影響範圍、證據收集與保全以及稽核頻率之適用政策法規的知識
KS1.7	用以搜集、保護與保全稽核證據之證據收集技術 (例如：觀察、調查、檢查、訪談、數據分析) 的知識
KS1.8	關於不同抽樣方法的知識
KS1.9	關於報告和溝通技巧 (例如：促進、談判、解決衝突、稽核報告結構) 的知識
KS1.10	關於稽核品質保證系統與架構的知識
<b>範圍 2：資訊治理與管理</b> —提供必要的領導力、組織結構和流程使能達到組織目標與支持其策略。	
<b>範圍 1：任務描述</b>	
T2.1	評估資訊治理結構的有效性，以判斷資訊技術決策、方向和績效是否支持組織的策略與目標。
T2.2	評估資訊組織結構與人力資源 (人員) 管理，以判斷其是否支持組織的策略與目標。
T2.3	評估資訊策略，包括資訊方向以及策略之發展、核准、建置和維護，以配合組織的策略與目標。
T2.4	針對發展、核准、建置、維護和監控等方面來評估機構的資訊政策、標準、程序和流程，以判斷其是否支持資訊策略並符合法規與法律要求。
T2.5	評估品質管理系統是否合乎需要，以判斷其是否以具成本效益的方式支持機構的策略與目標。
T2.6	評估資訊管理與監控的控制項 (例如：持續監控、品質保證 [QA])，以符合組織的政策、標準與程序。
T2.7	評估資訊資源投入、使用和配置實務 (包括優先順序的標準)，以配合組織的策略與目標。
T2.8	評估資訊外包策略和政策以及合約管理措施，以判斷其是否支持組織的策略與目標。
T2.9	評估風險管理措施，以判斷機構的資訊相關風險是否獲得適當的管理。
T2.10	評估監控和認證實務，以判斷委員會和執行管理階層是否收到充分並即時的資訊技術效能的相關資訊。
T2.11	評估機構的營運持續計劃，以判斷組織在資訊服務中斷期間持續重要業務作業的能力。

內容領域 (範圍)	
<b>範圍 2：知識面描述</b>	
KS2.1	關於資訊治理、管理、安全與控制框架以及相關標準、指引及實務的知識
KS2.2	關於組織的資訊技術策略目的、政策、標準和程序以及各項基本元素的知識
KS2.3	關於資訊相關的組織結構、角色與職責的知識
KS2.4	關於資訊策略、政策、標準與程序之發展、建置與維護的知識
KS2.5	關於組織的技術方向與資訊架構，及其設定長期戰略方向之內涵的知識
KS2.6	關於影響組織之相關法律、法規與業界標準的知識
KS2.7	關於品質管理系統的知識
KS2.8	關於成熟度模型運用的知識
KS2.9	關於程序最佳化技術的知識
KS2.10	關於資訊資源投資與包括優先順序標準在內之配置作法 (例如：組合管理、價值管理、專案管理) 的知識
KS2.11	關於選擇資訊技術供應商、合約管理、關係管理與績效監控流程 (包括第三方外包關係) 的知識
KS2.12	關於企業風險管理的知識
KS2.13	關於監控和報告資訊績效之作法 (例如：平衡計分卡和關鍵績效指標 [KPI]) 的知識
KS2.14	關於用於施行營運持續計劃之資訊技術人力資源 (人員) 管理措施的知識
KS2.15	關於營運衝擊分析 (BIA) 與營運持續計劃 (BCP) 相關性的知識
KS2.16	關於營運持續計劃 (BCP) 與測試方法發展與維護之標準與程序的知識
<b>3. 範圍 3：資訊系統取得、發展與建置—提供認證服務，確保資訊系統的取得、發展、測試與建置實務符合組織的策略與目標。</b>	
<b>範圍 3：任務描述</b>	
T3.1	評估對資訊系統取得、發展、維護與後續汰換之投資提議的業務需求，以判斷其是否符合企業目標。
T3.2	評估專案管理做法與控制是否符合企業成本效益需求的考量並管理組織的風險。
T3.3	進行技術審查，以判斷專案的處理是否符合專案計劃、是否有充分的文件支援，以及狀態報告是否正確無誤。
T3.4	評估資訊系統在需求、取得、發展與測試階段期間的控管，以符合組織的政策、標準、程序與適用的外部要求。
T3.5	評估資訊系統對實施及移轉到正式環境的準備程度，以判斷是否符合專案可交付成果、控制及組織的需求。
T3.6	對系統進行建置後的審查，以判斷是否符合專案可交付成果、控管及組織的需求。
<b>範圍 3：知識面描述</b>	
KS3.1	關於效益實現實務(例如：可行性研究、企業案例、總擁有成本[TCO]、投資回報率(ROI)) 的知識
KS3.2	關於專案治理機制 (例如：指導委員會、專案督導委員會、專案管理辦公室) 的知識
KS3.3	關於專案管理架構、實踐與工具的知識
KS3.4	關於專案所應用之風險管理措施的知識
KS3.5	關於資料、應用程式和技術相關之資訊技術結構 (例如：分散式應用系統、以網頁為基礎的應用程式、網路服務和多層式架構應用系統) 的知識
KS3.6	關於採購實務 (例如：廠商評估、廠商管理、託管) 的知識
KS3.7	關於需求分析和控制措施 (例如：需求確認、追溯、差異分析、弱點管理、安全需求) 的知識
KS3.8	關於專案成功標準與風險的知識
KS3.9	關於確保交易及資料完整性、正確性、有效性與授權之控制目標與技術的知識

內容領域 (範圍)	
<i>範圍 3：知識面描述 (續)</i>	
KS3.10	關於系統開發方法和工具及其優缺點 (例如：敏捷開發法、雛型法、快速應用開發 [RAD]、物件導向設計技術) 的知識
KS3.11	關於資訊系統開發相關測試方法與實踐的知識
KS3.12	關於資訊系統開發相關組態設定與發佈管理的知識
KS3.13	關於系統移轉與基礎設施佈署的做法及資料轉換工具、技術與程序的知識
KS3.14	關於建置後的目標審查與做法 (例如：專案結案、控制實施、效益實現和績效評估) 的知識
範圍 4：資訊系統的營運、維護及支持—確保資訊系統營運、維護與支援流程符合組織的策略與目標。	
<i>範圍 4：任務描述</i>	
T4.1	定期審查資訊系統，以判斷其是否持續符合組織目標。
T4.2	評估服務水準管理措施，以判斷內部與外部服務提供者的服務水準是否有完整規範和管理。
T4.3	評估第三方管理措施，以判斷提供者是否符合組織預期的控制水準。
T4.4	評估系統與使用者程序，以判斷排程與非排程的流程是否持續受到管理直到完成。
T4.5	評估資訊系統維護流程，以判斷其是否受到有效控管且持續支持組織目標。
T4.6	評估資料管理措施，以判斷資料庫的完整性與最佳化。
T4.7	評估容量與效能監控工具及技術的使用，以判斷資訊技術服務是否符合組織的目標。
T4.8	評估問題和事件管理措施，以判斷事件、問題或錯誤是否即時得到記錄、分析與解決。
T4.9	評估變更、組態設定與發佈管理措施，以判斷對組織正式環境進行的排程與非排程變更是否有妥善的控制與記錄。
T4.10	評估備份和復原規定是否合乎需要，以判斷恢復流程所需之資訊的可獲得性。
T4.11	評估組織的災難復原計劃，以判斷在發生災難事件時是否有恢復處理資訊技術的能力。
<i>範圍 4：知識面描述</i>	
KS4.1	關於服務水準管理措施與服務水準協議中的要素的知識
KS4.2	關於監控第三方是否符合組織內部控管之技術的知識
KS4.3	關於管理排程與非排程之系統與使用者程序的知識
KS4.4	關於硬體與網路元件、系統軟體及資料庫管理系統相關技術概念的知識
KS4.5	關於確保系統介面完整性之控制技術的知識
KS4.6	關於軟體授權和盤存措施的知識
KS4.7	關於系統恢復工具和技術 (例如：硬體容錯、單點故障消除、叢集) 的知識
KS4.8	關於資料庫管理措施的知識
KS4.9	關於容量規劃與相關監控工具及技術的知識
KS4.10	關於系統效能監控流程、工具與技術 (例如：網路分析工具、系統使用率報告、負載平衡) 的知識
KS4.11	關於問題與事件管理措施 (例如：服務台、問題升級處理程序、追蹤) 的知識
KS4.12	關於對正式系統和(或)基礎設施之排程與未排程之管理程序，包含變更、組態、發佈和修補補丁的管理做法的知識
KS4.13	關於資料備份、儲存、維護、保留和還原措施的知識
KS4.14	關於災難復原相關法規、法律、合約與保險議題的知識

## 內容領域 (範圍)

### 範圍 4：知識面描述 (續)

KS4.15 關於營運衝擊分析 [BIA] 與災難復原計劃間之關係的知識

KS4.16 關於災難復原計劃之開發與維護的知識

KS4.17 關於用以監控約定協議之備援場所與方法 (例如：熱備援場地、暖備援場地、冷備援場地) 的知識

KS4.18 關於用以調用災難復原計劃之流程的知識

KS4.19 關於災難復原測試方法的知識

**範圍 5：資訊資產的保護——確保組織的安全政策、標準、程序和控制在足以保證資訊資產的機密性、完整性和可用性。**

### 範圍 5：任務描述

T5.1 評估資訊安全政策、標準與程序的完整性並符合普遍接受的做法。

T5.2 評估系統與邏輯安全控管的設計、建置與監控，以驗證資訊的機密性、完整性和可用性。

T5.3 評估資料分類流程與程序的設計、建置與監控，以符合組織的政策、標準、程序及適用的外部要求。

T5.4 評估實體存取與環境控制的設計、建置和監控，以判斷資訊資產是否獲得妥善的保護。

T5.5 評估用以儲存、擷取、傳送及處置資訊資產的流程與程序 (例如：備份媒體、異地儲存、書面/列印資料及電子媒體)，以判斷資訊資產是否獲得妥善的保護。

### 範圍 5：知識面描述

KS5.1 關於安全控管 (包括安全宣導方案) 之設計、建置與監控技術的知識

KS5.2 關於安全性事件監控和回應相關流程 (例如：問題升級處理程序、緊急事件回應小組) 的知識

KS5.3 關於用以識別、授權與限制使用者取得需獲授權功能與資料之邏輯存取控制的知識

KS5.4 關於硬體、系統軟體 (如：應用程式、作業系統) 與資料庫管理系統相關之安全控管的知識

KS5.5 關於系統虛擬化相關風險與控制的知識

KS5.6 關於網路安全控管之組態設定、建置、營運及維護的知識

KS5.7 關於電腦網路與網際網路安全裝置、通訊協定和技術的知識

KS5.8 關於資訊系統攻擊方法與技術的知識

KS5.9 關於偵測工具和控制技術 (例如：惡意軟體、病毒偵測、間諜軟體) 的知識

KS5.10 關於安全測試技術 (例如：入侵測試、弱點掃描) 的知識

KS5.11 關於資料外洩相關風險與控制的知識

KS5.12 關於加密相關技術的知識

KS5.13 關於公開金鑰基礎設施 (PKI) 元件與數位簽章技術的知識

KS5.14 關於點對點計算、即時通訊與網路技術 (例如：社交網路、留言板、部落格) 相關風險與控制的知識

KS5.15 關於使用行動與無線裝置相關控管與風險的知識

KS5.16 關於語音通訊安全性 (例如：PBX、VoIP) 的知識

KS5.17 關於在調查取證中遵循之證據保全技術與流程 (例如：資訊技術、流程、證據保管之連續性) 的知識

KS5.18 關於資料分類標準與配套程序的知識

KS5.19 關於用以識別、授權與限制使用者取得需獲授權設施之實體存取控制的知識

KS5.20 關於環境保護裝置與配套措施的知識

KS5.21 關於用以儲存、擷取、傳送和處置機密資訊資產之流程和程序的知識



# 準備 2012 年 CISA 考試

2012 年 CISA 準備考試和專業進修的複習資源

---

成功的 Certified Information Systems Auditor® (CISA®) 考生擁有完整而系統的學習計劃。為協助考生們擬定成功的學習計劃，ISACA® 為考生們提供了幾種學習輔導以及複習課程。其中包括：

## 學習輔導

- *CISA® Review Manual 2012*
- *CISA® Review Questions, Answers & Explanations Manual 2011*
- *CISA® Review Questions, Answers & Explanations Manual 2011 Supplement*
- *CISA® Review Questions, Answers & Explanations Manual 2012 Supplement*
- *CISA® Practice Question Database v12*

若要訂購上述複習資料，請造訪 [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks)。

## 複習課程

- 以章節進行的複習課程 ([www.isaca.org/cisareview](http://www.isaca.org/cisareview))
- CISA® 線上複習課程 ([www.isaca.org/elearning](http://www.isaca.org/elearning))