

ISO 27001 資訊安全管理系統稽 核員

認證題庫共**200**題

認證檢定考試說明

本認證檢定採單科測驗制，每科考試內容與配分方式如下：

是非題：**15** 題

選擇題：**10** 題

每題配分：**4** 分

全卷 總分為 **100** 分，

成績達 **60** 分(含)以上者為合格。

考試時間為 **60** 分鐘，

請考生於規定時間內完成作答。

ISO 27001 資訊安全管理系統稽核員 是非題

1. ISO 27001為資訊安全管理系統標準。
答案: 是
解析: ISMS標準。
2. ISO 27001強調資訊機密性、完整性與可用性。
答案: 是
解析: CIA三要素。
3. ISO 27001屬於ISO 9000系列。
答案: 否
解析: 屬ISO 27000系列。
4. ISMS需建立資訊安全政策。
答案: 是
解析: 政策要求。
5. ISO 27001採用PDCA管理循環。
答案: 是
解析: 管理模式。
6. 資訊資產不需盤點。
答案: 否
解析: 需資產識別。
7. ISO 27001支持風險導向思維。
答案: 是
解析: 風險管理。
8. ISMS不需文件化資訊。
答案: 否
解析: 文件要求。
9. ISO 27001支持持續改善。
答案: 是
解析: PDCA概念。

10. 資訊安全只包含IT系統安全。

答案:否

解析:含人員與流程。

11. ISMS需建立風險評估程序。

答案:是

解析:風險管理。

12. ISO 27001鼓勵建立控制措施。

答案:是

解析:Annex A控制。

13. 資訊安全不需教育訓練。

答案:否

解析:訓練必要。

14. ISO 27001支持內部稽核。

答案:是

解析:稽核要求。

15. ISMS需建立紀錄保存。

答案:是

解析:紀錄管理。

16. ISO 27001只適用大型企業。

答案:否

解析:適用所有組織。

17. 資訊安全風險需定期檢討。

答案:是

解析:風險更新。

18. ISO 27001支持管理審查。

答案:是

解析:管理要求。

19. ISMS需建立資產分類。

答案:是

解析:資產管理。

20. 資訊安全與人員管理無關。

答案:否

解析:人員安全。

21. ISO 27001支持存取控制。

答案:是

解析:Access control。

22. ISMS需建立事件通報機制。

答案:是

解析:事件管理。

23. 資訊安全不需備份。

答案:否

解析:備份重要。

24. ISO 27001支持營運持續管理。

答案:是

解析:BC整合。

25. ISMS需建立變更管理。

答案:是

解析:變更控制。

26. ISO 27001鼓勵資安風險降低措施。

答案:是

解析:風險處理。

27. 資訊安全只需技術控制。

答案:否

解析:管理與技術。

28. ISMS需建立供應商安全管理。

答案:是

解析:供應鏈安全。

29. ISO 27001支持密碼管理。

答案:是

解析:認證控制。

30. 資訊安全不需監測。

答案:否

解析:監測必要。

31. ISO 27001支持事件回應機制。

答案:是

解析:事件處理。

32. ISMS需建立文件控制。

答案:是

解析:文件管理。

33. ISO 27001支持法規遵循。

答案:是

解析:合規要求。

34. 資訊安全不需績效評估。

答案:否

解析:績效監測。

35. ISMS需建立風險處理計畫。

答案:是

解析:風險處理。

36. ISO 27001支持資安文化建立。

答案:是

解析:文化建立。

37. 資訊安全與實體安全無關。

答案:否

解析:實體安全。

38. ISMS需建立備援與復原機制。

答案:是

解析:復原能力。

39. ISO 27001支持持續監測控制措施。

答案:是

解析:控制監測。

40. 資訊安全不需政策支持。

答案:否

解析:政策必要。

41. ISO 27001支持風險評估與處理。

答案:是

解析:風險管理。

42. ISMS需建立資安目標。

答案:是

解析:目標管理。

43. ISO 27001支持教育訓練與意識提升。

答案:是

解析:awareness。

44. 資訊安全只關於資料保護。

答案:否

解析:含系統與流程。

45. ISMS需建立通訊安全控制。

答案:是

解析:通訊安全。

46. ISO 27001支持稽核證據保存。

答案:是

解析:稽核要求。

47. 資訊安全不需管理層支持。

答案:否

解析:領導作用。

48. ISMS需建立弱點管理。

答案:是

解析:漏洞管理。

49. ISO 27001支持控制措施有效性評估。

答案:是

解析:控制評估。

50. ISO 27001目的是保護資訊資產。

答案:是

解析:ISMS目的。

51. ISMS需建立資安風險處理流程。

答案:是

52. ISO 27001支持資訊分類與標示。

答案:是

53. 資訊安全事件不需記錄。

答案:否

54. ISO 27001鼓勵建立密碼政策。

答案:是

55. ISMS需建立備份政策。

答案:是

56. ISO 27001支持弱點評估。

答案:是

57. 資訊安全不需供應商管理。

答案:否

58. ISO 27001支持事件回應程序。

答案:是

59. ISMS需建立安全通訊機制。

答案:是

60. ISO 27001只關注技術安全。

答案:否

61. ISMS需建立存取權限管理。

答案:是

62. ISO 27001支持資料保護措施。

答案:是

63. 資訊安全不需監測系統活動。

答案:否

64. ISO 27001鼓勵日誌管理。

答案:是

65. ISMS需建立營運持續資訊安全措施。

答案:是

66. ISO 27001支持安全配置管理。

答案:是

67. 資訊安全與實體設備無關。

答案:否

68. ISO 27001支持人員安全控制。

答案:是

69. ISMS需建立帳號管理。

答案:是

70. ISO 27001支持多因素驗證概念。

答案:是

71. 資訊安全不需安全測試。

答案:否

72. ISO 27001支持惡意程式防護。

答案:是

73. ISMS需建立變更記錄。

答案:是

74. ISO 27001支持系統備援。

答案:是

75. 資訊安全不需資安政策審查。

答案:否

76. ISO 27001支持加密控制。

答案:是

77. ISMS需建立設備安全管理。

答案:是

78. ISO 27001支持供應鏈資安評估。

答案:是

79. 資訊安全事件不需回報。

答案:否

80. ISO 27001支持資訊安全指標監測。

答案:是

81. ISMS需建立權限審查機制。

答案:是

82. ISO 27001支持資料刪除與銷毀控制。

答案:是

83. 資訊安全不需內部控制措施。

答案:否

84. ISO 27001支持資安事件調查。

答案:是

85. ISMS需建立設備存放安全措施。

答案:是

86. ISO 27001支持備援測試。

答案:是

87. 資訊安全不需供應商契約要求。

答案:否

88. ISO 27001支持網路安全控制。

答案:是

89. ISMS需建立安全開發控制。

答案:是

90. ISO 27001支持風險監測。

答案:是

91. 資訊安全不需稽核追蹤。

答案:否

92. ISO 27001支持事件通報流程。

答案:是

93. ISMS需建立資安改善機制。

答案:是

94. ISO 27001支持雲端安全管理。

答案:是

95. 資訊安全不需管理審查。

答案:否

96. ISO 27001支持安全測試與評估。

答案:是

97. ISMS需建立通訊安全政策。

答案:是

98. ISO 27001支持資安教育訓練。

答案:是

99. ISMS導入可降低資訊安全風險。

答案:是

100. ISO 27001目的是建立ISMS並保護資訊資產。

答案:是

ISO 27001 資訊安全管理系統稽核員 選擇題

1. ISO 27001主要內容為:

- A. 環境管理
- B. 資訊安全管理系統
- C. 能源管理
- D. 職業安全

答案:B

2. CIA三要素包含:

- A. 成本、控制、分析
- B. 控制、稽核、分析
- C. 機密性、完整性、可用性

D. 政策、程序、紀錄

答案:C

3. ISMS主要管理方式為:

A. SWOT

B. ERP

C. ROI

D. PDCA循環

答案:D

4. 資訊資產盤點屬於:

A. 資產管理

B. 行銷管理

C. 財務管理

D. 招募管理

答案:A

5. 風險評估主要目的為:

A. 增加文件

B. 識別資安風險

C. 招募人員

D. 財務管理

答案:B

6. Annex A主要用途為:

A. 財務控制

B. 招募流程

C. 控制措施參考

D. 行銷流程

答案:C

7. 資訊安全政策應由誰核准?

A. 員工

B. 稽核員

C. 供應商

D. 最高管理階層

答案:D

8. 存取控制主要目的為:

A. 限制未授權存取

B. 增加文件

C. 招募人員

D. 行銷管理

答案:A

9. 多因素驗證屬於:

A. 財務控制

B. 身分驗證控制

C. 行銷控制

D. 招募控制

答案:B

10. 備份控制主要目的為:

A. 增加文件

B. 管理員工

C. 確保資料可復原

D. 招募人員

答案:C

11. 資安事件管理主要目的為:

A. 增加文件

B. 招募人員

C. 行銷管理

D. 回應與控制事件

答案:D

12. 內部稽核主要目的為:

A. 驗證ISMS符合性

B. 增加文件

C. 招募人員

D. 財務管理

答案:A

13. 管理審查主要用途為:

A. 行銷規劃

B. 評估ISMS績效

C. 招募規劃

D. 財務規劃

答案:B

14. 資安教育訓練主要目的為:

A. 增加文件

B. 招募員工

C. 提升安全意識

D. 財務控制

答案:C

15. 日誌管理主要用途為:

A. 行銷資料

B. 招募紀錄

C. 財務紀錄

D. 追蹤系統活動

答案:D

16. 加密控制主要目的為:

A. 保護資料機密性

B. 財務保護

C. 行銷保護

D. 招募保護

答案:A

17. 供應商資安管理主要用途為:

A. 行銷合作

B. 降低供應鏈風險

C. 招募合作

D. 財務合作

答案:B

18. 弱點管理主要目的為:

A. 增加文件

B. 招募人員

C. 修補安全漏洞

D. 財務管理

答案:C

19. 實體安全控制主要用途為:

A. 行銷管理

B. 招募管理

C. 財務管理

D. 保護設備與設施

答案:D

20. 通訊安全控制主要目的為:

A. 保護資料傳輸

B. 行銷保護

C. 招募管理

D. 財務管理

答案:A

21. 資訊分類主要用途為:

A. 財務分析

B. 保護資訊資產

C. 行銷分析

D. 招募分析

答案:B

22. 變更管理主要目的為:

A. 增加文件

B. 招募人員

C. 控制系統變更風險

D. 財務控制

答案:C

23. 備援系統主要用途為:

A. 行銷支援

B. 招募支援

C. 財務支援

D. 提高可用性

答案:D

24. 權限審查主要目的為:

A. 確認存取權限適當

B. 招募人員

C. 行銷管理

D. 財務管理

答案:A

25. 安全配置管理主要用途為:

A. 行銷管理

B. 降低系統風險

C. 招募管理

D. 財務管理

答案:B

26. 惡意程式防護屬於:

A. 財務控制

B. 行銷控制

C. 技術安全控制

D. 招募控制

答案:C

27. 安全測試主要用途為:

A. 招募人員

B. 行銷分析

C. 財務分析

D. 驗證系統安全性

答案:D

28. 風險處理計畫主要用途為:

A. 降低資安風險

B. 行銷管理

C. 招募管理

D. 財務管理

答案:A

29. 安全開發控制主要用途為:

A. 招募系統

B. 保護應用程式安全

C. 行銷系統

D. 財務系統

答案:B

30. 稽核證據主要用途為:

A. 行銷分析

B. 招募紀錄

C. 支持稽核結論

D. 財務紀錄

答案:C

31. 資安目標應:

A. 隨意設定

B. 可量測

C. 忽略

D. 刪除

答案:B

32. ISMS範圍應:

A. 忽略

B. 明確定義

C. 刪除

D. 模糊設定

答案:B

33. 風險接受準則主要用途為:

A. 行銷決策

B. 決定可接受風險

C. 招募決策

D. 財務決策

答案:B

34. 控制措施有效性評估主要目的為:

A. 行銷評估

B. 確認控制有效

C. 招募評估

D. 財務評估

答案:B

35. ISMS文件控制主要用途為:

A. 行銷文件

B. 確保文件正確版本

C. 招募文件

D. 財務文件

答案:B

36. 稽核計畫主要用途為:

A. 招募計畫

B. 安排稽核活動

C. 行銷計畫

D. 財務計畫

答案:B

37. 管理階層角色為:

A. 忽略ISMS

B. 提供支持與資源

C. 停止管理

D. 刪除政策

答案:B

38. 資訊安全文化主要用途為:

A. 行銷文化

B. 提升安全意識

C. 招募文化

D. 財務文化

答案:B

39. 控制措施選擇依據為:

A. 行銷需求

B. 風險評估結果

C. 招募需求

D. 財務需求

答案:B

40. 營運持續資訊安全控制主要用途為:

A. 行銷保護

B. 確保資訊服務持續

C. 招募保護

D. 財務保護

答案:B

41. 雲端安全管理主要用途為:

A. 行銷雲端

B. 保護雲端資料

C. 招募雲端

D. 財務雲端

答案:B

42. 資安事件回報主要目的為:

A. 增加文件

B. 快速處理事件

C. 招募人員

D. 財務管理

答案:B

43. 資訊生命週期管理主要用途為:

A. 行銷管理

B. 資料保護與銷毀

C. 招募管理

D. 財務管理

答案:B

44. 控制措施文件主要用途為:

A. 行銷管理

B. 說明安全控制

C. 招募管理

D. 財務管理

答案:B

45. 稽核發現主要用途為:

A. 行銷改善

B. 改善ISMS

C. 招募改善

D. 財務改善

答案:B

46. 風險監測主要用途為:

A. 行銷監測

B. 持續管理風險

C. 招募監測

D. 財務監測

答案:B

47. 控制措施監測主要用途為:

A. 行銷監測

B. 評估控制績效

C. 招募監測

D. 財務監測

答案:B

48. 安全事件調查主要用途為:

A. 行銷分析

B. 找出事件原因

C. 招募分析

D. 財務分析

答案:B

49. ISMS導入效益為:

A. 增加文件

B. 降低資安風險

C. 招募增加

D. 財務增加

答案:B

50. ISO 27001最終目標為:

A. 建立行銷制度

B. 保護資訊資產

C. 建立財務制度

D. 建立招募制度

答案:B

51. 稽核員確認風險評估程序時, 最重要檢視:

A. 是否一致且可重複

B. 行銷策略

C. 招募流程

D. 財務報表

答案:A

52. 若資產盤點不完整, 最可能影響:

A. 行銷管理

B. 風險評估結果

C. 招募制度

D. 財務制度

答案:B

53. 稽核存取控制時應優先確認：

- A. 行銷資料
- B. 招募制度
- C. 權限核准與記錄
- D. 財務流程

答案：C

54. 若系統未保留日誌，可能影響：

- A. 行銷分析
- B. 招募紀錄
- C. 財務紀錄
- D. 事件追蹤能力

答案：D

55. 資安事件通報流程缺失屬於：

- A. 程序控制缺失
- B. 行銷問題
- C. 招募問題
- D. 財務問題

答案：A

56. 稽核供應商安全時應確認：

- A. 行銷合作
- B. 契約資安要求
- C. 招募合作
- D. 財務合作

答案：B

57. 若備份未測試，最可能影響：

- A. 行銷資料
- B. 招募資料
- C. 復原能力
- D. 財務資料

答案：C

58. 風險處理計畫應包含：

- A. 行銷目標
- B. 招募目標
- C. 財務目標
- D. 控制措施與責任

答案:D

59. 稽核實體安全時應確認：

- A. 設備存取限制
- B. 行銷制度
- C. 招募制度
- D. 財務制度

答案:A

60. 若資安政策未定期檢討，代表：

- A. 行銷問題
- B. 管理缺失
- C. 招募問題
- D. 財務問題

答案:B

61. 多因素驗證主要降低：

- A. 行銷風險
- B. 招募風險
- C. 身分冒用風險
- D. 財務風險

答案:C

62. 弱點掃描主要目的為：

- A. 行銷測試
- B. 招募測試
- C. 財務測試
- D. 發現系統漏洞

答案:D

63. 稽核文件控制時應檢查：

- A. 版本與核准
- B. 行銷版本
- C. 招募版本
- D. 財務版本

答案:A

64. 若變更管理缺失, 可能造成:

- A. 行銷失誤
- B. 系統安全風險
- C. 招募失誤
- D. 財務失誤

答案:B

65. 稽核教育訓練時應確認:

- A. 行銷成果
- B. 招募成果
- C. 訓練紀錄
- D. 財務成果

答案:C

66. 安全開發控制主要降低:

- A. 行銷風險
- B. 招募風險
- C. 財務風險
- D. 應用程式漏洞

答案:D

67. 稽核加密控制時應確認:

- A. 金鑰管理
- B. 行銷機制
- C. 招募機制
- D. 財務機制

答案:A

68. 若資安目標無法量測, 代表:

- A. 行銷問題
- B. 目標設定不當
- C. 招募問題
- D. 財務問題

答案:B

69. 稽核日誌管理時應確認:

- A. 行銷紀錄
- B. 招募紀錄
- C. 日誌保留與檢視
- D. 財務紀錄

答案:C

70. 若存取權限未定期檢討, 可能造成:

- A. 行銷問題
- B. 招募問題
- C. 財務問題
- D. 未授權存取

答案:D

71. 稽核備援系統時應確認:

- A. 備援測試紀錄
- B. 行銷系統
- C. 招募系統
- D. 財務系統

答案:A

72. 稽核控制措施有效性時應查看:

- A. 行銷成果
- B. 績效指標
- C. 招募成果
- D. 財務成果

答案:B

73. 若事件回應未演練, 可能造成:

- A. 行銷問題
- B. 招募問題
- C. 應變能力不足
- D. 財務問題

答案:C

74. 稽核供應鏈資安時應確認:

- A. 行銷契約
- B. 招募契約
- C. 財務契約
- D. 風險評估紀錄

答案:D

75. 安全配置管理主要降低:

- A. 系統錯誤設定風險
- B. 行銷風險
- C. 招募風險
- D. 財務風險

答案:A

76. 若資安事件未調查原因, 代表:

- A. 行銷問題
- B. 改善機制不足
- C. 招募問題
- D. 財務問題

答案:B

77. 稽核通訊安全時應確認:

- A. 行銷流程
- B. 招募流程
- C. 傳輸保護措施
- D. 財務流程

答案:C

78. 若資產分類不正確，可能造成：

- A. 行銷問題
- B. 招募問題
- C. 財務問題
- D. 保護不足

答案：D

79. 稽核風險監測時應確認：

- A. 風險檢討紀錄
- B. 行銷監測
- C. 招募監測
- D. 財務監測

答案：A

80. 稽核帳號管理時應確認：

- A. 行銷帳號
- B. 帳號建立與刪除流程
- C. 招募帳號
- D. 財務帳號

答案：B

81. 若控制措施未監測，可能造成：

- A. 行銷問題
- B. 招募問題
- C. 控制失效
- D. 財務問題

答案：C

82. 稽核資料銷毀控制時應確認：

- A. 行銷銷毀
- B. 招募銷毀
- C. 財務銷毀
- D. 安全刪除程序

答案：D

83. 稽核雲端安全時應確認：

- A. 雲端安全責任分工
- B. 行銷服務
- C. 招募服務
- D. 財務服務

答案:A

84. 若ISMS範圍未明確，可能造成：

- A. 行銷問題
- B. 稽核困難
- C. 招募問題
- D. 財務問題

答案:B

85. 稽核實體設備安全時應確認：

- A. 行銷設備
- B. 招募設備
- C. 設備保護措施
- D. 財務設備

答案:C

86. 若管理審查未執行，代表：

- A. 行銷問題
- B. 招募問題
- C. 財務問題
- D. 管理系統缺失

答案:D

87. 稽核控制措施選擇時應依據：

- A. 風險評估
- B. 行銷需求
- C. 招募需求
- D. 財務需求

答案:A

88. 稽核資安文化時應確認：

- A. 行銷文化
- B. 員工資安意識
- C. 招募文化
- D. 財務文化

答案：B

89. 若日誌未保護，可能造成：

- A. 行銷問題
- B. 招募問題
- C. 稽核證據失效
- D. 財務問題

答案：C

90. 稽核弱點管理時應確認：

- A. 行銷漏洞
- B. 招募漏洞
- C. 財務漏洞
- D. 修補紀錄

答案：D

91. 稽核風險接受時應確認：

- A. 管理層核准
- B. 行銷核准
- C. 招募核准
- D. 財務核准

答案：A

92. 若控制措施未文件化，可能造成：

- A. 行銷問題
- B. 稽核證據不足
- C. 招募問題
- D. 財務問題

答案：B

93. 稽核資安事件時應確認：

- A. 行銷紀錄
- B. 招募紀錄
- C. 事件處理流程
- D. 財務紀錄

答案：C

94. 稽核改善措施時應確認：

- A. 行銷改善
- B. 招募改善
- C. 財務改善
- D. 矯正措施紀錄

答案：D

95. 若內部稽核未依計畫執行，代表：

- A. 稽核管理缺失
- B. 行銷問題
- C. 招募問題
- D. 財務問題

答案：A

96. 稽核控制措施監測時應確認：

- A. 行銷監測
- B. 監測結果紀錄
- C. 招募監測
- D. 財務監測

答案：B

97. 稽核通報流程時應確認：

- A. 行銷流程
- B. 招募流程
- C. 通報紀錄
- D. 財務流程

答案：C

98. 若資安政策未宣導, 可能造成:

- A. 行銷問題
- B. 意識不足
- C. 招募問題
- D. 財務問題

答案: B

99. 稽核風險處理時應確認:

- A. 行銷控制
- B. 控制措施實施
- C. 招募控制
- D. 財務控制

答案: B

100. ISO 27001稽核員最重要能力為:

- A. 行銷能力
- B. 客觀評估ISMS
- C. 招募能力
- D. 財務能力

答案: B