Chương 3:

Bảo mật Phần I: Kiểm toán Hệ điều hành và Mạng

1. Rủi ro hệ điều hành

Các rủi ro liên quan đến tính toàn vẹn của HDH

- Các rủi ro về các tai nạn liên quan đến phần cứng lỗi trong các ứng dụng của người dùng
- Truy cập trái phép vào DL & xâm phạm quyền riêng tư để thu lợi tài chính.
- Tăng rủi ro liên quan đến PM hủy diệt:
  - Người có đặt quyền lạm dụng truy cập và cài các PM hủy duyệt vào trong hệ thống
  - Các cá nhân bên ngoài xâm nhập bất hợp pháp vào hệ thống
  - Hệ thống bị lỗi

2. Kiểm soát HDH:

- Đặc quyền truy cập
- Xác thực truy cập qua id và password
- Kiểm tra pm và chương trình khi tái và cài vào máy, pm diệt virus và phát hiện các pm độc hại
- Set up nhật ký kiểm toán(audit trails)

2.1. Đặc quyền truy cập

Mục tiêu:

- Xác minh các đặc quyền truy cập phù hợp với các chức năng tách biệt và chính sách tổ chức.

Thủ tục kiểm toán:

- Rà soát các chính sách để tách các chức năng không tương thích.
- Chọn mẫu, xem xét các đặc quyền của người dùng đặt biệt là các quyền truy cập vào DL và các chương trinh ứng dụng
- Xem xét người dùng có ý thức và trách nhiệm hay chưa để duy trì tính báo mật
- Xem xét kiểm tra thông qua an ninh của các nhân viên có đặc quyền
- Xem lại thời gian đăng nhập được phép của người dùng. Quyền phải tương xứng với các nhiệm vụ thực hiện

2.2. Xác thực truy cập qua id và password

Mục tiêu :

- Đảm bảo các chính sách password đầy đủ và hiệu quả để kiểm soát quyền truy cập vào HDH

Thủ tục kiểm toán:

- Xác minh tất cả NV đều yêu cầu password truy cập vào HT và các NV mới thì được hướng dẫn về đặt password
- Đảm bảo các biện pháp kiểm soát yêu cầu thay đổi mật khẩu thường xuyên
- Rà soát lại các file pass xem có pass nào yếu hay không
- Xác minh mã hóa pas
- Đánh giá các tiêu chuẩn của pass
- Xem lại ác chính sách về lockout tài khoản và quy trinh xử lý

2.3. Kiểm tra pm và chương trình khi tái và cài vào máy, pm diệt virus và phát hiện các pm độc hại

Mục tiêu kiểm toán:

- Xác minh tính hiệu quả của các thủ tục để bảo vệ khỏi các chương trình như vi rút, worms, back door, bom logic và ngựa Trojan

Thủ tục kiểm tra:

- Kiểm tra về tính hiệu quả của các pm virus, các pm này co được capaj nhạt thường xuyên
- Kiểm tra các pm mới khi được cài vào ht có kiểm tra
- Kiểm tra sự an toàn của pm mới (pm được phê duyệt , nhà cung cấp uy tín)
- Kiểm tra ý thức và trách nhiệm của NV trong việc cài đặt các pm đọc hại hay virus

Mục tiêu kiểm toán: screen: 9:39

Thủ tục kiểm tra : 9:39

27:

Mục tiêu kiểm toán: 10:41

Nho:

- **Ngăn chặn hoặc phát hiện các truy cập k hợp pháp**
- **Dữ liệu bị lấy không thể xem được**
- **Đảm bảo tính bảo mật và toàn vẹn của dữ liệu**

Tường lửa -> dos, ip giả mạo
Ips -> ddos

1.Khi lập kế hoạch kiểm toán để

a) Tất cả các ý trên đều đúng
b) Đánh giá rủi ro tiềm tàng của khách hàng
c) Đánh giá rủi ro kiểm soát và rủi ro phát hiện
d) Kiểm tra hiệu quả của kiểm soát nội bộ

2. Các hành vi không đảm bảo an ninh đối với mật khẩu (password) ?

a) Hiển thị mật khẩu khi đăng nhập
b) Mật khẩu đơn giản và dễ đoán
c) Quên mật khẩu hoặc không thường xuyên thay đổi mật khẩu
d) Các câu trên đều đúng

3. Nhận định nào sau đây không phải thủ tục kiểm toán hệ điều hành?

a) Xác định dấu vết kiểm toán được kích hoạt và cập nhật thường xuyên
b) Kiểm tra password có được mã hóa và thay đổi thường xuyên
c) Kiểm tra sự hợp lý về chính sách phân quyền cho các bộ phận
d) Kiểm tra hàng tồn kho có được phê duyệt trước khi xuất kho

4.Các cơ sở dẫn liệu đối với kiểm toán các khoản mục trên báo cáo tình hình tài chính?

a) Đầy đủ, quyền và nghĩa vụ, đánh gái và phân bố, hiện hữu, phát sinh, chính xác, phân loại, đúng kỳ và trình bày
b) Đầy đủ, quyền và nghĩa vụ, hiện hữu, chính xác, phân loại và trình bày
c) Đầy đủ, quyền và nghĩa vụ, đánh giá và phân bố, hiện hữu, chính xác, phân loại, đúng kỳ và trình bày
d) Đầy đủ, quyền và nghĩa vụ, đánh giá và phân bố, hiện hữu, chính xác, phân loại và trình bà

5.Tấn công từ chối dịch vụ DOS là gì ?

a) Kết nối với cơ sở dữ liệu trung tâm tăng rủi ro dữ liệu sẽ có thể truy cập được đối với nhân viên
b) Tấn công nhằm làm sập một máy chủ hoặc mạng khiến người dùng khác không thể truy cập vào máy chủ hay mạng đó
c) Gái mạo để dành quyền truy cập vào máy chủ Web và thực hiện hành phí trái pháp luật mà không lộ danh tính người dùng
d) Lợi dụng những lỗ hổng về bảo mật cũng như sự không hiểu biết để giành quyền điều khiển máy tính của nhân viên tấn công vào các máy tính khác

6.Các rủi ro sau đây không là rủi ro kiểm soát?

a) Nhân viên có thể sử dụng đặc quyền của mình để truy cập trái phép vào sổ cái để thay đổi dữ liệu gây sai xót trọng yếu trên báo cáo tài chính
b) Kiểm soát viên không phát hiện được sai sót trọng yếu về khoản nợ phải trả trên báo cáo tài chính
c) Để khuyến khích bán hàng công ty nới rộng điều kiện tín dụng đối với các khách hàng mới
d) Công ty đang bị kiện bởi một khách hàng. Khách hàng này cáo buộc công ty bán sản phẩm kém chất lượng gây thiệt hại kinh tế cho khách hàng

7.Ghi lại cá thủ tục thẩm vấn các hồ sơ hợp lệ bằng cách ?

a) Kiểm tra phiên bản, kiểm tra tính hợp lý (reasonableness check), kiểm tra dấu (sign check)
b) Kiểm tra tính hợp lý (reasonableness check), kiểm tra dấu (sign check)
c) Kiểm tra nhãn bên trong và bên ngoài, kiểm tra tính hợp lý (reasonableness check), kiểm tra dấu (sign check)
d) Kiểm tra tính hợp lý (reasonableness check), kiểm tra dấu (sign check), kiểm tra trình tự (sequence check)

……..

8.Thử nghiệm cơ bản bao gồm ?

a) Thử nghiệm chi tiết và thử nghiệm kiểm soát
b) Thử nghiệm kiểm soát, thủ tục phân tích và thử nghiệm chi tiết
c) Thử nghiệm chi tiết và thủ tục phân tích
d) Thử nghiệm kiểm soát và thủ tục phân tích

9.Mục tiêu của hệ thống dấu vết kiểm soát ?

a) Phát hiện các truy cập trái phép
b) Ghi nhận các nghiệp vụ kinh tế phát sinh tại doanh nghiệp
c) Tái tạo lại các sự kiện
d) A và B đều đúng

10.Thiết bị gọi là gì?

a) Yêu cầu người dùng quay số để nhập và mật khẩu được xác nhận
b) Yêu cầu gửi các tin nhắn kiểm soát và phản hồi một cách ngẫu nhiên khiến kẻ xâm nhập khó vượt qua
c) Ghi lại tất cả các lần truy cập đã cố gắng với ID người dùng, thời gian truy cập và vị trí
d) Chèn một số thứ tự trong mỗi tin nhắn để ngăn chặn các nỗ lực xóa, thay đổi hoặc sao chép một tin nhắn

11.Kiểm soát rủi ro từ các cuộc tấn công DDOS ?

a) Sử dụng hệ thống ngăn chặn xâm nhập (ISP) với tính năng kiểm tra gói chuyên sâu (DPI)
b) Sử dụng tường lửa
c) Sử dụng phần mềm an ninh
d) Các câu trên đều đúng

12.Mã hóa là gì?

a) Hai câu trên đều sai
b) Hai câu trên đều đúng
c) Người dùng sử dụng một thuật toán mã jhóa để chuyển đổi thông điệp văn bản rõ ràng ban đầu thành một văn bản mã hóa được giải mã ở đầu nhãn
d) Chuyển đổi dữ liệu thành mã bí mật để lưu trữ và truyền tải

13.Mục đích của ngôn ngữ báo cáo kinh doanh mở rộng (XBRL)

a) Đảm bảo các báo cáo tài chính đều được trình bày trung thực và hợp lý
b) Tất cả các ý trên
c) Giúp cập nhật kịp thời các thông tin tài chính và kiểm soát nội bộ của doanh nghiệp cho nhà quản trị
d) Để chuẩn hóa các phương pháp cho chuẩn bị, công bố và trao đổi thông tin tài chính

14.Thực hiện kiểm tra dữ liệu giao dịch để đảm bảo không lỗi trước khi xử lý, có 3 loại?

a) Thẩm vấn tại hiện trường và thẩm vấn tiệp
b) Thẩm vấn tại hiện trường, ghi lại các thử tục thẩm vấn
c) Thẩm vấn tại hiện trường, ghi lại các thủ tục thẩm vấn và thẩm vấn tiệp, thẩm vấn ban giám đốc
d) Thẩm vấn tại hiện trường, ghi lại các thủ tục thẩm vấn và thẩm vấn tiệp

15.Nhận định nào sau đây là sai?

a) Rủi ro về các phần mềm độc hại do cá nhân có đặc quyền truy cập trái phép vào hệ thống
b) Rủi ro cố ý đối với tính toán toàn vẹn của hệ điều hành bao gồm truy cập trái phép vào hệ thống và vi phạm quyền riêng tư để đạt lợi ích tài chính
c) Rủi ro từ các cuộc tấn công vào hệ thống mạng để lấy thông tin dữ liệu hay thay đổi cấu trúc dữ liệu
d) Kiểm soát hệ điều hành (operating systems) chỉ bao gồm rủi ro cố ý từ kiểm soát đặc quyền truy cập và các chương trình virus hay độc hại

16.Mục tiêu nào dưới đây là mục tiêu kiểm toán dấu vết kiểm toán

a) Đảm bảo hệ thống dấu vế kiểm toán đã được thiết lập ghi nhận lại các giao dịch phát sinh tại công ty
b) Đảm bảo hệ thống dấu vết kiểm toán đã được thiết lập thích hợp để ngăn ngừa và phát hiện các hành vi lạm dụng và xây dụng lại các sự kiện chính và lập kế hoạch phân bố nguồn lực
c) Đảm bảo hệ thống dấu vế kiểm toán đã được thiết lập ghi lại các giao dịch phát sinh tại công ty xây dựng lại các sự kiện chính liên quan đến tài nguyên hệ thống
d) Đảm bảo hệ thống dấu vết kiểm toán đã được thiết lập ghi nhận lại các giao dịch phát sinh tại công ty, ngăn ngừa và phát hiện các hành vi lạm dụng quyền truy cập trái phép vào hệ thống

17.Các nhận định nào sau đây không phải mục tiêu kiểm soát điều hành

a) Bảo vệ tài sản của công ty chống lại sựu thông đồng của các nhân viên trong công ty
b) Tự bảo vệ chống lại sự giả mạo của người dùng
c) Bảo vệ các mô-đun ứng dụng của người dùng khỏi phá hủy hoặc làm hỏng các mô-đun khác
d) Bảo vệ người dùng khỏi truy cập, phá hủy hoặc làm hỏng chương trình hoặc duex liệu của người dùng khác

18.Nhận định nào sau đây sai về rủi ro kiểm toán?

a) Tăng thủ tục kiểm toán để giảm rủi ro kiểm toán
b) Rủi ro tiềm tăng và rủi ro kiểm soát càng thấp thì rủi ro kiểm toán càng thấp
c) Rủi ro tiềm tàng và rủi ro kiểm soát càng cao thì thủ tục kiểm toán càng tăng

d) Rủi ro tiềm tàng và rủi ro kiểm soát càng cao thì rủi ro phát hiện theo chấp nhận được càng cao

19.Nhận định nào sau đây không phải mục tiêu kiểm toán đặc quyền?

a) Xác minh chính sách phân chia trách nhiệm của công ty là hợp lý
b) Xác minh phân chia trách nhiệm giữa các phòng ban phù hợp với chính sách công ty
c) Xác minh mỗi nhân viên không đảm nhận nhiều vị trí công việc trong công ty
d) Xác minh các đặc quyền truy cập phù hợp với việc phân chia các chức năng và chính sách tổ chức không tương thích

20.Các lỗi chuyển vị được kiểm soát bằng?

a) Các số kiểm tra (Check digits)
b) Kiểm tra giới hạn
c) Kiểm tra tính hợp lệ
d) Kiểm tra dữ liệu bị thiếu

21.Thủ tục kiểm toán "Xác minh rằng phần mềm mới đã được thử nghiệm trên cá máy tạm độc lập trước khi triển khai" nhằm kiểm toán gì?

a) Internet
b) Đặc quyền truy cập
c) Chương trình virus và hủy hoại
d) Dấu vết kiểm toán

22.Các rủi ro liên quan đến internet?

a) Chặn tin nhắn mạng, truy cập cơ sở dữ liệu công ty, nhân viên đặc quyền
b) Chặn tin nhắn mạng và các cuộc tấn công DOS
c) Giả mạo IP và tấn công từ chối dịch vụ DOS
d) Chặn tin nhắn mạng và truy cập cơ sở dữ liệu công ty

23.Run to run controls để đảm bảo ?

a) Các câu trên đều đúng
b) Hoàn thành thông qua dữ liệu kiểm soát hàng loạt bao gồm: số lô duy nhất, ngày, mã giao dịch, số ghi bản, tổng giá trị đô la (tổng số kiểm soát) và tổng số bấm
c) Dấu vết kiểm tra giao dịch được tạo ra
d) Tất cả các hồ sơ được xử lý, không có hồ sơ nào được xử lý nhiều hơn một lần

24.Các kỹ thuật xử lý lỗi phổ biến đối với kiểm soát xử lý?

a) Từ chối dữ liệu đầu vào và sửa lỗi
b) Sửa ngay lập tức tạo tiệp lỗi và từ chối lô
c) Xóa dữ liệu bị lỗi, tạo tiệp lỗi và từ chối lô
d) Không xử lý dữ liệu bị lỗi

25.Nhận định sau đây là đúng?

a) Cấu trúc kiểm soát nội bộ càng yếu thì rủi ro kiểm soát càng cao và kiểm soát viên phải thực hiện càng ít thử nghiệm cơ bản hơn
b) Cấu trúc kiểm soát nội bộ càng mạnh thì rủi ro kiểm soát càng thấp và kiểm toán viên pahir thực hiện càng ít thử nghiệm cơ bản hơn
c) Cấu trúc kiểm soát nội bộ càng mạnh thì rủi ro kiểm soát càng thấp và kiểm toán viên phải tăng trải nghiệm cơ bản hơn

d) Cấu trúc kiểm soát nội bộ càng yếu thì rủi ro kiểm soát càng thấp và kiểm toán viên phải thực hiện càng ít thử nghiệm cơ bản hơn

26.Kiểm soát IT bao gồm?

a) Kiểm soát ứng dụng, phân chia trách nhiệm và giám sát
b) Ủy quyền giao dịch, phân chia trách nhiệm, giám sát
c) Kiểm soát bao quát (general controls) và kiểm soát ứng dụng (application controls)
d) Giám sát, kiểm soát bao quát và kiểm soát ứng dụng

27.Mục đích của kiểm soát đầu ra?

a) Đảm bảo đầu ra của hệ thống không bị mất, thất lạc hoặc bị hỏng và chính sách bảo mật không bị vi phạm
b) Đảm bảo đầu ra của hệ thống không bị mất thất lạc hoặc bị hỏng và chính sách bảo mật không bị vi phạm, các dữ liệu trung thực và hợp lý
c) Đảm bảo đầu ra của hệ thống không bị mất
d) Đảm bảo đầu ra của hệ thống không bị mất thất lạc hoặc bị hỏng

28.Các rủi ro liên quan đến đánh hơi (siffing) để chặn tin nhắn mạng?

a) Đánh chặn ID người dùng, mật khẩu, email bí mật và các tệp dữ liệu tài chính
b) Lợi dụng những lỗ hổng về bảo mật cũng như sự không hiểu biết để giành quyền điều khiển máy tính của nhân viên tấn công vào các máy tính khác
c) Tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy caaph vào máy chủ hay mạng đó
d) Kết nối với cơ sở dữ liệu trung tâm tăng rủi ro dữ liệu sẽ có thể truy cập được đối với nhân viên

29.Kỹ thuật phản hồi là gì?

a) Chèn một số thứ tự trong mỗi tin nhắn để ngăn chặn các nổ lực cáo, thay đổi hoặc sao chép một tin nhắn
b) Yêu cầu gửi các tin nhắn kiểm soát và phản hồi một cách ngẫu nhiên khiến kẻ xâm nhập khó vượt qua
c) Ghi lại tất cả các lần truy cập đã cố gắng với ID người dùng, thời gian truy cập và vị trí
d) Yêu cầu người dùng quay số để nhập và mật khẩu được xác định

30.Tấn công DDOS là gì?

a) Tấn công nhằm làm sập một máy chủ hoặc mạng , khiến người dùng khác không thể truy cập vào máy chủ hay mạng đó
b) Kết nối với cơ sở dữ liệu trung tâm tăng rủi ro dữ liệu sẽ có thể truy cập được đối với nhân viên
c) Giả mạo để giành quyền truy cập vào máy chủ Web và thực hiện hành phí trái phép luật mà không lộ danh tính người dùng
d) Lợi dụng những lỗ hổng về bảo mật cũng như sựu không hiểu biết để giành quyền điều khiển máy tính của nhân viên tấn công vào các máy tính khác

31.Nhận định nào sau đây sai về rủi ro kiểm toán?

a) Rủi ro tiềm tàng và rủi ro kiểm soát càng cao thì rủi ro phát hiện theo chấp nhận được càng cao
b) Rủi ro tiềm tàng và rủi ro kiểm soát càng cao thì thủ tục kiểm toán càng tăng
c) Tăng thủ tục kiểm toán để giảm rủi ro kiểm toán

d) Rủi ro tiềm tàng và rủi ro kiểm soát càng thấp thì rủi ro kiểm toán càng thấp

32.Mục tiêu của hệ thống dấu vết kiểm toán?

a) Tái tạo lại sự kiện
b) Ghi nhận các nghiệp vụ kinh tế phát sinh tại doanh nghiệp
c) A và B đều đúng
d) Phát hiện các truy cập trái phép

33.Mục tiêu nào bên dưới không phải mục tiêu của hệ thống kiểm soát nội bộ?

a) Đo lượng sự tuân thủ với các chính sách và thủ tục quy định của ban quản lý
b) Giúp công ty quản lý chi phí hiệu quả
c) Bảo vệ tài sản của công ty
d) Thúc đẩy hiệu quả trong hoạt động của công ty

34.Kiểm soát rủi ro từ các cuộc tấn công DDOS?

a) Sử dụng tường lửa
b) Các câu trên đều đúng
c) Sử dụng phần mềm an ninh
d) Sử dụng hệ thống ngăn chặn xâm nhập (IPS) với tính năng kiểm tra gói chuyên sâu (DPI)

35.Nhận định nào sau đây là sai đối với kiểm toán nội bộ?

a) Kiểm toán nội bộ là một chức năng thẩm định độc lập để kiểm tra và đánh giá các hoạt động bên trong và như một dịch vụ cho một tổ chức
b) Kiểm toán nội bộ đánh giá các hoạt động liên quan đến kiểm toán tài chính, hoạt động, tuân thủ và gian lận của công ty
c) Kiểm toán nội bộ là kiểm toán độc lập về báo cáo tài chính và báo cáo cho ủy ban kiểm toán của ban giám đốc
d) Kiểm toán nội bộ do ban giám đốc lập nên

36.Nhận định nào sau đây là sai về các nguồn gây rủi ro về chương trình phá hoại cho hệ điều hành?

a) Cá nhân cố tình hay vô ý chèn virus và cá chương trình phá hoại vào hệ điều hành
b) Các cuộc tấn công DOS và DDOS vào hệ điều hành
c) Nhân viên lạm dụng quyền hạn
d) Các cá nhân duyệt qua hệ điều hành để xác định và khai thác các lỗi bảo mật

37.Thiết bị gọi lại là gì ?

a) Yêu cầu gửi các tin nhắn kiểm soát và phản hồi một cách ngẫu nhiên khiến kẻ xâm nhập khó vượt qua
b) Chèn một số thứ tựu trong mỗi tin nhắn để ngăn chặn các nổ lực xóa, thay đổi hoặc sao chép một tin nhắn
c) Yêu cầu người dùng quay số để nhập và mật khẩu được xác định
d) Ghi nhận tất cả các lần truy cập đã cố gắng với ID người dùng, thời gian truy cập và vị trí

38.Kiểm toán công nghệ thông tin?

a) Đánh giá mức độ đầy đủ của các kiểm soát nội bộ
b) Đánh giá mức độ đầy đủ của hệ thống ứng dụng đẻ đáp ứng nhu cầu xử lý
c) Đảm bảo rằng các tài sản được kiểm soát bởi các hệ thống đó được bảo vệ đầy đủ

d) Tất cả các ý đều đúng

39.Mục đích của ngôn ngữ báo cáo kinh doanh mở rộng (XBRL)?

a) Để chuẩn hóa các phương pháp cho chuẩn bị, công bố và trao đổi thông tin tài chính
b) Giúp cập nhật kịp thời các thông tin tài chính và kiểm soát nội bộ của doanh nghiệp cho nhà quản trị
c) Đảm bảo các báo cáo tài chính đều được trình bày trung thực và hợp lý
d) Tất cả các ý trên

40.Các cơ sở dẫn liệu đối với kiểm toán các khoản mục trên báo cáo tình hình tài chính?

a) Đầy đủ, quyền và nghĩa vụ, hiện hữu, chính xác, phân loại và trình bày
b) Đầy đủ, quyền và nghĩa vụ, đánh giá và phân bổ, hiện hữu, chính xác, phân loại và trình bày
c) Đầy đủ, quyền và nghĩa vụ, đánh giá và phân bổ, hiện hữu, chính xác, phân loại đúng kỳ và trình bày
d) Đầy đủ, quyền và nghĩa vụ, đánh giá và phân bổ, hiện hữu, phát sinh, chính xác, phân loại đúng kỳ và trình bày

41.Mục đích cảu ngôn ngữ báo cáo kinh doanh mở rộng (XBRL)?

a) Để chuẩn hóa các phương pháp cho chuẩn bị, công bố và trao đổi thông tin tài chính
b) Giúp cập nhật kịp thời các thông tin tài chính và kiểm soát nội bộ của doanh nghiệp cho nhà quản trị
c) Tất cả các ý trên
d) Đảm bảo các báo cáo tài chính đều được trình bày trung thực và hợp lý

42.Đánh số thứ tự tin nhắn là gì?

a) Ghi lại tất cả các lần truy cập đã cố gắng với ID người dùng, thời gian và vị trí
b) Chèn một số thứ tự trong mỗi tin nhắn để ngăn chặn các nỗ lực xóa, thay đổi hoặc sao chép một tin nhắn
c) Yêu cầu người dùng quay số để nhập và mật khẩu được xác định
d) Yêu cầu gửi các tin nhắn kiểm soát và phản hồi một cách ngẫu nhiên khiến kẻ xâm nhập khó vượt qua

43.Các rủi ro nào sau đây không phải rủi ro đối với hệ thống báo cáo tài chính?

a) Rủi ro không kiểm soát việc thu tiền của nhân viên bán hàng với khách hàng
b) Rủi ro truy cập trái phép vào sổ cái và thay đổi dữ liệu sổ cái
c) Rủi ro dấu vết kiểm toán bị lỗi
d) Rủi ro số dư sổ cái tài khoản thì không cân với tổng số dư các các sổ chi tiết của tài khoản đó

44.Mục tiêu nào sau đây là mục tiêu kiểm toán đối với các chương trình hủy hoại và virus?

a) Xác minh tính hiệu quả của các thủ tục kiểm soát để bảo vệ chống lại các chương trình độc hại và virus
b) Đảm bảo phần mềm duyệt virus được cập nhật và hoạt động hiệu quả
c) Đảm bảo các cá nhân không lạm dụng quyền hạn để cài các phần mềm độc hại vào hệ điều hành
d) Các câu trên đều đúng

45.Mục đích chính của kiểm toán độc lập?

a) Kiểm tra việc tuân thủ theo quy trình kiểm soát nội bộ
b) Thu nhập bằng chứng liệu báo cáo tài chính cso trung thực và hợp lý
c) Phát hiện sai sót và gian lận
d) Xác minh hiệu quả của hệ thống kiểm soát nội bộ

46.Dấu vết kiểm toán về giám sát các sự kiện là?

a) Tóm tắt các giao dịch phát sinh tại công ty
b) Ghi lại các lần gõ phím của người dùng và phản hồi hệ thống

c) Tóm tắt các hoạt động chính liên quan đến tài nguyên hệ thống
d) Tóm tắt các sự kiện bất thường phát sinh tại công ty

47.Mục tiêu kiểm toán đối với kiểm soát đe dọa lật đổ?

a) Xác minh các kiểm soát mạng đủ để duy trì tính toàn vẹn và bảo mật của dữ liệu
b) Xác minh tính bảo mật và tính toàn vẹn của các giao dịch
c) Các câu trên đều đúng
d) Xác định các kiểm soát mạng có thể ngăn chặn và phát hiện các truy cập bất hợp pháp

48.Các lỗi chuyển vị được kiểm soát bằng ?

a) Kiểm tra giới hạn
b) Kiểm tra tính hợp lệ
c) Các số kiểm tra (Check digits)
d) Kiểm tra dữ liệu bị thiếu

49.Kiểm tra tính hợp lệ như thế nào?

a) So sánh thực tế với các giá trị có thể chấp nhận được
b) Xác định dữ liệu ở dạng sai
c) Sử dụng để kiểm tra các khoảng trống
d) Kiểm tra số tiền vượt quá giới hạn cho phép

50.Thủ tục kiểm toán nào đây không phải thủ tục kiểm toán về kiểm soát hệ thống dấu vết kiểm toán?

a) Sử dụng các công cụ trích xuất dữ liệu để tìm kiếm các điều kiện xác định như: người dùng trái phép; thời gian không hoạt động; khoảng thời gian hoạt động bao gồm cả thời gian đăng nhập và đăng xuất; lần đăng nhập không thành công; và truy cập cụ thể
b) Xác minh dấu vết kiểm toán đã được kích hoạt theo chính sách công ty
c) Kích hoạt hệ thống dấu vết kiểm toán để phát hiện các truy cập trái phép, tái tạo lại sự kiện liên quan đến tài nguyên hệ thống
d) Lấy mẫu các trường hợp vi phạm bảo mật và đánh giá cách xử lý của chúng để đánh giá hiệu quả của nhóm bảo mật

51.Nhận định nào sau đây là sai?

a) Rủi ro tiềm tàng và rủi ro kiểm soát làm tăng mức độ của các thủ tục kiểm toán cần thiết để giảm rủi ro phát hiện xuống mức có thể chấp nhận được
b) Nếu rủi ro tiềm tàng và rủi ro kiểm soát thấp, kiểm toán viên cần ít thủ tục kiểm toán hơn
c) Rủi ro tiềm tàng và rủi ro kiểm soát cao, rủi ro phát hiện cần được giảm thông qua tăng các thủ tục kiểm toán
d) Nếu rủi ro tiềm tàng và rủi ro kiểm soát thấp, kiểm toán viên cần thực hiện nhiều thủ tục kiểm toán hơn