פתרון שאלה 1

סעיף 1

מטרת תקן ביקורת 94 הינה לקבוע כללים והנחיות לרואה החשבון המבקר כאשר הלקוח שלו משתמש בלשכות שרות. התקן מפרט אילו דוחות יכולים רואי החשבון של הגוף המבוקר לקבל מרואי החשבון של לשכת השרות.

על פי התקן המבקר נדרש לשקול כיצד השימוש של הגוף ה מבוקר בלשכת בהשרות משפיע על הבקרה הפנימית שלו כך שהמבקר יהיה מסוגל לזהות ולהעריך את הסיכון להצגה מוטעית מהותית ולתכנן ולבצע את נהלי ביקורת נוספים.

בסעיף 10 התקן קובע שעל המבקר להשיג ראיות אודות האפקטיביות של הבקרות וזאת כאשר רמת הסיכון של לשכת השרות גבוהה או כאשר הבדיקות המבססות אינן מספיקות . כדי להשיג ראיות ביקורת לגבי האפקטיביות של הבקרות ניתן לבצע את הבדיקות הבאות (חלקן או כולן):

1. בדיקת הבקרות של הגוף המבוקר על לשכת השרות.
2. קבלת דוח של ששל מבקר לשכת השרות המחווה דעה באשר לאפקטיביות הבקרה (TYPE B)
3. עריכת ביקור וביצוע בדיקות בקרה בלשכת השרות על ידי רואה החשבון המבקר.

בסעיף 18 התקן קובע כי כאשר רואה החשבון המבקר מתבסס על דוחות של רואה החשבון של לשכת השרות (הן מסוג א' והן מסוג ב') אסור לו להתייחס לכך בחוות דעתו.

סעיף 2

עובדים המקבלים שכר אינו תואם את מספר עובדי החברה בפועל.

שימוש בטכניקת ביקורת ישות דמה integrated test facility ITF אשר באמצעותה המבקר יוצר ישות ארגונית נפרדת המשולבת באופן שוטף בתהליך עיבוד הנתונים בארגון . דוגמאות לישויות דמה: חברה נוספת , סניף נוסף , עובד פיקטיבי , מחסן מלאי נוסף ,לקוח פיקט יבי, הודעות פיקטיביות.

המבקר מפעיל תוכנת ניפוי על מנת לוודא כי נתוני הניסוי לא נכללו בנתוני המקור . השיטה מאפשרת בחינה איכותית לאורך זמן של הפעילות ומאפשרת בחינה של הבקרות המפצות.

שיעור ההנחות הניתנות למספר לקוחות אינו תואם את מדיניות החברה

כריית נתונים (data mining) הינה שיטה מתקדמת לטיפול בכמויות גדולות של מידע דרכי פעולה אוטומטיים שהפעלתם מאתרת דפוסי התנהגות שלא היו ברורים מראש . תוכנת כריית נתונים משלבת מספר תחומים : זיהוי מאפיינ י בסיס, בנית מודלים שונים של שליפת נתונים , חיפוש ושליפת הנתונים בהתאם למו דלים שנבנו והצגה באמצעות גרפים . טכניקה זו מסייעת בשליפת נתונים ממגוון מאגר המידע (לא רק נתונים חשבונאיים) ויצירת קשרים בינהם.

באמצעות טכניקה זו ניתן לשלוף נתונים אשר יצליבו בין נתוני ההתקשרות ושיעור ההנחה שנקבע לבין שיעור ההנחה בפועל.

תוכנת מדף לביקורת - תוכנת המדף מספקת אפשרויות לגישה וביצוע פעולות על הנתונים הנשלפים מתוך מאגר הנתונים . באמצעות תוכנת הביקורת יכולים המבקרים לאסוף ראיות לגבי איכות הרשומים ביישומים . לתוכנות ביקורת יש גם נקודות תורפה . חסרונן העיקרי הוא שלא ניתן לבחון באמצעותן את איכות היישום עצמו. המבקר בודק את איכות הנתונים.

<u>פתרון שאלה מס׳ 2</u>

כחלק מתהליך הביקורת על המבקר צריך להעריך את מידת חשיבות זמינות ותיקון מערכות המידע הממוחשבות להפעלת הארגון. ישנם ארגונים שמערכות המידע הממוחשבות שלהן הינן קריטיות והכרחיות לפעילותם והשבתת מערכות המידע הממוחשבות שלהם עלולה לשתקם. מאידך, ישנם ארגונים בהם מערכות המידע הממוחשבות הינן פחות קריטיות והנזק הנובע מהשבתת שירותי המחשב הינו קטן יחסית.

להלן נהלי ביקורת מרכזיים לבדיקת תוכנית התאוששות מאסון (DRP):

- בדיקה שקיימת תוכנית התאוששות מאסון ערוכה בכתב ומעודכנת.
- בדיקה שהתוכנית אושרה על ידי גורם מוסמך.
- בדיקה שבעלי התפקידים הרלוונטיים מודעים לתכנים המצוינים בתוכנית להתאוששות מאסון.
- בדיקת קיומו של אתר חרום ומיקומו
- בדיקה כי נבדקה תקינות אתר החרום
- בדיקה שתוכנית ההתאוששות מאסון כוללת התייחסות לתקלות בזמן קצר ובזמן ארוך.
- בדיקה כי קיים ערך גיבויים של הנתונים והתוכנה (כולל שמירת גיבויים בכספות חסינות אש באתר הארגון וכן באתר מחוץ לארגון).
- בדיקה כי בוצע שיחזור מוצלח של גיבוי הנתונים והתוכנה.
- בחינת יכולת הארגון לטפל בתקלות של הטווח הקצר כגון: נפילת מתח, ניתוק ושיבוש בקווי התקשורת, ציוד קצה ותקלות בציוד המחשוב.
- בחינת קיומן של מתודולוגיות לטיפול באסונות , הן בקרותן והן בשלב הבא הכולל את הפעלת מהלך השיקום עד לחזרה לעבודה רגילה.

<u>פתרון שאלה מס׳ 3</u>

1. עם התפתחות הסחר האלקטרוני ניצבות בפני עולם המשפט סוגיות משפטיות חדשות שטרם נדרשו להתמודד עימן, על כן הוצעה הצעת חוק מסחר אלקטרוני התש״ח.
ההצעה נועדה לענות על שאלות כדלהלן:

- מניעת מחלוקות משפטיות בהעדר חיקוק

- האם חל צורך בשינוי אופן תיעוד עסקאות שלגביהן היום קיימת דרישה בכתב
- האם ניתן לתבוע בגין עוולות בנזיקין מסחר מסוג זה והאם קיימת אחריות צדדים שלישיים
- האם התקשרות טכנולוגית נחשבת כחוזה?
- היכן נכרת החוזה?
- מה נחשב הצעה ומה נחשב קיבול? האם כאשר הרוכש לחץ על "מקבל" בצג המחשב שלו, או כאשר היצרן/משווק קיבל את ההסכמה?
- מהי תקפות החתימה האלקטרונית?
- מה ההתייחסות לנפילות תקשורת?

2. <u>סיכונים במסחר באינטרנט</u>

כאמור בתקן ביקורת 95 סעיף 18 " ההנהלה ניצבת בפני סיכונים עסקיים רבים ,הקשורים לפעילויות הסחר האלקטרוני של הגוף המבוקר ,לרבות:

- פגיעה במהימנות העסקאות (integrity) ,אשר השפעתה עלולה לגדול עקב היעדר נתיבי ביקורת נאותים ,המתועדים על-גבי נייר או באמצעים אלקטרוניים.
- סיכוני אבטחה של סחר אלקטרוני ,לרבות התקפות וירוסים ופוטנציאל לתרמית מצד לקוחות ,עובדים ואחרים ,באמצעות גישה בלתי-מורשית.
- מדיניות חשבונאית בלתי הולמת ,הקשורה למשל להיוון הוצאות כגון ,עלויות פיתוח אתר אינטרנט ,הבנה שגויה של הסדרים חוזיים מורכבים ,תרגום מטבעות זרים ,הפרשות לאחריות או החזרות ,וסוגיות הכרה בהכנסה.
- אי-עמידה בדרישות מיסוי ודרישות חוקיות ופיקוח אחרות ,במיוחד כאשר עסקאות הסחר האלקטרוני באינטרנט מבוצעות בין מדינות.
- אי-יכולת להבטיח ,כי חוזים שנחתמו באמצעים אלקטרוניים בלבד הינם מחייבים.
- שימוש נרחב בסחר אלקטרוני ככלי לניהול מערכות עסקיות משמעותיות או ביצוע עסקאות אחרות באינטרנט.
- כשלים או" נפילות "של מערכות ותשתית.

<u>תשובה מס' 4</u>

<u>בקרות קלט במערכת "לקוחות"</u>

- שימוש בשדות חובה, כגון: תעודת זהות של המשקיע, מספר משקיע, כמות מניות, גובה ההוראה, מטבע ההוראה וכדומה.
- בחירה מרשימה (Combo box)- בחירת מספר משקיע, סוג נייר הערך, סוג מטבע מרשימה קיימת.
- בקרת סיפרת ביקרות - תקינות תעודת הזהות/ חשבון בנק של המשקיע.

- הקלדת תאריך ערך של העסקה בפורמט מוגדר DD/MM/YYY
- חסימת אפשרות להזנת הוראה כפולה.
- חסימת אפשרות להזרמת הוראה שלא בשעות פעילות הבורסה.
- חסימת הזנת לימיט שלא בהתאם לסוג נייר ערך הנבחר.

<u>תוכנית ביקורת למערכות המידע המעורבות בתהליכים:</u>

1. קבע את רמת סיכון הביקורת הנדרשת לדעתך ואמוד את רמת סיכון החשיפה לאור תוצאות הסקר על הבקרה הפנימית בו נאמדה רמת סיכון הבקרה והסיכון שבמהות.
2. בדוק את האם קיים תהליך מתן הרשאות מסודר למערכות המידע.
3. וודא שבוצעה סקירה תקופתית של מתן הרשאות על ידי גורם מוסמך.
4. וודא כי רק לדילרים קיימת הרשאה להזנת הוראות המשקיע (מערכת "לקוחות") ולשידור פעולות לבורסה (מערכת "עסקאות".
5. בדוק כי המתכנתים לא יכולים להזרים הוראות לבורסה, על ידי בדיקה האם קיימת להם גישה לסביבת הייצור.
6. בדוק כי קיימת הפרדת תפקידים בין העובד שמקים את המשקיע במערכת לעובד שמזרים את הוראות הקניה והמכירה לבורסה.
7. בדוק האם קיימים משתמשים גנריים (Super users, Administrators), וודא שהמשתמשים לא יכולים לבצע פעולות ברוקראז' עבור המשקיעים.
8. בדוק האם קיימת הרשאה למשתמשים להתחבר מרחוק (VPN או אופציה אחרת) למערכות.
9. בדוק כי אחת לתקופה מבוצעים ניסיונות חדירה למערכות.
01. וודא כי רק גורמים מורשים רשאים לגשת לחדר המחשב בו מאוחסנים שרתי המערכות.
11. בדוק האם קיימת מדיניות סיסמאות למערכות.
21. וודא שהסיסמאות שניתנו הן מורכבות.
31. בדוק כי קיימת מדיניות החלפת סיסמאות ברורה.
41. בדוק האם קיים נוהל גיבויים ושחזורים.
51. בדוק האם בוצעו גיבויים למערכות (בזמן אמת).
61. וודא שהגיבויים בוצעו בהצלחה על ידי סקירת לוג גיבויים.
71. בדוק האם בוצעו שחזורים לגיבויי המערכות.
81. וודא שהשחזורים בוצעו בהצלחה, במידה ולא קבל הסברים.
91. וודא כי קיימת תוכנית להתאוששות מאסון כתובה ומעודכנת.
02. בדוק האם קיימות בקרות סביב ממשק נתונים בין מערכת "לקוחות" למערכת "עסקאות".
12. בדוק באמצעות תוכנות ביקורת (ACL/ IDEA/SQL SERVER/ACCESS) שהוראות עברו בשלמות ובדיוק ממערכת ה"לקוחות" למערכת "עסקאות".
22. בדוק האם קיים צוות מקצועי האחראי לטיפול בתקלות במערכות.

32. בדוק האם במהלך שנת הביקורת היו תקלות במערכות. במידה וכן, ברר מתי וכיצד טופלו.
42. בדוק האם קיים נוהל ביצוע שינויים במערכות.
52. בדוק האם בוצעו שינויים במערכות במהלך שנת הביקורת.
62. במידה ובוצעו שינויים, בדוק האם הם אושרו על ידי גורם מוסמך.
72. במידה ובוצעו שינויים, בדוק האם בוצעו בדיקות QA ובדיקות קבלה על ידי המשתמשים.
82. בדוק כי השינוי בוצע בסביבת TEST.
92. סקור פרוטוקולים מישיבות דירקטוריון בהן דנו בשינויים/פיתוחים/תקלות במערכות המידע.
03. בדוק האם לא קיימים משקיעים כפולים במערכת "לקוחות".
13. בדוק האם עמלת הקניה/מכירה שנגבתה מהמשקיע היא בהתאם להסכם מולו.
23. בדוק האם בוצעו פעולות בסכומים חריגים. במידה וכן, וודא שאושרו על ידי גורם מוסמך.
33. בדוק כי סליקת כספי המשקיע בוצעה לחשבון העו"ש של המשקיע.
43. בדוק האם הועברו כספים לחשבון עו"ש של משקיע בהפסדים.
53. בדוק האם הועברו כספים לחשבונות עו"ש של הדילרים.
63. בדוק האם בוצעו פעולות שלא בשעות פעילות הבורסה.
73. בדוק האם הוזרמו הוראות כפולות.
83. בדוק האם קיימת מדיניות דיווח ל"רשות לאיסור הלבנת הון" בעסקאות בסכומים גבוהים (בהתאם לחוק איסור הלבנת הון וצו איסור הלבנת הון).
93. בדוק האם קיים קצין אבטחת מידע.

תשובה לשאלה מס' 9

נדרש 1. בדיקת איכות הבקרות הפנימיות הקיימות במערכת המלאי.

להלן עיקרי טכניקות הביקורת באמצעות מחשב (C.A.A.T's), המסיעות בבדיקת איכות הבקרות הפנימיות הקיימות במערכת המלאי:

	טכניקה	דוגמא ליישום הטכניקה
1.	שימוש בישות דמה (Integrated Test Facility).	הגדרת מחסן מלאי נוסף כישות דמה והזנה אליו של כניסות ויציאות של פריטים כדי לבחון האם המערכת מאפשרת לפריטים להיכנס ליתרה שלילית במחסן.
2.	יצירת סביבת טסט נפרדת לצורך הזנת נתונים לבדיקת הבקרה הפנימית.	הקמת פריט, הזרמת תנועות מלאי לפריט זה, ובדיקה האם המערכת מאפשרת לשנות את הגדרת יחידת המידה של הפריט במצב בו יתרת המלאי שלו חיובית.

נדרש 2. ביקורת בגישת בדיקות מבססות (בדיקת הנתונים)

להלן עיקרי טכניקות הביקורת באמצעות מחשב (C.A.A.T's), שניתן ליישמן בביקורת לקוחות חו"ל בגישת בדיקות מבססות:

	טכניקה	דוגמא ליישום הטכניקה
1.	שימוש בתוכנת מדף לביקורת.	ניתוח נתוני חשבוניות לאיתור הנחות חריגות שניתנו.
2.	סימולציה במקביל (Parallel Simulation) לצורך השוואה בין תוצאות חישוביות של התוכנה הנבדקת ע"י המבקר בהשוואה לתוצאות המתקבלות משימוש בתכנה אמינה אחרת.	בדיקת גיול חובות של הלקוחות.
3.	שימוש בתוכנת שירות לבדיקת איכות הנתונים.	הצלבה בין נתוני תעודות משלוח שהופקו ללקוחות לבין נתוני חשבוניות שהופקו על מנת לאתר ניפוקים שלא חויבו.
4.	שימוש בתוכנות לשליפה (SQL וכדי)	איתור מכירות שבוצעו לפריט מסוים בתחתך תאריכים מבוקש.
5.	תוכנות כריית נתונים	ביצוע שליפות בהסתמך על קשרים חריגים בין נתונים הן בבסיסי המידע בארגון והן בבסיסי מידע חיצוניים כגון מאגרים באינטרנט. לדוגמה: עריכת השוואה בין נתוני האשראי ללקוח, האופן בו פרע חובותיו לארגון בתקופות קודמות ומידע בדבר מצבו הכלכלי ויכולת החזר חובותיו בהסתמך על מאגרי מידע גלויים.

תשובה לשאלה מס' 9 - המשך

נדרש 3. בדיקת אבטחת מערכות המידע

להלן עיקרי טכניקות הביקורת שניתן ליישמן בבדיקת נאותות אבטחת מערכות המידע:

1. בדיקת יישום אמצעי אבטחה פיזיים למניעה, גילוי, תיעוד ותיקון של חשיפות. לצורך זה יקיים המבקר בירורים עם בעלי תפקידים שונים במערכות המידע ואצל המשתמשים, וכן יבצע תצפיות בחדר המחשב ובמקומות בהם נמצא ציוד פריפריאלי רלבנטי.

2. הדפסת פרופילי הרשאות וקודי משתמשים ששוייכו לכל פרופיל. בדיקה האם ההרשאות ניתנו בהתאם לסמכויות של המשתמשים השונים, ללא הרשאות עודפות.

3. בדיקת ניהול סיסמאות בגוף המבוקר. לצורך זה ישלוף המבקר פרמטרים רלבנטיים לאבטחת המידע ברמת הרשת וברמת האפליקציה, כגון: אורך הסיסמה, תדירות החלפתה, מורכבות הסיסמה (עירוב תווים אלפנומריים ונומריים ללא חזרה), שמירת סיסמאות היסטוריות לצורך מניעת השימוש החוזר בסיסמה, הגבלת מספר ניסיונות כושלים בעת הזנת סיסמה וכדי.

4. ניתוח פקודות יומן ידניות שהוזנו בסכומים חריגים, או בימים או בשעות חריגות.

5. עיון בסקר בטיחות וניסיונות חדירה שבוצעו ע"י מומחה מקצועי, לצורך הערכת האפקטיביות של אמצעים שננקטו.

6. בחינת קיומם של אמצעי אנטי וירוס, מסנני תוכן, מערכת לאיתור ניסיונות חדירה ו- Firewall בקישוריות שבין רשת החברה לאינטרנט.

7. בחינת קיומו של יומן אירועים (LOG), האופן בו הוא נבדק ובדיקת רישומים חריגים בו.

נדרש 4. בדיקת קוד המקור

מערכות המידע הממוחשבות בסביבת העבודה המבוקרת יכולות להיות כתובות בשפות פיתוח שונות. לכל שפה נקודות חולשה וחוזקה וכן סטנדרטים שונים לכתיבת הפקודות. לצורך בדיקת קוד המקור של התכניות הנבדקות, יש להכיר את שפת הפיתוח בה נכתבה המערכת הממוחשבת, יתרונותיה, חסרונותיה והסטנדרטים שנקבעו לפיתוח בשפה האמורה.

בדיקת קוד המקור אינה יכולה לעמוד בפני עצמה כטכניקת ביקורת, אולם עשויה לתרום במקרים מסויימים לשיפור איכות הבדיקה, לדוגמא: לצורך בדיקה של הגדרת תנאי שליפה של אוכלוסיה ספציפית. עם זאת, ברוב המקרים בדיקת קוד המקור אינה טכניקת ביקורת אפקטיבית וקיים ספק אם השקעת המשאבים בבדיקה זו תהיה בעלת תועלת העולה על עלותה.

בביקורת מערכות מידע מזווית ראות החשבון המבקר יש חשיבות רבה לביקורת הנתונים המהווים בסיס לנתוני הדוחות הכספיים. ביקורת קוד המקור כשלעצמה אינה מספקת בטחון מלא באשר לנאותות הנתונים, אלא מתמקדת בתהליכים, עיבודים ובקרות אפליקטיביות.