אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד א' – 24.02.10
ענת ארביב, רו"ח

פתרון מבחן בביקורת מערכות מידע ממוחשבות (ממ"מ)
(66-720-70)

משך הבחינה: שלוש שעות

הוראות לנבחן:

1. אין להיעזר בכל חומר שהוא מלבד גיליוי הדעת – 66, 93, 94, 95, 98 שניתן להכניס לבחינה. (ללא שום כיתוב עליהם מלבד סימון בטוש זוהר).
2. כתוב בדיו ובכתב יד ברור.
3. ענה על כל השאלות בצורה תמציתית וענייינית.
4. נמק את תשובותיך.
5. יש להחזיר את מחברות הבחינה בסוף הבחינה. את השאלון ניתן לקחת (בחינה לא חסויה).

רואה חשבון נתקל בעבודתו היומיומית בצורך להביע את דעותיו ומסקנותיו, לרבות בדוחות הנערכים על ידיו, בשפה ברורה וחד-משמעית. על אף שמטרתה הראשונית של בחינה זו היא לבחון את הידע של הסטודנט בביקורת מערכות מידע וביישום הנושאים שנלמדו בקורס, תובא בחשבון, בעת קביעת הציון, גם יכולתו של הסטודנט לארגן את מחשבותיו וידיעותיו ולהביען בצו רה ברורה ומסודרת.

בהצלחה !!!!

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד א' – 24.02.10
ענת ארביב, רו"ח

שאלה מספר 1 – 30 נקודות

משרדך משמש כרואה חשבון של חברת תהל (להלן: "החברה"). החברה עוסקת בייצור ומכירה של מוצרי טקסטיל לבית. החברה מייצרת ע"ב הזמנות מלקוחות מראש באופן הבא:

- לקוח פונה לחברה ומבצע הזמנה באמצעות הטלפון.
- מוקדן במחלקת ההזמנות מזין את ההזמנה ב מודול המכירות במערכת ה- ERP של החברה. מערכת שפותחה באופן עצמאי ע"י מתכנתים של החברה.
- ההזמנה נקלטת במחלקת הייצור לצורך ביצוע ההזמנה . המוצר נשלח ללקוח באמצעות שליח של החברה בצירוף של תעודת משלוח וחשבונית, אשר מופקים ממערכת המכירות.
- עם קבלת התשלום מהלקוח (לרב באמצעות כרטיס אשראי) מופקת קבלה מהמודול הפיננסי.

לאחרונה החברה החליטה ל העביר את שירות המענה הטלפוני לקבלת הזמנות מלקוחות לחברה חיצונית. החברה החיצונית תתממשק מרחוק למערכת ERP של החברה לצורך הזנת ההזמנות מלקוחות.

נדרש:

1. פרט את הסיכונים הפוטנציאליים הגלומים לדעתך במערכת של החברה. (5 נק')
2. לצורך ביצוע ביקורת על שלמות ההכנסות , פרט את טכניקות הביקורת בה תנקוט. (15 נק')
3. פרט את הבקרות אשר לדעתך צריכות להיות עם העברת מוקד ההזמנות לחברה חיצונית . (10 נק')

פתרון שאלה מספר 1 –

נדרש 1 –

סיכונים בפיתוח עצמי במערכת ERP:

- מכיוון שהמערכת אינה תוכנת מדף והיא פותחה באופן עצמי יתכנו שגיאות תוכנה (באגים).
- תיתכן מיעוט בבקרות אפליקטיביות (יישומיות) בשלב הקלט, העיבוד והפלט.
- תתיכן מיעוט באמצעי האבטחה שהוגדרו במערכת , כגון: ניהול הרשאות גישה וסיסמאות.
- תלות במתכנתים של החברה המבוקרת.

סיכונים עם העברת השירות לחברה חיצונית:

- ממשק לא מאובטח בין המבוקר לחברה החיצונית, לדוגמא חוסר ב-FW.

- סביבת בקרה לא נאותה בחברה החיצונית , לדוגמא אי ביצוע גיבויים באופן תקין , אבטחה פיזית לקויה, ניהול הרשאות גישה לקוי, סיסמאות אינן מורכבות ועוד.
- זליגת נתונים – גורם שאינו מורשה מצליח להגיע אל הנתונים.
- שינוי נתונים – גורם שאינו מורשה מצליח להגיע אל הנתונים המועברים בתקשורת ולשנותם.
- זיוף – גורן שאינו מורשה מצליח להוסיף נתונים.
- יציבות פיננסית של החברה החיצונית.
- שמירה על סודיות המידע המגיע לחברה החיצונית.

נדרש 2 –

שימוש בתוכנה ייעודית לביקורת כדוגמת IDEA לצורך ביצוע השוואת פרטי העסקאות שרשומות במודול התפעולי אל מול הרישום במודול הפיננסי . הבדיקה תאמת שכל עסקת מכירה שנרשמה במודול המכירות והופקה בגינה חשבונית תרשם בגינה פקודת יומן במודול הפיננסי . כמו כן, ניתן לבצע השוואה נוספת באמצעות תוכנה ייעודית לביקורת , לביצוע השוואת נתונים בין החשבוניות שהופקו לגביה בפועל (לקבלות שהופקו בעת קבלת תקבול).

נדרש 3 –

- Firewall
- מנגנוני הצפנה (סימטרית/א-סימטרית) עבור הנתונים המועברים בתקשורת.
- הגנה על קווי התקשורת בין המבוקר לחברה החיצונית מפני גישה פיזית.
- VPN (Virtual Private Network).
- יומן אירועים (LOG) המנהל רישום של כל הפעולות שביצעו משתמשי הקצה.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד א' – 24.02.10
ענת ארביב, רו"ח

שאלה מספר 2 – 40 נקודות

להלן פרוט של ארבעה אירועים בלתי תלויים שהתרחשו בחברות שונות , בהם נתקלת בעבודתך כרואה החשבון המבקר , במסגרת ביקורת מערכות מידע ממוחשבות כחלק מתהלך הביקורת של הדוחות הכספיים השנתיים :

1. חברת התבור הינה חברה מובילה במשק ליצור מזון . מערכת המלאי בחברה נבנתה במיוחד על ידי מומחים בתחום על מנת לעמוד בדרישות ניהול המלאי המחמירות שקבע מנהל החברה. בנוסף נבנה למערכת המלאי ממשק מיוחד למערכת ה נה"ח, תוכנת מדף פופולאריות, לביצוע הרישומים הכספיים של החברה.

2. רואה חשבון דובדבני התמנה למבקר "חברת אופקים " שהינה החברה הציבורית השניי ה בגודלה בארץ. מאחר ורו"ח דובדבני רצה לתת ערך מוסף רב לחברה הוא החליט כי הביקורת תבוצע אך ורק על ידי שימוש בטכניקות ביקורת ממוחשבות.

3. רואה חשבון ישראל ישראלי התמנה למ בקר של חברת נועה , חברה לייצור יהלומים. החברה משתמשת בשירותי חברת חלום לחישוב השכר . הרואה חשבון טוען שמכיוון שהוא לא הרו "ח של חברת חלום אין הוא צריך לבדוק את הבקרות בחברת אלא רק הבקרות בחברת נועה.

4. חברת תרגום הינה חברת כח אדם . לחברה יש עשרות מערכות לצורך הפעלת פעילותיה. רו"ח זיו טוען שאין הוא צריך לבדוק את מערכת דיווח שעות נוכחות ובדיקת מערכת השכר בהחלט מספקת לצורך מתן חוות הדעת.

פרט ונמק את ההשפעה אם קיימת של כל אחד מהאירועים והמצבים שפורטו לעיל על ביקורת מערכות המידע ממוחשבות במסגרת תהליך הביקורת של הדוחות הכספיים של החברות (כל סעיף יש להתייחס בנפרד).

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד א' – 24.02.10
ענת ארביב, רו"ח

פתרון שאלה מספר 2 –

נדרש 1 –

חברת תבור פיתחה באופן עצמי מערכת מלאי התואמת את צרכי החברה מערכת המלאי מתממשקת למערכת הכספים שינה תוכנת מדף לביצוע הרישומים הכספיים של החברה.

הוראות מס הכנסה (ניהול פנקסי חשבונות) התשל"ג 1973 כוללות במסגרת מערכת הספרים שעל הנישום לנהל, גם מערכות רישומיות הכוללות מידע ונתונים כמותיים על המלאי ועל תנועות בו, הזמנות מלאי ועוד. במקרה שלפנינו פתחה החברה מודל מיוחד למלאי אשר יענה לכל צורכי החברה וכן ממשק למערכת הכספים. שתי המערכות הללו נדרשות לעמוד בהוראות ניהול ספרים על מנת להיחשב כמערכות קבליות.

לפיכך, על המבקר במסגרת ביצוע הביקורת לקבל אישור תוכנה ממס הכנסה עבור מערכת הנה"ח שהינה תוכנת מדף ולבצע בדיקות מטעמו באמצעות שימוש בטכניקת ביקורת (Test Data) לבדיקה שאכן מערכת המלאי עומדת בהוראות ניהול ספרים.

מכיוון שמדובר במערכת מלאי, שפותחה באופן עצמי, המתממשקת למערכת הנה"ח, על המבקר לבצע ביקורת ממשקים, בדיקת שלמות הנתונים המועברים ממערכת המלאי למערכת הנה"ח.

נדרש 2 –

רואה חשבון דובדבני החליט כי הביקורת תבוצע אך ורק על ידי שימוש בטכניקות ביקורת ממוחשבות. תקן ביקורת 93 העוסק בהבנה של הגוף המבוקר וסביבתו והערכת סיכונים המתייחסים להצגה מוטעית מהותית מתייחס לנושא במספר סעיפים.

סעיף 61 לתקן מציין כי בקרות ידניות עשויות יותר להתאים כאשר נדרש להפעיל שיקול דעת ולנקוט באמצעי זהירות למשל בעסקאות גדולות בלתי רגילות שאינן חוזרות ונשנות, נסיבות בהן קשה לחזות טעות, נסיבות משתנות המחייבות בקרה ספציפית, מעקב אחר אפקטיביות של בקרות ממוכנות. סעיף 62 לתקן מציין כי בקרות ממוחשבות מסייעות בבחינת עסקאות בעלות היקפים גדולים אשר חוזרות על עצמן וניתן לבצע בקרה לתהליך הממוכן.

בהתאם רו"ח דובדבני נדרש לשקול האם השימוש בביקורת מערכות מידע בלבד יסייע לו בבחינת האפקטיביות של הבקרות והאם השימוש בבדיקות אלו נכון לכל הפעילות המבוצעת בחברה.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד א' – 24.02.10
ענת ארביב, רו"ח

נדרש 3 –

מאחר ומדובר בלשכת שירות יש לפעול ע"פ תקן ביקורת 94. 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 השרות 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 מבקר לשכת השרות המחווה דעה באשר לאפקטיביות הבקרה TYPE II.
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.

רו"ח דובדבני טועה בדבריו, במידה והוא לא מקבל דוח מסוג TYPE II, עליו לבצע בדיקות בקרה לצורך בדיקת אפקטיביות הבקרה גם בלשכת שירות.

נדרש 4 –

מאחר ומערכת השכר מתבססת על מערכת דווח שעות הנוכחות (שהינה מערכת כספית), יש צורך לבדוק גם את המערכת הזו ולא ניתן להסתמך על בדיקת מערכת השכר בלבד. כמו כן, מאחר ומדובר בחברת כוח אדם הרי שמדובר בסעיף מהותי. המסקנה היא שרו"ח זיו טועה בדבריו.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד א' – 24.02.10
ענת ארביב, רו"ח

שאלה מספר 3 – 20 נקודות

ענה בקצרה על כל אחד מהמושגים הבאים:

1. חתימה אלקטרונית מאובטחת.
2. Data mining כריית נתונים.
3. בקרות כלליות.
4. BCP/DRP.

פתרון שאלה מספר 3 –

נדרש 1 - חתימה אלקטרונית מאובטחת

באפריל 2001 קיבלה הכנסת את חוק חתימה אלקטרונית, התשס"א 2001, ומכוחו נחקקו בהמשך שנת 2001 גם שתי סדרות של תקנות. החוק קובע את חלוקת האחריות במקרים שונים בין החותם, המסתמך על החתימה והגורם המאשר שהנפיק את התעודה לחתימה האלקטרונית. מטרתו של החוק היא להתאים את הדינים הקיימים לעידן התקשורת המקוונת.

החוק מגדיר מונחים של "חתימה אלקטרונית", "חתימה אלקטרונית מאובטחת" ו"חתימה אלקטרונית מאושרת". חתימה אלקטרונית מאובטחת היא ייחודית לבעל החתימה, ומאפשרת את זיהויו, והופקה באמצעי חתימה הניתנים לשליטתו הבלעדית של בעל החתימה ומאפשרת לזהות שינוי שבוצע במסר לאחר מועד החתימה.

נדרש 2 - Data mining כריית נתונים

כריית נתונים הוא תהליך של ייצור יחסי גומלין בין חלקי הנתונים. טכניקה זו יכולה לנבא מגמות עתידיות והתנהגויות ומאפשרת לקבל החלטות עסקיות פרו-אקטיביות, מבוססות מידע. מטרת הכרייה היא חקר וניתוח הנתונים והמידע, מסביבות שונות, באמצעים אוטומטיים ככל שניתן, לצורך גילויים של דפוסים.

נדרש 3 - בקרות כלליות

הבקרות הממוחשבות יכולות להיות או יישומיות או כלליות. משמעותה של בקרה כללית הינה בקרה המשפיעה על שני יישומים לפחות (או יותר).

דוגמאות לבקרות כלליות

- בקרות על פיתוח ותחזוקת תוכנות (מדובר בבקרה כללית מכיוון שאם יש חולשה בבקרה על תהליך הפיתוח של התוכנות אזי כל תוכנה שתפותח יהיה בה את הליקוי).
- קובץ log/ קובץ אירועים של המערכת, זוהי בקרה כללית המתעדת את כל הכניסות של המשתמשים אל המחשב, תוך ציון שם המשתמש, שעת ההתחברות והקבצים והיישומים שאליהם הוא ניגש.

- אבטחה פיזית בחדר שרתים (הכניסה לחדר שרתים באמצעות תג עובד וממודרת לגורמים בלבד, UPS, מצלמות, מזגן, מטף כיבוי אש וכו').
- בקרת גישה – הרשאות גישה וניהול סיסמאות, על סיסמת הכניסה להיות מורכבת.
- הצפנות
- FW.
- DMZ
- VPN
- ביצוע גיבויים ושמירת הקלטות בכספת חסינת אש.
- נהלים בנושא מערכות מידע.

נדרש 4 –

תוכנית התאוששות מאסון היא תוכנית הכוללת תהליכים, מדיניות ונהלים המשמשים להתאוששות מאסון המשבית לזמן לא קצר את התשתית הטכנולוגית החיונית לפעילותו של ארגון.

מרכיבים אשר מומלץ לכלול במסגרת תוכנית להמשכיות עסקית:

1. המטרות, הדרישות והתוצרים של כל אחד משלבי התוכנית.
2. מתקנים חלופיים לביצוע המשימות והפעילויות.
3. משאבי מידע קריטיים, לרבות נתונים ומערכות.
4. כוח האדם האחראי להשלמת המשימות.
5. תזמון המשימות ותעדופן.
6. שמירת עותקים עדכניים מהתוכנית מחוץ לארגון.
7. התייחסות לאנשי מפתח ולהאצלת סמכויות, רשתות תקשורת וכיסוי ביטוחי.
8. גיבויים. התוכנית אמורה לכלול את הציוד הדרוש, על-מנת להמשיך בפעילות העסקית הקריטית.
9. ארגון והאצלת סמכויות
10. רשתות תקשורת מהוות רכיב חשוב ביותר בארגונים, ולפיכך יש ליתן עדיפות גבוהה ליישום נהלים באשר להשבת פעילותן. כמו-כן, רשתות תקשורת חשופות לסיכונים ייחודיים נוספים, כגון: שיבושים של נתיבים מרכזיים, חתכים בכבלי תקשורת, כשלים בתוכנות התקשורת, וסיכוני אבטחת מידע בתקשורת.

תוכנית לשעת חירום אמורה לטפל בתקלות קצרות טווח כגון:

- הפסקת חשמל.
- תקלות ציוד.
- תקלות תוכנה.

- אי תקינות הנתונים.

תוכנית לשעת חירום אמורה לטפל גם בתקלות ארוכות טווח ובמצבי אסון הגורמים להשבתה כוללת של שירותי מחשוב בארגון.
תוכנית החירום צריכה להיות ערוכה בכתב , מעודכנת, זמינה ומוכרת לבעלי התפקידים הרלוונטיים בארגון ורצוי שהארגון יתרגל עצמו למצב זה.
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 ע לולה לשתקם . מאידך, ישנם ארגונים בהם מערכות המידע הממוחשבות הינן פחות קריטיות והנזק הנובע מהשבתת שירותי המחשב הינו קטן יחסית.
ראשית, על המבקר לוודא כי קיים גיבוי מושלם של הנתונים והתוכנה (כולל שמירת גיבויים בכספות חסינות אש באתר הארגון וכן באתר מחוץ לארגון).
שנית, יש לבחון את יכולת הארגון לטפל בתקלות של הטווח הקצר כגון : נפילת מתח, ניתוק ושיבוש בקווי התקשורת, ציוד קצה ותקלות בציוד המחשוב.
לבסוף, יש לבחון את קיומן את מתודולוגיות לטיפול באסונות , הן בקרותן והן בשלב הבא הכולל את הפעלת מהלך השיקום עד לחזרה לעבודה רגילה.
היעדר תוכנית לשעת חירום מסודרת וכתובה אינו פוגע בשלמותם , אמינותם ודיוקם של הנתונים וכשלעצמו אינו משפיע על תהליך הביקורת או על עיתויה . היעדר תוכניות החירום בארגונים בהם הדבר קריטי צריך להיבדק כחלק ממכלול הסיכונים בפניהם ניצב הארגון ומהווה פגם במערך הבקרה הפנימית בתחום מערכות המידע הממוחשבות.

<u>שאלה מספר 4 – 10 נקודות</u>
ציין 10 הוראות ניהול ספרים הרלוונטיות לספר ראשי ממוחשב.

<u>פתרון שאלה מס' 4 –</u>
הפקה זמינה של פלט חזותי ופלט מודפס של כל רשומות הקובץ הקבוע או חלק מהן, לפי סדר רישומן, תוך ציון המספר העוקב של כל רשומה.

ציון הפרטים האלה בפלט חזותי ובפלט מודפס : שם הנישום, התקופה שאליה מתייחס הפלט, מהות הפלט, תאריך הפקת הפלט, מספר סידורי של כל דף וכן סימן סיום הפלט.

ציון בצורה בולטת של המלה "טיוטה" על גבי פלט חזותי או פלט מודפס, המופקים מקובץ זמני.

הפקת פלט מודפס של תיעוד פנים המפורט בפרק ב' מקובץ קבוע בלבד, בציון המלה "מקור" על גבי עותק אחד בלבד והמלה "העתק" על גבי העותקים האחרים.

<u>אוניברסיטת בר – אילן</u>
<u>ביקורת מערכות מידע ממוחשבות (ממ"מ)</u>
<u>סמסטר א' – מועד א' – 24.02.10</u>
<u>ענת ארביב, רו"ח</u>

בתוכנה לניהול מערכת חשבונות ממוחשבת המפיקה מסמכים ממוחשבים תתקיים שיטה לאיתור אותם מסמכים

מערכת חשבונות ממוחשבת, המפיקה תיעוד פנים, תצוייד במיתקן הגנה למקרה של הפסקת זרם החשמל

ינהל המבקש ספר כרוך של לקוחות שיכלול רשימה של רוכשי התוכנה ושוכריה (להלן - לקוחות), הכוללת, לגבי כל לקוח, שם, כתובת עסק, מספר הרישום כעוסק על פי חוק מע"מ ומספר הטלפון.

המנהל ינהל מרשם תוכנות לניהול מערכת חשבונות ממוחשבת המיועדות למכירה, להשכרה או לשימושו של אחר

המנהל ירשום תוכנה במרשם וישלח למבקש תעודת רישום, לאחר ששוכנע כי התקיימו הדרישות כאמור בפסקה הקודמת ; רישום כאמור יהא תקף עד תום שלוש שנות מס מהמועד שהופקה בו תעודת הרישום ;

המנהל יימנע מרישום תוכנה או יבטל רישומה, אם לדעתו קיים ספק סביר לגבי מידת עמידתה בדרישות הוראות אלה.

<u>בהצלחה.....לכולם.....נצמר !!</u>