

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

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

משך הבחינה : שלוש שעות

הוראות לנבחן :

1. אין להיעזר בכל חומר שהוא מלבד גילויי 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 ועניינית.
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 ידי, 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 וידעותיו ולהביען בצורה ברורה ומסודרת.

בהצלחה !!!!

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

שאלה מספר 1 – 30 נקודות

הנך רואה החשבון המבקר של חברת האלפים בע"מ. חברה המוכרת ציודי סקי ללקוחות בסיטונאות ובקמעונאות. החברה משתמשת במערכת SAP לניהול מרבית פעילותיה, לרבות: רכש, ניהול מלאי, מכירות והנהלת חשבונות. ניהול השכר לעובדי החברה מבוצע בתוכנת מדף לשכר.

נדרש 1:

פרט מהם החסרונות והיתרונות הקיימים במערכת SAP. (10 נק')

נדרש 2:

פרט את טכניקות ביקורת אשר לדעתך ניתן ליישם לצורך בדיקת איכות הבקורות הפנימיות הקיימות במודול לניהול המלאי. עבור כל טכניקת ביקורת, תן 2 דוגמאות לבדיקות. (10 נק')

נדרש 3:

פרט את טכניקות ביקורת אשר לדעתך ניתן ליישם לצורך בדיקת תקינות הממשק בין מערכת שכר לרישום בספרים במערכת הנהלת חשבונות. (10 נק')

פתרון שאלה מס' 1 –

נדרש 1 –

יתרונות מערכת SAP שינה מערכת ERP –

1. אינטגרטיביות – המערכת יוצרת אינטגרציה בין המחלקות ללא צורך בממשקים.
2. בסיס נתונים מרכזי אחד.
3. אמינות המערכת – המערכת מותקנת בארגונים רבים ברחבי העולם.
4. עדכניות הרישום בספרי החשבונות – הרישום בספרים מתבצע בדר"כ עם סיום הקלדת הפעולה העסקית.

חסרונות –

1. לוקליזציה – התאמה לדרישות בארץ.
2. קסטומיזציה – התאמה לצרכי הארגון.
3. תהליך ההטמעה – מע' ERP הינה מע' יקרה ותהליך ההטמעה עשוי להמשך זמן רב יחסית.
4. מורכבות המערכת – מקשה על המשתמשים בלימוד אחר תפעול המערכת, מהווה פוטנציאל לטעויות.

נדרש 2 –

טכניקות הביקורת שייסעו לי לבדוק את אפקטיביות הבקורות במערכת הינן:

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

1. Test Data – ניתן לבצע טסטים בסביבת הטסטים אשר מופרדת מסביבת הייצור לבדיקת, בין היתר, הבקורות הבאות : מלאי שלילי – המערכת לא מאפשרת להיכנס למלאי שלילי. תאריך קליטה – יש לבדוק שלא ניתן להזין תאריך קליטה עתידי , שדה התאריך בפורמט תקין והינו שדה חובה להזנה , לא ניתן להזין באופן ידני מק "ט אלא רק באמצעות בחירה מתוך רשימה (Combo BOX).
2. ITF(Integrated Test Facility) – ביצוע טסטים בסביבת הייצור אך על ישות דמה / מחסן מלאים דמה/ סניף דמה.

נדרש 3–

טכניקות הביקורת שייסעו לי לבדוק את תקינות הממשק בין מערכת שכר לרישום ב ספרים במערכת הנהלת חשבונות הינן :

1. תוכנה ייעודית לביקורת – יש לקבל נתונים הן ממערכת השכר והן ממערכת הנה "ח ולבצע השוואה בתוכנת הביקורת . יש לשלוף רשומות שקיימות במערכת השכר אך לא עברו למערכת הנה "ח, רשומות הקיימות במערכת הנה "ח אך לא קיימים במערכת השכר ורשומות שקיימות בשתי המערכות אך בסכומים שונים.
2. ITF – ניתן לבצע תסריט בדיקה שיכלול קליטת עובד ותנאי שכר במערכת השכר וקליטת הנתונים במערכת הנה "ח. נבדוק שהעברת הנתונים בוצעה בשלמות ונרשמה פקודת יומן תקינה.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
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 מתהליך הביקורת של הדוחות הכספיים השנתיים:

1. רואה חשבון מצליח התמנה השנה למבקר בחברת הצדפים שהינה חברה ציבורית המייצרת ומוכרת תכשיטים מצדפים. רו"ח טוען שאין צורך בביצוע סקר בקרה פנימית בסביבת מערכות מידע מכיוון שג"ד 66 כבר בוטל.
2. רואה חשבון דובדבני התמנה למבקר "חברת אופקים" שהינה החברה הציבורית השנייה 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 למבקר של חברת נועה, חברה לייצור יהלומים. החברה משתמשת בשירותי חברת חלום לחישוב השכר. לצורך ביצוע הביקורת השנתית, רואה החשבון קיבל מחברת חלום דוח סוג א' על התכנון והביצוע של בקרה פנימית.
4. מעיון בממצאי הדוח של המבקר הפנימי של החברה נמצא כי למתכנתים של מערכת SAP יש הרשאת גישה לסביבת הייצור לצורך נתינת הרשאות גישה לעובדים.

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).

פתרון שאלה מס' 2 –

1. ג"ד 66 אכן בוטל. תקן ביקורת 93 ו-98 החליפו את ג"ד 66 וג"ד 80 החל מה-1.1.2009. כחלק מתכנון הביקורת והכרת הגוף המבוקר, ע"פ תקן 93 יש לבצע סקר בקרה פנימית בסביבת מערכות מידע. בסקר בקרה פנימית רו"ח המבקר סוקר את המערכות שיש

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

בחברה והבקורות הכלליות הקיימות בארגון לרבות נהלים , אבטחת מידע, הרשאות גישה, סיסמאות, גיבויים, תהליך פיתוח וניהול שינויים ועוד.

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 בקורות ידניות עשויות יותר להתאים כאשר נדרש להפעיל שיקול דעת ולנקוט באמצעי זהירות למשל בעסקאות גדולות בלתי רגילות שאינן חוזר וות ונשנות , נסיבות בהן קשה לחזות טעות , נסיבות משתנות המחייבות בקרה ספציפית , מעקב אחר אפקטיביות של בקורות ממוכנות . סעיף 62 לתקן מציין כי בקורות 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 הבקורות והאם השימוש בבדיקות אלו נכון לכל הפעילות המבוצעת בחברה.

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 הבקורות וזאת כאשר רמת הסיכון של לשכת השרות גבוהה או כאשר הבדיקות המבססות אינן מספיקות. כדי להשיג ראיות ביקורת לגבי האפקטיביות של הבקורות ניתן לבצע את הבדיקות הבאות (חלקן או כולן):

1. בדיקת הבקורות 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.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

4. מתכנתים המורשים לגשת לסביבת הפיתוח אינם מורשים לגשת גם לסביבת הייצור .
יתרה מכך, מכיוון שתפקידם גם לתת הרשאות במערכת ה-SAP יש להם הרשאה רחבה מאוד בסביבת הייצור. כפי שמתואר קיימת פגיעה בעקרון הפרדת התפקידים . יש למנוע גישת מתכנתים לסביבת הייצור.

שאלה מספר 3 – 20 נקודות

ענה על כל אחד מהמושגים הבאים :

1. חתימה אלקטרונית מאושרת.
2. Data mining כריית נתונים.
3. בקורות יישומיות.
4. BCP/DRP.

פתרון שאלה מספר 3 –

נדרש 1 – חתימה אלקטרונית מאושרת

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.

חתימה אלקטרונית מאושרת הינה חתימה מאובטחת אשר יש לה תעודה של גורם מאשר – גוף רשמי שאושר על ידי שר המשפטים.

נדרש 2 – 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 – בקורות יישומיות

תקן 93 הגדיר את המונח בקרה יישומית - בקורות יישום הינן תהליכים ידניים או ממוכנים המופעלים בדרך כלל ברמה של תהליך עסקי. בקורות יישום עשויות להיות בקורות מונעות או

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

בקורות חושפות המיועדות לוודא את מהימנות הרישומים החשבונאיים. בהתאם לכך, בקורות יישום קשורות לתהליכי הייזום, הרישום, העיבוד והדיווח של עסקאות או מידע כספי אחר. בקורות אלו מסייעות להבטיח שהעסקאות שבוצעו הינן מאושרות ונרשמו ועובדו באופן מלא ובמדויק. דוגמאות לכך כוללות בדיקות של נתוני קלט ובדיקות של רצף אסמכתאות יחד עם מעקב ידני על דוחות חריגים או תיקון במועד הזנת הנתונים.

נדרש 4 – BCP/DRP

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.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

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 עלולה לשתקם . מאידך, ישנם ארגונים בהם מערכות המידע הממוחשבות הינן פחות קר יטיות 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.

אוניברסיטת בר – אילן
ביקורת מערכות מידע ממוחשבות (ממ"מ)
סמסטר א' – מועד ב' – 21.03.10
ענת ארביב, רו"ח

שאלה מספר 4 – 10 נקודות

הנך רואה החשבון המבקר של חברת סחר בע "מ. החברה, לאחרונה, הרחיבה את פעילות המכר שלה גם באמצעות האינטרנט. לקוחות החברה יכולים כעת לרכוש מוצרים של החברה דרך אתר האינטרנט. פרט את הסיכונים שאתה כרואה חשבון היית מזהה כתוצאה מחרבת הפעילות והמלץ לחברה מנגנוני בקרה שיכולים למזער את הסיכונים.

פתרון שאלה 4 –

תקן ביקורת 95 דן בנושא של סחר אלקטרוני המפרט את הסיכונים ואמצעים להתמודדות עם הסיכונים.

זה/זה.....לחבר !!