<u>אוניברסיטת בר – אילן</u>
<u>ביקורת מערכות מידע (מ״מ)</u>
<u>סמסטר ב׳ – מועד ב׳ – 11.08.08</u>
<u>אייל אסייג, רו״ח</u>

מבחן בביקורת מערכות מידע (מ״מ) (71-720-66)

משך הבחינה: שלוש וחצי שעות

הוראות לנבחן:

1. אין להיעזר בכל חומר שהוא מלבד גיליויי הדעת – 66, 93, 94, 95 שניתן להכניס לבחינה – **<u>ספר בלבד</u>** (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 בצורה ברורה ומסודרת.

בהצלחה !!!!

אוניברסיטת בר – אילן
ביקורת מערכות מידע (מ״מ)
סמסטר ב׳ – מועד ב׳ – 11.08.08
אייל אסייג, רו״ח

שאלה מספר 1 – 25 נקודות

הינך משמש כרואה חשבון המבקר של חברת בוק בע״מ המפעילה רשת חנויות לספרים הפרוסות ברחבי הארץ (להלן החברה). בנוסף לשירות הניתן בחנויות, מפעילה החברה אתר אינטרנט , שבאמצעותו ניתן לראות , להבין ולרכוש ספרים בחנות הוירטואלית של החברה . לאחר פעולת הקניה וביצוע התשלום בגינה, דואגת החברה לשלוח את הספרים לבית הלקוח.
הקניות באמצעות אתר האינטרנט, נעשות ללא מסמכים חתומים.

לקוחות אשר אינם מעוניינים לקנות ספרים באמצעות אתר האינטרנט, יכולים לקנותם באמצעות השירות הטלפוני של החברה, או לחליפין לקנותם בדרך הרגילה בחנויות.

נידרש:

א. פרט את החשיפות והסיכונים שבפניהם ניצבת החברה כתוצאה מקניות באמצעות אתר האינטרנט, בהשוואה לקניות בחנויות. (5 נקודות)

ב. פרט והסבר מה הן הבקרות שהיית מצפה למצוא בחברה במטרה להקטין את החשיפות הקיימות כתוצאה מהקניות באמצעות האינטרנט כאמור בסעיף א׳ לעיל (5 נקודות)

ג. פרט והסבר באילו טכניקות ביקורת באמצעות מחשב (CAAT's) תשתמש על מנת לבדוק את המהימנות (Integrity) של העסקאות המתבצעות באמצעות אתר האינטרנט . (5 נקודות)

ד. הסבר ונמק האם ניתן לוותר על בדיקת ערוץ המכיר ות באמצעות אתר האינטרנט של החברה, אם מכירות אלה יהוו רק 6% מסכום המכירות הכולל של החברה. (4 נקודות)

ה. הסבר את המושגים הבאים, הצג את הסיכונים בכל מושג והסבר כיצד משפיע הסיכון על נוהלי הביקורת. כל מושג 2 נק׳:

1. ISP מול ASP
2. רציפות תהליכים באתר סחר אלקטרוני
3. Non- repudiation

אוניברסיטת בר – אילן
ביקורת מערכות מידע (מ"מ)
סמסטר ב' – מועד ב' – 11.08.08
אייל אסייג, רו"ח

פתרון שאלה 1

נדרש א – החשיפות והסיכונים העיקריים בקניות באינטרנט

1. כשלים אפשריים בזיהוי ואימות לקוחות
2. פגיעה במהימנות העסקאות עקב העדר נתיבי ביקורת נאותים ומתועדים כתוצאה מהעדר בקרות קלט ו/או עיבוד מספקות
3. אפשרות למחלוקת על תנאי הסחר , לרבות העד ר אפשרות לעריכת שינויים בהזמנה , לאחר שנקלטה ולפני משלוחה ללקוח
4. סיכוני אבטחת מידע המצוי במאגרי המידע הממוחשבים , לרבות: גישה בלתי מורשית להשגת פרטים על לקוחות, אמצעי התשלום שלהם, חשיפת המידע בפני מתחרים ועוד.
5. חשיפה לכשלים או נפילות של האתר , עקב תקלות טכניות , התקפות האקרים לסתימת האתר, התקפות וירוסים / תולעים לשם שיבוש האתר או הריסתו.
6. חדירה דרך אתר האינטרנט של החברה למערכות מחשב האחרות שלה כתוצאה מליקויים בהגנת הממשק שבין אתר האינטרנט לבין רשת החברה (ליקוי ב- FW ובחיבורי ה- DMZ)

נדרש ב – הבקרות העיקריות להקטנת החשיפות והסיכונים העיקריים בקניות באינטרנט

1. קביעת מדיניות ברורה של הנהלת החברה בכל הקשור למכלול נושאי טכנולוגיית מידע של האתר, לרבות בסוגיות חוק ופיקוח ואבטחת מידע
2. פיקוח ובקרה של דירקטוריון החברה על מדיניות ההנהלה בכל הכרוך בהפעלת אתר האינטרנט לרבות: מדיניות ניהול טכנולוגיות המידע , אבטחת מידע , עקרונות גיבוי והתאוששות האתר ועל מערכות מידע אחרות
3. שימוש אפקטיבי בטכנולוגיות של חומות אש (Firewall ו- DMZ), מסנני תוכן (Content-Filtering), מערכות לאיתור ניסיונות חדירה (Ids), תוכנות אנטי וירוס וכל זאת בשביל להגן על אתר האינטרנט ועל מערכות מידע אחרות.
4. שימוש אפקטיבי בהצפנת התשדורות בין הלקוחות לבין מחשב החברה וקיום בקרה ושמירה על מפתחות הפענוח וההצפנה.
5. מעקב שוטף של גורמי אבטחת המידע אחר שינויים טכנולוגיים באתר , ושינויים תוכניים במערכות המידע עצמן, ובדיקה כי שינויים אלו לא פגעו באבטחת המידע של האתר
6. עריכת סקר בטיחות תקופתי של האתר על ידי מנהל אבטחת המידע , לבדיקת האפקטיביות של אמצעי הבקרה , לצורך איתור ליקויים , הסקת מסקנות והמלצות לשיפורים.
7. ייזום ניסיונות חדירה מבוקרים על ידי מנהל אבטחת מידע (עם או ללא סיוע מגורמי ם חיצוניים), במטרה לוודא את איכות אבטחת המידע הלכה ולמעשה

8. בדיקת נתיבי הביקורת של כל הפעילות המבוצעת באתר , כולל ביצוע הזמנות ושינויים בפרטי ההזמנות
9. בדיקת אישורים לביצוע שינויים אדמיניסטרטיביים , כולל שינויים בסיסמאות וכן שינויים בהזמנות ישלחו במייל ללקוחות
01. קביעת קריטריונים לאישור פרטי עסקאות על ידי גורם נוסף לפני ביצוען על ידי מחלקת המשלוחים.

נדרש ג – טכניקות ביקורת עיקריות באמצעות מחשב לבדיקת מהימנות העסקאות באינטרנט

1. בבחינת מהימנות בקרות הקלט והעיבוד רצוי להשתמש בעיקר בטכניקות המאמתות את קיום הבקרות. טכניקות אלו כוללות הזרמה של עסקאות בסביבת דמה (Test Data), תוך מעקב אחר התהליך המלא של העסקה, ובדיקת קיום בקרות ונתיבי ביקורת לעסקה, או לחליפין, ביצוע בדיקות בסביבת העבודה החיה , אלא שאז קיימת הגבלה לבדיקה של עסקאות אשר בוצעו בפועל של ידי לקוחות וחשש לשיבוש הנתונים החיים.
2. בדיקת היבטי אבטחת מידע הקשורים למהימנות העסקאות על ידי עיון בסקרי סיכונים ובתוצאות מבחני החדירה אשר נערכו על ידי הארגון , וכן על ידי שליפת דוחות מתוך המערכות השונות, לרבות ה- LOG מחומת האש, ממסנני התוכן ומהמערכות לאיתור ניסיונות חדירה.
3. סקירת נ תוני תקלות שנרשמו ביומן מערכת (LOG) לרישום תלונות של לקוחות באמצעות חישובי ממוצעי סוגים של תקלות , התקנת "סוכנים" – Agents של מערכות לכריית נתונים לשם איסוף נתונים ומגמות על סוגי תקלות או כמעט טעויות ועוד .

נדרש ד – וויתור על בדיקת ערוץ המכירות באמצעות אתר האינטרנט

לא ניתן לוותר על בדיקת ערוץ המכירות באמצעות אתר האינטרנט של החברה , וזאת מהנימוקים הבאים:

1. ערוץ המכירות באמצעות האינטרנט אינו שולי , ומהווה כ- 6% ממחזור המכירות הכולל של החברה ויתכן ותהייה לו השפעה מהותית על הדוחות הכספיים
2. ערוץ המכירות באמצעות האינ טרנט יוצר חשיפות לסיכונים רבים יחסית לערוצי המכירות הרגילים האחרים (ראה סעיף 1 לעיל)

בסעיף 5 בג"ד 86 בדבר מהותיות בביקורת נאמר כדלקמן: " בתכנון הביקורת המבקר קובע רמה כמותית של מהותיות שתהא מקובלת על מנת לאתר הצגה מוטעית מהותית . עם זאת יש צורך לשקול את הס כום (כמות) והאופי (איכות) של הצגה מוטעית .... ". לא צוינו בגילוי הדעת הנחיות כמותיות ואיכותיות ברורות. חשיפתו של אתר האינטרנט והסיכונים המובנים בו מהווים שיקול איכותי של השפעה מטעה מהותית מעבר להיבט הכמותי.

נדרש ה– הסבר המושגים

סעיף 1 - ISP מול ASP

הסבר המושגים: כאמור בסעיף 16 לג"ד 95, ISP- Internet Service Provider – הינם ספקי שירותי גישה לאינטרנט , ו- ASP – Applications Service Provider – הינם ספקי שירותי יישום.ISP מאפשר חיבור לקוחות לרשת האינטרנט ואילו ASP מספק שירותי יישומים (כמו קופות רושמות, מערכות לניהול מלאי, נוכחות ועוד) וזאת באמצעות השכרת התוכנה בלא הצורך בקנייתה באמצעות האינטרנט.

יתרונות בולטים : ASP - חסכון בעלויות רכישת תוכנות , ניהולם ותחזוקתם, ISP – שרתי ה-WEB שלו מבטיחים רמת אבטחה ושרידות גבוהים.

חסרונות בולטים : המידע בשירותי ASP של הח ברה נמצא אצל ספק היישום ותלוי ברמת הבקרה הפנימית של ספק היישום, ספק ה- ISP מכיר את חיבורי האינטרנט של החברה

השפעה על נוהלי הביקורת : מכיוון שגם ה- ASP וגם ה- ISP הם ספקי מיקור חוץ , אזי על פי ג"ד 95 ס' 17, יש לבחון את "... מדיניות, נהלים ורישומים שונים, המשמשים את ספק השירות... ", כלומר על המבקר להכיר ".. לשקול את הסדרי מיקור החוץ , כדי לזהות כיצד הגוף המבוקר מגיב לסיכונים הנובעים מהפעילויות שהועברו למיקור חוץ " – משמעות הדבר , לבחון הן את הסיכון בכישלון השירות הניתן וכן את סוגית אבטחת המידע הנמצא אצל ספק מיקו ר החוץ.

סעיף 2 - רציפות תהליכים באתר סחר אלקטרוני

הסבר המושג: כאמור בסעיף 31 לג"ד 95, " רציפות התהליכים מתייחסת לדרך שבה טכנולוגיות מידע משתלבות זו בזו, וכתוצאה משילוב זה פועלות למעשה כמערכת אחת . ..." כלומר, בסביבה של סחר אלקטרוני, רציפות התהליכים מתייחסת לדרך שבה המידע זורם "מקצה לקצה" כלומר מאתר האינטרנט למערכות הפנים ארגוניות.

סיכונים בולטים : במידה וחלק מהמידע אובד, תהייה פגיעה בשלמות נתוני הדוח הכספי , במידה והמערכות לא עובדות באופן מסונכרן , יתכנו מצבים של שיבוש המידע שיגרום לפגיעה באמינות המידע (Integrity).

השפעה על נוהלי הביקורת : על פי ג"ד 95 ס' 32- 33, יש לבחון את "... שלמות ודיוק עיבוד העסקאות ואיחסון המידע , עיתוי ההכרה בהכנסה ממכירות ... (שיבושים ברישום התקופה החשבונאית – א.א), ... אמצעי הבקרה המפקחים על שילוב עסקאות הסחר האלקטרוני .. " כלומר במסגרת הביקורת יש לבחון את שלמות העסקאות , עיתויי ההכרה בהכנסה ואת הבקרות

המפקחות על מעבר מידע מאתר הסחר אל המערכות הפנים ארגוניות . בדיקת היבטי אבטחת מידע הקשורים למהימנות העסקאות על ידי עיון בסקרי סיכונים ועוד.

סעיף 3- non repudiation

הסבר המושג: כאמור בסעיף 19 לג"ד 95, על הגוף המבוקר להוסיף אמצעים שנועדו " .. להשיג הסכמה על תנאי המסחר , לרבות הסכמה על תנאי המשלוח ותהליכי יישוב מחלוקות , העשויים לעסוק במעקב אחר עסקאות , ונהלים שיבטיחו שמי מהצדדים לעסקה לא יוכל לאחר מכן להכחיש את מתן הסכמתו לתנאים שסוכמו (נהלי אי הכחשה – non repudiation) . "

סיכונים בולטים : באינטרנט בחנות הוירטואלית , בניגוד לחנות הפיזית , הקונה לא רואה ומדבר עם המוכר. כל העסקה נעשית באמצעות תקשורת מחשבים בין קונה לבין מערכת מחשב – אתר האינטרנט. מצב זה יכול ליצור מחלוקות ואי הבנה מצד הקונה או מצד המוכר . לכן דורש גילוי הדעת להוסיף אמצעים שיבטיחו שמה שסוכם באתר האינטרנט יחייב את הקונה כך שלא יוכל להתכחש (שימוש במפתחות פרטיים וציבוריים וזאת על ידי יישום טכנולוגית ה- PKI)

השפעה על נוהלי הביקורת : על פי ג"ד 95 ס' 26 קובע שמידע יחשב כמאובטח רק אם תשתית האבטחה בגוף המבוקר תבטיח בין היתר , נוהלי אי הכחשה . (היא צריכה להבטיח גם דרישות הרשאה, אימות זהות , חיסיון, מהימנות, אי הכחשה , זמינות). במידה והבקרה הפנימית לא מבטיחה שהמידע יחשב כמאובטח , הרי שמדובר בליקוי בבקרה הפנימית שיש לפצותו על ידי בדיקות מבססות באתר האינטרנט למשל על ידי הורדת קבצי במכירות וניתוחם באמצעות תוכנות ביקורת כגון ACL.

שאלה מספר 2 – 30 נקודות

הינך רואה חשבון של חברת מאי בע "מ החל משנת 2002. לחברה יש מערכת לניהול מלאי . מידי חודש לאחר ספירת המלאי וניתוח ההפרשים , מועברת פקודת יומן אוטומ טית לעדכון המלאי בהנה"ח כך שיתאים לתוצאות הספירה בפועל.

נדרש:

א. בהנחה שבחרת להשתמש בטכניק ת ביקורת של ניסוי מבחן לביצוע בדיקת העברת הנתונים ממערכת המלאי למערכת הנהלת החשבונות, ציין את היתרונות והחסרונות של השימוש בסוג בדיקה זו. (5 נקודות).

ב. בהנחה שבחרת להשתמש בטכניקת ביקורת של תוכנת מדף לביקורת מסוג IDEA לביצוע בדיקת העברת הנתונים ממערכת ה מלאי למערכת הנהלת החשבונות , ציין

את היתרונות והחסרונות של השימוש בסוג בדיקה זו ופרט את ההבדלים בין תוכנת ביקורת לניסוי מבחן. (9 נקודות).

ג. מנהל הכספים של החברה פנה אליך שתסייע לו למציאת תוכנה חדשה שתחליף את תוכנת המלאי הקיימת בחברה לאור גידול במספר פריטי המלאי. תאר את השלבים בבחירת תוכנה חדשה וציין את תפקידך כמבקר בכל שלב. (16 נקודות).

<u>פתרון שאלה מספר 2</u>

<u>נדרש א'</u>

הדרך ליישום שיט ת נתוני מבחן היא באמצעות הקמת סביבת טסט , העתקת סביבת הייצור אל הטסט, הזרמת נתונים ידועים ממערכת ה מלאי אל מערכת ה נה"ח ובדיקה כי נתונים אלו הגיעו כהלכה להנה"ח. שיטה זו היא הפחות מומלצת , זאת מכיוון שהבדיקה בוחנת את תקינות תוכנת הממשק ולא את תקינות הנתונים שזרמו בפועל במערכת האמיתית.

יתרונות בשימוש ב נתוני מב חן : בדיקת הממשק בסביב ת ניסוי בקלות יחסית על ידי הזרמת תנועות ידועות למלאי ובדיקה כי הגיעו בהצלחה להנה"ח, בדיקת מנגנוני הבקרה הקיימים לרבות הרשאות וסיסמאות, מתן סביבה לביצוע בדיקות סבירות, גלישה (Overflow), עומסים וכו'

החסרונות הבולטים : הנתונים המוזרמים (מדגם) אינם בהכרח מייצגים את כל אפשרויות הנתונים.

<u>נדרש ב'</u>

בטכניקת ביקורת מסוג שימוש בתוכנת ביקורת IDEA הבדיקה בדרך כלל יותר רחבה . בשיטה זו נבדוק את הממשק לא על ידי הזרמת נתוני מבחן שהם במהותם מדגם , אלא על ידי בדיקת כמות רבה של נתונים שזרמו **בפועל** ולא מדגם ממערכת המלאי אל הנה"ח.
היתרון הגדול של שימוש בתוכנת ביקורת זה התגברות על החיסרון הבולט שפורט בנדרש א , כלומר ה- IDEA מאפשר בדיקה של תקופה ארוכה במערכת, על כל הנתונים שזרמו, כלומר בדרך זו מכסים את רוב סוגי הטעויות האפשריות ולא רק ברמת היתכנות , אלא הלכה ולמעשה האם באמת היו טעויות בממשק , מהו סכומם ובאיזה עיסקה זה קרה . בנתוני מבחן אנו בודקים את הבקרות במערכת ולא את הנתונים שזרמו הלכה למעשה.

<u>נדרש ג'</u>

השלבים בבחירת תוכנה חדשה :

שלב הייזום – שלב הייזום כולל שכנוע ההנהלה הבכירה בדבר הצורך בהחלפת מערכת , ביצוע הגדרת דרישות עיקרית (ברמת על). במידה וההנהלה שוכנעה עוברים לחקר ישימות שבו בוחנים היתכנות כלכלית (מבחן עלות תועלת הכולל - הפצת RFP לבתי תוכנה ולמחלקת ה- IT בחברה,

סקירת עלויות התוכנות הקיימות , בדיקת ROI של המערכת) וכן בחינת היתכנות טכנולוגית וארגונית. לאחר קבלת אישור מההנהלה להמשך הפרויקט ובחירת החלופה הרלוונטית (רכש או פיתוח – make or buy) פועלים כך :

- אם הוחלט על רכש תוכנת מדף – שלב הבניה מצטמצם רק לפיתוח נהלים לתהליכים העסקים, במידה ונדרש (אם המערכת החדשה תחייב שינוי בתהליכי עבודה – יש לכתוב נוהל עבודה חדשה), בשלב היישום – הדרכה על המערכת החדשה , ביצוע הסבה לפי שיטות ההסבה המקובלות (עם טיוב או בלעדיו , הסבת חלוץ – pikot, בדיקת מועד ההסבה הצפוי, שיטת תיעוד ההסבה ועוד) וביצוע בדיקות קבלה על ידי המשתמשים . כל התהליכים עד עתה (הגדרה, בניה ויישום) בוצעו בסביבת טסט. במידה והמערכת החדשה עברה בהצלחה את כל השלבים , היא מועברת אל סביבת הייצור (שלב התחזוקה) שם המערכת תהיה מרבית חייה, שם נבצע את ביקורת מערכות המידע עד אשר המערכת כבר לא תענה על צרכי המשתמשים ויהיה צורך לסיים את חייה ולהתחיל מחזור חיים חדש .
- אם הו חלט על פיתוח עצמי – מה שמתווסף לפסקה הקודמת זה שבשלב הבניה המתכנתים כותבים את תוכניות המחשב של המערכת החדשה וזאת בהתאם לנוהלי פיתוח ותחזוקה (אישור מנהל IT, הכנת מסמכי אפיון ועיצוב על ידי מנתח מערכות , פיתוח תוכנה על ידי מתכנת , ביצוע בדיקות Unit & Integration Tests, ביצוע אותם בדיקות על ידי מתכנת אחר, בדיקות קבלה על ידי משתמשים, אישור QA).

לגבי תפקיד רו"ח המבקר- על המבקר , בכל מצב , להקפיד שהייעוץ שינתן לחברה לא יפגום ביכולת שלו לבצע ביקורת עליה, ולא יפגע באי תלות ו. בעבודת הייעוץ יקפיד להציג את האפשרויות השונות והחברה היא זו שתבחר את האפשרות , כך שהמבקר לא יהיה מעורב בקבלת החלטות עסקיות ויתמקד בהיבטי הבקרה בלבד במערכת.
רו"ח מבקר **לא יהיה** מעורב ב : חקר ישימות (קבלת החלטות עסקיות) , עיצוב ותכנות (בשני תהליכים אלה למעשה בונים את המערכת ולכן אסור לרו "ח שתהיה מעורב ות), פיתוח נהלים . בשלבים אלה מקבלים החלטות עסקיות , בונים את המערכת וקובעים את נוהלי התהליכים העסקיים החדשים . כל הנושאים הללו יבדקו על ידי רואה החשבון במהלך הביקורת ולכן עליו להימנע מלהיות מעורב בהם מכיוון שזה עלול ליצור ניגוד ענינים . בכל יתר שלבי מחזור החי ים יכול רו"ח המבקר להיות מעורב (במגבלות שפורטו)

אוניברסיטת בר – אילן
ביקורת מערכות מידע (מ"מ)
סמסטר ב' – מועד ב' – 11.08.08
אייל אסייג, רו"ח

שאלה מספר 3 – 10 נקודות

החברה אותה אתה מבקר משתמשת ב מיקור חוץ הניתן על ידי בית תוכנה חיצוני לתמיכה במערכת השכר, ענה על השאלות הבאות:

1. פרט את היתרונות והחסרונות של מיקור החוץ על החברה. (6 נקודות)
2. הסבר מה הה שלכות של מיקור החוץ על עבודת הביקורת ועל חוות דעת רואה החשבון המבקר, כאמור בגילוי דעת 94. (4 נקודות)

פתרון שאלה מספר 3

1. כאמור בג"ד 94, משמעות המושג מיקור חוץ הוא רכישת שירותים לתאגיד מחברות חיצוניות לו, המתמחות במתן שירותים מקצועיים כתחליף לגיוס , הכשרת והרחבת כוח האדם ב תאגיד. שימוש בשי רותי Outsourcing הנה תפיסה ניהולית ההולכת ומתפתחת בשנים האחרונות הקובעת כי על התאגיד להתרכז ולהתמקד בתחומי פעילותו העסקית העיקרית ("ליבת העסק") ולא בתחומים שאינם בליבת הפעילות, שאותם בד"כ נוציא למיקור חוץ.

יתרונות בולטים: חסכון בעלויות ע "י השגת חלופות זולות (לרבות חסכון בעלויות הכשרה ולימוד), ניצול ניסיון (לרבות בניהול סיכונים) קיים במקום למידתו וצבירתו , מניעת יחסי עובד מעביד, שמירה על חדשנות טכנולוגית ועוד.

חסרונות/סיכונים בולטים: שיתוף גורמים זרים במידע ארגוני , סכנה לניהו ל כושל של שירות מיקור החוץ עקב חוסר הכרות עם ספק מיקור החוץ , אין מדובר בעובד עם נאמנות ומחויבות לארגון, סיכון בניהול שמירה ואחסון הידע הארגוני ועוד.

2. השפעה על נוהלי הביקורת: על פי ג"ד 95 יש לבחון את "... מדיניות, נהלים ורישומים שונים, המשמשים את ספק השי רות... ", כלומר על המבקר להכיר ".. לשקול את הסדרי מיקור החוץ , כדי לזהות כיצד הגוף המבוקר מגיב לסיכונים הנובעים מהפעילויות שהועברו למיקור חוץ " – משמעות הדבר , לבחון הן את הסיכון בכישלון השירות הניתן וכן את סוגית אבטחת המידע הנמצא אצל ספק מיקור החוץ . את חוו ת הדעת על לשכת השירות (הקבלן שנותן את שירות מיקור החוץ) ניתן להכין באופן ישיר על ידי רו "ח המבקר של החברה המשתמשת בשירותי לשכת השירות או לקבל חוו "ד (מטיפוס A או B) מרואה חשבון המבקר את לשכת השירות. חוות הדעת שייתן רו"ח המבקר את לשכת השירות תכלול בטיפוס A התייחסות לתכנון הבקרות ואילו בטיפוס B התייחסות הן לתכנון הבקרות והן לאפקטיביות של הבקרות והכול כאמור בג "ד 94.

אוניברסיטת בר – אילן
ביקורת מערכות מידע (מ"מ)
סמסטר ב' – מועד ב' – 11.08.08
אייל אסייג, רו"ח

שאלה מספר 4 – (20 נקודות)

להלן תיאור של מספר אירועים ומצבים שונים, בלתי תלויים זה בזה, המתייחסים לחברות שונות, בהם נתקלת בעבודתך כרואה חשבון המבקר, במסגרת ביקורת מערכות מידע ממוחשבות , כחלק מתהליך הביקורת של דוחותיהן הכספיים השנתיים :

1. חברת אלחוט בע "מ, הינה חברת טלפונים סלולאריים גדולה בעלת מאות אלפי לקוחות . החברה מפעילה מערכות מחשב רבות התומכות בפעילויותיה . חשב החברה טען בפניך , כי לצורך מתן חוות דעת על הדוחות הכספיים , אין צורך שתבדוק מערכות מידע ממוחשבות המכילות נתונים כמותיים בלבד , ואין בהן ערכים כספיים , כגון : מערכת המנויים, המערכת לאיתור וניהול תקלות ברשת הטלפונית, מערכת ניהול שעות נוכחות העובדים וכו'.
2. בתקציב השנתי של תפעול מערכות המידע הממוחשבו ת בחברת יהלום בע "מ, תוקצבו לכל אחד מהמשתמשים העיקריים במערכות, סכומים למימון פניותיהם הישירות לבתי התוכנה השונים, לשם ביצוע שינויים שוטפים , עדכונים ושדרוגים במערכות המידע , הנדרשים על ידם במהלך השנה.
3. חברת אודם בע "מ לא דרשה מחברת המחשבים , ממנה רכשה תוכנות שפ ותחו עבורה , להפקיד בידה או בידי נאמן עותק של תוכנות מקור (SOURCE).
4. דוח ביקורת אותו ערך המבקר הפנימי של חברת טורקיז בע "מ מצביע על ליקויים מהותיים בתחום הבקרות הפנימיות במערכות מידע ממוחשבות מסוימות שבשימוש החברה . בתגובה לממצאי דוח הביקורת , השיב מנהל מערכות המידע בחברה , כי היות שבית התוכנה ממנו נרכשה המערכת הוא הספק העיקרי לתוכנות מהסוג האמור , מתקשה החברה לאלץ את בית התכנה לערוך את השינויים הנדרשים על ידי החברה .
5. בפגישות שקיימת עם מנהל מערכות המידע של חברת אמרלד בע "מ, התברר לך כי בית התוכנה, אשר פיתח ומתחזק א ת המערכות הראשיות של החברה , ובהן מערכת ההתחשבנות עם לקוחותיה (BILLING), קיבל הרשאות לגישה מרחוק למחשב החברה , וזאת לצורך תיקונים נדרשים מרחוק בתוכנות החברה . הרשאות אלה מאפשרות גם צפייה במאגרי המידע של החברה.

נדרש :

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

אוניברסיטת בר – אילן
ביקורת מערכות מידע (מ"מ)
סמסטר ב' – מועד ב' – 11.08.08
אייל אסייג, רו"ח

פתרון שאלה מספר 4

1. טענתו של חשב החברה אינה נכונה. מערכות מידע חשבונאיות הינן מערכות המכילות לא רק נתונים כספיים, אלא גם נתונים כמותיים, מהם נגזרים נתונים כספיים, המהווים בסיס לרישומים החשבונאיים, או המסייעים בבדיקתם, כגון: מידע על כמויות ותנועות כמותיות של המלאי, וותק לצורך חישוב הפרשה לפיצויי פרישה, מערכת מינויים וכו'.
על רואה חשבון המבקר, למפות את מערכות המידע הממ וחשבות הרלבנטיות לרישומים החשבונאיים, בין אם הן יוצרות או מהוות ישירות בסיס לרישומים חשבונאיים, כגון: מערכת המינויים, ובין אם הן מסייעות באימותם של רישומים או מידע חשבונאי, הכלולים בדוחות הכספיים, ולבדקן בהתאם.
מאידך, ישנן מערכות מידע בגוף המבוקר שאינן רל בנטיות לרישומים החשבונאיים, או שזיקתם לרישומים החשבונאיים הינה מועטה, ולכן בדר"כ אין צורך לערוך בהן ביקורת ממ"מ. כגון: מערכת לאיתור וניהול תקלות ברשת הטלפונית. ניתן להסתייע במערכת זו, שלכאורה אינה קשורה למערכת החשבונאית, בנסיבות מסוימות, לצורך הסבר על יריד ה בהכנסות ו/או גידול בהוצאות.

2. תהליך זה כרוך בסיכונים שיש למזערם, ככל שניתן, עקב חשש לביצוע שינויים במערכות מידע מסוימות בארגון, שלהן השפעה על מערכות אחרות בארגון ו /או העלולים לגרום לשיבושים במערכות המידע ולעלויות מיותרות, וכן לפגוע בנתיבי הבקרה הפנימית ו /או הביקורת של מערכות אלה.
לפיכך, חיוני קיומו של תאום מוקדם וקבלת אישור מרמה ממונה, בעלת ראיה כלל ארגונית, לכל שינוי מוצע במערכות המידע הממוחשבות, גם אם תיקצובו מאפשר זאת, וכל זאת לאחר עריכת מבחני קבלה נאותים ע"י המשתמשים.

3. תוכנת המקור מהווה את הבסיס למידע ה ממוחשב ואת הפלטפורמה לשינויים בתכנה ו/או תחזוקתה ו /או תיקון תקלות. תכנת המקור מהווה את לב המערכת הממוחשבת, ולפיכך, הינה חיונית ביותר להמשך תפקודן הסדיר של מערכות המידע בגוף המבוקר.
קיימת חשיפה לסיכונים של שיבושים במערכת המידע במקרים בהן, מסיבות שונות, חברת המחשבים ו /או בית התכנה יפסיקו מתן שירותים לגוף המבוקר ואז עלול הגוף להזדקק לתכנת המקור וקיימת חשיבות לנגישותה.
מומלץ שעותק של קוד המקור של התכנה יופקד במקום מובטח המקובל על הצדדים ויהיה נגיש, בעת הצורך לגוף המבוקר.
על רואה החשבון המבקר להפנות תשומת ליב ו של הגוף המבוקר לסיכונים הכרוכים באמור לעיל, וזאת במסגרת סקר הסיכונים שהוא עורך בחברה, במסגרת ביקורת ממ"מ כחלק מביקורת הדוחות הכספיים.

4. הליקויים שנמצאו בבקרה הפנימית בתחום מערכות המידע אצל הגוף המבוקר, ותשובת מנהל מערכות מידע כי החברה מתקשה בתיקון הליקויים, מחייב את רואה החשבון המבקר לפעול כדלקמן:

- לוודא קיומן של בקרות פנימיות ידניות המפצות על הליקויים המהותיים שנמצאו בתחום הבקרות הפנימיות בממ"מ.
- להרחיב את היקף הבדיקות המבססות באמצעות ביקורת ידנית לצורך אימות נאותות המידע בדוחות הכספיים.
- להפנות תשומת לב הנהל ת הגוף המבוקר לליקויים בבקרות הפנימיות במערכות הממוחשבות, ולחשיפות לסיכונים אפשריים כתוצאה מכך , לרבות השפעה על נאותות המידע בדוחות הכספיים.

5. מתן הרשאה לבית התוכנה לגישה מרחוק למערכות המידע של הגוף המבוקר תורמת לשיפור השירות ולצמצום פערי הזמנים ממועד איתור ת קלות ועד לתיקונן ע "י בית התוכנה. יתרון זה מלווה בחשיפה לסיכונים אפשריים של הגוף המבוקר לשינויים בלתי מורשים במערכות המידע , העלולים לגרום לשיבושים במערך הנתונים ו /או לתרמיות ומעילות לרבות השפעה על נאותו המידע בדוחות הכספיים . כן נחשפת החברה לחשיפת נתוניה ונת וניה לקוחותיה וספקיה לגורמים בלתי מורשים , ולעבירה על חוק הגנת הפרטיות.

מומלץ כי רו"ח יפעל כדלקמן:

- ירחיב את היקף ביקורת ממ "מ בכל הקשור באבטחת המידע , לרבות FW, הצפנות, הפעלת מנגנוני ניתוק תקשורת וכו'.
- יוודא קיומן של בקרות פנימיות ממוחשבות וידניות על מערכות מידע, המיועדות למניעת שיבושים במערך המידע ו/או איתור תרמיות ומעילות.
- יוודא כי לא חלו שיבושים בנתונים המהווים את הבסיס למידע הכלול בדוחות הכספיים.
- יפנה תשומת לב להנהלת המבוקר לסיכונים האפשריים כתוצאה מכך.

אוניברסיטת בר – אילן
ביקורת מערכות מידע (מ"מ)
סמסטר ב' – מועד ב' – 11.08.08
אייל אסייג, רו"ח

שאלה מספר 5 – (15 נקודות)

בהתייחס לגילוי דעת 93 שפורסם לאחרונה, ענה על השאלות הבאות :

1. הסבר את השפעת פרסום גילוי דעת (ג"ד) 93 על גילוי דעת קיימים . ציין את הבעייתיות הנוצרת וכיצד היא נפתרת. (3 נקודות)
2. הסבר מה ההבדל בין מודל מעין –" COSO " שנקבע בג "ד 93 לבין מודל הבקרה הפנימית שנקבע בגל"ד 80 (3 נקודות)
3. כיצד מתייחס ג"ד 93 לחובת ביצוע ביקורת ממ"מ לעומת ג"ד 66 ? (3 נקודות)
4. כיצד מתייחס ג"ד 93 לנושא הסתמכות על מומחים לעומת ג"ד 66 ? (3 נקודות)
5. מהם הנושאים המופיעים בג"ד 66 בנספח א ואינם מופיעים בג"ד 93 ? (3 נקודות)

פתרון שאלה 5 – 15%

1. כאמור בג"ד 93 ס' 1 כאשר יפורסם גילוי הדעת בנושא "נוהלי המבקר במענה לסיכונים שהוערכו" המבוסס על ISA 330, יתבטל תוקפם של ג "ד 66 ו-80. ג"ד 93 יכנס לתוקף ב-1.1.2007 (ס' 124 לג"ד 93), במצב הביניים עד לפרסום גילוי הדעת הנוסף , גם 93 בתוקף וגם גילויי הדעת 66 ו- 80 בתוקף, מה יקרה אם הם יסתרו זה את זה ? הבעיה נפתרת (בהיבטי מערכות מידע בלבד) על ידי כך ש- 93 במקור לא ציין נוהלי ביקורת (זה יפורסם בעתיד) לכן אין התנגשות חריפה . ישנה הרחבה מהותית בנושא הגדרת הבקרה הפנימית , התייחסות למומחים, אין התייחסות לתחולת 66, כך שהפרסום לא פוגע ב נוהלי העבודה הקיימים על פי 66.

2. ההבדל העיקרי הוא בהתייחסות למערכות מידע כתהליך חוצה מבנה ארגוני ולא כיחידה נפרדת. מודל ה- COSO פירט את המבנה המלא של הבקרה הפנימית הכולל 5 שכבות אופקיות המפולחות ב- 3 רבדים ואילו הבקרה הפנימית ב- 80 הורכבה מ- 3 רבדים המתייחסים לדיווח הכספי (סביבת הבקרה ונוהלי הבקרה . נוהלי הבקרה פורקו למבקר פנים ולמנגנון האוטומטי של הבקרה כך שעובד לא יבצע תהליך מראשיתו ועד סופו ללא מעורבות של גורם נוסף – הפרדת תפקידים). 5 השכבות (ס' 43 לגל"ד 93) ב"מעין COSO " הם : סביבת הבקרה, הערכת סיכונים, מערכת המידע ותקשורת, קיום בקרות ומעקב אחר הבקרות . לא ניתנו הפילוחים ב- 93, אבל ברור שהכוונה לרובד הדיווח הכספי ב- COSO.

3. ג"ד 93 אינו מחייב ביצוע ביקורת IT אך גם אינו פוטר את רו "ח, כפי שעושה זאת ג"ד 66 במצבים מסויימים (ס' 4 ל- 66). אמירה ברורה תינתן בגילוי דעת שיתפרסם.

4. בעיקבות ביטולו הצפוי של 66, על ידי 93 פירסמה הלישכה את גילוי דעת 95 ובו קבעה שבסעיף 1 לג"ד 64 המשפט ... או על מנתחי מערכות שלגביהם יתפרסם גילוי דעת בעתיד" – יבוטל.

5. הנושאים המופיעים בגילוי דעת 66 – נספח א ואינם מופיעים ב- 93 הם: המבנה הארגוני של אגף מערכות מידע , החומרה והתוכנה הבסיסית , היות התוכנה תוכנת מדף נפוצה , מידת הריכוזיות או הביזור , זרימת הנתונים והממשקים , השיטות והתקופות לשמירת נתונים, קיומה של תוכנית לשעת חירום . בסעיפים 95-90 לגל"ד 93 מצויינים הנושאים הבאים (לא נדרש) – סעיף 90 – הדגשת פעולות הבקרה הקשורות להרשאה , סקירות ביצוע, עיבוד המידע, בקרות פיזיות והפרדת תפקידים . סעיף 94 מתמקד בבקרות כלליות ב- IT בהן: מרכז המידע והפעולות ברשת , רכישת תוכנות , שינויים ותחזוקת תוכנות , אבטחת גישה , רכישה פיתוח ותחזוקה של מערכת יישום . סעיף 95 מתמקד בבקרות היישום הקשורות לתהליכי הייזום , הרישום, העיבוד והדיווח של עסקאות או מידע כספי אחר. בקרות אלו מסייעות להבטיח שהעסקאות שבוצעו הינן מאושרות ונרשמו ועובדו באופן מלא ומדויק.

לה!....לה.....נצאר !!