

סקר מעילות ברשויות מקומיות

אפריל 2010



ALKALAY MONAROV
אלקלעי מונרוב

בקרה וניהול סיכונים

עופר אלקלעי, רו"ח, CIA, CFE
משרד: 03-6125612, נייד: 054-2479943
www.almo.co.il, ofera@almo.co.il

מטרת הסקר

- איתור תרחישים החשופים למעילות
- מתן המלצות לשיפור הבקורות ותהליכי העבודה
- סיוע למבקר הפנימי בקביעת תוכנית ביקורת מבוססת סיכונים
- הסקר לא נועד לאתר מעילות



התוצרים

- רשימת תרחישים בהם קיים סיכון למעילה ורמת הסיכון של אותו תרחיש (נע בציון שבין 1 ל 25)
- מיפוי תהליכים בעלי רמת סיכון גבוהה
- רשימת הבקורות הקיימות בפועל
- המלצות לשיפור תהליכי עבודה ובקורות
- לוחות זמנים ואחראי לתיקון הליקויים

החומר המשמש לסקר

- מבנה ארגוני
- ניתוח תהליכי עבודה ובקורות
- שיחות עם בעלי תפקידים
- דוחות ביקורת פנימית
- דוחות כספיים
- רשימת תרחישים פוטנציאליים



מתודולוגיה

- בחינת סביבת הבקרה
- ניתוח פרטני של תרחישים



מתודולוגיה - סביבת הבקרה

בחינה של התמודדות הארגון ברמה רוחבית עם סיכוני מעילות

- תהליכי קליטת עובדים
- קוד אתי
- קו חם
- הפרדת תפקידים
- רוטציה
- בדיקות אמינות ופוליגרף
- יציאה רצופה לחופשה
- נהלים כתובים
- אבטחת מידע
- ממונה למניעת מעילות



מתודולוגיה- בחינת תרחישים

בחינה של התמודדות הארגון ברמה רוחבית עם סיכוני מעילות

1. תהליכי קליטת עובדים

2. מהותיות הנזק (ניקוד 1-5)

מכפלת הפרמטרים נותנים ניקוד (1-25)

1-8	סיכון נמוך
9-15	סיכון בינוני
16-25	סיכון גבוה

1	עד \$K10
2	מ- \$K10 ל- \$K50
3	מ- \$K50 ל- \$K100
4	מ- \$K100 ל- \$M1
5	מעל ל- \$M1

1	חזקות מאוד
2	חזקות
3	בינוניות
4	חלשות
5	חלשות מאוד

דוגמא- העברות בנקאיות

התרחיש לביצוע מעילה

אחראית על התאמות הבנקים, תשלח בקשה לבנק לביצוע העברה בנקאית לחשבונה הפרטי, הכוללת חתימות ממזיפות של מורשי חתימה ותרשום פקודת יומן כוזבת.

בקורות מונעות ומאתרות

טופס העברה כולל את פרטי חשבון הבנק של החברה ופרטי חשבון הבנק של המוטב.

ליקויים בתהליכי העבודה והבקורות

לחברה אין מנגנון call back עם הבנק, לפיו פקיד הבנק נדרש לקבל אישור טלפוני מגורם מוסמך בחברה לפני ביצוע ההעברה, בנוגע לפרטי ההעברה. החברה אינה ממספרת את ההעברות.

רמת סיכון לתרחיש	מהותיות המעילה	טיב הבקורות	ניקוד
25	5	5	

המלצות לשיפור הבקורות

א-ביצוע העברות באמצעות תוכנת תקשורת לבנקים או אתר אינטרנט מאובטח, כאשר הגישה ניתנת באמצעות סיסמא למורשי החתימה. תבוצע התאמות בנקים ובקרה אחרי התשלומים.
 ב-ליישם בקרה של פניה מהבנקים לחברה לצורך אישור ההעברה (call back) בהסכם כתוב עם הבנק. יש להגדיר לבנקים את הגורמים המוסמכים לאישור טלפוני שאינו הגורם ששולח את הבקשה להעברה לבנק.
 ג-מספור ההעברות, לצורך בקרה על רציפותן.

התייחסות החברה

א-הנושא יבחן מול מערכות מידע.
 ב-תבחן האפשרות לאישור העברה עם הבנק ע"י מנהל מחלקת הגזברות והנח"ש, מעל לסכום מהותי שיקבע.
 ג-דורש פיתוח.

דוגמא- קליטת ספקים

<p>התרחיש לביצוע מעילה</p> <p>עובד החברה ישנה את פרטי חשבון הבנק של ספק קיים ויצרף טופס הקמת ספק מזויף.</p>			
<p>בקורות מונעות ומאתרות</p> <p>מנהלת המחלקה, שאין לה הרשאה להקים ספק ולעדכן פרטי חשבון בנק במערכת הממוחשבת, מבצעת בקרה אחר שינויים במספר חשבון הבנק של הספקים הקיימים במערכת. במהלך החודש היא נוהגת להפיק דוח לוג שינויים, המצביע על שינויים בחשבונות הבנק של הספקים. הדוח נבדק למול טופס הקמת ספק, החתום על ידיו.</p>			
<p>ליקויים בתהליכי העבודה והבקורות</p> <p>לא נערכת שיחת טלפון עם הספק לצורך אימות כי הוא עומד מאחורי הבקשה לשינוי. לאור האמור אין בקרה כי הטופס לא מזויף.</p>			
רמת סיכון לתרחיש	מהותיות המעילה	טיב הבקורות	ניקוד
16	4	4	

דוגמא- קליטת ספקים- המשך

המלצות לשיפור הבקורות

א-יש לערוך שיחת טלפון עם מורשי החתימה אצל הספק לצורך בדיקה כי המסמך אינו מזויף.
ב-במקרה של שינוי של פרטי חשבון הבנק של הספק, יש לדרוש העתק המחאה מבוטלת.
ג-יש להפיק דו"ח לוג שינויים, לפני אישור קובץ התשלומים, הכולל שינוי

התייחסות החברה

מקובל

דוגמא- המחאות

<p>התרחיש לביצוע מעילה</p> <p>שינוי שם המוטב על גבי ההמחאה המיועדת לתשלום, על ידי הגורם אשר שולח את ההמחאות בדואר. לדוגמא שינוי מוטב מ"ביטוח לאומי" ל "ביטוח לאומי החזר לשכיר".</p>			
<p>בקורות מונעות ומאתרות</p> <p>אין</p>			
<p>ליקויים בתהליכי העבודה והבקורות</p> <p>הלקוח לא מגיע לקחת את השיק באופן אישי.</p> <p>שם המוטב על גבי ההמחאה אינו סגור באמצעות כוכביות.</p>			
רמת סיכון לתרחיש	מהותיות המעילה	טיב הבקורות	ניקוד
20	4	5	

דוגמא- המחאות- המשך

המלצות לשיפור הבקורות

א-הדפסת כוכביות בצדי שם המוטב למניעת אפשרות להוספת פרטים. ניתן לבצע זאת אוטומטית על כל המחאה, באמצעות תוכנת ההדפסה.

ב-העברת רשימה של כל ההמחאות המיועדות לתשלום עם שם המוטב והסכום לבנק.

ג-הוספת הערה שאסור לבצע שינויים על גביי המחאה.

ד-דרישה מהבנק כי בעת קבלת המחאה מעל סכום שיקבע ע"י החברה תיערך שיחה טלפונית לאימות

תגובות החברה

המלצות א-ג מקובלות ד' לא ישים לאור היקף ההמחאות

דוגמא- מס"ב

<p>התרחיש לביצוע מעילה</p> <p>ביצוע שינויים בקובץ התשלומים שנשמר בדיסקט ע"י מנהלת מחלקת גזברות, טרם שידור הקובץ השמור על הדיסקט למס"ב והעלמות לאחר מכן.</p>			
<p>בקרות מונעות ומאתרות</p> <p>מבוצעת התאמת בנק אשר תאתר שינוי בין הסכום לתשלום בקובץ לבין הסכום ששולם בפועל. קיים מעקב תזרימי אחר הסכום המיועד לתשלום ויורד מחשבון הבנק של החברה.</p>			
<p>ליקויים בתהליכי העבודה והבקרות</p> <p>הקובץ נשמר בדיסקט לאחר אישורו על ידי מורשי החתימה בחברה, במועד זה, כל מי שיש לו גישה לכספת וידע בשפת התכנות של הקובץ, יכול לבצע שינויים בנתוני הקובץ. העדר בקרה מגלה של ביצוע שינויים בקובץ לפני שידור הקובץ למס"ב לביצוע התשלומים.</p>			
רמת סיכון לתרחיש	מהותיות המעילה	טיב הבקרות	ניקוד
16	4	4	
<p>המלצות לשיפור הבקרות</p> <p>א-שינוי שיטת השידור למס"ב מדיסקט לשידור ישיר מהמערכת באמצעות קו תקשורת חד כיווני אשר ימנע אפשרות כניסה למערכת.</p> <p>ב-השוואה בין הנתונים בדוחות המס"ב ששודרו, לטופס אישור שידור שמתקבל ממס"ב.</p>			
<p>התייחסות החברה</p> <p>המלצה לגבי שינוי שיטת השידור וביצועה ישירות מהמחשב מקובלת. קובץ המס"ב יישמר ברשת, לא תינתן הרשאת שינוי לקובץ הנ"ל לאחר יצירתו. השידור יתבצע מהמחשב המותקן ברשת.</p>			

דוגמא- גבייה

התרחיש לביצוע מעילה			
עורך הדין יגבה כספיים מהחייבים אך לא יעביר אותם לחברה.			
בקורות מונעות ומאתרות			
<p>החברה מבצעת ביקורת רבעונית במשרדי עורכי הדין הפעילים וביקורת שנתית במשרדי עורכי הדין הלא פעילים. יציין כי מדובר בביקורת קצרה. במסגרת הביקורות נבדקים תיקים ללא פעילות, תיקים אשר לא נפתח בגינם תיק בהוצל"פ וכד'.</p> <p>בדיקת שלמות התשלומים המגיעים בזמן סגירת התיק.</p> <p>עורכי הדין נמצאים בבקרה חודשית על ביצועי הגבייה, עורך דין שאינו גובה טוב ירד בדירוג.</p>			
ליקויים בתהליכי העבודה והבקורות			
לא מבוצעת בדיקה כי כל הכספים בגינן הופקו קבלות פיקדון הועברו לחברה.			
ניקוד	ניקוד	ניקוד	ניקוד
9	3	3	
המלצות לשיפור הבקורות			
<p>א-לבצע בדיקות במשרדי עורכי הדין על מכלול הגביה המבוצעת במשרד כולל בדיקת הנהלת החשבונות שלהם וניתוח חשבון הנאמנות.</p> <p>ב-לבצע בדיקות על שינויים שבוצעו בנתונים באמצעות קובץ LOG (שינויים ומחיקות בנתונים קודמים).</p> <p>ג-לערוך שיחות טלפון מדגמיות עם חייבים לצורך אימות סכומי התשלום.</p>			
התייחסות החברה			
<p>לחברה מודול "עודכנית פוקוס", כיום לא נעשה בו שימוש רב. בנוסף, נכנסה מערכת חדשה "גבע" אשר תסייע לבקר את נתוני הגבייה בתיקים ואת הנעשה בתיקי הגבייה במשרדי עורכי הדין.</p> <p>החברה מבצעת בקרה תקופתית במשרדי עורכי הדין באמצעות גורם חיצוני המתמחה בנושא, עד כה בוצעו בקורות בשני משרדים.</p>			

דוגמא- תשלומים לספקים

התרחיש לביצוע מעילה			
עובד במחלקת ספקים יפתח ספק פיקטיבי במערכת ה- ERP עם פרטי חשבון הבנק שלו, יזין חשבונית כוזבת לספק זה ויבצע תשלום.			
בקורות מונעות ומאתרות			
בטרם תשלום החשבונית, היא עוברת סבב חתימות ידני.			
ליקויים בתהליכי העבודה והבקורות			
פתיחת חשבון ספק מבצעת על ידי גורם אחד ללא אישור מובנה במערכת של גורם מאשר. קיימים ספקים לא פעילים שמוגדרים במערכת ה- ERP. לכל עובד במדור ספקים ישנה אפשרות להקים ספק במערכת.			
רמת סיכון לתרחיש	מהותיות המעילה	טיב הבקורות	ניקוד
16	4	4	
המלצות לשיפור הבקורות			
א-יש לשנות את תהליך העבודה כך שלצורך פתיחת ספק חדש ידרשו שני גורמים. גורם קולט וגורם מאשר.			
ב-יש לעשות שימוש שוטף בקובץ לוג שינויים בקובץ אב ספקים.			
ג-יש לבדוק באופן שוטף / תקופתי אם כללי הפרדת הסמכויות במערכת נשמרים: שהפקידה שמזינה ספקים חדשים לא תורשה גם להזין לאמת ולשחרר חשבונית או לבצע התאמת בנקים.			
ד-יש לבצע הצלבה בין מספרי חשבון בנק וכתובות של ספקים לבין פרטי העובדים אחת לתקופה.			
ה-יש למחוק מהמערכת ספקים שאין בהם פעילות או לחילופין לסמן אותם כלא פעילים.			

דוגמא- תשלומים לספקים- המשך

התייחסות החברה

א-מערכת המידע אינה תומכת בהמלצה זו, אין אפשרות לבצע הפרדת תפקידים בין קולט השינוי ומאשר השינוי - דורש פיתוח.

ב-אין רזולוציה של שדה. דורש פיתוח. יבדק על ידי מנהלת מערכות מידע.

ג-מדור ספקים אינו מבצע התאמות בנק, אין אפשרות להפריד בין מקים הספק לקולט הספק עקב עליות שכר ומצבת עובדים.

ד-תבחן האפשרות להקים דוח המצליב בין חשבונות בנק הספקים לעובדים.

ה-אין אפשרות למחוק ספקים מהמערכת אנו נאמץ את ההמלצה לטיוב ספקים כלא פעילים.

דוגמא- שכר

<p>התרחיש לביצוע מעילה</p> <p>מנהלת מדור שכר תקים עובד פיקטיבי במערכת "חילן" ותעביר את השכר לחשבונה הפרטי או לחשבון של גורם מקורב.</p>			
<p>בקרות מונעות ומאתרות</p> <p>אין</p>			
<p>ליקויים בתהליכי העבודה והבקרות</p> <p>הקמת פרטי חשבון של עובד לא מתבצעת באמצעות גורם קולט וגורם מאשר. אין הפרדת תפקידים בשלב הקמת עובד חדש במערכת ולמנהלת מדור שכר קיימת אפשרות להקים עובד פיקטיבי.</p>			
	טיב הבקרות	מהותיות המעילה	רמת סיכון לתרחיש
	5	4	20
<p>ניקוד</p>			
<p>המלצות לשיפור הבקרות</p> <p>א-כל הקמה של פרטי חשבון בנק או שינוי בפרטים יעשה באמצעות גורם קולט ומאשר. המקרים החריגים יבדקו פרטנית כי לא מדובר בבני זוג העובדים בחברה ולהם חשבון בנק אחד.</p> <p>ב-ביצוע בקרה מדגמית אחר דיווחי הנוכחות על ידי גורם מחוץ למשאבי אנוש.</p> <p>ג-בקרה תקציבית של הוצאות שכר לכל מחלקה.</p>			
<p>התייחסות החברה</p> <p>ההמלצות מקובלות</p>			

דגשים לעריכת הסקר

- תהליכים בהם ניתן לתת הטבות לבעל תפקיד כגון: ביטול קנסות, שינוי חיובי ארנונה, קידום בקשות במחלקות השונות, אי העברה לטיפול משפטי, מתן פטורים הנחות והטבות וכד'
- תהליכים בהם אין בקרה נוספת על פעילות עובד
- זיהוי תהליכים בהם ניתן לעשות שימוש במסמך מזויף
- בדיקת פעולות היכולות לשנות טבלאות ומסדי נתונים



ALKALAY MONAROV

א ל ק ל ע י מ ו נ ר ו ב

בקרה וניהול סיכונים

**תודה על ההקשבה
שאלות ?**