ניהול סיכונים Risk Management

תחום ניהול הסיכונים משתנה מאוד בשנים האחרונות עם כניסתן לתוקף של רגולציות כמו באזל 2, סרבנס אוקסלי, ועדת בכר וחשיפה לסיכונים תפעוליים הנובעים מאסונות, מלחמות או הונאות.
ללא בקרות נאותות, רמת אבטחת מידע מספקת והפרדת תפקידים נאותה, החברות יכולות בקלות יתרה לאבד שליטה על הנעשה במערכת המידע.
מצב זה עלול, בין היתר, להביא לאובדן כספי ניכר הנובע מהסתמכות על נתונים שגויים בעת קבלת החלטות.
ניהול הסיכונים בשלב ההטמעה ו/או בשלב שלאחר ההטמעה יביא לניהול ויישום נכון של המערכת ,יקטין את הסיכונים העלולים לנבוע בעתיד, יאפשר לארגון להפיק את מירב הפונקציונליות האפשרית מהמערכת בהתאם לאופי פעילותו ויאפשר לייעל את תהליכי העבודה.
עם זאת, יש לשים לב כי ניהול הסיכונים ייעשה על ידי חברה מיומנת ובעלת מתודולוגית עבודה, הן בתחום ה ERP והן בתחום ניהול הסיכונים.

המהות והמטרה
סקר סיכונים בסביבת מערכות מידע (להלן - סקר סיכונים) הינו סקר הנערך במטרה לזהות, להעריך ולדרג את רמות הסיכון הקיימות בכל אחת ממערכות המידע הפועלות בארגון.

מהו סיכון
מקובל להגדיר סיכון כאפשרות שאיום כלשהו ינצל פגיעות של נכס, או קבוצת נכסים, על-מנת לגרום להפסד, או לנזק לנכסי הארגון.

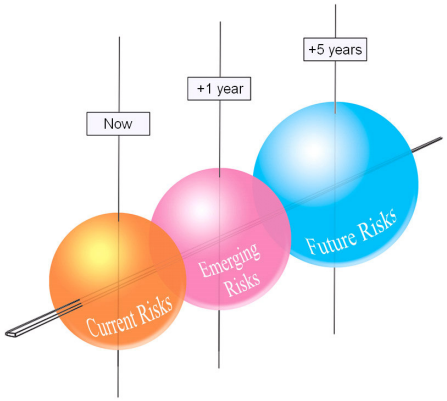
מרכיבי הסיכון

א. נכסים: לדוגמה: מידע (נתונים), חומרה, תוכנה, שירותים הניתנים על ידי הארגון, מסמכים, והון אנושי (למשל: עובדי יחידת מערכות מידע).
ב. איומים: לדוגמה: שגיאות, גרימת נזק במתכוון, הונאה, מעילה, כשל חומרה או תוכנה.
על הארגון להעריך את ההסתברות למימוש איום, לצורך כימות תוחלת השפעתו ודירוג האיומים בהתאם להשפעתם.
ג. פגיעות: למשל: כאשר חסר הידע הדרוש לצורך תפעול ותחזוק מערכות המידע, או למשל: כאשר קיימים בארגון כשלים, או חשיפות לכשלים אפשריים בתחום אבטחת המידע.

ההשלכות של פגיעה באמינות, בסודיות או בזמינות המידע

ההשלכות של פגיעה באמינות, בסודיות או בזמינות המידע מקבלות ביטוי, על-פי רוב, ב:

1. אובדן כספי.
2. הפרת חוק.
3. אובדן מוניטין (סיכון לקוחות וכוח-אדם וכן אובדן אמון).
4. אובדן הזדמנויות עסקיות.
5. פגיעה ביעילות תפעולית.
6. פגיעה בפעילות העסקית של הארגון.



דוגמאות לסיכונים

1. סיכונים עסקיים - הסיכון שיגרם לארגון הפסד כספי כתוצאה מטעות, שגיאה או שימוש בלתי מורשה במערכות המידע.
2. סיכונים הנובעים מהתשתית המחשובית הקיימת בארגון, למשל: סיכון הנובע משימוש בתוכנות ו/או חומרות ישנות (ישימות טכנולוגית), חוסר בתיעוד של פיתוח מערכות מידע, תדירות לקויה בעדכון גרסאות ובביצוע שינויים ושיפורים במערכות, וכמו כן תחזוקה לא נאותה של מערכות מידע בארגון.
3. עבודה מחוץ למערכות המידע של הארגון, כדוגמת גיליונות אקסל.
4. פגיעה באמינות הנתונים כתוצאה ממורכבות המערכת, ריבוי ממשקים חיצוניים (הנאותות וההשפעה שלהם על מערכות מידע אחרות הפועלות בארגון) וכמות העיבודים.
5. חשיפה לסיכונים בתחום אבטחת המידע הלוגית; למשל: כאשר מערכת ההרשאות ו/או מערך הסיסמאות נמצאו לקויים.
6. חשיפה לסיכונים בתחום אבטחת המידע הפיסית - גישה פיסית למערכות המחשב; למשל: לא קיימת הגבלה פיסית למשתמשים מורשים בלבד.
7. סיכוני תקשורת הנובעים מעצם קיומם של מוקדי השקה, בין הרשתות הפנימיות של הארגון, לבין הרשתות הציבוריות; למשל: כאשר המערכת מקושרת לאינטרנט וקיימת אפשרות גישה מרחוק למערכת, אולם לא קיימים מנגנוני הגנה, כגון: FIREWALL ו-RAS (או נמצא, כי סט החוקים של מנגנוני הגנה אלה אינו נאות).
8. אי מוכנות הארגון (לאור ליקויים טכניים), או אי קיומם של נהלים בנוגע ליכולתו של הארגון להתאושש במקרה של אסון (DRP - Disaster Recovery Plan).
9. אי קיומן של בקרות יישום נאותות במערכות המידע (בקרות קלט, עיבוד ופלט).
10. אי נאותות של הסכמי התקשרות שנחתמו בין הארגון לבין גורמים חיצוניים (נותני שירותים); למשל: הסכם שנחתם בין הארגון לבין בית תוכנה מסוים אינו מגדיר מדדי ביצוע, לוחות זמנים ותבחינים לביצוע מבחני הקבלה ולאופן המעבר לסביבת הייצור (PRODUCTION).

סיווג הבקרות

הקשר בין סיכון לבין בקרה מתבטא ביכולת לזהות את הסיכונים הטמונים במערכות המידע; מחד, ואת הבקרות שנועדו למזער את הסיכונים שזוהו; מאידך. מקובל לסווג את הבקרות ל-3 קבוצות עיקריות, כמפורט להלן:

בקרות מונעות (Preventive Controls)

הבקרות המונעות נועדו לסייע למבקר בעיקר ב:

- פיקוח על נתונים ופעילויות.
- צפיית שגויים טרם התרחשותן והפעלת הצעדים הדרושים לביצוע התיקון.
- מניעת שגיאות, מחדלים או נזק מכוון.

דוגמאות:

- סינון עובדים איכותיים.
- הפרדת תפקידים.
- נהלים לאישור עסקאות ולרישומן.
- בדיקות עריכה ממוחשבות (EDIT CHECKS).
- שימוש בתוכנות אבטחה ייעודיות להגבלת גישה לוגית לתוכניות ולנתונים.

בקרות מגלות/מדווחות (Detective/Reporting Controls)

בקרות המסייעות באיתור חריגים, מחדלים או נזק מכוון.

דוגמאות:

- סיכומי סרק.
- נקודות בקרה - POINTS CHECK- .
- בדיקת ECHO –בתקשורת- .
- הודעות שגיאה בקלטות גיבוי.
- בדיקה כפולה של חישובים.
- דיווחים תקופתיים על פעילות, לרבות ניתוחי סטיות.
- פונקצית המבקר הפנימי.

בקרות מתקנות -Controls Corrective-

הבקרות המתקנות מסייעות בעיקר ב:

- תיקון פעולות שאותרו על-ידי הבקרות המגלות/המדווחות.
- הפחתת השפעת האיום.
- זיהוי הסיבה לבעיות.

דוגמאות:

- נוהלי גיבויים –BACKUP-.
- נוהלי "ריצה" מחדש –RERUN-.

מתודולוגיה לביצוע סקר סיכונים

אחת ממתודולוגיות אלו הנה מתודולוגית ניהול סיכונים שפותחה בשנים האחרונות על בסיס ידע וניסיון בינלאומי בהטמעה וסקירה של מערכות ERP. מתודולוגיה זו מספקת מענה מקיף לצורכי ניהול הסיכונים וכוללת התייחסות גם לכלי עבודה ממוכנים, המאפשר עד הוק לסקור באופן ממוכן את הפרמטרים במודול הבסיסי ותקפות הפרדת תפקידים, במערכות ERP של חברת SAP ו- Oracle.

1. זיהוי מערכות המידע הפועלות בארגון:

1.1. על המבקר לזהות את כל מערכות המידע הפועלות בארגון, לרבות מערכות מידע הנמצאות בשלבי פיתוח.
1.2. יש לאתר את כל העובדים האחראים על כל אחת ממערכות המידע שזוהו. אחריותם של עובדים אלה עשויה להיות אחריות אדמיניסטרטיבית, כגון: בעלות על מידע או אחריות תפעולית.
1.3. יש לערוך פגישות עם עובדים (כמפורט בסעיף 1.2 לעיל), על-מנת לקבל הסברים ונתונים בנוגע לתהליכים העסקיים המבוצעים על-ידי כל אחת ממערכות המידע שזוהו.
2. זיהוי האיומים והשפעתם על נכסי המידע.
3. זיהוי הבקרות שנועדו להפחית את הסיכון והשפעתו, ובנוסף - תעדוף הבקרות לפי מידת האפקטיביות, היעילות ושקולי עלות-תועלת.
4. המלצה על הטמעת בקרות על-פי שיקולי עלות-תועלת ובהתחשב בשיקולים, כמפורט להלן:
4.1. עלות הבקרה ביחס לתועלת הנובעת מהפחתת הסיכון.
4.2. מידת הסיכון לה מוכנה ההנהלה להיחשף.
4.3. שיטה מועדפת להפחתת הסיכון:
4.3.1. ביטול הסיכון.
4.3.2. הפחתת הסבירות להתרחשות הסיכון.
4.3.3. הפחתת השפעת הסיכון.
4.3.4. ביטוח מפני הסיכון.

כיצד משליך סקר הסיכונים על תהליך הביקורת?
ההשלכה של סקר הסיכונים על תהליך הביקורת, מקבלת ביטוי באמצעות "גישת ביקורת מבוססת סיכונים" (Risk Based Audit Approach).
גישת ביקורת כאמור כוללת, על-פי רוב, מספר שלבים, כמפורט להלן:

1. איסוף מידע ותכנון הביקורת
   1.1. הבנת הסביבה העסקית של הגוף המבוקר.
   1.2. תוצאות ביקורות משנים קודמות.
   1.3. דוחות כספיים עדכניים.
   1.4. חקיקה.
   1.5. סקירת סיכונים שבמהות.
2. הבנת מערך הבקרה הפנימית
   2.1. סביבת הבקרה.
   2.2. נוהלי הבקרה.
   2.3. הערכת סיכון הבקרה.
   2.4. הערכת סיכון החשיפה.
   2.5. הערכת הסיכון הכולל.
3. ביצוע בדיקות ציות
   3.1. בחינת מדיניות ונהלים.
   3.2. בחינת בקרות מנהלתיות, כגון: הפרדת תפקידים.
4. ביצוע בדיקות מבססות
5. סיכום הביקורת
   5.1. ניסוח המלצות.
   5.2. עריכת דוח ביקורת.

סיכונים בסביבת מערכות מידע מהווים, על-פי רוב, איום לסודיות המידע (CONFIDENTIALITY), זמינות המידע (AVAILABILITY) ולאמינותו (DATA INTEGRITY). כך למשל: פגיעה בסודיות עלולה להיווצר כתוצאה מזליגת נכסים מוחשיים/לא מוחשיים מהארגון. זמינות נתונים עלולה להיפגע, למשל: כאשר הארגון לא נערך בצורה הראויה לנושא התאוששות מאסון (DRP). אמינות הנתונים עלולים להיפגע, למשל: כאשר נמצא, כי בקרות היישום אינן נאותות.

כיצד משליך סקר הסיכונים על מערכות ה- ERP?

על מנת להבטיח עבודה מוצלחת של מערכת ERP, מומלץ להשתמש במתודולוגיה מובנית לניהול סיכונים. כפועל יוצא מכך פותחו בעולם מתודולוגיות לניהול סיכוני הטמעת מערכות ERP, אשר מסייעות לארגונים לנהל את הסיכונים בשלב ההטמעה או בשלב שלאחר ההטמעה (Post Implementation Review).

סקירה זו תאפשר לאבחן האם מערכת ה- ERP המוטמעת מספקת את המידע המצופה ממנה ברמת דיוק, שלמות ותקפות נאותים.

- מערכות ERP מפחיתות באופן ניכר את הניירת המועברת בין מחלקות הארגון. נתיב הביקורת המסורתי המשמש את הארגון, על מנת להתחקות אחר אי סדרים וטעויות נעלם ודורש יצירת תהליכי בקרה ממוחשבים;
- הטמעת מערכת ERP בארגון גורמת בדרך כלל לבחינה מחודשת ושינוי של תהליכי העבודה. לעיתים, השינויים הנדרשים בתהליכי העבודה מהותיים ביותר, דבר החושף את הארגון לסיכון של חוסר תפקוד בימים הראשונים של העלאת המערכת.
- מערכת ה-ERP משתמשת בבסיס נתונים אחד לגבי כלל פעילויות המחשוב בחברה (כספים, שיווק, כוח אדם, ייצור, מלאי וכו') ובכך מונעת היווצרות של כפילות בנתונים, צורך בעדכון חוזר של בסיס המידע במקרה של שינוי ואו כשל, וחיסכון בתהליכי בקרה על מנת לוודא כי בסיסי הנתונים אכן מסנכרנים ומעודכנים.
- מערכת ה ERP משמשת את כלל עובדי הארגון. יישומים מסווגים, כגון מערכת הכספים שהייתה נחלתם של אנשי הכספים בלבד, הנם חלק ממערכת זו. הדבר חושף את הארגון לסיכון של זליגת מידע, סיכון שיש לנהלו באמצעות תכנון קפדני של קבוצות המשתמשים ורמת ההרשאות במערכת.
- אחד מיתרונות ה- ERP נובע מהאופן שבו המודולים השונים במערכת מזינים אחד את השני בזמן אמת. יתרון זה חושף את הארגון גם לסיכון היות והעדר בקרות קלט מתאימות תגרור טעויות בכל המודולים הרלוונטיים למערכת.
- הטמעת מערכת לא מהווה שינוי טכנולוגי בלבד אלא שינוי בחשיבה ובדרכי ההתנהגות של העובדים. מידת המוכנות של העובדים מבחינת הכשרה ותרגול העבודה בסביבה החדשה עשוי להקטין סיכון זה;
- הבקרות במערכות ERP מוגדרות ומנוהלות על ידי פרמטרים רבים שמאוחסנים בטבלאות שונות במערכת ולשם תחזוקתן נדרש ידע מעמיק ומקצועי;
- עקב לוח זמנים צפוף בשלב ההטמעה והרצון העז לקצר עד כמה שניתן את שלב המעבר בין מערכות המחשוב הישנות למערכת ה ERP, נוטים ארגונים להזניח את יישום הבקרות והטיפול באבטחת המידע של המערכת.
- הצורך הקיים בדרך כלל בגיור המערכות לישראל, כגון: התאמה להוראות ניהול ספרים, ניהול הערכים הכספים במספר מטבעות ועוד.
- הצורך בהמרת הנתונים ממערכות מחשב קודמות בחברה למערכת החדשה לעיתים גורם לאי דיוק במערכת החדשה.

ליקויים במערך הכספים

1. תשלומים שעובדים ביצעו לעצמם
2. תשלומים שעובדים ביצעו עבור בני משפחותיהם
3. תשלומים שבוצעו במזומנים
4. מערכת התשלומים שימש להחזרים של קופה קטנה
5. ניתנה הרשאה למספר רב של עובדים לבצע החזרים בגין קופה קטנה. כדי להתאים את התשלומים למערכת, ההחזרים בוצעו לפי ת"ז פיקטיבית
6. נמצאו ליקויים בהזנה של מספר האסמכתא המזכה בהחזר כספי
7. נמצאו מקרים שעובדים קבלו מספר החזרים בגין אותה אסמכתא
8. נמצא שקיימת אפשרות לבצע פעולת תשלום במינוס
9. נמצאו מקרים בהם נמצאו במערכת חשבונות בנק "מוזרים". למשל: מספר בנק 1, מספר סניף 1, מספר חשבון 1.
10. נמצא שקיימת פירצה בבקרה המאפשרת לעובד לשנות פרטי חשבון של ספק לפרטי החשבון שלו, להעביר לחשבון זה תשלומים, ולבצע את השינוי בחזרה
11. בוצעו תשלומים לחייבים, ללא קיזוז
12. נמצאו חייבים שלא נמצאה להם הערת חוב במערכת העזר הממוחשבת
13. נמצאו מקרים של כפילות במספרי זהות של לקוחות שונים בערכת הממוכנת
14. נמצאו מקרים בהם הופיעו אותם לקוחות במערכת פעמיים עם אותם מספרי זיהוי.

התוצר הסופי

של עבודת ניהול סיכונים הינו דוח כתוב להנהלת הארגון בו מפורטים החולשות בבקרות והסיכונים שעולים במהלך הסקירה, והפתרונות הנדרשים ליישום לשם הקטנת החשיפות. כמו כן, דירוג הליקויים והפתרונות הנדרשים בהתאם לחומרתם ולדחיפות המומלצת ליישומם, על פי הדרוג הבא:

• חולשה שיכולה להשפיע באופן מהותי על הבקרה הפנימית של המערכת ועל אמינות הנתונים ולכן מומלץ ליישם בקרות בנושא מהר ככל האפשר;
• נושאים חשובים לבקרה הפנימית ולהפחתת הסיכונים במערכת בכללותה אך לא מחייבים נקיטת צעדים מיידים;
• שיפורים מומלצים לבקרה הפנימית או ליעילות המערכת אך אינם קריטיים לבקרת המערכת.

לסיכום:
ללא בקרות נאותות, רמת אבטחת מידע מספקת והפרדת תפקידים נאותה, החברות יכולות בקלות יתרה לאבד שליטה על הנעשה במערכת המידע. מצב זה העלול בין היתר להביא לאובדן כספי ניכר הנובע מהסתמכות על נתונים שגויים בעת קבלת החלטות.
ניהול הסיכונים בשלב ההטמעה ואו בשלב שלאחר ההטמעה יביא לניהול ויישום נכון של המערכת ,יקטין את הסיכונים העלולים לנבוע בעתיד, יאפשר לארגון להפיק את מירב הפונקציונליות האפשרית מהמערכת בהתאם לאופי פעילותו ויאפשר לייעל את תהליכי העבודה. עם זאת יש לשים לב כי ניהול הסיכונים יעשה על ידי חברה מיומנת ובעלת מתודולוגית עבודה הן בתחום ה ERP והן בתחום ניהול הסיכונים.

הכותב הוא רואה חשבון מצוות המומחים של שחף יעוץ