חשיבות הפרדת תפקידים ועקרונותיה

הפרדת תפקידים (Segregation Of Duties) הינה אחת הבקרות החשובות למניעת טעויות ואיתור מעילות. הפרדת תפקידים מבוססת על התפיסה לפיה יש להפריד פעולה למספר מטלות, כך שמספר אנשים יבצעו את הפעולה ולא אדם אחד יבצע פעולה אחת מתחילתה ועד סופה. בתהליך יישום ההרשאות במערכת Oracle Application (ובמערכות אחרות) יש לוודא שההרשאות המתוכננות עבור כל משתמש במערכת לא יכללו קונפליקטים. קונפליקטים מתקיימים במקרים בהם שתי הרשאות או יותר מהוות יחדיו הפרה של כללי הפרדת תפקידים. לצורך בחינה של הנושא, יש לבדוק את התפקידים שהוגדרו אל מול מטריצות המפרטות את הקונפליקטים בהתאם ל- Best Practice מקובלים.לעיתים אנו נתקלים בארגונים במצבים בהם לעובדים קיימות הרשאות גורפות המאפשרות להם לבצע מעגלים עסקיים שלמים. לדוגמא: משתמשים בעלי הרשאה לבצע מעגל ספקים שלם, להקים עובד ולעדכן לו דרגת שכר, להקים לקוח ולשנות מחירוני לקוחות ועוד דוגמאות.

מצב בו קיימות לעובדים הרשאות גורפות או עודפות חושף את הארגון לתרמית בשל העובדה שהעובדים הינם בעלי הרשאות מעבר להגדרת התפקיד שלהם או הרשאות היוצרות פגיעה בעיקרון הפרדת התפקידים. למשל - עובד בעל הרשאות למעגל ספקים שלם יוכל לבצע את כל הפעילות מול הספק: החל משלב הגדרת הספק, דרך ביצוע הזמנת רכש, הזנת חשבונית ספק ועד שלב התשלום לספק. במצב זה עובד אשר ירצה להקים ספק פיקטיבי ולהעביר לו תשלומים פיקטיביים יוכל לבצע זאת בנקל. בחלק ניכר מן הארגונים הבקרות הידניות המבוצעות על התשלומים לא יגלו פעולת תרמית שכזו.

דרך יעילה לבדיקת חשיפות במערך ההרשאות והפרדת התפקידים הינה שימוש בכלים ייעודיים אשר פותחו לשם ניתוח הפרדת התפקידים. באמצעות כלים אלו ניתן לאתר משתמשים שניתנו להם הרשאות שאינן נכללות בהגדרת תפקידם, משתמשים להם הרשאות המהוות פגיעה בכללי הפרדת תפקידים, פרצות אבטחת מידע ועוד. בשוק קיימים כלים מספר כגון Logical Apps, Approva, מודול ICM של Oracle ו- VIRSA, כלי ה- SOD של Deloitte המנטרים נושא זה Online. כמו כן מבצעות חברות ייעוץ בדיקות Snapshot נקודתיות לאיתור קומפליקטים או הרשאות עודפות בנקודת זמן מסוימת.

לקבלת החלטה אם להשתמש באחד מהכלים השונים או בבדיקות ה-Snapshot השונות משקללים הארגונים שיקולים שונים כגון עלויות, מענה על דרישות רגולציה, היכולת להקטין חשיפה למעילות ואי סדרים וידידותיות הכלים או הדוחות. בשנים האחרונות עיקר הבקרה בתחום נעשתה באמצעות שימוש בדוחות Snapshot אך עם התקדמות מערך הבקרה ושיפור הטכנולוגיה בארגונים, יותר ויותר ארגונים עוברים לשימוש הכלי בקרה.