

תמצית דוח ביקורת פנימית – ניהול פרויקטי מערכות מידע

הביקורת הפנימית במשרד מבקר המדינה נערכת על ידי משרד ארנסט יאנג (ישראל) בע"מ (להלן: "המבקר הפנימי"). המבקר הפנימי מעסיק יועצים מקצועיים לביצוע הביקורות, לרבות רואי חשבון, כלכלנים, משפטנים, מוסמכים במנהל עסקים, מומחי תוכן בתחום מערכות המידע והסייבר, יועצים בתחום ניהול הסיכונים ומומחי תוכן בתחומים שונים.

כללי –

- ▶ תפיסת הטכנולוגיה הדיגיטלית במשרד מתמקדת בשילוב של יכולת פנים-משרדית עם מיקור חוץ לפעילות מערך המחשוב ותחזוקת מערכות המידע. המשרד מעדיף להשתמש בטכנולוגיות מוכחות ונפוצות, במיוחד במגזר הציבורי, ומעדיף התקשרויות ארוכות טווח עם ספקים יציבים על בסיס מכרזים פומביים. עם זאת, ישנה הנחיה להרחיב התקשרויות עם ספקים קטנים יותר.
- ▶ הקמת מערכות מחשוב ופיתוחן נתמכת על ידי מסגרות ארגוניות, בין היתר, ועדת היגוי עליונה לתקשוב ולסייבר, ועדת היגוי לפרויקט, מינהלת הפרויקט ונציגות המשתמשים.
- ▶ בניית הפתרונות הטכנולוגיים ותחזוקתם מתבצעת בהתאם למדיניות מוגדרת ונוהלי עבודה סדורים, בהתבסס על הנחיות רשות התקשוב הממשלתי ומתודולוגיות מקצועיות מקובלות, כולל ניהול סיכונים.

מטרת הביקורת - להעריך את תהליכי העבודה ובחינת יעילות ואפקטיביות של התהליך לרבות ההטמעה והבקורות בתחום ניהול פרויקטי מערכות מידע, על מנת להסיק על מידת היעילות בתהליכים ואפקטיביות הפיקוח והבקרה.

היקף הביקורת - הביקורת התמקדה בתהליכי ניהול פרויקטים באגף טכנולוגיות דיגיטליות ומידע (טד"ם) והממשק עם ספקים חיצוניים. הביקורת בדקה פרויקטי מערכות, חלקם SAAS וחלקם ONPREM אשר ייצגו סוגי פרויקטים שונים (פיתוח/תחזוקה/ מוצר מדף) ובשלב שונים של ה- Lifecycle של המערכות (טרם עלייה לאוויר, עדכון גרסה ומוצר מדף).

הבדיקה נערכה בהיבטים ושילבים של התהליך באופן המאפשר ראייה רוחבית והשוואתית. הליקויים שנמצאו, הינם נכון למועד ביצוע השיחות והבדיקות שנערכו.

▶ להלן התחומים בהם נערכו הבדיקות, עבור כל אחד מהפרויקטים שנבדקו :

- | | |
|---|--|
| ■ מודל עבודה עם ספקים חיצוניים. | ■ תוכנית שדרוג גרסה של המערכת. |
| ■ תכנון מול ביצוע בניהול הפרויקטים. | ■ תיעוד ושימור ידע בפיתוח המערכת. |
| ■ תהליך אפיון הדרישות על ידי הגורם העסקי. | ■ העברת המערכת מפיתוח לתחזוקה. |
| ■ תהליך בדיקות המערכת ומעורבות הגורם העסקי בבדיקות. | ■ היבטי הטעמת הנחיות אבטחת מידע בפרויקטים. |
| ■ ניהול השינוי / הטמעת המערכות. | ■ היבטי משאבי אנוש בפרויקטים. |

▶ להלן עיקרי הממצאים:

ניהול פרויקטים ושקיפות בתהליכים במשרד - נמצא כי ניהול הפרויקטים במשרד מתבצע בהתאם למתודולוגיות מקצועיות, כולל מתודולוגיית ניהול פרויקטים (PM) והנחיות משרד מבקר המדינה. תהליך ניהול הפרויקטים כולל הבנה מקצועית של המערכת ודרישות המשתמשים, ניהול תקציב בסינרגיה מלאה, ועבודה במקביל על גרסאות שונות עם אינטראקציה שוטפת עם בעלי העניין. עם זאת, נמצא כי ניתן לשפר את השקיפות בתהליכים, במיוחד בנוגע להענקת הרשאות גישה נאותות לנציגי הלקוח. הביקורת המליצה, בין היתר, להקים אמנת שירות מוסכמת בין המשרד לספקים, שתכלול הגדרת קריטריונים לשביעות רצון, מנגנוני יישוב פערים, ו- SLA לניהול הבקשות לשינויים ושיפורים, כדי לשפר את השקיפות בתהליכי העבודה, להבטיח תקשורת ברורה בין הצדדים, ולספק מסגרת ניהולית שתשפר את המעקב אחר ביצועי הפרויקטים.

תהליך ניהול הפרויקטים: תכנון, ביצוע ואיכות הצוותים - נמצא כי תהליך ניהול הפרויקטים במשרד מתבצע בהתאם לתכנון שנתי של הפעילות, הכולל לוחות זמנים קבועים מראש ותיאום עם הגורמים העסקיים. התכנון מתבצע ביעילות, עם ניהול משאבים קבועים, יחד עם זאת ניתן לשפר את עדכון לוחות הזמנים ותהליך קבלת ההחלטות, מה שיוביל לתיאום טוב יותר בין הגורמים המעורבים. בנוסף, נמצא כי איכות הצוותים המעורבים בפרויקטים דורשת שיפור. הטכנולוגיות שנבחרו עבור הפרויקטים מתאימות במועד הבחירה, אך יש צורך לבחון את המעבר למערכות מבוססות ענן ולוודא שהן עונות על הדרישות העסקיות. הביקורת המליצה, בין היתר, לבנות תכנון מפורט לכל פרויקט, שיכלול הגדרת משימות, לוחות זמנים, וערוצי תקשורת ברורים בין בעלי העניין. להקפיד על עדכונים שוטפים ושקופים לגורמים העסקיים, כדי לשפר את תהליך קבלת ההחלטות ולמנוע עיכובים וחוסר תיאום.

תהליך אפיון הדרישות וניהול השינויים בפרויקטים - נמצא כי תהליך אפיון הדרישות מול הגורם העסקי מתבצע בצורה מסודרת, כאשר הדרישות המתקבלות מתאפיינות בהיכרות טובה עם המערכת. מסמכי האפיון מאושרים וחתומים על ידי הגורמים הרלוונטיים, אך ניתן לשפר את השקיפות באפיון הטכני מצד הספק ולשתף ולאשרר את התוצר הסופי, בפרויקטים מסוימים חסר מסמך אפיון סופי חתום. כמו כן, נמצא כי ניתן לשפר את התיעוד בתהליך ניהול השינויים דבר שיספר אתשימור הידע הארגוני וביכולת ניהול השינויים בעתיד. הביקורת המליצה, בין היתר, לשפר את תהליך אפיון הדרישות וניהול השינויים, תוך שימת דגש על שקיפות ותקשורת בין הגורמים המעורבים. מומלץ להעמיק את הדרישות באפיון כדי להבטיח שהדרישות יהיו מקיפות ומפורטות, ולשפר את תהליך המעקב אחרי השינויים באמצעות תיעוד מלא והוספת תסריטי בדיקות.

תהליך בדיקות המערכת - נמצא כי חסר מסמך אסטרטגיית הבדיקות בכל אחת מהמערכות שנבדקו, תהליך הבדיקות אינו מתועד בצורה מסודרת, והדרישות לא תואמות את האפיון, כמו כן בדיקות קבלה מתבצעות אך ללא תהליך מסודר של כתיבת תסריטים מראש, דבר שמקשה על תיעוד ומעקב אחר ביצוע הבדיקות. כמו כן, לא מתבצעות בדיקות גרסיה במערכות מסוימות. הביקורת המליצה על הכנת מסמך אסטרטגיית בדיקות מסודר עבור כל פרויקט, ולהתאים אותו לכל מערכת קיימת במשרד, לרבות תיעוד מפורט של הבדיקות הנדרשות, קישור ישיר בין תסריטי הבדיקות למסמך האפיון ותהליך מסודר לביצוע הבדיקות.

ניהול השינוי והטמעת המערכת - נמצא כי תהליך ניהול השינוי והטמעת המערכת אינו מבוצע על בסיס מתודולוגיה של ניהול שינוי במערכות מידע ואינו מתועד בצורה מסודרת, כאשר חסרה תוכנית תקשורת ברורה ומובנית ותוכנית לטיפול בהתנגדויות של הגורמים הרלוונטיים. הביקורת המליצה, בין היתר, על הטמעת מתודולוגיה לניהול השינוי והכשרה של סוכני שינוי כדי להבטיח הטמעה מוצלחת של המערכת ושיפור את חווית המשתמש באמצעות בדיקות שמישות והדרכה מקיפה.

ניהול שדרוג גרסה: תהליכים, תקשורת ואתגרים - נמצא כי תוכנית השדרוג של המערכת מתבצעת בצורה מסודרת ושיטתית, עם תהליך ברור לאיסוף דרישות ואישור תכולה. עם זאת, ישנם פערים בתקשורת בין הגורמים המעורבים, דבר שעלול לגרום לתקלות ולפגיעה במאגרי המידע. בנוסף, לא נמצאה תוכנית שדרוג או טופס מוכנות בפרויקטים מסוימים, דבר שמקשה על היערכות לתקלות ומוביל לעיכובים. הביקורת המליצה, בין היתר, לבנות מתודולוגיה מסודרת לתהליך השדרוג, הכוללת תיעוד מלא, תקשורת ושיתוף פעולה בין כל הגורמים המעורבים, וטופס מוכנות לעלייה לאוויר עם ניתוח סיכונים.

תיעוד ושימור ידע בפיתוח המערכת - נמצא כי תהליך תיעוד ושימור הידע בפיתוח המערכת אינו מתנהל בצורה מסודרת, כאשר חסרה מתודולוגיה ברורה לשמירת הידע. תהליך התיעוד מתבצע באמצעות מערכת ייעודית, אך לא קיים תיעוד מספק לפעולות שבוצעו בעבר. בנוסף, באחד מהפרויקטים שנבדקו ישנה תלות במפתח אחד ללא תיעוד של ההתאמות והשיפורים. היעדר נהלי תיעוד מסודרים חושף את המשרד לאתגרים בנוגע ליציבות המערכת ותחזוקתה בעת ויוצרת תלות בספק. הביקורת המליצה, בין היתר, להטמיע נהלי תיעוד ושימור ידע מסודרים לכל המערכות ולכל בעלי התפקידים הקריטיים, ולהקים מערכת לניהול ידע מרכזית שתשמור על כל תיעודי הפיתוח והשינויים במערכת.

העברת המערכת מפיתוח לתחזוקה - נמצא כי תהליך העברת המערכת מפיתוח לתחזוקה מתבצע בצורה מסודרת במערכות מסוימות, עם צוותים המנהלים את התחזוקה במקביל לפיתוח. עם זאת, ישנם שיקולים שיש לבחון בנוגע להפרדת צוותי התחזוקה והפיתוח, כדי לשפר את ניהול התחזוקה. הביקורת המליצה, בין היתר לבנות תוכנית תחזוקה מסודרת לכל מערכת, שתכלול ניהול שינויים, גיבויים, שדרוגים ובדיקות גרסיה לאחר שדרוגים. יש להקפיד על הכנת תוכנית העברת אחריות מסודרת בעת המעבר מגוף מפתח לגוף מתחזק, ולבצע ניהול סיכונים לשלב המעבר לסביבת הייצור, כולל פיתוח מנגנוני תמיכה ובקרת איכות.

אבטחת מידע בפרויקטים - נמצא כי חסר נוהל פיתוח מאובטח במערכות שנבדקו, דבר שמוביל לחשיפה לאירועי אבטחת מידע ולסיכונים של זליגת מידע רגיש יחד עם זאת, רמת אבטחת המידע של המערכות שנסקרו היתה גבוהה ביותר. הביקורת המליצה, בין היתר, על הקמת נוהל פיתוח מאובטח שיכלול הנחיות לקוד מאובטח, טיפול בתקלים ועמידה בתקני אבטחת מידע בכל שלב בפיתוח.

תגובת המשרד - רוב המלצות הביקורת מקובלות.