תקן 1202 לביקורת והבטחה של מערכות מידע - הערכת סיכונים בתכנון

האופי הייחודי של הביקורת וההבטחה של מערכות מידע (IS) והכישורים הנדרשים לביצוע פעילות שכזו דורשים יצירת תקנים החלים באופן ספציפי על הביקורת וההבטחה של מערכות המידע. הפיתוח וההפצה של התקנים לביקורת והבטחה של מערכות מידע מהווים אבן פינה של התרומה המקצועית של ISACA® לקהילת הביקורת.

תקנים לביקורת והבטחה של מערכות מידע מגדירים דרישות חובה לביצוע ביקורות ולהכנת דוחות בתחום מערכות המידע והם מיידעים:

- אנשי מקצוע בתחום הביקורת וההבטחה של מערכות מידע לגבי הרמה המינימלית של הביצועים המקובלים הדרושים למילוי תחומי האחריות המקצועיים המוגדרים בקוד האתיקה המקצועית של ISACA.
- מנהלים ובעלי עניין אחרים לגבי הציפיות המקובלות בתחום ביחס לעבודתם של אנשי המקצוע.
- בעלי תעודת (CISA®) Certified Information Systems Auditor® על הדרישות מהם. אי ציות לתקנים אלה עלול להוביל לחקירת ההתנהלות של בעלי תעודת CISA מצד מועצת המנהלים של ISACA או ועדה מתאימה, וכן בסופו של דבר, עלול להוביל לנקיטת צעדים משמעתיים.

אנשי מקצוע בתחום הביקורת וההבטחה של מערכות מידע צריכים לכלול הצהרה במסגרת תוצרי עבודתם, במקום בו הדבר הולם, על כך שהפעילות שהם ביצעו תואמת לתקני הביקורת וההבטחה של מערכות מידע של ISACA, או לתקנים מקצועיים מתאימים אחרים.

מסגרת *ITAF*™ לאנשי מקצוע בתחום הביקורת וההבטחה של מערכות מידע מספקת רמות רבות של הכוונה:

- **תקנים**, המחולקים לשלוש קטגוריות:
  - **תקנים כלליים (סדרה 1000)**— אלה הם עקרונות מנחים שלפיהם מתנהל מקצוע הביקורת וההבטחה של מערכות מידע. הם חלים על הביצוע של כל המשימות, ומתייחסים לאתיקה מקצועית, לאי-תלות, לאובייקטיביות ולהקפדה ההולמת את אנשי המקצוע בתחום הביקורת וההבטחה של מערכות מידע, וכן לידע, למיומנות ולכישורים שלהם. ההצהרות על הציות לתקנים (**מודגשות**) הן בגדר חובה.
  - **תקני ביצוע (סדרה 1200)**—מתייחסים לביצוע המשימות, כגון: תכנון ופיקוח, תיחום, סיכון ומהותיות, גיוס משאבים, פיקוח וניהול משימות, ראיות הביקורת וההבטחה והפעלת שיקול דעת מקצועי והקפדה הולמת.
  - **תקני דיווח (סדרה 1400)**—מתייחסים לסוגי הדוחות, אמצעי העברת המידע והמידע המועבר.
- **קווים מנחים**, התומכים בתקנים ומחולקים גם הם לשלוש קטגוריות:
  - קווים מנחים כלליים (סדרה 2000)
  - קווים מנחים לביצוע (סדרה 2200)
  - קווים מנחים לדיווח (סדרה 2400)
- **כלים וטכניקות**, המספקים הכוונה נוספת לאנשי מקצוע בתחום הביקורת וההבטחה של מערכות מידע, למשל: סקירות טכניות, תכניות ביקורת/הבטחה של מערכות מידע, משפחת המוצרים של COBIT® 5.

מילון מקוון של מונחים הנמצאים בשימוש ב-ITAF נמצא בכתובת *www.isaca.org/glossary*.

כתב ויתור: ISACA יצר מדריך זה כדי שישמש רמה מינימאלית של הביצועים המקובלים הדרושים למילוי תחומי האחריות המקצועיים המוגדרים בקוד האתיקה המקצועית של ISACA. ISACA אינו מתחייב שהשימוש במוצר זה יבטיח תוצאה מוצלחת. אין להתייחס לפרסום בתור פריט שחובה לכלול בהליכים או בדיקות מקובלים, או להשתמש בו במקום הליכים ובדיקות אחרים שמטרתם הסבירה היא השגת אותן התוצאות. בעת קביעת ההתאמה של הליך או בדיקה ספציפיים, אנשי מקצוע בתחום הביקורת צריכים להפעיל את שיקול הדעת המקצועי שלהם בהתאם לנסיבות הביקורת הספציפיות של המערכות או הסביבה של מערכות המידע הנתונות.

הוועדה Professional Standards and Career Management Committee של ISACA (PSCMC) מחויבת לקבלת ייעוץ נרחב בעת ההכנה של התקנים וההכוונה. לפני הפרסום של כל מסמך, מתפרסמת ברחבי העולם טיוטה לצורך קבלת הערות מהציבור הרחב. ניתן גם לשלוח הערות לתשומת הלב של האחראי על פיתוח התקנים המקצועיים לכתובת הדואר האלקטרוני (*standards@isaca.org*), למספר הפקס (1443. 253 .1.847+) או לכתובת הדואר הרגיל (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

תקן 1202 לביקורת והבטחה של מערכות מידע - הערכת סיכונים בתכנון

הצהרות

1202.1 **פונקציית הביקורת וההבטחה של מערכות המידע תשתמש בגישה הולמת להערכת סיכונים ובמתודולוגיה תומכת לפיתוח התוכנית הכוללת לביקורת של מערכות המידע, ותיקבע סדרי עדיפויות להקצאה יעילה של משאבי ביקורת מערכות המידע.**

1202.2 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יזהו ויעריכו סיכונים הנוגעים לתחום הנמצא בבחינה בעת תכנון כל ופעילות התקשרות והתקשרות.**

1202.3 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישקלו סיכונים הנוגעים לנושא, סיכוני ביקורת וחשיפה קשורה של התאגיד.**

היבטים עיקריים

בעת תכנון פעילויות מתמשכות, פונקציית הביקורת וההבטחה של מערכות המידע אמורה:

- לנהל ולתעד, לפחות פעם בשנה, הערכת סיכונים כדי לסייע בפיתוח התוכנית לביקורת מערכות מידע.
- לכלול, כחלק מהערכת הסיכונים, את התוכניות האסטרטגיות והיעדים הארגוניים ואת המסגרות והיוזמות של תאגיד לניהול סיכונים.
- עבור כל התקשרות לביקורת והבטחה של מערכות מידע, יש לכמת ולהצדיק את כמות משאבי ביקורת מערכות מידע הדרושים לעמידה בדרישות ההתשקרות.
- להשתמש בהערכות סיכונים בעת בחירת תחומים ופריטים לביקורת, ובקבלת החלטות לגבי תכנון וניהול של התקשרויות מסוימות של ביקורת והבטחה של מערכות מידע.
- לקבל אישור של הערכת הסיכונים מבעלי העניין בביקורת ומגורמים מתאימים אחרים.
- לתעדף ולקבוע את מועד העבודה הקשורה לביקורת ולהבטחה של מערכות המידע בהתבסס על הערכות סיכונים.
- בהתבסס על הערכת הסיכונים, יש לפתח תוכנית אשר:
  - משמשת כמסגרת לפעילויות של ביקורת והבטחה של מערכות מידע
  - לוקח בחשבון דרישות ופעילויות שאינן קשורות לביקורת והבטחה של מערכות מידע
  - מתעדכנת לפחות פעם בשנה ומאושרת על-ידי האחראים לממשל
  - מתייחסת לתחומי האחריות כפי שהוגדר באמנת הביקורת

בעת תכנון התקשרות מסוימת, אנשי מקצוע בתחום הביקורת וההבטחה של מערכות המידע אמורים:

- לזהות ולהעריך את הסיכונים הקשורים לתחום הנמצא בבחינה.
- לבצע, עבור כל התקשרות, הערכה מקדימה של הסיכונים הקשורים לתחום הנמצא בבחינה. היעדים של כל התקשרות ספציפית צריכים לשקף את התוצאות של הערכת הסיכונים המקדימה.
- בעת בחינת תחומי הסיכון ותכנון התקשרות ספציפית, יש לשקול ביקורות, סקירות וממצאים קודמים, כולל פעילויות מתקנות. יש גם לשקול את תהליך הערכת הסיכונים הכולל של מועצת המנהלים.
- לנסות להפחית את סיכון הביקורת לרמה מקובלת, ולעמוד ביעדי הביקורת באמצעות הערכה מתאימה של נושא מערכות המידע ושל הבקרות הקשורות, בעת התכנון והביצוע של ביקורת מערכות המידע.
- בעת תכנון הליך ביקורת מערכות מידע ספציפי, יש להכיר בכך שככל שסף המהותיות נמוך יותר, כן הציפיות מהביקורת מדויקות יותר וסיכון הביקורת רב יותר.
- כדי להפחית סיכונים בשל מהותיות גבוה יותר, יש לפצות על-ידי הרחבת הבדיקה של הבקרות (מצמצם סיכון בקרה) ו/או על-ידי הרחבת הליכי בדיקה מבססת (צמצום סיכון גילוי) לקבלת הבטחה ברמה גבוהה יותר.

מונחים

מונח	הגדרה
אמנת ביקורת	מסמך המאושר על-ידי הגורמים האחראים על המשילות אשר מגדיר את המטרה, הסמכות ותחומי האחריות של פעילות הביקורת הפנימית האמנה אמורה: • לקבוע את מעמדה של פונקציית הביקורת הפנימית בתוך התאגיד • להרשות גישה לרשומות, אנשי צוות ומתקנים פיזיים הרלוונטיים לביצוע של התקשרויות ביקורת והבטחה של מערכות מידע • להגדיר את היקף הפעילות של פונקציית הביקורת
סיכון ביקורת	הסיכון להסקת מסקנה שגויה בהתבסס על ממצאי הביקורת. שלושת המרכיבים של סיכון הביקורת הם: • סיכון בקרה • סיכון גילוי • סיכון טבוע
סיכון נושא הביקורת	סיכון הקשור לתחום הנמצא בבחינה: • סיכון עסקי (יכולת הלקוח לשלם, כשרות אשראי, גורמי שוק וכו') • סיכון חוזי (חבות, מחיר, סוג, קנסות וכו') • סיכון מדינתי (פוליטיקה, סביבה, ביטחון וכו') • סיכון פרויקט (משאבים, כישורים, מתודולוגיה, יציבות המוצר וכו') • סיכון טכנולוגי (פתרון, ארכיטקטורה, רשת תשתית של חומרה ותוכנה, ערוצי אספקה וכו') ראה 'סיכון טבוע'.
סיכון בקרה	הסיכון שקיימת שגיאה מהותית שמערכת הבקרה הפנימית לא תמנע או לא תזהה בזמן. ראה 'סיכון טבוע'.
סיכון זיהוי	הסיכון שההליכי בדיקת מהות של איש המקצוע המבצע את הביקורת או ההבטחה של מערכת המידע לא יזהו שגיאה העלולה להיות מהותית בנפרד או בשילוב עם שגיאות אחרות. ראה 'סיכון ביקורת'.
סיכון טבוע	רמת הסיכון או החשיפה מבלי לקחת בחשבון פעולות שבהן ההנהלה נקטה או עשויה לנקוט (למשל, יישום בקרות). ראה 'סיכון בקרה'.
מהותיות	מושג ביקורת הנוגע לחשיבות של פריט מידע ביחס להשפעתו על תפקוד הישות שבה מתבצעת הביקורת. ביטוי למשמעותו או לחשיבותו היחסית של נושא מסוים בהקשר של התאגיד כולו.
הערכת סיכונים	תהליך המשמש לזיהוי והערכה של סיכונים וההשפעות הפוטנציאליות שלהם הערכות סיכונים משמשות לזיהוי אותם פריטים או תחומים שיש בהם סיכון גבוה, נקודות תורפה או חשיפה של התאגיד שיש לכלול בתוכנית הביקורת השנתית של מערכות המידע. הערכות סיכונים משמשות גם לניהול סיכוני ביצוע הפרויקט ותועלותו.

בדיקת מבססות	השגת ראיות ביקורת לגבי השלמות, הדיוק או הקיום של פעילויות או עסקאות במהלך תקופת הביקורת

קישורים לקווים מנחים

סוג	שם
קו מנחה	2202 - הערכת סיכונים בתכנון

תאריך כניסה לתוקף

תקן זה של ISACA נכנס לתוקף עבור כל פעילויות הביקורת וההבטחה של מערכות מידע החל מ-1 בנובמבר, 2013.