תקן 1005 לביקורת והבטחה של מערכות מידע - הקפדה מקצועית הולמת

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 1005 לביקורת והבטחה של מערכות מידע - הקפדה מקצועית הולמת

הצהרות

1005.1 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יפגינו הקפדה מקצועית הולמת, כולל ציות לתקני ביקורת מקצועיים ישימים בתכנון ובביצוע של התקשרויות ובדיווח על תוצאותיהן.

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- לבצע את ההתקשרות מתוך אמינות והקפדה.
- להפגין הבנה ומיומנות מספיקות כדי להשיג את יעדי ההתקשרות.
- לשמור על הטלת ספק מקצועית לאורך כל ההתקשרות.
- לשמור על מיומנות מקצועית על-ידי התעדכנות בהתפתחויות בתקנים המקצועיים וציות להם.
- להסביר לחברי הצוות את התפקידים ותחומי האחריות שלהם, ולהבטיח את הציות של הצוות לתקנים המתאימים בעת ביצוע ההתקשרויות.
- לטפל בכל החששות שעלו ביחס להחלת תקנים במהלך ביצוע ההתקשרות.
- לקיים תקשורת יעילה עם בעלי עניין רלוונטיים במהלך ההתקשרות.
- לנקוט באמצעים סבירים להגנה על מידע אשר מושג או מתקבל במהלך ההתקשרות מפני מחשיפה או גילוי בלתי מכוונים לגורמים בלתי מורשים.
- להוביל את כל ההתקשרויות תוך שמירה על קונצפט הבטחה סבירה בתודעה. רמת הבדיקות תשתנה בהתאם לסוג ההתקשרות.

הערה: הקפדה מקצועית הולמת פירושה הקפדה ומיומנות סבירות, ולא היעדר מוחלט של שגיאות או ביצועים יוצאי דופן.

מונחים

מונח	הגדרה
הטלת ספק מקצועית	גישה המחייבת הלך מחשבה חוקרני ובחינה ביקורתית של ראיות הביקורת. מקור: המוסד האמריקני לרואי חשבון (AICPA) AU 230.07

קישורים קווים מנחים

סוג	שם
קו מנחה	2005 - הקפדה מקצועית הולמת

תאריך כניסה לתוקף

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