תקן 1004 לביקורת והבטחה של מערכות מידע - צפי סביר

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 1004 לביקורת והבטחה של מערכות מידע - ציפיות סבירות

הצהרות

1004.1 **לאנשי המקצוע בתחום ביקורת והבטחה של מערכות מידע יהיה צפי סביר שניתן להשלים את ההתקשרות בהתאם לתקני הביקורת וההבטחה של מערכות המידע ובמקרה הצורך, בהתאם לתקני מקצוע ותעשיה הולמים אחרים או לתקנות רלוונטיות, וכי היא תוביל לחוות דעת או מסקנה מקצועית.**

1004.2 **לאנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יהיה צפי סביר שהיקף ההתקשרות מאפשר להגיע למסקנות בנושא הנדון ומיתייחס לכל המגבלות.**

1004.3 **לאנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יהיה צפי סביר שההנהלה מבינה את מחויבויותיה ואת אחריותה באשר לספק בעיתו מידע הולם ורלוונטי הדרוש לביצוע ההתקשרות.**

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- ליטול על עצמם התקשרות לביצוע הביקורת או ההבטחה של מערכות המידע רק אם ניתן להשלים את העבודה בהצלחה בהתאם לתקנים המקצועיים.
- ליטול על עצמם את התקשרות לביצוע הביקורת או ההבטחה של מערכות המידע רק אם ניתן להעריך את נושא ההתקשרות כנגד קריטריונים רלוונטיים.
- לבחון את היקף ההתקשרות לביצוע הביקורת או ההבטחה של מערכות המידע כדי לקבוע אם היא מתועדת בבירור ומאפשרת הסקת מסקנות בנוגע לנושא.
- לזהות הגבלות כלשהן המושמות על ההתקשרות לביצוע ולטפל בהן, לרבות הגבלת גישה למידע הולם, רלוונטי בזמן המתאים.
- לבחון אם ההיקף מספיק כדי לאפשר הבעת חוות דעת מבקר לגבי הנושא. הגבלות החלות על ההיקף עשויות להתרחש כאשר המידע הדרוש להשלמת ההתקשרות אינו זמין, כאשר מסגרת הזמן המופיעה בהתקשרות ההבטחה של מבקר מערכות המידע אינה מספיקה, או כאשר ההנהלה מנסה להגביל את ההיקף לתחומים נבחרים. במקרים שכאלה, ניתן לשקול סוגי התקשרות אחרים כגון תמיכה בדוחות כספיים מבוקרים, בסקירות של בקרות , בציות לתקנים ונהלים נדרשים או בציות להסכמים, רשיונות, חוקים ותקנות.

מונחים

מונח	הגדרה
חוות דעת מבקר	הצהרה רשמית מצדו של איש המקצוע בתחום הביקורת או ההבטחה של מערכות המידע, אשר מתארת את היקף הביקורת, ההליכים ששימשו להפקת הדוח והאם הממצאים אכן מאשרים עמידה בקריטריוני הביקורת. סוגי חוות הדעת הם: • **חוות דעת לא מסויגת**—לא מציינת שום חריגות או שהחריגות המצוינות אינן מסתכמות לכדי ליקוי משמעותי. • **חוות דעת מסויגת**—מציינת חריגות המסתכמות בליקוי משמעותי (אך לא נקודת תורפה מהותית) • **חוות דעת שלילית**—מציינת ליקוי משמעותי אחד או יותר המסתכם לכדי נקודת תורפה מהותית

	הערה: הימנעות ממתן חוות דעת מתרחשת כאשר למבקר אין אפשרות להשיג ראיות ביקורת עליהן ניתן לבסס חוות דעת, או אם לא ניתן לגבש חוות דעה עקב אינטראקציה אפשרית בין גורמי אי ודאות רבים והשפעתם המצטברת האפשרית.

קישורים לקווים מנחים

סוג	שם
קו מנחה	2004 - צפי סביר

תאריך כניסה לתוקף

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