תקן 1205 לביקורת והבטחה של מערכות מידע - ראיות

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).

הצהרות

1205.1 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישיגו ראיות הולמות ומסַפקות כדי להסיק מסקנות סבירות שעליהן יתבססו תוצאות ההתקשרות.

1205.2 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יעריכו עד כמה הראיות מסַפקות לתמיכה במסקנות ולהשגת יעדי ההתקשרות.

היבטים עיקריים

בעת ביצוע ההתקשרות, אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע נדרשים:

- להשיג ראיות הולמות ומסַפקות, כולל:
  - ההליכים כפי שבוצעו
  - התוצאות של ההליכים שבוצעו
  - מסמכי מקור (בפורמט אלקטרוני או בנייר), רשומות ומידע מסייע שתמכו בהתקשרות
  - ממצאים ותוצאות של ההתקשרות
  - תיעוד לכך שהעבודה בוצעה תוך ציות לחוקים, לתקנות ולכללי המדיניות החלים
- להכין תיעוד, אשר עליו:
  - להישמר ולהיות זמין לתקופת זמן ובפורמט התואמים למדיניות הארגון המבצע את הביקורת או ההבטחה ולתקנים מקצועיים, לחוקים ולתקנות הרלוונטיים
  - להיות מוגן מפני חשיפה או שינוי בלתי מורשים לכל אורך הכנתו ושמירתו
  - להיות מושמד כראוי בתום תקופת השמירה
- לשקול אם הראיה מספיקה כדי לתמוך בהערכה של רמת סיכון הבקרה בעת השגת הראיה כתוצאה ממְבדק בקרות .
- לזהות, להצליב ולקטלג כראוי את הראיה.
- לשקול מאפיינים כגון מקור, טבע (למשל, כתוב, מילולי, חזותי, אלקטרוני) ואוטנטיות (למשל, חתימות דיגיטלית וידנית, חותמות) של הראיה בעת הערכת מהימנותה.
- לשקול מהם האמצעים היעילים ביותר מבחינת עלות-תועלת וזמינות לאיסוף הראיות הדרושות כדי לעמוד ביעדים ובסיכונים של ההתקשרות. עם זאת, קושי או עלות אינם מהווים תירוץ תקף לוויתור על הליך נחוץ.
- לבחור את ההליך המתאים ביותר לאיסוף ראיות, בהתאם לנושא הנבדק (כלומר, טבעו, עיתוי הביקורת, שיקול דעת מקצועי). הליכים המשמשים להשגת הראיות כוללים:
  - תחקור ואמות
  - ביצוע מחדש
  - חישוב מחדש
  - חישוב
  - ניתוח אנליטי
  - בדיקה
  - תצפית
  - שיטות מקובלות אחרות
- לשקול את מקורו ואת טבעו של כל מידע המושג כדי להעריך את מהימנותו ודרישות נוספות לאימותו. באופן כללי, מהימנות הראיה גדול יותר כאשר היא:
  - כתובה ולא מילולית
  - מושגת ממקורות בלתי תלויים
  - מושגת על-ידי איש המקצוע ולא על-ידי הישות המבוקרת
  - מאושרת על-ידי גורם בלתי תלוי
  - נשמרת על-ידי גורם בלתי תלוי
  - מתקבלת כתוצאה מבדיקה
  - מתקבלת כתוצאה מתצפית

- להשיג ראיות אובייקטיביות שהן מספיקות כדי לאפשר לגורם בלתי תלוי ומוסמך לבצע

תקן 1205 לביקורת והבטחה של מערכות מידע - ראיות

היבטים עיקריים המשך

מחדש את הבדיקות ולהגיע לאותן התוצאות והמסקנות.

- להשיג ראיות התואמות למהותיות הנושא ולסיכון הכרוך בו.
- לשים דגש הולם על הדיוק והשלמות של המידע, כאשר המידע המושג מהתאגיד משמש את איש המקצוע, המבצע את הביקורת או ההבטחה של מערכות המידע, לצורך ביצוע הליכי ביקורת.
- לחשוף כל מצב שבו לא ניתן להשיג ראיות מספקות באופן שהוא עקבי עם מסירת תוצאות התקשרות הביקורת או ההבטחה של מערכות המידע.
- להגן על הראיות מפני גישה ושינויים בלתי מורשים.
- לשמור ראיות, לאחר השלמת עבודת הביקורת או ההבטחה של מערכות המידע, לאורך תקופת הזמן הנדרשת לשם ציות לכל החוקים, התקנות וכללי המדיניות החלים.

מונחים

מונח	הגדרה
ראיה הולמת	מדד האיכות של הראיה
ראיה מַספקת	מדד הכמות של הראיה; תומכת בכל השאלות המהותיות בנוגע ליעדים ולהיקף של הביקורת. ראה 'ראיה'.

קישורים לקווים מנחים

סוג	שם
קו מנחה	2205 - ראיות

תאריך כניסה לתוקף

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