תקן 1206 לביקורת והבטחה של מערכות מידע - שימוש בעבודה של מומחים אחרים

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 1206 לביקורת והבטחה של מערכות מידע - שימוש בעבודה של מומחים אחרים

הצהרות

1206.1 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישקלו להשתמש בעבודה של מומחים אחרים עבור ההתקשרות, במקרים המתאימים.**

1206.2 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יעריכו ויאשרו את מידת ההתאמה של הכישורים המקצועיים של המומחים האחרים וכן את המיומנות, הניסיון הרלוונטי, המשאבים, אי התלות ותהליכי בקרת האיכות של המומחים לפני ההתקשרות.**

1206.3 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יעריכו, יבחנו ויאמדו את עבודתם של המומחים האחרים כחלק מההתקשרות, ויתעדו את המסקנה לגבי היקף השימוש בעבודתם וההסתמכות עליה.**

1206.4 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יקבעו אם העבודה של המומחים האחרים, אשר אינם חלק מצוות ההתקשרות, נאותה ושלמה לצורך הסקת מסקנות לגבי יעדי ההתקשרות הנוכחית, ויתעדו בבירור את המסקנות.**

1206.5 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יקבעו אם ניתן להסתמך על העבודה של המומחים האחרים, ואם ניתן לשלבה ישירות בדוח או שיש להפנות אליה בנפרד.**

1206.6 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יחילו הליכי בדיקות נוספים לשם השגת ראיות הולמות ומספיקות, בנסיבות שבהן העבודה של המומחים האחרים לא מספקת ראיות הולמות ומספיקות.**

1206.7 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יספקו חוות דעת או מסקנה הולמת לגבי הביקורת, ויכללו כל מגבלת היקף שבגינה ראיות נדרשות לא הושגו באמצעות הליכי בדיקות נוספים.**

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- לשקול שימוש בעבודה של מומחים אחרים במהלך ההתקשרות כאשר קיימים אילוצים (למשל, ידע טכני הנדרש כתוצאה מאופי המשימות לביצוע, משאבי ביקורת מצומצמים, אילוצי זמן) העלולים לפגוע בעבודה שיש לבצעה, או כאשר ישנם יתרונות פוטנציאליים מבחינת איכות ההתקשרות.
- לתעד את ההשפעה על השגת יעדי ההתקשרות, אם לא ניתן להשיג את המומחים הדרושים, ולהוסיף משימות ספציפיות בתוכנית ההתקשרות כדי לנהל את דרישות הסיכון ודרישות ראיות.
- לשקול את אי התלות של מומחים אחרים בעת השימוש בעבודה שלהם.
- להשיג גישה לכל מסמכי העבודה, התיעוד התומך והדוחות של המומחים האחרים, כאשר גישה שכזו אינה יוצרת סוגיות משפטיות.
- לקבוע ולהסיק לגבי היקף השימוש בעבודה של מומחים אחרים וההסתמכות עליה, כאשר למומחים לא ניתנה גישה לרשומות עקב סוגיות משפטיות.
- לתעד את השימוש בעבודה של מומחים אחרים בדוח.

מונחים

מונח	הגדרה
מומחים אחרים	פנימיים או חיצוניים לתאגיד, מומחים אחרים מתייחס ל: • מבקר מערכות מידע ממשרד חיצוני לראיית חשבון. • יועץ ניהול. • מומחה בתחומה של ההתקשרות אשר מונה על-ידי ההנהלה הבכירה או על-ידי הצוות.

תקן 1206 לביקורת והבטחה של מערכות מידע - שימוש בעבודה של מומחים אחרים

קישורים לקווים מנחים

סוג	שם
קו מנחה	2206 - שימוש בעבודה של מומחים אחרים

תאריך כניסה לתוקף

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