תקן 1203 לביקורת והבטחה של מערכות מידע - ביצוע ופיקוח

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 Certified Information Systems Auditor® (CISA®) 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 1203 לביקורת והבטחה של מערכות מידע - ביצוע ופיקוח

הצהרות

1203.1 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יבצעו את העבודה בהתאם לתוכנית המאושרת של ביקורת מערכות המידע כדי להתמודד עם הסיכונים שזוהו, ובהתאם ללוח הזמנים המוסכם.

1203.2 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יפקחו על צוותי ביקורת מערכות המידע שמצויים באחריותם, כדי להשיג את יעדי הביקורת ולעמוד בבדרישות תקני הביקורת המקצועיים הרלוונטיים.

1203.3 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יקחו על עצמם רק משימות התואמות לידע ולמיומנויות שלהם, או משימות שלגביהן הם צופים שיש ביכולתם לרכוש את המיומנויות המתאימות במהלך ההתקשרות, או שיבצעו אותן תחת פיקוח.

1203.4 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישיגו ראיות הולמות ומספקות להשגת יעדי הביקורת. הממצאים והמסקנות של הביקורת יגובו על-ידי ניתוח ופרשנות הולמים של הראיות האלו.

1203.5 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יתעדו את תהליך הביקורת, תוך תיאור עבודת הביקורת וראיות הביקורת התומכות בממצאים ובמסקנות.

1203.6 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יזהו ויסיקו מסקנות על פי ממצאים.

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע נדרשים:

- להתאים את הכישורים והניסיון לצורכי ההתקשרות בעת הקצאת חברים לצוות.
- להוסיף משאבים חיצוניים, לצוות ביקורת מערכות המידע, במקרים המתאימים ולוודא שעבודתם נמצאת תחת פיקוח הולם.
- לנהל את התפקידיהם ותחומי אחריותם של חברים ספציפיים בצוות הביקורת של מערכות המידע לכל אורך ההתקשרות, תוך התייחסות לנקודות הבאות לכל הפחות:
  - תפקידי ביצוע וסקירה
  - אחריות לתכנון המתודולוגיה והגישה
  - יצירת תוכניות הביקורת או ההבטחה
  - ביצוע העבודה
  - התמודדות עם סוגיות, חששות ובעיות כשהם מופיעים
  - תיעוד והבהרה של הממצאים
  - כתיבת הדוח
- לוודא שכל משימה המבוצעת במסגרת ההתקשרות על-ידי חבר(י) צוות נבדקת על-ידי חבר צוות מתאים אחר.
- להשתמש בראיית הביקורת הטובה ביותר שניתן להשיגה. עליה להיות מתואמת לחשיבותו של יעד הביקורת ולזמן ולמאמץ הנדרשים להשגת הראיה.
- להשיג ראיה נוספת אם, לדעתו המקצועית, הראיה שהושגה אינה עומדת בקריטריונים ואינה הולמת ומספיקה כדי לחוות דעה או לתמוך בממצאים ובמסקנות.
- לסדר ולתעד את העבודה שבוצעה במהלך ההתקשרות – לפי הליכים מוגדרים, מתועדים ומאושרים מראש.
- לכלול בתיעוד את הפרטים הבאים:
  - יעדי הביקורת והיקף העבודה, תוכנית הביקורת, שלבי הביקורת שבוצעו, הראיות שנאספו, הממצאים, המסקנות וההמלצות
  - פרטים מספיקים שיאפשרו לאדם שקול ומעודכן לבצע מחדש את המשימות שבוצעו במהלך ההתקשרות ולהגיע לאותה המסקנה
  - זיהוי של האנשים שביצעו כל משימה ותפקידם בהכנה ובסקירה של התיעוד
  - התאריך שבו התיעוד הוכן ונבחן

תקן 1203 לביקורת והבטחה של מערכות מידע - ביצוע ופיקוח

היבטים עיקריים המשך

- להשיג תיאורים רלוונטיים בכתב מהמבוקר אשר מבהירים בצורה מפורטת את התחומים הקריטיים של ההתקשרות, סוגיות שהועלו והפתרון שניתן להן, וטענות שהציג המבוקר.
- לוודא שהתיאורים של המבוקר נושאים תאריך וחתומים על ידו, לאשרור אחריותו ביחס להתקשרות.
- לתעד ולשמור במסמכי העבודה כל תיאור שהתקבל במהלך ביצוע ההתקשרות, בין בכתב ובין בעל פה.

קישור לתקנים ולקווים מנחים

סוג	שם
תקן	1005 - הקפדה מקצועית הולמת
תקן	1205 - ראיות
תקן	1401 - דיווח
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.