תקן 1401 לביקורת והבטחה של מערכות מידע - דיווח

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 1401 לביקורת והבטחה של מערכות מידע - דיווח

הצהרות

1401.1 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יספקו, עם השלמת ההתקשרות, דוח שנועד לתיאור התוצאות, ובכלל זה:

- **זיהוי התאגיד, הנמענים המיועדים וכל הגבלה החלה על תוכנו ועל הפצתו**
- **ההיקף, יעדי ההתקשרות, תקופת הכיסוי והאופי, העיתוי ומימדי העבודה שבוצעה**
- **הממצאים, המסקנות וההמלצות**
- **כל סייג או הגבלה בהיקף שיש לאיש המקצוע המבצע את הביקורת וההבטחה של מערכות המידע ביחס להתקשרות**
- **חתימה, תאריך ותפוצה לפי התנאים של אמנת הביקורת או מכתב ההתקשרות**

1401.2 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יוודאו שהממצאים בדוח הביקורת מגובים על-ידי ראיות הולמות ומַספקות.

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- להשיג מהמבוקר, תיאורים רלוונטיים בכתב אשר מבהירים בצורה מפורטת את התחומים הקריטיים של ההתקשרות, סוגיות שהועלו והפתרון שניתן להן, וטענות שהציג המבוקר.
- לוודא שתאורי 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. עבור התקשרויות אישור, יש להשיג מהמבוקר תיאורים כתובים כדי לצמצם אפשרות לאי הבנה.
- להתאים את הפורמט והתוכן של הדוח כדי לתמוך בסוג ההתקשרות המבוצעת, כגון:
  - ביקורת (ישירה או אישור)
  - סקירה (ישירה או אישור)
  - הליכים מוסכמים
- לתאר בדוח חולשות מהותיות או משמעותיות ואת השפעתן על השגת יעדי ההתקשרות.
- לדון בתוכן טיוטת הדוח עם ההנהלה הממונה על הנושא לפני הסיכום וההפצה, ולכלול את תגובת ההנהלה לממצאים, למסקנות ולהמלצות בדוח הסופי, היכן שרלוונטי.
- לדווח על ליקויים משמעותיים וחולשות מהותיות בסביבת הבקרה למופקדים על המשילות, ובמקרים המתאימים, לרשות האחראית, ולחשוף בדוח כי אלה כבר דווחו.
- לאזכר דוחות נפרדים אחרים בדוח הסופי.
- לדווח להנהלת המבוקר על ליקויי בקרה פנימית שאינם משמעותיים אך גם אינם זניחים. במקרים כאלה צריכים לידע את האחראים על המשילות או הרשות האחראית על כך שליקויים אלה בבקרה הפנימית כבר דווחו להנהלת המבוקר.
- לזהות תקנים שיושמו בביצוע ההתקשרות, ולדווח על כל אי ציות לתקנים אלה, לפי העניין.

מונחים

מונח	הגדרה
מידע רלוונטי	בנוגע לבקרות, מידע שמגלה למבצע הערכה דבר מה משמעותי לגבי פעולתן של הבקרות שברקע או של רכיב בקרה. מידע המאשר ישירות את פועלת הבקרות הינו רלוונטי ביותר. מידע הנוגע באופן עקיף לפעולת הבקרות יכול גם להיות רלוונטי, אם כי פחות רלוונטי מאשר מידע ישיר. עיין ביעדי איכות המידע של COBIT 5
מידע מהימן	מידע שהוא מדויק, ניתן לאימות, ובא ממקור אובייקטיבי. עיין ביעדי איכות המידע של COBIT 5
מידע מסַפק	מידע נחשב למסַפק כאשר מבצעי ההערכה אספו ממנו כמות מספקת לשם הסקת מסקנה סבירה. עם זאת, כדי שמידע יהיה מסַפק, קודם כול עליו להיות מתאים. עיין ביעדי איכות המידע של COBIT 5
מידע מתאים	מידע רלוונטי (כלומר, מתאים למטרה לה הוא נועד), מהימן (כלומר, מדויק, ניתן לאימות וממקור אובייקטיבי) וזמין (כלומר, מופק ונמצא בשימוש במסגרת זמן מתאימה). עיין ביעדי איכות המידע שלCOBIT 5
מידע זמין	מידע אשר מופק ונמצא בשימוש במסגרת זמן המאפשרת למנוע או לגלות ליקויי בקרה לפני שהם הופכים למהותיים עבור התאגיד. עיין ביעדי איכות המידע של COBIT 5.

קישור לתקנים ולקווים מנחים

סוג	שם
קו מנחה	2401 - דיווח

תאריך כניסה לתוקף

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