תקן 1001 לביקורת והבטחה
1001 - אמנת ביקורת

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 1001 לביקורת והבטחה של מערכות מידע - אמנת ביקורת

הצהרות

1001.1 **הפונקצייה לביקורת והבטחה של מערכות מידע, תתעד את תפקידי הביקורת כראוי באמנת ביקורת, תוך ציון המטרה, האחריות, הסמכות ואחריותיות.**

1001.2 **הפונקצייה לביקורת והבטחה של מערכות מידע תדאג להסכמה על אמנת הביקורת ותביא לאישורה ברמה המתאימה בתוך התאגיד.**

היבטים עיקריים

פונקציית הביקורת וההבטחה של מערכות מידע אמורה:

- להכין אמנת ביקורת להגדרת הפעילויות של הביקורת וההבטחה הפנימיות של מערכות המידע בצורה מפורטת מספיק כדי להבהיר את הנקודות הבאות:
  - הסמכות, המטרה, תחומי האחריות והמגבלות, של הגורם המבצע את הביקורת וההבטחה של מערכות המידע
  - אי-התלות והאחריותיות של פונקציית הביקורת וההבטחה של מערכות המידע
  - התפקידים ותחומי האחריות של הגוף המבוקר במהלך פעילות ביקורת או פעילות הבטחה של מערכות מידע
  - תקנים מקצועיים שעל איש המקצוע בתחום הביקורת וההבטחה של מערכות מידע לציית להם בעת הביצוע של פעילויות הקשורות לביקורת והבטחה של מערכות מידע
- לבחון את אמנת הביקורת לפחות פעם בשנה, או בתדירות גבוהה יותר אם תחומי האחריות משתנים.
- לעדכן את אמנת הביקורת כנדרש כדי להבטיח שהמטרה ותחומי האחריות עדיין מתועדים באופן הולם.
- להציג באופן רשמי את אמנת הביקורת בפני הגוף שבו מתבצעת הביקורת בכל פעילות של ביקורת והבטחה של מערכות מידע.

מונחים

מונח	הגדרה
פעילות הבטחה	בחינה אובייקטיבית של ראיות למטרת הערכה של תהליכים של ניהול סיכונים, בקרה או פיקוח עבור התאגיד. הערה לגבי ההיקף: דוגמאות לכך כוללות פעולות הקשורות לפיננסים, ביצועים, ציות לנהלים ואבטחת מערכות
אמנת ביקורת	מסמך המאושר על-ידי הגורמים המופקדים על המשילות, אשר מגדירים את המטרה, הסמכות והאחריות של פעילות הביקורת הפנימית. האמנה אמורה: • לקבוע את מעמדה של פונקציית הביקורת הפנימית בתוך התאגיד • לאפשר גישה לרשומות, אנשי צוות ומתקנים פיזיים הרלוונטיים לביצוע של פעילות ביקורת והבטחה של מערכות מידע • להגדיר את היקף הפעילות של פונקציית הביקורת
פעילות ביקורת	משימת ביקורת, מטלה או פעילות סקירה ספציפית, כגון ביקורת, סקירת הערכה עצמית של בקרה, בחינת הונאה או ייעוץ. פעילות ביקורת עשויה לכלול מטלות או פעילויות מרובות המיועדות להשיג סדרה ספציפית של יעדים הקשורים זה לזה.

אי-תלות	החופש ממצבים המאיימים על האובייקטיביות או על מראית עין של אובייקטיביות. יש לטפל באיומים שכאלה על האובייקטיביות ברמת המבקר, ברמת הפעילות, ברמה הפונקציונלית וברמה הארגונית. *אי-תלות מתייחסת לאי-תלות מחשבתית ולמראית עין של אי-תלות.*

קישורים קווים מנחים

סוג	שם
קו מנחה	2001 - אמנת ביקורת

תאריך כניסה לתוקף

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