תקן 1003 לביקורת והבטחה של מערכות מידע - אי-תלות מקצועית

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).

ISACA 2012-2013 Professional Standards and Career Management Committee

Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

תקן 1003 לביקורת והבטחה של מערכות מידע - אי-תלות מקצועית

הצהרות

1003.1 איש המקצוע בתחום הביקורת וההבטחה של מערכות המידע יהיה עצמאי ואובייקטיבי הן בעמדה והן בנראות בכל הנושאים הקשורים להבת הביקורת וההבטחה.

היבטים עיקריים

אנשי מקצוע בתחום הביקורת וההבטחה של מערכות מידע אמורים:

- לבצע את ההתקשרות לביקורת והבטחה של מערכות המידע מתוך הלך רוח לא מגמתי וללא משוא פנים, בעת הטיפול בבעיות הקשורות להבטחה והגעה למסקנות.
- להיות בלתי תלויים בפועל, אך גם להפגין אי-תלות בכל עת.
- לחשוף את פרטי הליקוי בפני הגורמים המתאימים אם אי-התלות נפגעת בפועל או למראית עין.
- להעריך את אי התלות באופן קבוע יחד עם ההנהלה וועדת הביקורת, אם קיימת ועדה שכזו.
- להימנע מלמלא תפקידים שאינם קשורים לביקורת, במסגרת יוזמות של מערכות מידע, אשר דורשים נטילת תחומי אחריות ניהוליים, משום שתפקידים אלה עלולים לפגוע באי התלות של הגורם בעתיד.

מונחים

מונח	הגדרה
ליקוי	מצב הגורם לנקודת תורפה או ליכולת מופחתת להוצאה לפועל של יעדי ביקורת ליקוי באי התלות הארגונית ובאובייקטיביות האישית עשויים לכלול ניגודי עניינים אישיים, מגבלות היקף, הגבלת הגישה לרשומות, אנשי צוות, ציוד או מתקנים ומגבלות של משאבים (כגון מימון או ציוות).
אי-תלות	חופש ממצבים המאיימים על האובייקטיביות או על מראית עין של אובייקטיביות. יש לטפל באיומים שכאלה על האובייקטיביות ברמת המבקר, הפעילות, וברמות הפונקציונלית והארגונית. אי-תלות מתייחסת לאי-תלות מחשבתית ולמרעית עין של אי-תלות.
מרעית עין של אי-תלות	מניעת עובדות או נסיבות בעלות משמעות רבה כל כך שגורם חיצוני שקול ומיודע עלול להסיק, לאור העובדות והנסיבות הספציפיות, שהאמינות, האובייקטיביות או יכולת הטלת ספק מקצועית מצדם של החברה, פונקציית הביקורת או צוות הביקורת נפגעו.
אי-תלות מחשבתית	הלך רוח המאפשר להביע מסקנות ללא השפעות הפוגעות בשיקול הדעת המקצועי, וכך מאפשר לאדם לפעול מתוך אמינות, אובייקטיביות ויכולת מקצועית להטיל ספק.
אובייקטיביות	היכולת להפעיל שיקול דעת, להביע דעות ולהציג המלצות ללא משוא פנים

©2013 ISACA כל הזכויות שמורות.

קישורים קווים מנחים

סוג	שם
קו מנחה	2003 - אי-תלות מקצועית

תאריך כניסה לתוקף

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

© ISACA 2013 כל הזכויות שמורות.