

# תקן 1006 לביקורת והבטחה של מערכות מידע – מומחיות



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 מיישמים:

- 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 משמעותיים.

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 הכוללת את אנשי המקצוע בתחום הביקורת וההבטחה של מערכות מידע, וכן לידע, למימונות 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 הכוללת.
  - **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, טכניות ביקורת/הבטחה של מערכות מידע, משפחת המוצרים של COBIT® 5.

מילון מקוון של מונחים הנמצאים בשימוש ב-ITAF נמצא בכתובת [www.isaca.org/glossary](http://www.isaca.org/glossary).

**כתב ויתור:** ISACA יצר מדריך זה כדי שישמש רמה מינימלית 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](mailto:standards@isaca.org)). למספר הפקס (+1.847. 253. 1443) 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 1006 לביקורת והבטחה של מערכות מידע - מומחיות

הצהרות

- 1006.1** אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע, יחד עם גורמים אחרים המסייעים להם במשימתם, יהיו בעלי מומחיות וכישורים הולמים בביצוע ההתקשרויות של ביקורת והבטחה של מערכות מידע וכן תהיה להם המיומנות המקצועית לביצוע העבודה הדרושה.
- 1006.2** אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע, יחד עם גורמים אחרים המסייעים להם במשימתם, יהיו בעלי ידע הולם בנושא הנדון.
- 1006.3** אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישמרו על המיומנות המקצועית שלהם על-ידי רכישת מתמשכת של השכלה והכשרה מקצועית, הולמות.

היבטים  
עיקריים

- אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:
- להפגין זמינות של מיומנות מקצועית הולמת (כישורים, ידע וניסיון רלוונטיים להתקשרות המתוכננת) לפני תחילת העבודה.
  - להעריך אמצעים חלופיים להשגת הכישורים, כולל שימוש בקבלני משנה, הוצאת חלקים מהמשימות למיקור חוץ, דחיית המשימה עד למועד שבו כישורים שכאלה יהיו זמינים או בדרך אחרת, להבטחה שהכישורים המתאימים יהיו זמינים.
  - לוודא שחברי הצוות אשר אינם בעלי הסמכה CISA או הסמכה מקצועית רלוונטית אחרת, ואשר מעורבים בהתקשרות לביצוע הביקורת וההבטחה של מערכות המידע, יהיו בעלי השכלה פורמאלית, הכשרה וניסיון תעסוקתי מספיקים.
  - לספק הבטחה ברמה סבירה, בעת הובלת צוות לביצוע התקשרות ביקורת או הבטחה של מערכות מידע, שכל חברי הצוות הינם בעלי מיומנות ברמה המקצועית המתאימה לביצוע עבודתם.
  - לצבור ידע מספק בתחומים מרכזיים כדי לאפשר את ביצוע התקשרות הביקורת או ההבטחה של מערכות המידע בצורה אפקטיבית ויעילה, יחד עם מומחים וחברי צוות אחרים.
  - לעמוד בדרישות הכשרה מקצועית מתמשכת או התפתחות מקצועית של CISA או הסמכות מקצועיות רלוונטיות אחרות.
  - להתעדכן בידע המקצועי באופן קבוע באמצעות קורסי השכלה, סמינרים, כנסים, שידורי אינטרנט (webcasts) והכשרה תוך כדי העבודה, כדי לספק רמת שירות מקצועית ההולמת את דרישות התפקיד של מבצע ביקורת או הבטחה של מערכות מידע.

מונח	הגדרה
מיומנות	היכולת לבצע משימה, פעולה או פונקצייה ספציפית בצורה מוצלחת
מומחיות	מחזיק בכישורים ובניסיון

מונחים

סוג	שם
קו מנחה	2006 - מומחיות

קישורים  
לקווים  
מנחים

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

תאריך כניסה  
לתוקף