תקן 1201 לביקורת והבטחה של מערכות מידע - תכנון התקשרויות

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).

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 1201 לביקורת והבטחה של מערכות מידע - תכנון ההתקשרות

הצהרות

1201.1 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יתכננו כל התקשרות לביקורת והבטחה של מערכות מידע תוך התייחסות לגורמים הבאים:

- **יעד(ים), היקף, מסגרת זמן ותוצרים**
- **ציות לחוקים הרלוונטיים ולתקני ביקורת מקצועיים**
- **שימוש בגישה המבוססת על סיכונים במקרים המתאימים**
- **סוגיות ספציפיות להתקשרות**
- **דרישות תיעוד ודיווח**

1201.2 אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יפתחו ויתעדו תוכנית של פרויקט התקשרות לביצוע ביקורת או הבטחה של מערכות מידע, אשר תתאר את הנקודות הבאות:

- **האופי, היעדים, מסגרת הזמן ודרישות המשאבים של ההתקשרות**
- **התזמון וההיקף של הליכי הביקורת להשלמת ההתקשרות**

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- להבין את ההפעילות המבוקרת. היקף הידע הנדרש ייקבע על פי האופי של התאגיד, הסביבה שלו, תחומי הסיכון ויעדי ההתקשרות.
- לשקול קבלת הדרכה או הכוונה בנושא, בהתאם לחוקים, לתקנות, לכללים, להנחיות ולהוראות של הממשלה או התעשייה.
- לבצע הערכת סיכונים כדי לספק הבטחה סבירה שכל הנושאים המהותיים יטופלו כהלכה במהלך ההתקשרות. לאחר מכן ניתן לפתח אסטרטגיות ביקורת, רמות מהות ודרישות משאבים.
- לפתח את תוכנית פרויקט ההתקשרות באמצעות מתודולוגיות מתאימות לניהול פרויקטים כדי לוודא שהפעילויות יישארו במסלול הנכון ובתוך התקציב.
- לכלול בתוכנית סוגיות תלויות-משימה, כגון:
  - זמינות משאבים עם הידע, הכישורים והניסיון מתאימים
  - זיהוי כלים הדרושים לאיסוף ראיות, ביצוע בדיקות והכנה/סיכום של מידע לשם דיווח
  - קריטריוני הערכה שיהיו בשימוש
  - דרישות דיווח והפצה של דוחות
- לתעד את תוכנית פרויקט ההתקשרות לביצוע הביקורת או ההבטחה של מערכות המידע כדי כך שתכלול בבירור את הנושאים הבאים:
  - יעד(ים), היקף ותזמון
  - משאבים
  - תפקידים ותחומי אחריות
  - תחומי סיכון מזוהים וההשפעה שלהם על תוכנית ההתקשרות
  - כלים וטכניקות לשימוש
  - ראיונות לגילוי עובדות שיש לקיימם
  - מידע רלוונטי שיש להשיגו
  - הליכים לאימות או לתיקוף המידע שהושג והשימוש בו כראיה
  - הנחות בנוגע לגישה, למתודולוגיה, להליכים ולתוצאות ולמסקנות הצפויות
- לקבוע את מועד ביצוע ההתקשרות תוך התחשבות, במידת האפשר, בלוח הזמנים, בזמינות ובהתחייבויות ודרישות אחרות של ההנהלה והגוף המבוקר.
- להתאים את תוכנית הפרויקט במהלך הביצוע של התקשרות הביקורת או ההבטחה של מערכות המידע כדי לתת את הדעת לסוגיות העולות במהלך ההתקשרות, כגון סיכון חדש, הנחות לא נכונות או ממצאים הנובעים מהליכים שכבר בוצעו.
- עבור התקשרויות פנים-ארגוניות:
  - לתקשר את אמנת הביקורת לגוף המבוקר; במקרים המתאימים, יש להשתמש במכתב התחייבות או מסמך דומה להבהרה נוספת או לאשרר את המעורבות בהתקשרויות ספציפיות
  - להסביר את התוכנית לגוף המבוקר כך שיהיה מיודע באופן מלא, ויוכל לספק גישה הולמת לאנשים, למסמכים ולמשאבים אחרים בעת הצורך

כל הזכויות שמורות. ©2013 ISACA

תקן 1201 לביקורת והבטחה של מערכות מידע - תכנון ההתקשרות

היבטים עיקריים המשך

- עבור התקשרויות חוץ-ארגונית:
  - להכין מכתב התקשרות נפרד עבור כל התקשרות חיצונית לביצוע ביקורת והבטחה של מערכות מידע
  - להכין תוכנית פרויקט עבור כל התקשרות חיצונית לביקורת והבטחה של מערכות מידע. התוכנית צריכה ,לכל הפחות, לתעד את היעד(ים) וההיקף של ההתקשרות.

קישורים לקוים מנחים

סוג	שם
קו מנחה	2201 - תכנון התקשרות

תאריך כניסה לתוקף

תקן זה של ISACA נכנס לתוקף עבור כל התקשרויות ביקורת והבטחה של מערכות מידע החל מ-1 בנובמבר, 2013.

כל הזכויות שמורות.
© ISACA 2013