תקן 1207 לביקורת והבטחה של מערכות מידע - אי סדרים ומעשים לא חוקיים

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 1207 לביקורת והבטחה של מערכות מידע - אי סדרים ומעשים לא חוקיים

הצהרות

1207.1 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישקלו את הסיכון הטמון באי סדרים ובמעשים לא חוקיים במהלך ההתקשרות.**

1207.2 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ינקטו גישה של הטלת ספק מקצועית במהלך ההתקשרות.**

1207.3 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יתעדו כל אי סדר או מעשה לא חוקי וידווחו עליהם לגורמים המתאימים בהקדם.**

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- להפחית את סיכון הביקורת לרמה מתקבלת על הדעת בעת התכנון והביצוע של ההתקשרות על-ידי:
  - מודעות לכך ששגיאות מהותיות, ליקויי בקרה או מידע מסולף הנובעים מאי סדרים ומעשים לא חוקיים יכולים להתקיים, ללא קשר להערכת הסיכון הטמון באי סדרים ובמעשים לא חוקיים
  - השגת הבנה של התאגיד והסביבתו, כולל אמצעי בקרה פנימיים המיועדים למנוע או לגלות אי סדרים ומעשים לא חוקיים הקשורים לנושא, להיקף וליעדים של ההתקשרות
  - השגת ראיות הולמות ומספקות כדי לקבוע אם יש להנהלה או לגורמים אחרים בתאגיד ידע בפועל, חשדות או טענות על קיומם של אי סדרים או מעשים לא חוקיים
- להביא בחשבון קשרים יוצאי דופן או בלתי צפויים העשויים להצביע על סיכון לשגיאות מהותיות, ליקויי בקרה או מידע מסולף כתוצאה מאי סדרים ומעשים לא חוקיים במהלך ביצוע הליכי הביקורת.
- לתכנן ולבצע הליכים לבדיקת ההלימות של בקרות פנימיות ואת הסיכון שההנהלה עוקפת בקרות המיועדות למנוע או לגלות אי סדרים ומעשים לא חוקיים.
- להעריך אם שגיאות, ליקויי בקרה או מידע מסולף שזוהו מצביעים על אי סדר או מעשה לא חוקי. אם קיים חשש שכזה, יש להתחשב בהשלכות בנוגע להיבטים אחרים של ההתקשרות, ובמיוחד במה שנוגע למצגי ההנהלה.
- להשיג מצגים בכתב מההנהלה לפחות פעם בשנה, או לעתים יותר קרובות בהתאם להתקשרות, על מנת:
  - לאשר את אחריות ההנהלה לתכנון ולהטמעה של בקרות פנימיות למניעה ולגילוי של אי סדרים ומעשים לא חוקיים.
  - לחשוף את התוצאות הנוגעות לכל הערכת סיכונים המצביעה על קיום אפשרי של שגיאות, ליקויי בקרה או מידע מסולף כתוצאה מאי סדרים או מעשים לא חוקיים.
  - לחשוף את ידיעת ההנהלה על אי סדרים ומעשים לא חוקיים, המשפיעים על התאגיד בהקשר להנהלה ולעובדים הממלאים תפקידים משמעותיים בבקרה הפנימית.
  - לחשוף את ידיעת ההנהלה על טענות או חשדות לאי סדרים ולמעשים לא חוקיים המשפיעים על התאגיד, כפי שנמסרו על ידי עובדים, עובדים לשעבר, גופי פיקוח ואחרים.
- לדווח בזמן:
  - לדרג הניהולי המתאים על כל מידע שזוהה או הושג לגבי קיום אפשרי של אי סדרים מהותיים או מעשיים לא חוקיים
  - למופקדים על המשילות על כל אי סדר מהותי ומעשה לא חוקי שבהם מעורבים הנהלה או עובדים הממלאים תפקיד משמעותי בבקרה הפנימית
- לדווח לאחראים על המשילות על כל חולשה מהותית בעיצוב וביישום בקרות פנימיות שנועדו למנוע ולגלות אי סדרים ומעשים לא חוקיים אשר זוהו במהלך ההתקשרות, אפילו אם הם מחוץ להיקפה המוגדר.

תקן 1207 לביקורת והבטחה של מערכות מידע - אי סדרים ומעשים לא חוקיים

היבטים עיקריים המשך

- לשקול את דרישות הדיווח המשפטיות והמקצועיות החלות לפי הנסיבות.
- לשקול פרישה מביצוע ההתקשרות אם שגיאות מהותיות, ליקויי בקרה, מידע מסולף או מעשים לא חוקיים משפיעים על המשך הביצוע של ההתקשרות.
- לתעד את כל התקשורות, התכנונים, התוצאות, ההערכות והמסקנות בנוגע לאי סדרים מהותיות ולמעשים לא חוקיים שדווחו להנהלה, לאחראים על המשילות, לגופי הפיקוח ואחרים.

מונחים

מונח	הגדרה
אי סדר	הפרה של מדיניות ניהול או דרישת הסדרה שנקבעה. עשוי להיות מורכב מסילוף מידע מכוון או השמטה מכוונת של מידע בנוגע לתחום הנמצא תחת ביקורת או לתאגיד ככלל, רשלנות חמורה או מעשים לא חוקיים שלא במכוון.
סילוף מידע מהותי	הצהרה שקרית במתכוון או שלא במתכוון המשפיעה על התוצאות של הביקורת במידה משמעותית
הטלת ספק מקצועית	גישה המחייבת הלך מחשבה חוקרני ובחינה ביקורתית של ראיות הביקורת. מקור: המוסד האמריקני לרואי חשבון(AICPA) AU 230.07

קישור לתקנים והנחיות וקוויו מנחים

סוג	שם
תקן	1008 - קריטריונים
תקן	1202 - הערכת סיכונים בתכנון
תקן	1205 - ראיות
קו מנחה	2206 - שימוש בעבודה של מומחים אחרים
קו מנחה	2207 - אי סדרים ומעשים לא חוקיים

תאריך כניסה לתוקף

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