תקן 1204 לביקורת והבטחה של מערכות מידע - מהותיות

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 1204 לביקורת והבטחה של מערכות מידע - מהותיות

הצהרות

1204.1 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יקחו בחשבון חולשות פוטנציאליות או היעדר של בקרות בזמן תכנון התקשרות, ואם חולשות או היעדר בקרות אלו עלולות להוביל לליקוי משמעותי או לחולשה מהותית.**

1204.2 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יתחשבו במהותיות ובקשר שלה לסיכון הביקורת בעת קביעת האופי, התזמון וההיקף של הליכי הביקורת.**

1204.3 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יקחו בחשבון את ההשפעה המצטברת של חולשות או ליקויי בקרה לא מהותיים, ואם היעדר בקרות מוביל לליקוי משמעותי או חולשה מהותית.**

1204.4 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע יספקו את הפרטים הבאים בדוח:**

- **היעדרן של בקרות או בקרות לא יעילות**
- **חשיבות ליקוי הבקרה**
- **הסבירות שחולשות אלו יובילו לליקוי משמעותי או לחולשה מהותית**

היבטים עיקריים

בעת ביצוע התקשרות, אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- להחיל את רעיון המהותיות בעת:
  - תכנון וביצוע של ההתקשרות
  - הערכת ההשפעה של פריטים, תהליכים, בקרות או שגיאות ספציפיים

  כל ליקוי, חולשה או היעדרם של מדיניות, הליכים ובקרות הולמים צריכים להיבחן בנסיבות המסוימות של ההתקשרות.
- להתחשב בהגדרות של מהותיות כאשר רשויות חקיקה או הסדרה מספקות אותן.
- לשים לב לכך שהערכת המהותיות וסיכון הביקורת עשויים להשתנות מפעם לפעם, בהתאם לנסיבות ולסביבה המשתנה.
- לנסות להפחית את סיכון הביקורת לרמה מתקבלת על הדעת ולעמוד ביעדים בעת התכנון והביצוע של ההתקשרות.
- להתחשב במהותיות בעת קביעת האופי, התזמון וההיקף של הליכי הביקורת.
- להפחית את סיכון הביקורת בתחומים בעלי מהותיות יותר גבוהה באמצעות הרחבת הבדיקה של הבקרות (הפחתת סיכון הבקרה) ו/או הרחבת ההליכים של הבדיקות המבססות (הפחתת סיכון הגילוי).
- להעריך את ההשפעה של בקרות מפצות והאם הן יעילות בקביעה אם ליקוי בקרה או צירוף של ליקויים מהווה חולשה מהותית.
- לשקול את ההשפעה המצטברת של שגיאות או כשלי בקרה מרובים בעת קביעת המהותיות.
- לשקול לא רק את מימדיהם אלא גם את אופיים של ליקויי הבקרה, ואת הנסיבות המיוחדות להתרחשותם, בעת ביצוע הערכת השפעתם הכוללת על חוות הדעת או המסקנה של הביקורת.

מונחים

מונח	הגדרה
סיכון הביקורת	הסיכון להסקת מסקנה שגויה בהתבסס על ממצאי הביקורת. שלושת המרכיבים של סיכון הביקורת הם: • סיכון בקרה • סיכון גילוי • סיכון טבוע
חולשה מהותית	ליקוי או צירוף של ליקויים בבקרה פנימית, כך שקיימת אפשרות סבירה שלא יימנע או לא יתגלה בזמן סילוף מידע מהותי. חולשה בבקרה נחשבת למהותית אם היעדר הבקרה מכשיל את היכולת להבטיח באופן סביר שיעדי הבקרה יושגו. חולשה המסווגת כמהותית מצביעה על הנקודות הבאות: • בקרות לא קיימות ו\או לא בשימוש ו\או לא הולמות • יש צורך בהסלמה קיים יחס הפוך בין מהותיות לבין רמת סיכון ביקורת המתקבל על דעתם של אנשי המקצוע בתחום הביקורת או ההבטחה של מערכות המידע, כלומר, ככל שרמת המהותיות גבוהה יותר, כן יהיה סיכון ביקורת הקביל נמוך יותר, *ולהפך*.
מהותיות	מושג ביקורת הנוגע לחשיבות של פריט מידע ביחס להשפעתו על תפקוד הישות שבה מתבצעת הביקורת. ביטוי למשמעותו או לחשיבותו היחסית של נושא מסוים בהקשר של התאגיד כולו.

קישור לתקנים והנחיות ולקוויו מנחים

סוג	שם
תקן	1201 - תכנון התקשרות
תקן	1202 - הערכת סיכונים בתכנון
תקן	1207 - אי סדרים ומעשים לא חוקיים
תקן	1401 - דיווח
קו מנחה	2202 - הערכת סיכונים בתכנון
קו מנחה	2004 - מהותיות

תאריך כניסה לתוקף

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