תקן 1008 לביקורת והבטחה של מערכות מידע - קריטריונים

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 1008 לביקורת והבטחה של מערכות מידע - קריטריונים

הצהרות

1008.1 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ייבחרו קריטריונים, על פיהם יעריכו את הנושא, כך שיהיו אובייקטיביים, רלוונטיים, מדידים, מובנים, מוכרים, מהימנים מוסמכים ונהירים לכל הקוראים והמשתמשים של הדוח או זמינים להם.**

1008.2 **אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע ישקלו את מקור הקריטריונים ויתמקדו בקריטריונים שנקבעו על ידי גופים מוסמכים ורלוונטיים לפני שיקבלו קריטריונים מוכרים פחות.**

היבטים עיקריים

אנשי מקצוע בתחום ביקורת והבטחה של מערכות מידע אמורים:

- לשקול בזהירות את בחירת הקריטריונים ולהיות מסוגלים להצדיק את הבחירה.
- להפעיל שיקול דעת מקצועי כדי להבטיח שבעת החלתם, השימוש בקריטריונים יאפשר פיתוח של חוות דעת או מסקנה הוגנת ואובייקטיבית, אשר לא תטעה את הקורא או המשתמש. ידוע כי ההנהלה עשויה להגדיר קריטריונים שלא יענו על כל הדרישות.
- לשקול את מידת ההתאמה והזמינות של הקריטריונים בעת קביעת דרישות ההתקשרות.
- במקרים בהם קריטריונים אינם זמינים, חסרים או נתונים לפרשנות, יש לכלול תיאור וכל מידע אחר הדרוש כדי להבטיח שהדוח יהיה הוגן, אובייקטיבי ומובן, ולכלול בדוח את ההקשר לשימוש בקריטריונים.

יש להעריך את ההתאמה וההלימה של קריטריוני הערכת הנושא מול חמשת קריטריוני ההתאמה הבאים:

- **אובייקטיביות**—הקריטריונים חייבים להיות נטולים מכל הטיה העלולה להשפיע לרעה על הממצאים והמסקנות של איש המקצוע ולפיכך עלולים להטעות את המשתמשים בדוח.
- **שלמות**—הקריטריונים צריכים להיות שלמים במידה מספקת כדי שכל הקריטריונים שיכולים להשפיע על מסקנות איש המקצוע לגבי הנושא יהיו מזוהים וייעשה בהם שימוש בעת ביצוע התקשרות הביקורת או ההבטחה של מערכות המידע.
- **רלוונטיות**—הקריטריונים צריכים להיות רלוונטיים לנושא ולתרום לממצאים ולמסקנות העומדים ביעדים של התקשרות הביקורת או ההבטחה של מערכות המידע.
- **מדידות**—הקריטריונים צריכים לאפשר מדידה עקבית של הנושא ופיתוח מסקנות עקביות בעת החלתם על-ידי אנשי מקצוע שונים בנסיבות דומות.
- **מובנות**—הקריטריונים צריכים להיות ברורים ולא להיות נתונים לפרשנויות שונות מהותית מצדם של המשתמשים המיועדים.

מידת הקבלה של קריטריונים מושפעת מזמינותם למשתמשים בדוח של איש המקצוע, כך שיבינו את יסוד פעילות ההבטחה ואת רלוונטיות הממצאים והמסקנות. מקורות יכולים לכלול קריטריונים שהם:

- **מוכרים**—הקריטריונים צריכים להיות מוכרים מספיק כדי שהשימוש בהם לא יוטל בספק על-ידי המשתמשים המיועדים.
- **מוסמכים**—הקריטריונים שנבחרים צריכים לשקף הצהרות מוסמכות בתחום והם צריכים להלום את הנושא. לדוגמה, הצהרות מוסמכות יכולות להתקבל מגופים מקצועיים, קבוצות בתעשייה, גורמי ממשל וגופי פיקוח.

- **זמינים לציבור**—על הקריטריונים להיות זמינים למשתמשי הדוח של איש המקצוע. דוגמאות כוללות תקנים שפותחו על-ידי גופים מקצועיים לראיית חשבון ולביקורת כגון ISACA, איגוד רואי החשבון הבינלאומי (IFAC) וגופים ממשלתיים או מקצועיים מוכרים אחרים.
- **זמינים לכל המשתמשים**—כאשר הקריטריונים אינם זמינים לציבור, יש להביא אותם לידיעת כל המשתמשים באמצעות טענות המהוות חלק מהדוח של איש המקצוע. טענות מורכבות מהצהרות, לגבי הנושא, העומדות בדרישות של קריטריונים מתאימים כך שיהיו ניתנות לביקורת.

היבטים עיקריים המשך

בנוסף להתאמה ולזמינות צריכה בחירת הקריטריונים להבטחת מערכות מידע גם לקחת בחשבון את המקור – מבחינת השימוש והקהל הפוטנציאלי שלהם. לדוגמה, בעת עיסוק ברגולציות ממשלתיות, סביר שיתאים במיוחד השימוש בקריטריונים המבוססים על טענות שפותחו מתוך החוקים והתקנות החלים על הנושא. במקרים אחרים, ייתכן שקריטריונים של התעשייה או לשכות מסחר יהיו רלוונטיים יותר. להלן מפורטים מקורות אפשריים לקריטריונים, לפי הסדר שבו יש לשקול אותם:

- **קריטריונים שנקבעו על-ידי ISACA**—אלה קריטריונים ותקנים זמינים לציבור אשר עברו סקירת עמיתים ותהליך יסודי של בדיקת נאותות על ידי מומחים בינלאומיים מוכרים בתחומי ממשל, בקרה, אבטחה והבטחה של טכנולוגיות המידע.
- **קריטריונים שנקבעו על-ידי גופי מומחים אחרים**—בדומה לתקנים ולקריטריונים של ISACA, קריטריונים אלה רלוונטיים לנושא והם פותחו ונחשפו לסקירת עמיתים ועברו תהליך יסודי של בדיקת נאותות על ידי מומחים בתחומים שונים.
- **קריטריונים שנקבעו על-ידי חוקים ותקנות**—אף על פי שחוקים ותקנות יכולים לספק בסיס לקריטריונים, יש לנקוט זהירות בשימוש בהם. לעתים קרובות, הניסוח שלהם מורכב ויש לו משמעות משפטית ספציפית. במקרים רבים, ייתכן שיהיה צורך לנסח את הדרישות מחדש כטענות. יתר על כן, הבעת דעה לגבי חוקים מוגבלת בדרך כלל לאנשי מקצוע בתחום המשפט.
- **קריטריונים שנקבעו על-ידי תאגידים שאינם מקפידים על הליכים תקינים**—אלה כוללים קריטריונים רלוונטיים אשר פותחו על-ידי תאגידים אחרים שאינם מקפידים לפעול על פי תהליכים נאותים ואשר לא הועמדו לבחינת הציבור ולדיון ציבורי.
- **קריטריונים שפותחו במיוחד עבור ההתקשרות לביקורת או להבטחה של מערכות המידע**—אף על פי שקריטריונים שפותחו במיוחד עבור ההתקשרות לביקורת או להבטחה של מערכות המידע עשויים להיות הולמים, יש לנקוט משנה זהירות כדי להבטיח שקריטריונים אלה אכן עומדים בדרישות קריטריוני ההתאמה, בפרט שלמות, מדידות ואובייקטיביות. קריטריונים שפותחו במיוחד עבור התקשרות לביקורת או להבטחה של מערכות מידע מופיעים בצורת טענות.

יש לבחון בקפידה את קריטריוני הבחירה. אף על פי שחשוב לציית לחוקים ולתקנות מקומיים ויש להתייחס לכך כאל דרישה מחייבת, ברור שהתקשרויות רבות של ביקורת והבטחה של מערכות מידע כוללות תחומים, כגון ניהול שינויים, בקרות טכנולוגיות מידע כלליות ובקרת גישה, שאינם מכוסים על ידי החוק והתקנות. בנוסף, ענפים מסוימים, כגון ענף כרטיסי התשלום, קבעו דרישות חובה שיש לעמוד בהן. במקרים בהם דרישות החוק מבוססות עקרונות, איש המקצוע חייב לוודא שהקריטריונים שנבחרו עומדים ביעד ההתקשרות.

במהלך ההתקשרות, עשוי מידע נוסף להוביל לביטול הצורך בקריטריונים מסוימים לשם השגת היעדים. בנסיבות אלה, עבודה נוספת הקשורה לקריטריונים אינה נחוצה.

מונחים

מונח	הגדרה
קריטריונים	התקנים ובוחני-הביצועים (benchmarks) המשמשים למדידה ולהצגה של הנושא, ושכנגדם מבקר מערכות המידע מעריך את הנושא. הקריטריונים צריכים להיות: • אובייקטיביים—ללא הטיה • שלמים—הם צריכים לכלול את כל הגורמים הרלוונטיים להסקת מסקנה • רלוונטיים—הם צריכים להיות קשורים לנושא • מדידים—הם צריכים לאפשר מדידה עקבית בהתקשרות אישור, מדובר בבוחני-ביצועים שכנגדם ניתן להעריך את הטענה הכתובה של ההנהלה בנושא. מבצע הפעילות מגבש מסקנה הנוגעת לנושא תוך התייחסות לקריטריונים המתאימים.

קישורים לקווים מנחים

סוג	שם
קו מנחה	2008 - קריטריונים

תאריך כניסה לתוקף

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