תקני ביקורת מערכות מידע
אמנת ביקורת
מסמך מס' S1

Information Systems Audit and Control Association

טבעה המתמחה של ביקורת מערכות מידע והכישורים הנחוצים לביצוע ביקורות מסוג זה מחייבים תקנים שמתייחסים במפורש לתחום הביקורת של מערכות מידע. אחת ממטרותיו של ארגון Information Systems Audit and Control Association® (ISACA®) היא לקדם ברחבי העולם תקנים שיתנו מענה לחזון של הארגון. פיתוחם והנחלתם של תקני ביקורת מערכות מידע מהווים אבן פינה בתרומתו של ארגון ISACA לקהילת העוסקים בביקורת. המסגרת הכוללת של תקני ביקורת מערכות מידע מספקת הנחיות במספר רמות:

- **התקנים** מגדירים את דרישות החובה בכל הקשור לביקורת מערכות מידע ודיווח. התקנים מיידעים:
  - את מבקרי מערכות המידע בדבר הרמה המינימלית של ביצועים קבילים הנדרשת כדי לעמוד בחובות המקצועיות המפורטות בקוד האתיקה המקצועית של ארגון ISACA
  - את ההנהלה וגופים נוספים בעלי עניין בדבר הציפיות המקצועיות ממי שעוסקים בתחום בפועל
  - את המחזיקים בתעודת מבקר מערכות מידע מוסמך – Certified Information Systems Auditor® (CISA®) – בדבר הדרישות. אי-ציות לתקנים אלה עשוי להביא לפתיחתה של חקירה בנוגע להתנהלותו של המחזיק בתעודת CISA, שתנוהל על ידי מועצת המנהלים של ארגון ISACA או על ידי ועדה מתאימה של ארגון ISACA, ובסופו של דבר, לנקיטת אמצעים משמעתיים.
- **ההנחיות** מספקות הדרכה לגבי היישום של תקני ביקורת מערכות מידע. על מבקר מערכות המידע להביא אותן בחשבון בבואו לקבוע כיצד להטמיע את התקנים, להפעיל שיקול דעת מקצועי בכל הקשור ליישומם ולהיות מוכן להצדיק כל חריגה. הנחיות ביקורת מערכות מידע מיועדות לספק מידע נוסף בכל הקשור לעמידה בתקנים של ביקורת מערכות מידע.
- **הנהלים** מספקים דוגמאות לנהלים שלפיהם עשוי מבקר מערכות מידע לפעול במסגרת התקשרות לעריכת ביקורת. מסמכי הנהלים מספקים מידע בדבר האופן שבו יש לעמוד בדרישות התקנים בעת ביצוע עבודת ביקורת מערכות מידע, אולם הם אינם מגדירים את הדרישות. נוהלי ביקורת מערכות מידע מיועדים לספק מידע נוסף בדבר אופן הציות לתקני ביקורת מערכות המידע.

יש להשתמש במשאבי **CobiT®** כמקור הדרכה לגבי נוהלי העבודה המיטביים. מסמך המסגרת *CobiT Framework* קובע כי "ההנהלה נושאת באחריות לשמירה על כל נכסי הארגון. על מנת למלא את תפקידה זה, כמו גם לצורך השגת יעדיה, על ההנהלה ליצור מערכת נאותה של בקרה פנימית". CobiT מספק מערך מפורט של בקרות וטכניקות בקרה עבור סביבת הניהול של מערכות המידע. בחירת החומר הרלבנטי ביותר מתוך CobiT ביחס להיקף הביקורת הספציפית מבוססת על בחירת תהליכי טכנולוגיית מידע ספציפיים מתוך CobiT והתייחסות לקריטריונים של מידע CobiT.

כפי שמוגדר במסמך המסגרת *CobiT Framework*, כל אחד מהבאים מאורגן לפי תהליך ניהול טכנולוגיית מידע. CobiT מיועד לשימושן של הנהלות הארגון ומחלקת טכנולוגיית המידע, כמו גם לשימושם של מבקרי מערכות מידע; לפיכך, השימוש בו מאפשר הבנה של היעדים העסקיים, פרסום של נוהלי עבודה מיטביים ומתן המלצות המתבססות על בסיס התייחסותי תקני, מובן לכל, שזוכה להערכה כללית. CobiT כולל:

- יעדי בקרה – גילויי-דעת כלליים ומפורטים בכל הקשור לבקרה טובה מינימלית.
- נוהלי בקרה – נימוקים מעשיים והדרכה בדבר "אופן היישום" של יעדי הבקרה.
- הנחיות ביקורת – הנחיות בכל אחד מתחומי הבקרה בסוגיות של כיצד להשיג הבנה, להעריך כל אחת מהבקרות, לאמוד את מידת הציות ולאמת את הסיכון הנובע מבקרות שאינן מיושמות.
- הנחיות להנהלה – הנחיות בסוגיות של כיצד לאמוד ולשפר את ביצועי תהליך טכנולוגיית המידע, שימוש במודלים להערכת בשלות, מדדים וגורמי הצלחה קריטיים. ההנחיות מספקות מסגרת מכוונת-הנהלה עבור הערכה-עצמית רציפה ופעילה של בקרות, ומתמקדות במיוחד בתחומים הבאים:
  - מדידת ביצועים – באיזו מידה פונקציית טכנולוגיית המידע תומכת בדרישות העסקיות? ניתן להשתמש בהנחיות להנהלה לצורך תמיכה בסדנאות הערכה-עצמית, וכן ניתן לעשות בהן שימוש לתמיכה ביישומם של נוהלי ניטור ושיפור מתמיד על ידי ההנהלה, כחלק מתוכנית פיקוח על טכנולוגיית המידע.
  - מציאת פרופיל לבקרת טכנולוגיית מידע – לאיזה תהליכי טכנולוגיית מידע ישנה חשיבות? מהם גורמי ההצלחה הקריטיים עבור הבקרה?
  - מודעות – מהם הסיכונים הכרוכים באי-השגת היעדים?
  - מבחני ביצועים – מה עושים האחרים? כיצד ניתן למדוד ולהשוות תוצאות עסקיות? ההנחיות להנהלה מספקות מדדים לדוגמה, שמאפשרים להעריך את ביצועי פונקציית טכנולוגיית המידע במונחים עסקיים. סמני-היעד העיקריים משמשים לזיהוי ולמדידת התפוקות של תהליכי טכנולוגיית המידע, וסמני הביצועים העיקריים משמשים להערכת איכות הביצועים של התהליכים, באמצעות מדידת הגורמים המאפשרים את התהליך. שימוש במודלים להערכת בשלות ומאפייני בשלות מאפשר לבצע הערכות יכולת ומבחני ביצועים, שמסייעים להנהלה למדוד את יכולת הבקרה, לזהות פערי בקרה ולפתח אסטרטגיות לשיפור הבקרה.

מילון מונחים מוצג באתר האינטרנט של ארגון ISACA, בכתובת *www.isaca.org/glossary*. המלים "ביקורת" ו-"סקירה" משמשות לחילופין.

הודעת פטור מאחריות: ארגון ISACA תכנן את מערך ההדרכה הזה לצורך הצגת הרמה המזערית של ביצועים קבילים הנדרשת כדי לעמוד בדרישות האחריות המקצועית המפורטות בקוד האתיקה המקצועית של ISACA עבור מבקרי מערכות מידע. ארגון ISACA נמנע מכל טענה שיש בשימוש במוצר זה כדי להבטיח תוצאה מוצלחת. אין לראות פרסום זה ככולל את כל הנהלים והמבחנים הנאותים שעליהם יש להורות, באופן סביר, לשם השגת תוצאות זהות. בעת קביעת ההלימות של נוהל או מבחן ספציפי כלשהו, על איש המקצוע בתחום הבקרות להפעיל את שיקול דעתו המקצועי לגבי נסיבות הבקרה הספציפיות המוצגות על ידי המערכות או סביבת טכנולוגיית המידע המסוימות.

מועצת התקנים של ארגון ISACA מחויבת לעריכת התייעצויות בהיקף רחב בעת הכנתם של התקנים, ההנחיות והנהלים לביקורת מערכות מידע. לפני פרסומם של מסמכים כלשהם, מפיקה מועצת התקנים טיוטות-חשיפה עם תפוצה בינלאומית לצורך קבלת הערות מהציבור הרחב. במידת הצורך, מועצת התקנים פונה גם לאנשי מקצוע בעלי התמחות או עניין מיוחדים בנושא העומד לדיון, לשם התייעצות. מועצת התקנים מפעילה תוכנית פיתוח מתמדת ומברכת על קבלת משוב מחברי ארגון ISACA ומגופים בעלי עניין אחרים לזיהוי סוגיות שמתעוררות ומחייבות תקנים חדשים. הצעות מכל סוג שהוא יש לשלוח בדואר-אלקטרוני (standards@isaca.org), באמצעות פקס (+1.847.253.1443) או באמצעות הדואר (הכתובת מופיעה בסוף המסמך) אל ISACA International Headquarters, לידיעת מנהל המחקר, תקנים והקשרים האקדמיים. חומר זה פורסם ביום 15 אוקטובר 2004.

S1 אמנת ביקורת

מבוא

01 תקני ISACA כוללים עקרונות בסיסיים ונהלים יסודיים, שמסומנים בכתב מודגש ומהווים עקרונות ונהלים מחייבים, וכן הנחיות בתחומים אלה.

02 מטרתו של תקן ביקורת מערכות מידע זה היא לקבוע ולספק הנחיות בכל הקשור לאמנת הביקורת שבה נעשה שימוש במהלך תהליך הביקורת.

תקן

03 המטרה, האחריות, הסמכות וחובת הדיווח של פונקציית ביקורת מערכות המידע או מטלות ביקורת מערכות המידע צריכות להיות מתועדות כיאות באמנת ביקורת או במכתב התקשרות.

04 ההסכמה והאישור לאמנת הביקורת או למכתב ההתקשרות צריכים להינתן על ידי הדרג המתאים בארגון או בארגונים.

פרשנות

05 יש להכין אמנת ביקורת עבור הפעילויות השוטפות של פונקציית הביקורת הפנימית של מערכות המידע. יש לבחון את אמנת הביקורת מידי שנה, או לעתים תכופות יותר אם הוכנסו שינויים בתחומי האחריות. מבקר פנים של מערכות מידע עשוי לעשות שימוש במכתב התקשרות כדי להבהיר טוב יותר או לאשר את מעורבותו במטלות מסוימות שקשורות או שאינן-קשורות לביקורת. במקרה של ביקורת מערכות מידע חיצונית, יש בדרך כלל להכין מכתב התקשרות עבור כל מטלה שקשורה או שאינה-קשורה לביקורת.

06 אמנת הביקורת או מכתב ההתקשרות צריכים להיות מפורטים דיים ולהציג את המטרה, תחומי האחריות והמגבלות של פונקציית הביקורת או מטלת הביקורת.

07 אמנת הביקורת או מכתב ההתקשרות צריכים להיבחן באופן תקופתי, על מנת לוודא שהמטרה ותחומי האחריות תועדו כנדרש.

08 יש לעיין בהנחיות המפורטות להלן לקבלת מידע נוסף בכל הקשור להכנתם של אמנת ביקורת או מכתב התקשרות:

- הנחיית ביקורת מערכות מידע G5, אמנת ביקורת
- מסמך המסגרת *Framework* CobiT, יעד בקרה M4

תאריך תחולה

09 תחולתו של תקן ISACA זה הנו לגבי כל הביקורות של מערכות מידע תחל ביום 1 בינואר 2005 או לאחר מועד זה.

חברי מועצת התקנים של ארגון Information Systems Audit and Control Association 2005-2004

יו"ר, סרג'יו פלגינסקי, CISA	PricewaterhouseCoopers, אורוגואי
סויין אלדאל	Aldal Consulting, נורבגיה
ג'ון בברידג', CISA, CISM, CFE, CGFM, CQA	משרד מבקר המדינה של מסצ'וסטס, ארה"ב
ד"ר קלאודיו סילי, CISA, CISM, CIA, CISSP	Value Partners, איטליה
קריסטינה לדסמה, CISA, CISM	Citibank NA Sucursal, אורוגואי
אנדרו מקלאוד, CISA, CIA, FCPA, MACS, PCP	חבר מועצת העיר בריסביין, אוסטרליה
ו. מירה, CISA, CISM, ACS, CISSP, CWA	Microsoft Corporation, ארה"ב
ראבי מותוקרישנן, CISA, CISM, FCA, ISCA	NextLinx India Private Ltd., הודו
פטר ניבלט, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, אוסטרליה
ג'ון ג. אוט, CISA, CPA	Aetna Inc., ארה"ב
תומס תומפסון, CISA	Ernst & Young, איחוד האמירויות

© Copyright 2004
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
טלפון: +1.847.253.1545
פקס: +1.847.253.1443
דואר-אלקטרוני: *standards@isaca.org*
אתר אינטרנט: *www.isaca.org*