תקן ביקורת מערכות מידע

מסחר אלקטרוני – מסמך S16

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 ®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.

יעדי בקרה לטכנולוגיית מידע ולטכנולוגיה קשורה (COBIT® - *Control Objectives for Information and related Technology*) מהווים מסגרת פיקוח על טכנולוגיית המידע (IT) ומספקים מערך של כלי תמיכה שמאפשר למנהלים לגשר על הפערים הקיימים בין דרישות הבקרה, הסוגיות הטכניות והסיכונים העסקיים. מסגרת COBIT מאפשרת פיתוח של מדיניות ברורה ונוהלי עבודה מיטביים לצורך בקרה על טכנולוגיית המידע בכל רחבי הארגונים. היא שמה דגש על ציות לתקנות, מסייעת לארגונים להגדיל את הערך המופק מטכנולוגיית המידע, מאפשרת "יישור קו" לרוחב הארגון ומפשטת את יישום התפישות של מסגרת COBIT.

מסגרת COBIT מיועדת לשימושן של הנהלות התחום העסקי ומחלקת טכנולוגיית המידע, כמו גם לשימושם של מבקרי מערכות מידע; לפיכך, השימוש בה מאפשר הבנה של היעדים העסקיים והטמעה של נוהלי עבודה מיטביים, וכן מתן המלצות המתבססות על מסגרת המובנת לכל, שזוכה להערכה כללית. ניתן להוריד את COBIT מאתר האינטרנט של ארגון ISACA, בכתובת *www.isaca.org/cobit*. כפי שמוגדר במסמך המסגרת COBIT Framework, כל אחד מהמוצרים ו/או המרכיבים הקשורים הבאים מאורגן על פי תהליך ניהול טכנולוגיית מידע:

- יעדי בקרה – גילויי-דעת כלליים בדבר בקרה מינימלית נאותה בכל הקשור לתהליכי טכנולוגיית מידע
- הנחיות להנהלה – הנחיות בסוגיות של כיצד לאמוד ולשפר את ביצועי תהליך טכנולוגיית המידע, תוך שימוש במודלים להערכת בשלות; תרשימי אחריות, דין וחשבון, התייעצות ו/או יידוע (RACI); הגדרת מטרות; וכן מדדים. ההנחיות מספקות מסגרת מכוונת-הנהלה עבור הערכה-עצמית רציפה ופעילה של בקרות, ומתמקדות במיוחד בתחומים הבאים:
  - מדידת ביצועים
  - הגדרת פרופיל לבקרת טכנולוגיית מידע
  - מודעות
  - מבחני ביצועים
- נוהלי הבקרה של COBIT – גילויי-דעת בנושא סיכון וערך, וכן הדרכה בדבר 'כיצד ליישם' יעדי בקרה
- מדריך הבטחת טכנולוגיית מידע – הנחיות עבור כל אחד מתחומי הבקרה, המתייחסות לדרך שבה ניתן להשיג הבנה, להעריך כל אמצעי בקרה, לבחון את מידת הציות ולבסס את הסיכון הכרוך באמצעי בקרה שלא יושמו.

מילון מונחים מוצג באתר האינטרנט של ארגון ISACA, בכתובת *www.isaca.org/glossary*. המילים "ביקורת" ו-"סקירה" משמשות לחילופין בתקנים, בהנחיות ובנהלים לביקורת מערכות מידע.

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 ארגון ISACA. ארגון ISACA נמנע מכל טענה שיש בשימוש במוצר זה כדי להבטיח תוצאה מוצלחת. אין לראות בפרסום זה ככולל את כל הנהלים והמבחנים הנאותים, או כמוציא מן הכלל נהלים ומבחנים אחרים, 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 המערכת 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 טיוטת-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 וקשרים אקדמיים. חומר זה פורסם ביום 1 בדצמבר 2007.

מסחר אלקטרוני – מסמך S16

מבוא

01 תקני ISACA כוללים את העקרונות הבסיסיים והנהלים החיוניים, שמסומנים בכתב מודגש (אותיות שחורות) ומהווים עקרונות ונהלים מחייבים, וכן הנחיות בתחומים אלה.

02 מטרתו של תקן ISACA זה היא לקבוע תקנים ולספק הנחיות בכל הקשור לסקירת ביקורת של סביבות מסחר אלקטרוני.

תקן

03 בעת עריכת סקירה של סביבות מסחר אלקטרוני, על מבקר מערכות המידע לבחון את הבקרות בתחום זה ולאמוד את הסיכונים, על מנת לוודא שעסקאות מסחר אלקטרוני נתונות לבקרה נאותה.

הערות

04 מסחר אלקטרוני מוגדר כתהליכים שבאמצעותם מנהלים ארגונים את עסקיהם באופן אלקטרוני עם לקוחותיהם, ספקיהם ושותפיהם העסקיים החיצוניים האחרים, תוך שימוש באינטרנט כטכנולוגיה מאפשרת. לפיכך, הוא כולל מודלים עסקיים של מסחר אלקטרוני המכונים עסק-לעסק (B2B) ועסק-לצרכן (B2C).

05 על מבקר מערכות המידע להשתמש בטכניקה או בגישה מתאימה להערכת סיכונים בעת פיתוח תוכנית ביקורת מערכות המידע הכוללת; התוכנית צריכה לכלול התייחסות לסביבות מסחר אלקטרוני.

06 על מבקר מערכות המידע לשקול להשתמש בטכניקות של ניתוח נתונים, לרבות שימוש בביקורת/הבטחה רציפה, שמאפשרת למבקרי מערכות מידע לנטר את אמינות המערכות על בסיס מתמשך ולאסוף ראיות ביקורת סלקטיביות באמצעות המחשב בעת ביצוע סקירה של פעילויות מסחר אלקטרוני.

07 רמת הכישורים והידע הדרושים לצורך הבנת ההשלכות של הבקרה וניהול הסיכונים בתחום המסחר האלקטרוני משתנים בהתאם לדרגת המורכבות של פעילויות המסחר האלקטרוני של הארגון.

08 על מבקר מערכות המידע להבין את טיבו ואת חיוניותו של התהליך העסקי הנתמך על ידי יישום המסחר האלקטרוני לפני תחילת הביקורת, על מנת שניתן יהיה להעריך את התוצאות בהקשר המתאים.

09 למידע נוסף בכל הקשור למסחר אלקטרוני יש לעיין בהנחיות הבאות:

- הנחיה G21 – סקירת מערכות לתכנון משאבי הארגון (ERP)
- הנחיה G22 – סקירת תהליך מסחר אלקטרוני עסק-לצרכן (B2C)
- הנחיה G24 – בנקאות באינטרנט
- הנחיה G25 – סקירה של רשתות וירטואליות פרטיות (VPN)
- הנחיה G33 – שיקולים כלליים בנושא השימוש באינטרנט
- נוהל P6 – קירות אש (Firewalls)
- מסגרת COBIT ויעדי בקרה

תאריך תחולה

10 תקן ISACA זה יחול על ביקורות של מערכות מידע החל מיום 1 בפברואר 2008.

חברי מועצת התקנים של ארגון ISACA בשנים 2007-2008	
יו"ר, ראבי מותוקרישנן, CISA, CISM, FCA, ISCA	Capco IT Services India Private Limited, הודו
בראד דייויד צ'ין, CISA, CPA	Google Inc., ארה"ב
סרג'יו פלגינסקי, CISA	ICI Paints, אורוגוואי
מריה גונזלס, CISA	משרד הפנים, ספרד
ג'ון הו צ'י, CISA, CISM, CBCP, CFE	Ernst & Young, סינגפור
אנדרו ג'. מקלאוד, CISA, CIA, FCPA, MACS, PCP	חבר מועצת העיר בריסביין, אוסטרליה
ג'ון ג. אוט, CISA, CPA	AmerisourceBergen, ארה"ב
ג'ייסון תומפסון, CISA	KPMG LLP, ארה"ב
מירה ונקאטש, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., ארה"ב

© 2007 ISACA. כל הזכויות שמורות.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
טלפון: +1.847.253.1545
פקס: +1.847.253.1443
דוא"ל: *standards@isaca.org*
אתר אינטרנט: *www.isaca.org*