תקני ביקורת מערכות מידע
אי-סדרים ופעולות בלתי-חוקיות
מסמך מס' S9

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 (ISACA®) Information Systems Audit and Control Association® 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 וקשרים אקדמיים. חומר זה פורסם ביום 1 ביולי 2005.

S9 אי-סדרים ופעולות בלתי-חוקיות

מבוא

01 תקני ISACA כוללים עקרונות בסיסיים ונהלים חיוניים, 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 לאי-סדרים ולפעולות בלתי-חוקיות שעל מבקר מערכות המידע להביא בחשבון תוך כדי תהליך הביקורת.

תקן

03 בעת תכנון וביצוע הביקורת, על מבקר מערכות המידע להביא בחשבון את הסיכון הכרוך באי-סדרים ובפעולות בלתי-חוקיות, על מנת להפחית את סיכון הביקורת לרמה נמוכה.

04 על מבקר מערכות המידע לשמור על גישה של ספקנות מקצועית במהלך הביקורת, ולהכיר באפשרות שעלולים להימצא סילופים מהותיים בגלל אי-סדרים ופעולות בלתי-חוקיות, ללא קשר להערכת הסיכונים שערך בנושא.

05 על מבקר מערכות המידע להכיר ולהבין את הארגון ואת הסביבה הארגונית, לרבות את הבקרות הפנימיות.

06 על מבקר מערכות המידע להשיג ראיות ביקורת מספיקות והולמות על מנת לקבוע אם ידוע להנהלה או לגורמים אחרים בארגון על אי-סדרים ופעולות בלתי-חוקיות בפועל, או על חשדות או טענות לאי-סדרים ולפעולות בלתי-חוקיות.

07 בעת ביצוע נוהלי הביקורת כדי להכיר ולהבין את הארגון ואת הסביבה הארגונית, על מבקר מערכות המידע להביא בחשבון קשרים יוצאי דופן או לא-צפויים שעלולים להצביע על הסיכון של סילופים מהותיים בגלל אי-סדרים ומעשים בלתי חוקיים.

08 על מבקר מערכות המידע לתכנן ולבצע נהלים לבדיקת הלימות הבקרה הפנימית והסיכון הכרוך בעקיפת הבקרות על ידי ההנהלה.

09 במקרה שמבקר מערכות המידע מגלה סילוף, עליו להעריך אם סילוף כאמור עלול להצביע על אי-סדרים או על מעשה בלתי-חוקי. אם כך הם פני הדברים, על מבקר מערכות המידע להביא בחשבון את ההשלכות שיש לכך בכל הקשור להיבטים אחרים של הביקורת, ובמיוחד בקשר למצגים של ההנהלה.

10 על מבקר מערכות המידע לקבל לידיו מצגים בכתב מההנהלה לפחות פעם בשנה, או לעתים תכופות יותר, בהתאם להסכם ההתקשרות לעריכת הביקורת. על ההנהלה:

- **לאשר את אחריותה לתכנון ולהטמעה של בקרות פנימיות לצורך מניעה וגילוי של אי-סדרים ופעולות בלתי-חוקיות.**
- **להביא לידיעת מבקר מערכות המידע את תוצאות הערכת הסיכונים המעידה שייתכן שחל סילוף משמעותי כתוצאה מאי-סדרים או ממעשה בלתי-חוקי.**
- **להביא לידיעת מבקר מערכות המידע את כל הידוע לה על אי-סדרים או על פעולות בלתי-חוקיות שיש בהם כדי להשפיע על הארגון בכל הקשור:**
  - **להנהלה**
  - **לעובדים שממלאים תפקיד משמעותי בבקרה הפנימית**
- **להביא לידיעת מבקר מערכות המידע את כל הידוע לה על טענות כלשהן לאי-סדרים או לפעולות בלתי-חוקיות, או על חשדות כלשהן לאי-סדרים או לפעולות בלתי-חוקיות שיש בהם כדי להשפיע על הארגון, כפי שנמסרו לה על ידי עובדים, עובדים לשעבר, רגולטורים או גורמים אחרים.**

11 אם מבקר מערכות המידע מזהה מקרה מהותי של אי-סדרים או מעשה בלתי-חוקי, או שמגיע לידיו מידע בדבר אפשרות לאי-סדרים או למעשה בלתי-חוקי, עליו להביא עניינים אלה לידיעת דרג ההנהלה המתאים בהקדם האפשרי.

12 אם מבקר מערכות המידע מזהה מקרה של אי-סדרים או מעשה בלתי-חוקי מהותי שמעורבים בהם ההנהלה או עובדים שממלאים תפקידים משמעותיים בבקרה הפנימית, על מבקר מערכות המידע להביא עניינים אלה באופן מסודר לידיעת הגורמים המופקדים על הפיקוח.

13 על מבקר מערכות המידע להודיע לדרג המתאים בהנהלה ולגורמים המופקדים על הפיקוח על חולשות מהותיות בתכנון ובהטמעה של הבקרה הפנימית המיועדת למנוע ולגלות אי-סדרים ופעולות בלתי-חוקיות, שהגיעו לידיעתו של מבקר מערכות המידע במהלך הביקורת.

14 אם מבקר מערכות המידע נתקל בנסיבות יוצאות-דופן שיש בהן כדי להשפיע על יכולתו של מבקר מערכות המידע להמשיך בביצוע הביקורת בגלל סילוף או מעשה בלתי-חוקי מהותיים, על מבקר מערכות המידע לבחון את החובות המשפטיות והמקצועיות החלות בנסיבות אלה, לרבות השאלה אם חלה חובה על מבקר מערכות המידע לדווח על הממצאים לגורמים שעמם התקשר בהסכם, או במקרים מסוימים – לגורמים המופקדים על הפיקוח או לרשויות הקובעות תקנות בעניינים אלה, או לשקול לפרוש מהסכם ההתקשרות.

15 על מבקר מערכות המידע לתעד את כל התקשורת, התכנון, התוצאות, ההערכות והמסקנות בכל הקשור לאי-סדרים ולפעולות בלתי-חוקיות מהותיים שדווחו להנהלה, לגורמים המופקדים על הפיקוח, לרגולטורים ולגורמים אחרים.

הערות

16 על מבקר מערכות המידע לעיין בהנחיית ביקורת מערכות מידע G19, אי-סדרים ופעולות בלתי-חוקיות, הכוללת הגדרה המפרטת מהם אי-סדרים ומעשה בלתי-חוקי.

17 על מבקר מערכות המידע להגיע למידה סבירה של ביטחון שאין סילופים מהותיים בגלל אי-סדרים ופעולות בלתי-חוקיות. אין באפשרות מבקר מערכות מידע להגיע לביטחון מוחלט, בגלל גורמים כגון הפעלת שיקול דעת, היקף הבדיקות והמגבלות הטבעיות של בקרות פנימיות. ראיות הביקורת שעומדות לרשות מבקר מערכות המידע במהלך הביקורת צריכות להיות משכנעות, ולא דווקא מוחלטות.

18 הסיכון שלא יתגלה סילוף מהותי שהוא תוצאה ממעשה בלתי-חוקי, גבוה יותר מהסיכון שלא יתגלה סילוף מהותי כתוצאה מאי-סדרים או משגיאה, מכיוון שפעולות בלתי-חוקיות עלולות להיות מלוות בתחבולות מורכבות שמטרתן להסתיר או להעלים אירועים או סילופים מכוונים מפני מבקר מערכות המידע.

19 על מבקר מערכות המידע להיעזר בניסיון העבר שלו ובהיכרותו עם הארגון במהלך ביצוע הביקורת. בעת עריכת חקירות וביצוע נוהלי הביקורת, אין לצפות ממבקר מערכות המידע להתעלם באופן מלא מניסיון העבר, אולם יש לצפות ממנו לשמור על רמה של ספקנות מקצועית. מבקר מערכות המידע אינו צריך להסתפק בראיות ביקורת שהן פחות ממשכנעות, בהתבסס על האמונה שההנהלה והגורמים המופקדים על הפיקוח הם ישרים ופועלים מתוך יושרה. על מבקר מערכות המידע והצוות שנשכר לצורך ביצוע הביקורת לדון במידת הפגיעות של הארגון לאי-סדרים ולפעולות בלתי-חוקיות כחלק מתהליך התכנון ולאורך כל הביקורת.

20 על מנת להעריך את הסיכון של קיומם של אי-סדרים מהותיים ופעולות בלתי-חוקיות, על מבקר מערכות המידע לשקול להשתמש באמצעים הבאים:

- ניסיון העבר שלו עם הארגון (לרבות ניסיונו בכל הקשור ליושר וליושרה של ההנהלה ושל הגורמים המופקדים על הפיקוח)
- המידע שהושג באמצעות תשאול ההנהלה
- מצגי ההנהלה וחתימות אישור של הבקרה הפנימית
- מידע מהימן אחר שהושג במהלך הביקורת
- הערכת ההנהלה את הסיכון של אי-סדרים ופעולות בלתי-חוקיות, והתהליך של ההנהלה לגילוי ולמתן מענה לסיכונים אלה

21 יש לעיין בהנחיות הבאות לצורך קבלת מידע נוסף בנושא אי-סדרים ופעולות בלתי-חוקיות:

- הנחיית ביקורת מערכות מידע G5, אמנת ביקורת
- מסמך המסגרת COBIT Framework, יעדי בקרה DS3, DS5, DS9, DS11 ו-PO6
- חוק Sarbanes-Oxley משנת 2002
- החוק נגד שחיתות במדינות זרות משנת 1977

תאריך תחולה

22 תקן ISACA זה יחול על כל הביקורות של מערכות מידע שתחילתן ביום 1 בספטמבר 2005 או לאחריו.

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

יו"ר, סרג'יו פלגינסקי, CISA	ICI Paints, 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	Tangerine Consulting, איטליה
קריסטינה לדסמה, CISA, CISM	Citibank NA Sucursal, אורוגואי
אנדרו מקלאוד, CISA, CIA, FCPA, PCP	חבר מועצת העיר בריסביין, אוסטרליה
ו. מירה, CISA, CISM, ACS, CWA	Microsoft Corporation, ארה"ב
ראבי מותוקרישנן, CISA, CISM, FCA, ISCA	Ikanos Communications, הודו
פטר ניבלט, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, אוסטרליה
ג'ון ג. אוט, CISA, CPA	AmerisourceBergen, ארה"ב
תומס תומפסון, CISA	Ernst & Young, איחוד האמירויות

© Copyright 2005
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*