לשכת המבקרים הפנימיים - ישראל

המועצה המקצועית

כללים מקצועיים

בתוקף: החל מ- 1.1.2009

ראשי פרקים

1. הגדרת מקצוע הביקורת הפנימית 5
1.1 המבקר הפנימי כיועץ 6
1.2 תקנים מקצועיים מקובלים בביקורת פנימית 6

2. הקוד האתי 7
2.1 מבוא 7
2.1.1 כללי 7
2.1.2 תחולה ואכיפה 8
2.2 עקרונות 8
2.3 כללי התנהגות 8
2.3.1 יושרה 8
2.3.2 אובייקטיביות 8
2.3.3 סודיות 9
2.3.4 יכולת 9

3. תקנים מקצועיים לביקורת פנימית 10
3.1 מבוא 10
3.1.1 מטרות התקנים המקצועיים 10
3.1.2 מושגים בשימוש בתקנים המקצועיים 10
3.1.3 מבנה התקנים המקצועיים 11
3.1.4 סוגים של שירותי ביקורת 11
3.1.5 תהליך קביעת התקנים המקצועיים המקובלים 12
3.2 תקני תכונות 12
[1000] מטרה, סמכות ואחריות 12
[1010] הסתמכות על הגדרת מקצוע הביקורת הפנימית, הקוד האתי והתקנים המקצועיים בתקנון ביקורת פנימית 13
[1100] אי-תלות ואובייקטיביות 13
[1200] מקצועיות וזהירות מקצועית ראויה 15
[1300] תוכנית הבטחת איכות ושיפור 16
3.3 תקני ביצוע 19
[2000] ניהול הביקורת הפנימית 19
[2100] אופי העבודה 21
[2200] תכנון מטלת ביקורת 23
[2300] ביצוע מטלת ביקורת 25
[2400] דיווח על התוצאות 26
[2500] ניטור ההתקדמות 28
[2600] דיווח על רמה מסוימת של סיכון בלתי סביר 29

4. מילון מושגים מקצועיים 30

5. הנחיות מקצועיות 33

6. ניירות עמדה (Position Papers) 33

7. נוהלי יעץ (Practice Advisories) 33

8. הנחיות לפרקטיקה (Practice Guides) 34

9. תדריכי ביקורת ושאלונים (Audit Guides & Questionnaires) 34

10. הנוסח האנגלי של התקנים המקצועיים 35

תוכן עניינים מפורט

1. הגדרת מקצוע הביקורת הפנימית 5
1.1 המבקר הפנימי כיועץ........ 6
1.2 תקנים מקצועיים מקובלים בביקורת פנימית........ 6

2. הקוד האתי 7
2.1 מבוא 7
2.1.1 כללי........ 7
2.1.2 תחולה ואכיפה 8
2.2 עקרונות 8
2.3 כללי התנהגות 8
2.3.1 יושרה........ 8
2.3.2 אובייקטיביות 8
2.3.3 סודיות........ 9
2.3.4 יכולת 9

3. תקנים מקצועיים לביקורת פנימית........ 10
3.1 מבוא 10
3.1.1 מטרות התקנים המקצועיים........ 10
3.1.2 מושגים בשימוש בתקנים המקצועיים 10
3.1.3 מבנה התקנים המקצועיים........ 11
3.1.3.1 כללי 11
3.1.3.2 תקני תכונות (Attribute)........ 11
3.1.3.3 תקני ביצוע (Performance)........ 11
3.1.3.4 תקני יישום (Implementation)........ 11
3.1.4 סוגים של שירותי ביקורת 11
3.1.4.1 שירותי הבטחה........ 11
3.1.4.2 שירותי ייעוץ 11
3.1.5 תהליך קביעת התקנים המקצועיים המקובלים 12
3.2 תקני תכונות........ 12
[1000] מטרה, סמכות ואחריות 12
[1010] הסתמכות על הגדרת מקצוע הביקורת הפנימית, הקוד האתי והתקנים המקצועיים בתקנון ביקורת פנימית 13
[1100] אי-תלות ואובייקטיביות........ 13
[1110] אי-תלות ארגונית 13
[1111] קשרי גומלין ישירים עם הדירקטוריון 13
[1120] אובייקטיביות אישית........ 14
[1130] פגיעה באי-התלות או באובייקטיביות........ 14
[1200] מקצועיות וזהירות מקצועית ראויה 15
[1210] מקצועיות 15
[1220] זהירות מקצועית ראויה........ 16
[1230] פיתוח מקצועי מתמשך 16
[1300] תוכנית הבטחת איכות ושיפור 16
[1310] הדרישות מתוכנית להבטחת איכות ושיפור........ 17
[1311] הערכות פנימיות........ 17
[1312] הערכות חיצוניות 17
[1320] דיווח על התוכנית להבטחת איכות ושיפור........ 18
[1321] שימוש במילים "נערך בהתאם לתקנים המקצועיים הבינלאומיים" 18
[1322] גילוי אי-עמידה בתקנים........ 18
3.3 תקני ביצוע........ 19
[2000] ניהול הביקורת הפנימית 19
[2010] תכנון 19
[2020] דיווח ואישור 20
[2030] ניהול משאבים........ 20
[2040] מדיניות ונהלים........ 20

[2050] תיאום 20
[2060] דיווח להנהלה הבכירה ולדירקטוריון 20
[2100] אופי העבודה 21
[2110] שליטה 21
[2120] ניהול סיכונים 21
[2130] בקרה 22
[2200] תכנון מטלת ביקורת 23
[2201] שיקולי התכנון 23
[2210] מטרות מטלת הביקורת 24
[2220] היקף מטלת ביקורת 24
[2230] הקצאת משאבים למטלת ביקורת 25
[2240] תוכנית ביקורת 25
[2300] ביצוע מטלת ביקורת 25
[2310] זיהוי מידע 25
[2320] ניתוח והערכה 25
[2330] תיעוד המידע 26
[2340] פיקוח עצמי של הביקורת 26
[2400] דיווח על התוצאות 26
[2410] קריטריונים לדיווח 26
[2420] איכות הדיווחים 27
[2421] טעויות והשמטות 27
[2430] שימוש במילים "נערך בהתאם לתקנים מקצועיים מקובלים" 27
[2431] גילוי אי-עמידה בתקנים המקצועיים 28
[2440] הפצת התוצאות 28
[2500] ניטור ההתקדמות 28
[2600] דיווח על רמה מסוימת של סיכון בלתי סביר 29

4. מילון מושגים מקצועיים 30

5. הנחיות מקצועיות 33

6. ניירות עמדה (Position Papers) 33

7. נוהלי יעץ (Practice Advisories) 33

8. הנחיות לפרקטיקה (Practice Guides) 34

9. תדריכי ביקורת ושאלונים (Audit Guides & Questionnaires) 34

10. הנוסח האנגלי של התקנים המקצועיים 35

לשכת המבקרים הפנימיים בישראל – הגדרת המקצוע

1. הגדרת מקצוע הביקורת הפנימית

ביקורת פנימית הינה פעילות בלתי תלויה ואובייקטיבית של הבטחה וייעוץ, אשר מיועדת להוסיף ערך ולשפר את פעולות הארגון. היא מסייעת לארגון להשיג את מטרותיו בהבאת גישה שיטתית וממוסדת, לשם הערכה ושיפור האפקטיביות של תהליכי ניהול סיכונים, בקרה, פיקוח ושליטה.
הביקורת הפנימית, בהגדרתה, נערכת על-פי התקנים המקצועיים לביקורת פנימית של לשכת המבקרים הפנימיים, אשר מטילים על הביקורת הפנימית חובות ותפקידים ייחודיים לה, של בדיקת תקינותן של פעולות הארגון מבחינת שמירה על החוקים, על הניהול התקין, על טוהר המידות ועל חיסכון ויעילות.

The Internal Auditing Definition

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Supporting the Definition are the *Standards for the Professional Practice of Internal Auditing* which include specific internal auditing duties and functions such as examining the propriety of the organization's compliance with laws, proper management, integrity, thrift and efficiency.

הגדרת הביקורת הפנימית אושרה ביום כ"ג כסלו תשס"א, 20 דצמבר 2000 על-ידי המועצה המקצועית של הלשכה בישראל. היא כוללת שתי פיסקות: הראשונה - כללית, המחייבת את כל לשכות ה-IIA בעולם, ואשר ניסוחה באנגלית אושר על-ידי מועצת ה-IIA ביוני 1999; והשניה - ייחודית למדינת ישראל, שנוספה, על-דעת ה-IIA, להגדרה הכללית עקב הצורך לעמוד בדרישות מהביקורת הפנימית, הנובעות מהחוק בישראל. ביום כ"ה בניסן תשס"ב, 7 באפריל 2002 אישרה המועצה המקצועית שינוי בפיסקה השניה של ההגדרה, שנדרש לעשותו בשל כניסתם לתוקף, ביום 1.1.2002, של התקנים המקצועיים בביקורת פנימית.

1.1 המבקר הפנימי כיועץ

בהגדרת המקצוע מופיעה מטלת יעוץ. בדבר נשיא הלשכה שבפתח האוגדן המקצועי, ובהערת המועצה המקצועית באשר למטלה זו המופיעה בו, במילון המושגים בביקורת הפנימית, קיימות התייחסויות לשירותי/מטלות היעוץ. ניתנת בזאת התמקדות באשר להתייחסות הלשכה למטלת היעוץ כלהלן:

בהגדרת המקצוע ובתקנים המקצועיים לביקורת פנימית שהוצאו על-ידי ה-IIA והכלולים באוגדן מקצועי זה, ניתנת למבקר הפנימי האפשרות לשמש כיועץ לארגון שאותו הוא מבקר. יובהר, כי מדיניות הלשכה, בצמידות לחוקי מדינת ישראל ולמהות הביקורת הפנימית, רואה את מטלת הייעוץ המופיעה בהגדרת המקצוע ובתקנים – כעצה/המלצה המובאת במסגרת דוח ביקורת שהמבקר הפנימי באירגון מפיק כתוצאה מתהליכי ביצוע העבודה המקצועית.

זאת, מאחר שהמבקר הפנימי איננו יכול לבקר תוצאות של יעוץ שהוא עצמו יעץ לארגון המבוקר על-ידו.

בברכה,

שלמה קלדרון
נשיא הלשכה

1.2 תקנים מקצועיים מקובלים בביקורת פנימית

התקנים המקצועיים המקובלים במקצוע הביקורת הפנימית כוללים את הגדרת מקצוע הביקורת הפנימית, את הקוד האתי, את התקנים המקצועיים ואת ההנחיות המקצועיות.
פיתוח, התאמה וסקירה של התקנים המקצועיים המקובלים בביקורת פנימית הוא תהליך מתמשך, המבוצע על-ידי המועצה המקצועית של לשכת המבקרים הפנימיים בישראל. המועצה המקצועית של לשכת המבקרים הפנימיים בישראל מתבססת בעבודתה על הדין בישראל ועל מועצת התקנים המקצועיים הבינלאומית.

לשכת המבקרים הפנימיים - ישראל

הקוד האתי

2. הקוד האתי

2.1 מבוא

2.1.1 כללי

מטרת הקוד האתי של הלשכה היא לקדם תרבות אתית במקצוע הביקורת הפנימית.

ביקורת פנימית הינה פעילות בלתי תלויה ואובייקטיבית של הבטחה וייעוץ, אשר מיועדת להוסיף ערך ולשפר את פעולות הארגון. היא מסייעת לארגון להשיג את מטרותיו בהבאת גישה שיטתית וממוסדת, לשם הערכה ושיפור האפקטיביות של תהליכי ניהול סיכונים, בקרה, פיקוח ושליטה.

הביקורת הפנימית, בהגדרתה, נערכת על-פי התקנים המקצועיים לביקורת פנימית של לשכת המבקרים הפנימיים, אשר מטילים על הביקורת הפנימית חובות ותפקידים ייחודיים לה, של בדיקת תקינותן של פעולות הארגון מבחינת שמירה על החוקים, על הניהול התקין, על טוהר המידות ועל חיסכון ויעילות.

הקוד האתי נחוץ וראוי למקצוע הביקורת הפנימית; מקצוע המבוסס על אמון, המצוי בהבטחה האובייקטיבית, הנוגעת בתהליכי שליטה, ניהול סיכונים ותהליכי בקרה. הקוד האתי של הלשכה מרחיב מעבר להגדרה של ביקורת פנימית, בכך שהוא כולל שני מרכיבים חיוניים:

1. עקרונות הרלוונטיים למקצוע ולפרקטיקה הנהוגה בביקורת פנימית;
2. כללי התנהגות, המתארים נורמות התנהגות, המצופות ממבקרים פנימיים. כללים אלה הם כלי-עזר לפירוש העקרונות ביישומים מקצועיים, ומיועדים להתוות את ההתנהגות האתית של מבקרים פנימיים.

הקוד האתי, יחד עם המסגרת הבינלאומית לעיסוק מקצועי (International Professional Practices Framework) של IIA, ופרסומים רשמיים רלוונטיים אחרים של הלשכה, מנחים מבקרים פנימיים הנותנים שירות לאחרים. המונח "מבקרים פנימיים" מתייחס לחברי הלשכה, לבעלי הסמכה מקצועית של IIA, למועמדים לקבלת הסמכה ולמספקים שירותי ביקורת פנימית במסגרת הגדרת המקצוע.

2.1.2 תחולה ואכיפה

הקוד האתי חל על יחידים ועל ישויות, המספקים שירותי ביקורת פנימית.
לגבי חברי הלשכה, לגבי בעלי הַסְמָכוֹת מקצועיות של הלשכה ולגבי מועמדים לקבלת ההסמכות, הפרת הקוד האתי תישקל ותטופל בהתאם לתקנות הלשכה ולהנחיותיה המינהליות. העובדה, שהתנהגות מסוימת אינה מוזכרת בכללי ההתנהגות, אינה מונעת ממנה להיות בלתי מקובלת או בלתי ראויה, ולכן חבר או בעל הסמכה או מועמד להסמכה עלול להיות צפוי לצעדים משמעתיים.

2.2 עקרונות

מבקרים פנימיים נדרשים ליישם ולתמוך בעקרונות הבאים:

א. יושרה (integrity) – היושרה של המבקרים הפנימיים מבססת אמון ולכן מספקת בסיס להסתמכות על שיפוטם.

ב. אובייקטיביות – מבקרים פנימיים מציגים את הרמה הגבוהה ביותר של אובייקטיביות מקצועית באיסוף, בהערכה ובדיווח מידע אודות פעילות או תהליך נבחן. מבקרים פנימיים עושים הערכה מאוזנת של כל הנסיבות הרלוונטיות, ואינם מושפעים, באופן שאינו ראוי, מאינטרסים שלהם או מאחרים בקביעת עמדתם.

ג. סודיות – מבקרים פנימיים מכבדים את הערך והבעלות של המידע, שהם מקבלים, ואינם מגלים מידע ללא הרשאה מתאימה, אלא אם כן יש מחויבות משפטית או מקצועית לעשות כן.

ד. יכולת – מבקרים פנימיים מיישמים את הידע, הכישורים והניסיון, הדרושים לביצוע עבודת הביקורת הפנימית.

2.3 כללי התנהגות

2.3.1 יושרה

מבקרים פנימיים:

2.3.1.1 יבצעו עבודתם בהגינות, בשקידה, ובאחריות;

2.3.1.2 יצייתו לחוק ויתנו גילוי נאות כמצוּפֶּה לפי החוק והמקצוע;

2.3.1.3 לא יעסקו ביודעין בפעילויות לא חוקיות, ולא ייטלו חלק בפעילויות שאינן הולמות את המקצוע או את הארגון;

2.3.1.4 יכבדו ויתרמו ליעדים הלגיטימיים והאתיים של הארגון.

2.3.2 אובייקטיביות

מבקרים פנימיים:

2.3.2.1 לא ישתתפו בכל פעילות או מערכת יחסים העלולים לפגוע, או אשר ניתן להניח שיפגעו בהערכתם הנטולה משוא פנים. השתתפות זו כוללת פעילויות או קשרים, העלולים להיות בניגוד לאינטרסים של האירגון;

2.3.2.2 לא יקבלו דבר העלול לפגוע, או אשר ניתן להניח שיפגע בשיפוטם המקצועי;

2.3.2.3 יגלו את כל העובדות המהותיות, הידועות להם, אשר אי-גילוין, עלול לעוות את הדיווח אודות הפעילויות הנסקרות.

2.3.3 סודיות

מבקרים פנימיים:

2.3.3.1 יהיו זהירים באשר לשימוש ולשמירה של המידע שהושג במהלך עבודתם;

2.3.3.2 לא ישתמשו במידע לשם הפקת טובת הנאה אישית כלשהי, או באופן כלשהו, אשר עלול להיות בניגוד לחוק, או עלול לפגוע ביעדים הלגיטימיים והאתיים של האירגון.

2.3.4 יכולת

מבקרים פנימיים:

2.3.4.1 יעסקו אך ורק בשירותים, שלנתינתם יש להם: ידע, מיומנויות וניסיון הכרחיים;

2.3.4.2 יבצעו שירותי ביקורת פנימית בהתאם לתקנים לעיסוק מקצועי בביקורת פנימית;

2.3.4.3 ישפרו באופן מתמיד את מקצועיותם ואת האפקטיביות והאיכות של שירותיהם.

3. תקנים מקצועיים לביקורת פנימית

3.1 מבוא

פעילויות הביקורת הפנימית מתבצעות על-ידי אנשים מתוך ומחוץ לארגונים, בסביבות תרבותיות ומשפטית מגוונות, ובארגונים מגוונים במטרות, בגודל, במורכבות ובמבנה. הבדלים אלה יכולים להשפיע על עבודת הביקורת הפנימית בכל סביבה. עם זאת, עמידה בתקנים מקצועיים מקובלים, ובכללם התקנים המקצועיים של מקצוע הביקורת הפנימית, היא חיונית, כדי שמבקרים פנימיים ויחידת ביקורת פנימית יישאו באחריות המוטלת עליהם.
הנוסח של התקנים המקצועיים לביקורת פנימית שלהלן, מותאם לאמור לעיל בהגדרת המקצוע, ולסביבה המיוחדת של עבודת הביקורת הפנימית במדינת ישראל.

3.1.1 מטרות התקנים המקצועיים

התקנים המקצועיים נועדו לבאים:

א. להתוות עקרונות בסיסיים של הפרקטיקה של הביקורת הפנימית, כפי שצריכה להיות;
ב. לתת מסגרת לביצוע ולקידום תחום רחב של פעילויות ביקורת פנימית מוסיפות ערך;
ג. לבנות בסיס להערכת ביצועי הביקורת הפנימית;
ד. לטפח פעולות ותהליכים ארגוניים משופרים.

3.1.2 מושגים בשימוש בתקנים המקצועיים

התקנים המקצועיים הם עקרונות ממוקדים, המציבים דרישות מחייבות המורכבות מ:

א. הצהרות בדבר דרישות בסיסיות לפרקטיקה מקצועית של הביקורת הפנימית ולהערכה של אפקטיביות הביצועים, שהם ישימים באופן בינלאומי ברמה אירגונית וברמה של הפרט;
ב. ביאורים, המבהירים את המושגים והתפישות שבהצהרות.

התקנים המקצועיים משתמשים במושגים שניתנו להם משמעויות מסוימות, הנכללות במילון המושגים. בתקנים המקצועיים, משתמשים במושג "חייב" כדי לציין דרישה בלתי מותנית, ובמילה "ראוי" כאשר עמידה בהם מצוּפָּה, אלא אם כן, הנסיבות מצדיקות סטייה, בכפוף ליישום שיקול דעת מקצועי.

חיוני להפנים את ההצהרות והביאורים שלהם, כמו גם את המשמעויות שלהם מתוך מילון המושגים, כדי להבין וליישם את התקנים המקצועיים באופן נכון.

3.1.3 מבנה התקנים המקצועיים

3.1.3.1 כללי

התקנים המקצועיים מורכבים מתקני תכונות ("סדרת ה-1000"), מתקני ביצוע ("סדרת ה-2000") ומתקני יישום.

3.1.3.2 תקני תכונות (Attribute)

תקני תכונות עוסקים בתכונות, הנדרשות מיחידים ומארגונים, המבצעים פעילויות של ביקורת פנימית.

3.1.3.3 תקני ביצוע (Performance)

תקני ביצוע מתארים את אופי פעילויות הביקורת הפנימית ומספקים אמות מידה לאיכות, שלפיהן ניתן למדוד את ביצועי השירותים המסופקים.

3.1.3.4 תקני יישום (Implementation)

תקני תכונות ותקני ביצוע מתייחסים לכלל שירותי הביקורת הפנימית.

תקני היישום מרחיבים ומיישמים את תקני התכונות ואת תקני הביצוע, ומגדירים את הדרישות הישימות בסוגים מסוימים של ביקורות, כגון: שירותי הבטחה (A) שירותי ייעוץ (C), ביקורות במגזרים מסוימים המוסדרים בחקיקה ייחודית, וכדו'.

3.1.4 סוגים של שירותי ביקורת

3.1.4.1 שירותי הבטחה

שירותי הבטחה קשורים בעבודת מבקר פנימי, הבוחן באופן אובייקטיבי של רְאָיָה לשם מתן הערכה בלתי-תלויה, או מסקנה לגבי ישות, פעולה, תפקיד, תהליך, מערכת, או ענין אחר.

האופי וההיקף של מטלת הביקורת נקבעים על-ידי המבקר הפנימי.

ככלל, ישנם שלושה צדדים המעורבים בשירותי ההבטחה:

(1) האדם או הקבוצה המעורבים ישירות ביישות, בפעולה, בתפקיד, בתהליך, במערכת, או בענין אחר – בעל התהליך (המבוקר),

(2) האדם או הקבוצה המבצעים את ההערכה – המבקר הפנימי,

(3) האדם או הקבוצה המשתמשים בהערכה – המשתמש.

3.1.4.2 שירותי ייעוץ

שירותי ייעוץ הם בטבעם פעילויות מייעצות, והן בדרך-כלל מבוצעות על-פי בקשה מסוימת של לקוח המטלה.

האופי וההיקף של מטלת הייעוץ כפופים להסכם עם לקוח המטלה.

ככלל, ישנם שני צדדים המעורבים בשירותי ייעוץ:

(1) האדם או הקבוצה המציעים את העצה – המבקר הפנימי,

(2) האדם או הקבוצה המצפים לקבל את העצה – לקוח המטלה.

כאשר ניתנים שירותי ייעוץ ראוי שהמבקר הפנימי ישמור על אובייקטיביות ולא יקבל אחריות ניהולית.

3.1.5 תהליך קביעת התקנים המקצועיים המקובלים

פיתוח, התאמה וסקירה של התקנים המקצועיים המקובלים בביקורת פנימית הוא תהליך מתמשך, המבוצע על-ידי המועצה המקצועית של לשכת המבקרים הפנימיים בישראל. המועצה המקצועית של לשכת המבקרים הפנימיים בישראל מתבססת בעבודתה על הדין בישראל ועל מועצת התקנים המקצועיים הבינלאומית, אשר מקיימת דיונים ומפרסמת טיוטות לתגובות של אנשי מקצוע בביקורת הפנימית ברחבי העולם. כמו כן, המועצה המקצועית של לשכת המבקרים הפנימיים בישראל דנה ומתייעצת רבות לפני פרסום התקנים המקצועיים המקובלים.

3.2 תקני תכונות

[1000] מטרה, סמכות ואחריות

המטרה, הסמכות והאחריות של הביקורת הפנימית, חייבות להיות מוגדרות באופן פורמלי בתקנון ביקורת פנימית, בהתאם להגדרת המקצוע, לקוד האתי ולתקנים המקצועיים, ובכפוף לכל דין. על המבקר הפנימי הראשי לסקור מידי תקופה את תקנון הביקורת, ולהציגו בפני ההנהלה הבכירה והדירקטוריון לצורך אישורו.

<u>ביאור:</u>

תקנון הביקורת הפנימית הוא מסמך רישמי, המגדיר את מטרות יחידת הביקורת הפנימית, סמכויותיה ואחריותה. תקנון הביקורת הפנימית מבסס את מעמד יחידת הביקורת הפנימית בארגון; מסמיך גישה לרשומות, לעובדים ולרכוש פיזי הרלוונטיים לביצוע עבודת הביקורת, ומגדיר את תחום הפעילויות של הביקורת הפנימית. אישור סופי של תקנון ביקורת פנימית נתון בידי הדירקטוריון.

1000.A1- טבעם של שירותי ההבטחה, הניתנים לארגון, חייבת להיות מוגדרת בתקנון הביקורת הפנימית. אם צריכים להינתן שירותים כאלה לגופים מחוץ לארגון, מהותם של שירותים אלה, אף היא חייבת להיות מוגדרת בתקנון ביקורת פנימית.

1000.C1- מהות שירותי הייעוץ חייבת להיות מוגדרת בתקנון ביקורת פנימית.

[1010] הסתמכות על הגדרת מקצוע הביקורת הפנימית, הקוד האתי והתקנים המקצועיים בתקנון ביקורת פנימית

האופי המחייב של החקיקה בנושא הביקורת הפנימית, הגדרת המקצוע, הקוד האתי, התקנים וההנחיות המקצועיות, חייב לבוא לידי ביטוי בתקנון הביקורת הפנימית.
ראוי שהמבקר הפנימי הראשי ידון אודות החקיקה בנושא הביקורת הפנימית, הגדרת המקצוע, הקוד האתי, התקנים וההנחיות המקצועיות, עם ההנהלה הבכירה והדירקטוריון.

[1100] אי-תלות ואובייקטיביות

הביקורת הפנימית חייבת להיות בלתי-תלויה, ומבקרים פנימיים חייבים להיות אובייקטיביים בביצוע עבודתם.

<u>ביאור</u> :
אי-תלות היא החופש מתנאים, המאיימים על יכולתה של יחידת הביקורת הפנימית או של המבקר הפנימי הראשי למלא את אחריותו באופן בלתי מוטֶה.
להשגת מידת אי-התלות הדרושה ליישום אפקטיבי של האחריות של יחידת הביקורת הפנימית, תהיה למבקר הפנימי הראשי גישה ישירה ובלתי-מוגבלת להנהלה הבכירה ולדירקטוריון. זאת ניתן להשיג באמצעות מערכת יחסים של דיווחים הדדיים. איומים על אי-התלות יטופלו ברמה של המבקר היחיד, ברמת מטלת הביקורת, ברמה הפונקציונלית וברמה הארגונית.
אובייקטיביות היא גישה נפשית בלתי מוטָה, המאפשרת למבקרים פנימיים לבצע מטלות ביקורת באופן שבו הם מאמינים בתוצר עבודתם ושלא יהיו התפשרויות על האיכות. אובייקטיביות דורשת שמבקרים לא יכפיפו את שיפוטם בענייני ביקורת לאחרים. איומים על אי-התלות יטופלו ברמה של המבקר היחיד, ברמת מטלת הביקורת, ברמה הפונקציונאלית וברמה הארגונית.

[1110] אי-תלות ארגונית

המבקר הפנימי הראשי חייב לדווח לרמה בארגון, המאפשרת לביקורת הפנימית לבצע את המוטל עליה. על המבקר הפנימי הראשי לאשר לדירקטוריון, לפחות אחת לשנה, את קיומה של אי-תלות ארגונית של יחידת הביקורת הפנימית.

1110.A1- הביקורת הפנימית חייבת להיות חופשית מהתערבות בקביעת היקף הביקורת, אופן ביצוע העבודה, ודיווח התוצאות.

[1111] קשרי גומלין ישירים עם הדירקטוריון

המבקר הפנימי הראשי חייב לדווח ולהיות בקשרי גומלין ישירים עם הדירקטוריון.

[1120] אובייקטיביות אישית

מבקרים פנימיים חייבים להיות בעלי גישה נטולת פניות ומשוא פנים, ולהימנע מניגוד עניינים.

<u>ביאור:</u>

ניגוד עניינים הוא מצב, שבו למבקר פנימי, הנמצא בעמדה של אמון, יש התנגשות מקצועית או עניין אישי. עניינים מתנגשים כאלה עלולים להקשות עליו למלא את אחריותו ללא משוא פנים. ניגוד עניינים קיים אף בהיעדר תוצאות, שאינן אתיות או שאינן תקינות.

ניגוד עניינים יכול ליצור מצג של אי-תקינות, היכול לערער את האמון במבקר הפנימי, ביחידת הביקורת הפנימית ובמקצוע הביקורת הפנימית.

ניגוד עניינים יכול למנוע את יכולתו של היחיד לבצע את מחויבויותיו ואחריותו באופן אובייקטיבי.

[1130] פגיעה באי-התלות או באובייקטיביות

פגיעה, למעשה או לכאורה, באי-התלות או באובייקטיביות חייבת להיות מדווחת לגורם המתאים. אופי הגילוי תלוי באופי הפגיעה.

<u>ביאור:</u>

הפרה של אי תלות ארגונית ואובייקטיביות של היחיד, יכולה לכלול, בין היתר, ניגוד עניינים אישי, הגבלות היקף מטלת הביקורת, הגבלות על גישה לרשומות, לכוח אדם ולנכסים, והגבלות על משאבים כמו מקורות מימון.

הקביעה של הצדדים המתאימים, שחובה לגלות להם את פרטי ההפרה של אי-התלות או האובייקטיביות, תלויה בציפיות לאחריותם של יחידת הביקורת הפנימית ושל המבקר הפנימי הראשי כלפי ההנהלה הבכירה והדירקטוריון, כפי שמתואר בתקנון הביקורת הפנימית, ובהתאם לאופי ההפרה.

1130.A1- מבקרים פנימיים חייבים להימנע מלתת שירותים לגבי תחום מסוים שבעבר היה באחריותם. האובייקטיביות יכולה להיחשב כנפגמת, אם מבקר פנימי מבצע עבודה לגבי תחום שהיה באחריותו בשנה שחלפה.

1130.A2- מטלות הבטחה הכוללות תפקידים שבאחריות המבקר הפנימי הראשי, חייבות להיות בפיקוח גוף מחוץ לביקורת הפנימית.

1130.C1- מבקרים פנימיים רשאים לספק שירותי ייעוץ, הנוגעים לפעולות להן היו אחראים בעבר.

1130.C2- אם קיימת אפשרות לפגיעה באי-תלות או באובייקטיביות של מבקרים פנימיים, בנוגע לשירותי ייעוץ מוצעים, חובה לתת לכך גילוי ללקוח לפני קבלת מטלת-הייעוץ.

[1200] מקצועיות וזהירות מקצועית ראויה

פעילויות הביקורת הפנימית חייבות להתבצע במקצועיות ובזהירות מקצועית ראויה.

[1210] מקצועיות

מבקרים פנימיים חייבים להיות בעלי הידע, המיומנויות והכישורים האחרים, הדרושים לביצוע הפעילויות, שבאחריותם האישית. הביקורת הפנימית, כיחידה, חייבת להיות בעלת הידע, המיומנויות והכישורים, הדרושים לביצוע הפעילויות שבאחריותה.

<u>ביאור:</u>

ידע, מיומנויות ויכולות אחרות הם מונחים שבמקוּבָּץ מתייחסים לכישורים המקצועיים, הנדרשים ממבקרים פנימיים, כדי לשאת באופן אפקטיבי באחריות המקצועית שלהם. רצוי שמבקרים פנימיים יפגינו את המקצועיות שלהם על-ידי השגת הסמכות והכשרות מקצועיות מתאימות כדוגמת תעודת ההסמכה CIA, של לשכת המבקרים הפנימיים ושל ארגונים מקצועיים מתאימים אחרים.

1210.A1- המבקר הפנימי הראשי חייב להשיג ייעוץ וסיוע מספקים, אם למבקרים הפנימיים חסרים ידע, מיומנויות וכישורים, הדרושים לביצוע מטלת ביקורת כולה או חלקה.

1210.A2- מבקר פנימי חייב להיות בעל ידע מספק להעריך סיכון להונאה, ואת האופן שבו הוא מנוהל על-ידי הארגון. עם זאת, אין לצפות ממנו להיות בעל ההתמחויות של מי שתפקידו העיקרי הוא לגלות ולחקור הונאות.

1210.A3- מבקר פנימי חייב להיות בעל ידע מספק אודות עיקרי הסיכונים, הבקרות וטכניקות ביקורת מבוססות טכנולוגיה, הזמינות לביצוע עבודתו. עם זאת, לא ניתן לצפות מכל מבקר פנימי, שתהיה לו המומחיות של מבקר פנימי שאחריותו העיקרית היא ביקורת טכנולוגית מידע.

1210.C1- המבקר הפנימי הראשי חייב לסרב לקבל מטלות ייעוץ או להשיג ייעוץ מספק, אם למבקרים הפנימיים חסרי ידע, מיומנויות וכישורים, הדרושים לביצוע מטלת ייעוץ כולה או חלקה.

[1220] זהירות מקצועית ראויה

מבקרים פנימיים חייבים ליישם זהירות ומיומנות, המצופים ממבקר פנימי מוכשר וזהיר במידה סבירה. זהירות מקצועית ראויה, אין משמעה היעדר יכולת לטעות.

1220.A1- מבקרים פנימיים חייבים לנהוג בזהירות מקצועית ראויה על-ידי הפעלת שיקול דעת בנושאים הבאים:

- היקף העבודה הדרושה להשגת יעדי הביקורת;
- מורכבות יחסית, מהותיות ומשמעותיות של עניינים, אליהם מתייחסת הביקורת;
- התאמה ואפקטיביות של תהליכי שליטה, ניהול הסיכונים והבקרה;
- הסתברות לטעויות משמעותיות, להונאה, ולאי-ציות; וכן -
- עלות הביקורת יחסית לתועלת הפוטנציאלית.

1220.A2- כדי לפעול בזהירות מקצועית ראויה, מבקרים פנימיים חייבים לשקול שימוש בכלי ביקורת מבוססי טכנולוגיה ובטכניקות אחרות לניתוח נתונים.

1220.A3- מבקרים פנימיים חייבים להיות ערים לסיכונים משמעותיים, העלולים להשפיע על השגת יעדים, על פעולות או על משאבים. עם זאת, תהליכי הביקורת כשלעצמם, אפילו אם הם מבוצעים בזהירות מקצועית ראויה, אינם מבטיחים שכל הסיכונים המשמעותיים יזוהו.

1220.C1- מבקרים פנימיים חייבים לנהוג בזהירות מקצועית ראויה על-ידי הפעלת שיקול דעת בנושאים הבאים:

- צרכים וציפיות של לקוחות, כולל אופי, עיתוי ודיווח תוצאות מטלת-הייעוץ;
- מורכבות יחסית והיקף של עבודה, הדרושה להשגת יעדי מטלת-הייעוץ; וכן -
- עלות מטלת-הייעוץ יחסית לתועלת הפוטנציאלית.

[1230] פיתוח מקצועי מתמשך

מבקרים פנימיים חייבים לשפר את הידע, המיומנויות ויכולות נוספות שלהם באמצעות פיתוח מקצועי מתמשך.

[1300] תוכנית הבטחת איכות ושיפור

המבקר הפנימי הראשי חייב לפתח ולקיים תוכנית להבטחת איכות ושיפור, הכוללת את כל ההיבטים של פעילויות הביקורת הפנימית.

ביאור:

תוכנית להבטחת איכות ושיפור נועדה לאפשר הערכה של עמידת הביקורת הפנימית בהגדרת המקצוע ובתקנים המקצועיים, והערכה האם מבקרים פנימיים מיישמים את הקוד האתי. התוכנית מעריכה גם את היעילות והאפקטיביות של הביקורת הפנימית ומזהה אפשרויות לשיפור.

[1310] הדרישות מתוכנית להבטחת איכות ושיפור

תוכנית להבטחת איכות ושיפור חייבת לכלול הן הערכות פנימיות והן הערכות חיצוניות.

[1311] הערכות פנימיות

הערכות פנימיות חייבות לכלול:

- ניטור רציף של ביצועי הביקורת הפנימית; וכן -
- סקירות תקופתיות באמצעות הערכה עצמית על-ידי אנשי הביקורת הפנימית או הערכה על-ידי גורם מתוך הארגון, בעל ידע מספק אודות הפרקטיקה הנוהגת של מקצוע הביקורת הפנימית.

ביאור:

ניטור רציף הוא חלק משולב של הפיקוח היומי, הסקירה וההערכה של יחידת הביקורת הפנימית. ניטור רציף ניכלל בנהלים ובפרקטיקה השגרתיים לניהול יחידת הביקורת הפנימית, והוא אף משתמש בתהליכים, בכלים ובמידע, הדרושים להערכת העמידה בהגדרת המקצוע הקוד האתי והתקנים.

סקירות תקופתיות הן הערכות המבוצעות כדי להעריך עמידה בהגדרת המקצוע, בקוד האתי ובתקנים המקצועיים.

ידע מספק אודות הפרקטיקה הנוהגת של הביקורת הפנימית, דורש לפחות הבנה של כל המרכיבים של מסגרת הכללים המקצועיים הבינלאומיים של ה-IIA.

[1312] הערכות חיצוניות

הערכות חיצוניות חייבות להיערך לפחות אחת ל-5 שנים, על-ידי סוקר או צוות סקירה, מוסמך, בלתי-תלוי וחיצוני לארגון. על המבקר הפנימי הראשי לדון עם הדירקטוריון:

- בצורך האפשרי להערכות חיצוניות בתדירות תכופה יותר; וכן –
- בכישורים ואי-התלות של הסוקר או צוות הסוקרים, לרבות כל ניגוד עניינים אפשרי.

ביאור:

סוקר או צוות סקירה מוסמך מורכב מיחידים בעלי יכולת בפרקטיקה של מקצוע הביקורת הפנימית ובתהליך ההערכה החיצוני. הערכה של יכולת הסוקר או צוות הסקירה היא שיפוט, המתחשב בניסיון בביקורת פנימית ובהסמכות מקצועיות של היחידים, שנבחרו לבצע את הסקירה. ההערכה של הכישורים מתייחסת גם לגודל ולמורכבות של הארגונים, שהסוקרים היו קשורים איתם בעבר, בהשוואה לארגון, שהביקורת הפנימית שלו נסקרת.

סוקר יחיד או צוות סקירה בלתי תלויים משמעותם היעדר ניגוד עניינים ממשי או נצפה, והיעדר השתייכות או הימצאות בשליטת הארגון בו מצויה יחידת הביקורת הפנימית.

[1320] דיווח על התוכנית להבטחת איכות ושיפור

המבקר הפנימי הראשי חייב לדווח את תוצאות התוכנית להבטחת איכות ושיפור להנהלה הבכירה ולדירקטוריון.

ביאור:

הצורה, התוכן והתדירות של דיווח תוצאות התוכנית להבטחת איכות ושיפור נקבעים באמצעות דיונים עם ההנהלה הבכירה והדירקטוריון, ובשים לב לאחריות של יחידת הביקורת הפנימית ושל המבקר הפנימי הראשי כפי שנקבע בתקנון הביקורת הפנימית. כדי להציג עמידה בהגדרת מקצוע הביקורת הפנימית, בקוד האתי, ובתקנים, התוצאות של הערכה תקופתית פנימית וחיצונית ידווחו עם השלמתה, והתוצאות של הניטור הרציף ידווחו לפחות אחת לשנה. התוצאות כוללות את הערכת הסוקר או צוות הסקירה בהתייחס למידת העמידה.

[1321] שימוש במילים "נערך בהתאם לתקנים המקצועיים הבינלאומיים"

המבקר הפנימי הראשי יכול לציין, שהביקורת הפנימית עומדת בתקנים הבינלאומיים למקצוע הביקורת הפנימית, רק אם תוצאות התוכנית להבטחת איכות ושיפור תומכות בהצהרה זו.

[1322] גילוי אי-עמידה בתקנים

כאשר אי-העמידה בהגדרת מקצוע הביקורת הפנימית, בקוד האתי, או בתקנים, משפיעה על מכלול היקף פעולות של יחידת הביקורת הפנימית, על המבקר הפנימי הראשי לדווח על אי-העמידה והשלכותיה להנהלה הבכירה ולדירקטוריון.

3.3 תקני ביצוע

[2000] ניהול הביקורת הפנימית

המבקר הפנימי הראשי חייב לנהל באופן אפקטיבי את הביקורת הפנימית, כדי להבטיח שהיא מוסיפה ערך לארגון.

ביאור:

יחידת ביקורת פנימית מנוהלת באופן אפקטיבי כאשר:

- *התוצאות של עבודת יחידת הביקורת הפנימית עומדות במטרה ובאחריות, הנכללות בתקנון הביקורת הפנימית;*
- *יחידת הביקורת הפנימית עונה על הגדרת הביקורת הפנימית והתקנים המקצועיים; וכן*
- *היחידים שהם חלק מיחידת הביקורת הפנימית עומדים בקוד האתי בתקנים ובהנחיות המקצועיות.*

[2010] תכנון

המבקר הפנימי הראשי חייב להכין תוכניות עבודה מבוססות סיכונים, בהתאם למטרות האירגון, כדי להחליט על סדרי העדיפויות של הביקורת הפנימית.

ביאור:

המבקר הפנימי הראשי אחראי להכנת תוכנית עבודה מבוססת סיכונים. המבקר הפנימי הראשי לוקח בחשבון את מסגרת ניהול הסיכונים של הארגון, לרבות החלטות ההנהלה בעניין תיאבון לסיכון (רמת הסיכון שהארגון מוכן לקבל). אם לא קיימת בארגון מסגרת ניהול סיכונים, אזי יפעיל המבקר הפנימי הראשי שיקול דעת בדבר הסיכונים, לאחר התייעצות עם ההנהלה הבכירה והדירקטוריון.

2010.A1 - תוכניות העבודה של הביקורת הפנימית חייבות להתבסס על הערכת סיכונים מתועדת, המתבצעת לפחות אחת לשנה. הערות ההנהלה הבכירה והדירקטוריון חייבות להילקח בחשבון בתהליך זה.

2010.C1 - המבקר הפנימי הראשי חייב לשקול קבלת הצעות למטלות-ייעוץ בהתבסס על יכולת מטלות-הייעוץ לשפר את ניהול הסיכונים, להוסיף ערך ולשפר את פעולות האירגון. מטלות-ייעוץ שהתקבלו חייבות להיכלל בתוכנית העבודה.

[2020] דיווח ואישור

המבקר הפנימי הראשי חייב לדווח להנהלה הבכירה ולדירקטוריון, אודות תוכניות העבודה של הביקורת הפנימית והמשאבים הנדרשים, לרבות שינויים משמעותיים בתקופת ביניים, לצורך סקירה ואישור. המבקר הפנימי הראשי חייב לדווח גם על ההשלכות של הגבלות על משאבים.

[2030] ניהול משאבים

המבקר הפנימי הראשי חייב להבטיח שמשאבי הביקורת הפנימית הם מתאימים, מספקים והוקצו באופן אפקטיבי – והכל להשגת התוכנית המאושרת.

<u>ביאור:</u>

המילה "מתאימים" מתייחסת לתמהיל של ידע, מיומנות ויכולות, הנדרשים לביצוע התוכנית. המילה "מספקים" מתייחסת לכמות של משאבים הדרושים לסיום התוכנית. משאבים מנוצלים באופן אפקטיבי כאשר הם בשימוש בצורה ובאופן, המביאים ליישום אופטימלי של התוכנית המאושרת.

[2040] מדיניות ונהלים

המבקר הפנימי הראשי חייב לקבוע מדיניות ונהלים כדי להנחות את פעילות הביקורת הפנימית.

<u>ביאור:</u>

הצורה והתוכן של מדיניות ונהלים תלויים בגודל ובמבנה של יחידת הביקורת הפנימית והמורכבות של עבודתה.

[2050] תיאום

ראוי שהמבקר הפנימי הראשי ישתף במידע ויתאם פעילויות עם ספקים פנימיים וחיצוניים של שירותי הבטחה וייעוץ רלוונטיים, כדי להבטיח כיסוי נאות וצמצום כפל מאמצים.

[2060] דיווח להנהלה הבכירה ולדירקטוריון

המבקר הפנימי הראשי חייב לדווח מידי תקופה להנהלה הבכירה ולדירקטוריון אודות המטרות, הסמכויות, האחריות והביצועים של הביקורת הפנימית בהשוואה לתוכנית. הדיווח חייב לכלול גם נושאי חשיפות לסיכונים משמעותיים ובקרה, לרבות סיכוני הונאה, ענייני שליטה בארגון ונושאים נוספים לבקשת ההנהלה הבכירה והדירקטוריון.

ביאור:

התדירות והתוכן של הדיווח נקבעים בדיון עם ההנהלה הבכירה והדירקטוריון ותלויים בחשיבות המידע המדווח והדחיפות של הפעולות הקשורות שעל ההנהלה הבכירה או הדירקטוריון לבצע.

[2100] אופי העבודה

הביקורת הפנימית חייבת להעריך ולתרום לשיפור תהליכי השליטה, ניהול הסיכונים והבקרה, תוך שימוש בגישה שיטתית וממוסדת.

[2110] שליטה

הביקורת הפנימית חייבת להעריך את תהליך השליטה ולתת המלצות מתאימות לשיפור, בהיבט של השגת היעדים הבאים:

(1) קידום קוד אתי וערכים מתאימים בתוך הארגון;

(2) ניהול אפקטיבי של ביצועים ארגוניים ושל נשיאה באחריות (accountability);

(3) דיווח של מידע אודות סיכונים ובקרות לגורמים המתאימים באירגון;

(4) תיאום של פעילויות הדירקטוריון (כהגדרתו במילון המושגים), ההנהלה, המבקרים הפנימיים והמבקרים החיצוניים, ושל העברת המידע ביניהם.

2110.A1- הביקורת הפנימית חייבת להעריך את התכנון, היישום והאפקטיביות של היעדים, התוכניות והפעילויות של האירגון, בהתאמה לקוד האתי של האירגון.

2110.A2- הביקורת הפנימית חייבת להעריך האם השליטה בטכנולוגיות המידע של האירגון קיימת ותומכת באסטרטגיות הארגון וביעדיו.

2110.C1- מטרות מטלת-הייעוץ חייבות להיות עקביות עם הערכים הכוללים והיעדים של האירגון.

[2120] ניהול סיכונים

הביקורת הפנימית חייבת להעריך את האפקטיביות ולתרום לשיפור תהליכי ניהול סיכונים.

ביאור:

קביעה האם תהליכי ניהול סיכונים אפקטיביים היא שיפוט הנובע מהערכת מבקרים פנימיים ש:

- *יעדי האירגון תומכים ומתאימים למטרות האירגון,*
- *סיכונים משמעותיים מזוהים ומוערכים,*

- *תגובות הולמות לסיכונים נבחרות בהתאמה לסיכונים ולתיאבון הארגון לסיכון,*
- *מידע רלוונטי אודות סיכונים ניקלט ומדווח במועד בארגון, לצוות יישומי, להנהלה ולדירקטוריון כדי לממש את תחומי האחריות שלהם.*

תהליכי ניהול סיכונים מנוטרים באמצעות פעילויות מתמשכות של ההנהלה ו/או באמצעות הערכות נפרדות.

2120.A1- הביקורת הפנימית חייבת להעריך חשיפות לסיכונים המתייחסים לשליטה, לפעולות ולמערכות המידע של הארגון בהתייחס לבאים:

- אמינות ושלמות המידע הכספי והתפעולי;
- אפקטיביות ויעילות הפעולות;
- שמירה על נכסים; וכן
- עמידה בדרישות חוקים, תקנות וחוזים.

2120.A2- הביקורת הפנימית חייבת להעריך את הפוטנציאל להתרחשות הונאה וכיצד הארגון מנהל סיכוני הונאה.

2120.C1- במהלך ביצוע מטלת-ייעוץ, מבקרים פנימיים חייבים להתייחס לסיכונים בהתאמה למטרות מטלת-הייעוץ, ויהיו ערניים לקיומם של סיכונים משמעותיים נוספים.

2120.C2- ידע אודות סיכונים, שהושג במטלות-ייעוץ, חייב להיכלל על-ידי מבקרים פנימיים, בהערכה של תהליך ניהול סיכונים בארגון.

2120.C3- כאשר מסייעים להנהלה במיסוד או שיפור תהליכי ניהול סיכונים, מבקרים פנימיים חייבים להימנע מליטול כל אחריות ניהולית על ידי ניהול בפועל של סיכונים.

[2130] בקרה

הביקורת הפנימית חייבת לסייע לארגון בשימור בקרות אפקטיביות, על-ידי הערכה של אפקטיביות ויעילות הבקרות ועל-ידי קידום שיפורן המתמיד.

2130.A1- הביקורת הפנימית חייבת להעריך את ההלימות והאפקטיביות של הבקרות במענה לסיכונים במערכות השליטה, הבקרה והמידע של הארגון בהתייחס לבאים:

- אמינות ושלמות המידע הכספי והתפעולי;
- אפקטיביות ויעילות הפעולות;
- שמירה על נכסים; וכן
- עמידה בדרישות חוקים, תקנות וחוזים.

2130.A2- ראוי שמבקרים פנימיים יוודאו באיזו מידה נקבעו יעדים ומטרות לפעולות ולתוכניות, בהתאמה לאלה של האירגון.

2130.A3- ראוי שמבקרים פנימיים יסקרו פעולות ותוכניות, כדי לוודא באיזו מידה התוצאות עקביות עם היעדים והמטרות שנקבעו, כדי לקבוע האם פעולות ותוכניות מיושמות או מבוצעות על-פי הכוונה.

2130.C1- במהלך ביצוע מטלת-ייעוץ, מבקרים פנימיים חייבים להתייחס לבקרות בהתאמה למטרות מטלת-הייעוץ, ויהיו ערניים לענייני בקרה משמעותיים.

2130.C2- ידע אודות בקרות, שהושג במטלות-ייעוץ, חייב להיכלל על-ידי מבקרים פנימיים, בהערכת תהליכי בקרה באירגון.

[2200] תכנון מטלת ביקורת

מבקרים פנימיים חייבים לפתח ולתעד תוכנית לכל מטלת ביקורת, לרבות מטרות המטלה, היקפה, מועדי ביצועה והקצאת משאבים.

[2201] שיקולי התכנון

בתכנון מטלת הביקורת, מבקרים פנימיים חייבים לשקול את:

- המטרות של הפעילות הנסקרת וכן את האמצעים, המשמשים את הפעילות לבקר את ביצועיה;
- הסיכונים המשמעותיים לפעילות, ליעדיה, למשאביה ולפעולותיה, וכן את האמצעים בעזרתם נשמרות ברמה מקובלת ההשלכות בכוח של הסיכונים;
- ההתאמה והאפקטיביות של ניהול סיכוני הפעילות ותהליכי הבקרה בהשוואה למודל או למסגרת של בקרות רלוונטיים; וכן
- האפשרויות לביצוע שיפורים משמעותיים בניהול סיכוני הפעילות ובתהליכי הבקרה.

2201.A1- בתכנון מטלת ביקורת עבור גורמים מחוץ לאירגון, מבקרים פנימיים חייבים להגיע להבנה כתובה עם הגורמים החיצוניים לגבי מטרות, היקף, אחריות מתאימה ושאר ציפיות, לרבות הגבלות על הפצת תוצאות מטלת הביקורת ועל הגישה לרשומות הביקורת.

2201.C1- מבקרים פנימיים חייבים להגיע להבנה עם הלקוחות לגבי מטרות, היקף, אחריות מתאימה ושאר ציפיות הלקוח. במטלות-ייעוץ משמעותיות יש לתעד הבנה זו.

[2210] מטרות מטלת הביקורת

מטרות חייבות להיקבע לכל מטלת ביקורת.

2210.A1- מבקרים פנימיים חייבים לבצע הערכה ראשונית של סיכונים, הרלוונטיים לתחום המבוקר. מטרות הביקורת חייבות לשקף את תוצאות הערכה זו.

2210.A2- מבקרים פנימיים חייבים לשקול את ההסתברות של טעויות משמעותיות, הונאות, אי-ציות וחשיפות אחרות בעת פיתוח מטרות למטלת ביקורת.

2210.A3- יש צורך בקריטריונים מתאימים לשם הערכת בקרות. מבקרים פנימיים צריכים לוודא עד כמה ההנהלה קבעה קריטריונים, כדי לקבוע האם היעדים והמטרות הושגו. אם הקריטריונים מספקים, מבקרים פנימיים חייבים להשתמש בקריטריונים כאלה, כשהם מבצעים הערכה. אם הקריטריונים אינם מספקים, מבקרים פנימיים חייבים לפעול עם ההנהלה לפיתוח קריטריונים מתאימים להערכה.

2210.C1- מטרות מטלת-הייעוץ חייבות להתייחס לתהליכי שליטה, ניהול סיכונים ובקרות במידה המוסכמת עם הלקוח.

[2220] היקף מטלת ביקורת

ההיקף שנקבע חייב להיות מספק כדי לעמוד במטרות מטלת ביקורת.

2220.A1- היקף מטלת ביקורת חייב לכלול בחינה של מערכות, רשומות, כוח-אדם ונכסים פיסיים, הרלוונטיים למטלת ביקורת, לרבות אלה שבפיקוח גורם שלישי.

2220.A2- אם במהלך ביקורת, עולות אפשרויות משמעותיות למתן שירותי ייעוץ, ראוי להגיע להבנה כתובה, שתכלול את המטרות, ההיקף, האחריות המתאימה וציפיות אחרות; וכן לדווח על תוצאות שירותי הייעוץ על-פי התקנים המקצועיים הנוגעים לשירותי ייעוץ.

2220.C1- במהלך ביצוע מטלת-ייעוץ, מבקרים פנימיים חייבים להבטיח, שהיקף מטלת-הייעוץ מספק כדי לעמוד במטרות שהוסכמו. אם מבקרים פנימיים מפתחים הסתייגויות, במהלך ביצוע מטלת-הייעוץ, חובה עליהם לדון אודות הסתייגויות אלו עם הלקוח, כדי להחליט אם להמשיך בביצוע מטלת-הייעוץ.

[2230] הקצאת משאבים למטלת ביקורת

מבקרים פנימיים חייבים לקבוע משאבים מתאימים ומספקים להשגת מטרות מטלת ביקורת, בהתבסס על הערכה של האופי והמורכבות של כל מטלה, אילוצי הזמן והמשאבים הזמינים.

[2240] תוכנית ביקורת

מבקרים פנימיים חייבים להכין ולתעד תוכניות ביקורת להשגת מטרות מטלת ביקורת.

2240.A1- תוכניות ביקורת חייבות לכלול נהלים לזיהוי, לניתוח, להערכה ולתיעוד מידע במהלך הביקורת. תוכנית ביקורת חייבת להיות מאושרת לפני תחילת העבודה, וכל התאמה חייבת להיות מאושרת באופן מתאים.

2240.C1- תוכניות ביקורת למשימות ייעוץ עשויות להשתנות בצורה ובתוכן בהתאם לאופי מטלת-הייעוץ.

[2300] ביצוע מטלת ביקורת

מבקרים פנימיים חייבים לזהות, לנתח, להעריך ולתעד מידע מספק להשגת מטרות מטלת ביקורת.

[2310] זיהוי מידע

מבקרים פנימיים חייבים לזהות מידע מספק, אמין, רלוונטי ושימושי להשגת מטרות מטלת ביקורת.

ביאור:

מידע מספק הוא עובדתי, מתאים ומשכנע כך שאדם זהיר בעל ידע יגיע לאותן מסקנות כמו מבקר. מידע אמין הוא המידע הטוב ביותר הניתן להשגה תוך שימוש בטכניקות ביקורת מתאימות. מידע רלוונטי תומך בממצאי הביקורת ובהמלצותיה, והוא עקבי עם מטרות הביקורת. מידע שימושי עוזר לאירגון להשיג את יעדיו.

[2320] ניתוח והערכה

מבקרים פנימיים חייבים לבסס מסקנות ותוצאות של מטלת ביקורת על ניתוחים והערכות מתאימים.

[2330] תיעוד המידע

מבקרים פנימיים חייבים לתעד מידע רלוונטי כדי לתמוך במסקנות ובתוצאות של מטלת ביקורת.

2330.A1- המבקר הפנימי הראשי חייב לפקח על הגישה לרשומות הביקורת. המבקר הפנימי הראשי חייב לקבל, באופן מתאים, אישור של הנהלה בכירה ו/או יועץ משפטי לפני מסירה של רשומות כאלה לגורם חיצוני.

2330.A2- המבקר הפנימי הראשי חייב לפתח דרישות לשמירת רשומות הביקורת, ללא קשר למצע (מדיה) על-גביו מאוחסנות הרשומות. דרישות שמירה אלה חייבות להיות עקביות עם ההנחיות של הארגון ושל כל רגולטור רלוונטי, ועם דרישות אחרות.

2330.C1- המבקר הפנימי הראשי חייב לפתח מדיניות לשליטה באחזקה ובשמירה של רשומות מטלת ייעוץ, וכן במסירתם לצדדים פנימיים וחיצוניים. מדיניות זו חייבת להיות עקבית עם ההנחיות של הארגון ושל כל רגולטור רלוונטי, ועם דרישות אחרות.

[2340] פיקוח עצמי של הביקורת

חובה לפקח על עבודת הביקורת באופן נאות כדי להבטיח את השגת המטרות, הבטחת האיכות ופיתוח הצוות.

<u>ביאור:</u>

מידת הפיקוח הנדרשת תלויה במקצועיות ובניסיון של מבקרים פנימיים ובמורכבות מטלת ביקורת. על המבקר הפנימי הראשי חלה האחריות הכוללת לפיקוח על ביצוע מטלת ביקורת, בין אם מבוצעת על-ידי או עבור יחידת הביקורת הפנימית, אבל הוא יכול להאציל או ליעד אנשי יחידת הביקורת הפנימית, המנוסים באופן הולם, לבצע סקירה. ראיה הולמת לפיקוח מתועדת ונשמרת.

[2400] דיווח על התוצאות

מבקרים פנימיים חייבים לדווח על תוצאות מטלת ביקורת.

[2410] קריטריונים לדיווח

הדיווח חייב לכלול את מטרות מטלת ביקורת, היקף, מסקנות מתאימות, המלצות ותוכניות ליישומן.

2410.A1- הדוח הסופי של תוצאות מטלת ביקורת, חייב לכלול, על-פי הענין, חוות דעת כללית של מבקרים פנימיים ו/או מסקנותיהם.

2410.A2- רצוי שבדוח הסופי, יביעו מבקרים פנימיים הערכה לביצועים משביעי רצון.

2410.A3- בעת מתן דוח ביקורת לגורמים מחוץ לאירגון, חובה לכלול בדיווח הגבלות על הפצה ועל שימוש בדוח.

2410.C1- דיווח אודות התקדמות מטלת הייעוץ ותוצאותיה, ישתנה בצורה ובתוכן בהתאם לאופי של מטלת-הייעוץ והצרכים של הלקוח.

[2420] איכות הדיווחים

הדיווחים חייבים להיות מדויקים, אובייקטיביים, ברורים, תמציתיים, מועילים, שלמים ובמועד.

<u>ביאור:</u>

דוחות מדויקים הם נטולי טעויות ועיוותים והם נאמנים לעובדות המבססות אותם. דוחות אובייקטיבים הם הוגנים, אינם נושאים פנים, אינם מוטים והם תוצאה של הערכה מאוזנת והוגנת של כל העובדות הרלוונטיות והנסיבות. דוחות בהירים הם מובנים באופן קל ולוגי, והם נעדרים שפה טכנית לא הכרחית ומספקים את כל המידע המשמעותי והרלוונטי. דוחות תמציתיים הם ממוקדים ונעדרים פירוטים לא חיוניים, עודף פרטים, כפילויות וריבוי מילים. דוחות מועילים עוזרים ללקוחות הביקורת ולאירגון ומובילים לשינויים היכן שנדרשים. דוחות שלמים אינם חסרים פרטים, החיוניים לקהל היעד, וכוללים את כל המידע והנתונים המשמעותיים והרלוונטיים לצורך תמיכה בהמלצות ובמסקנות. דיווחים במועד הם מתוזמנים ומופצים בהתאם לחשיבות הנושא, ומאפשרים להנהלה לבצע פעולות תיקון מתאימות.

[2421] טעויות והשמטות

אם דיווח סופי כולל טעות או השמטה משמעותיים, המבקר הפנימי הראשי חייב לדווח את המידע המתוקן לכל הגורמים שקיבלו את הדיווח המקורי.

[2430] שימוש במילים "נערך בהתאם לתקנים מקצועיים מקובלים"

מבקרים פנימיים יכולים לדווח, שמטלות הביקורת שלהם "נערכו בהתאם לתקנים מקצועיים מקובלים של מקצוע הביקורת הפנימית", רק אם תוצאות של התוכנית לאבטחת איכות ושיפור תומכות בהצהרה זו.

[2431] גילוי אי-עמידה בתקנים המקצועיים

כאשר אי-עמידה בחקיקה, בהגדרת המקצוע, בקוד האתי או בתקנים המקצועיים, משפיעה על מטלת ביקורת מסוימת, דיווח אודות התוצאות חייב לגלות את:

- » קוד ההתנהגות או התקן המקצועי בהם לא היתה עמידה מלאה;
- » הסיבות לאי-העמידה;
- » השפעות אי-העמידה על מטלת ביקורת ועל התוצאות המדווחות.

[2440] הפצת התוצאות

המבקר הפנימי הראשי חייב להפיץ את התוצאות לגורמים המתאימים.

ביאור:

המבקר הפנימי הראשי, או מי שמונה על ידו, יסקור ויאשר את הדוח הסופי, לפני פירסומו ויחליט למי ואיך הוא יופץ.

2440.A1- המבקר הפנימי הראשי אחראי על דיווח התוצאות הסופיות לגורמים היכולים להבטיח שתינתן לתוצאות התייחסות ראויה.

2440.A2- בכפוף לכל דין, ובאישור של מי שהוסמך לכך באירגון, לפני הפצת הדוח על תוצאות סופיות לגורמים מחוץ לאירגון, חייב המבקר הפנימי הראשי:

- להעריך את פוטנציאל הסיכון לאירגון;
- להתייעץ עם ההנהלה הבכירה ו/או יועץ משפטי בהתאם לענין; וכן -
- לפקח על ההפצה, באמצעות הגבלות על השימוש בדוח.

2440.C1- המבקר הפנימי הראשי אחראי על דיווח התוצאות הסופיות של מטלת ייעוץ ללקוח.

2440.C2- נושאי שליטה, ניהול סיכונים ובקרה יכולים להיות מזוהים גם במהלך ביצוע מטלת ייעוץ. כאשר נושאים אלה משמעותיים לאירגון, חובה לדווח אודותם להנהלה הבכירה ולדירקטוריון.

[2500] ניטור ההתקדמות

המבקר הפנימי הראשי חייב להקים ולתחזק מערכת למעקב אחר התקדמות היישום של תוצאות מטלת ביקורת, שדווחו להנהלה.

2500.A1- המבקר הפנימי הראשי חייב למסד תהליך מעקב לשם ניטור והבטחה, שפעולות ההנהלה מיושמות באופן אפקטיבי, או שההנהלה הבכירה נטלה סיכון של אי-נקיטת פעולות.

2500.C1- הביקורת הפנימית חייבת לבצע מעקב אחר התקדמות היישום של תוצאות מטלות-ייעוץ, במידה המוסכמת עם הלקוח.

[2600] דיווח על רמה מסוימת של סיכון בלתי סביר

כאשר המבקר הפנימי הראשי סבור, שההנהלה הבכירה השלימה עם רמה מסוימת של סיכון שיורי, שעלול להיות בלתי-סביר לארגון, הוא חייב לשוחח על כך עם ההנהלה הבכירה. אם הסוגיה בענין הסיכון הבלתי-סביר אינה פתורה, המבקר הפנימי הראשי חייב לדווח אודות הענין לדירקטוריון לשם קבלת החלטה.

4. מילון מושגים מקצועיים

*

אובייקטיביות (Objectivity) – גישה בלתי מוטית, המאפשרת למבקרים פנימיים לבצע ביקורות באופן כזה, שתהיה להם אמונה כנה בתוצר עבודתם, ומבלי שייפול פגם משמעותי באיכותו. אובייקטיביות נדרשת ממבקרים פנימיים, כדי שלא יכפיפו את שיפוטם בענייני ביקורת לשיפוטם של אחרים.

אי-תלות (Independence) – החופש מתנאים המאיימים על האובייקטיביות או על האופן שבו היא נתפשת. איומים כאלה צריכים להיות מנוהלים ברמות של המבקר היחיד, המטלה, הפונקציה והאירגון.

ביקורת פנימית (Internal Audit Activity) – מחלקה, יחידה, צוות יועצים או אנשי מקצוע אחרים, המספקים שירותי הבטחה וייעוץ בלתי-תלויים ואובייקטיביים, ומיועדים להוסיף ערך ולשפר את פעולות האירגון. הביקורת הפנימית מסייעת לאירגון להשיג את מטרותיו על-ידי הבאת גישה שיטתית ומוּבְנית להערכה ולשיפור האפקטיביות של תהליכי שליטה, ניהול סיכונים ובקרה.

בקרה (Control) – כל פעולה הננקטת על-ידי ההנהלה, הדירקטוריון וגורמים אחרים, לשם קידום ניהול סיכונים, וכדי להגביר את ההיתכנות שיעדים ומטרות שנקבעו יושגו. ההנהלה מתכננת מארגנת, ומכוונת את ביצוען של פעולות מספקות, כדי לתת הבטחה סבירה שיעדים ומטרות יושגו.

בקרה הולמת (Adequate Control) – קיימת אם ההנהלה תיכננה וארגנה באופן, המספק הבטחה סבירה, שהסיכונים של האירגון מנוהלים באופן אפקטיבי, ושמטרות האירגון ויעדיו יושגו באופן יעיל וחסכוני.

בקרות טכנולוגית המידע (Information Technology Controls) – בקרות התומכות בניהול ובשליטה של העסק וכן מספקות בקרות טכניות וכלליות על תשתיות טכנולוגיות המידע כמו יישומים מידע תשתיות ואנשים.

דירקטוריון (Board) – מועצת מנהלים, מועצות סטטוטוריות, ועד מפקח או חבר נאמנים של מוסדות ללא כוונת רווח, וועדות ניהול עליונות שיועדו לשליטה בארגונים.

הונאה (Fraud) – כל פעולה לא חוקית המאופיינת ברמייה, בהסתרה או בהפרת אמון. פעולות אלו אינן תלויות באיום בשימוש באלימות או בהפעלת כוח. הונאות מבוצעות על-ידי יחידים או ארגונים, כדי להשיג כסף, רכוש או שירותים, כדי להימנע מתשלום או מהפסד של שירותים, או כדי להבטיח יתרון עסקי או אישי.

חייב (Must) – התקנים משתמשים במילה "חייב" כדי לציין דרישה בלתי-מותנית.

---

*תרגום המותאם לתנאים המיוחדים במדינת ישראל.
הנוסח האנגלי של מילון המושגים המקצועיים, מופיע בסוף הנוסח האנגלי של התקנים המקצועיים לביקורת פנימית.

טכניקות ביקורת מבוססות טכנולוגיה (Technology-based Audit Techniques) – כל כלי ביקורת אוטומטי, כדוגמת תוכנת ביקורת כללית, מחוללי נתוני מבחן, תוכניות ביקורת ממוחשבות, תוכניות שירות ייעודיות לביקורת, וכלי ביקורת ממוחשבים (CAATs).

להוסיף ערך (Add Value) – ערך, הנוצר על-ידי שיפור הזדמנויות להשגת יעדי הארגון, זיהוי שיפורים תפעוליים, ו/או הפחתת החשיפה לסיכונים באמצעות ביקורת ושירותי ייעוץ.

מבקר פנימי ראשי (Chief Audit Executive) – העֶמְדה הבכירה ביותר באירגון, האחראית על פעילויות הביקורת הפנימית. כאשר פעילויות הביקורת הפנימית מבוצעות על-ידי נותן שירותים חיצוני, המבקר הפנימי הראשי הוא יחיד האחראי לראייה הכוללת של חוזה השירות, להבטחה כוללת של איכות פעילויות הביקורת, לדיווח להנהלה הבכירה ולדירקטוריון, ולמעקב אחר תוצאות הביקורת.

מטלת ביקורת (Engagement) – משימת ביקורת פנימית מסויימת, מטלה, או פעילות סקירה, כדוגמת ביקורת פנימית, הערכה עצמית של בקרות, בחינת הונאה, או ייעוץ. ביקורת יכולה לכלול מספר מטלות או פעילויות, המיועדות להשיג מערך מסוים של מטרות קשורות.

מטרות מטלת ביקורת (Engagement Objectives) – הצהרות כוללות, שהוכנו על-ידי מבקרים פנימיים, המגדירות את ההישגים המיועדים של מטלת הביקורת.

מסגרת כללים מקצועיים בינלאומיים (International Professional Practices Framework) – המסגרת התפישתית, המארגנת את ההנחיות הסמכותיות שהוכרזו על ידי IIA. הנחיות סמכותיות מורכבות משתי קטגוריות: (1) מנדטורי (2) מומלץ ביותר.

משמעותיות (Significance) – החשיבות היחסית של עניין בהקשר שבו הוא נישקל, כולל גורמים כמותיים ואיכותיים, כדוגמת גודל, אופי, השפעה, רלוונטיות והשלכה. שיקול דעת מקצועי עוזר למבקרים פנימיים כאשר הם מעריכים את המשמעותיות של עניינים בהקשר של המטרות הרלוונטיות.

ניגוד עניינים (Conflict of Interest) – כל מערכת יחסים שהיא, או שהיא נראית ככזו, שאינה מתאימה לעניינים הטובים ביותר של האירגון. ניגוד עניינים עלול להטות את היכולת של היחיד מלבצע את מחויבויותיו ואחריותו באופן אובייקטיבי.

ניהול סיכונים (Risk Management) – תהליך לזיהוי, להערכה, לניהול ולבקרה של אירועים או מצבים בכוח, לשם מתן הבטחה סבירה באשר להשגת יעדי האירגון.

סביבת בקרה (Control Environment) – היחס והפעולות של הדירקטוריון באשר לחשיבות הבקרה באירגון. סביבת הבקרה מספקת את השיטה והמבנה להשגת המטרות הראשיות של מערכת הבקרה הפנימית. מערכת הבקרה הפנימית כוללת את המרכיבים הבאים:

- יושרה וערכים אתיים;
- פילוסופיית ההנהלה וסגנון התפעול;
- מבנה ארגוני;
- הטלת סמכות ואחריות;
- מדיניות משאבי אנוש ויישומה;
- יכולת של כוח-האדם.

סיכון (Risk) – האפשרות שאירוע שיתרחש ישפיע על השגת יעדים. סיכון נמדד במונחים של השפעות והיתכנות.

סיכונים שיוריים (Residual Risks) – הסיכונים הנותרים לאחר שההנהלה נקטה פעולות להפחתת ההשלכות וההיתכנות של ארוע שלילי, לרבות פעילויות בקרה בתגובה לסיכון.

ספק שירותים חיצוני (External Service Provider) – אדם או תאגיד, מחוץ לאירגון, בעל ידע, מיומנות וניסיון מיוחדים בתחום מקצועי מסויים.

פגמים (Impairments) – פגמים באי-התלות הארגונית ובאובייקטיביות האישית יכולים לכלול ניגוד עניינים אישי; הגבלות על היקף; הגבלות על גישה לרשומות, לכוח אדם ולנכסים; והגבלת המשאבים (מימון).

ציות (Compliance) – עמידה במדיניות, בתוכניות, בנהלים, בחוקים, בתקנות, בחוזים או בדרישות אחרות.

קוד אתי (Code of Ethics) – הקוד האתי של לשכת המבקרים הפנימיים בישראל כולל את העקרונות הרלוונטיים למקצוע ולפרקטיקה של הביקורת הפנימית, ואת כללי ההתנהגות המתארים את ההתנהגות המצופה ממבקרים פנימיים. הקוד האתי מתייחס לצדדים ולגורמים הנותנים שירותי ביקורת פנימית. מטרת הקוד האתי הינה לקדם תרבות אתית במקצוע הביקורת הפנימית.

ראוי (Should) – התקנים משתמשים במילה "ראוי" כאשר עמידה בהם מצוּפָּה, אלא אם כן, הנסיבות מצדיקות סטייה, בכפוף ליישום שיקול דעת מקצועי.

שירותי הבטחה (Assurance Services) – שירותי ביקורת המבוססים על בחינה אובייקטיבית של רְאָיָה לשם מתן הערכה בלתי-תלויה על תהליכי שליטה, ניהול סיכונים ובקרה באירגון. דוגמאות לסוגי ביקורות יכולות לכלול: פיננסיות, ביצועיות, הלימות הבקרות, אבטחת המערכות וביקורות שקידה נאותה (due-diligence).

שירותי ייעוץ (Consulting Services) – פעילויות מייעצות ושירותים קשורים הניתנים ללקוח, שאופיים והיקפם מוסכמים איתו. פעילויות אלו נועדו להוסיף ערך ולשפר את תהליכי השליטה, ניהול הסיכונים והבקרה באירגון. המבקר הפנימי לא יקבל עליו אחריות ניהולית לגבי פעילויות אלו*[1].

שליטה (Governance) – השילוב של תהליכים ניהוליים ומבנים ארגוניים, המיושמים על-ידי הדירקטוריון, כדי ליידע, לכוון, לנהל ולנטר את הפעילויות של האירגון להשגת יעדיו.

שליטה בטכנולוגית המידע (Information Technology Governances) – מורכבת ממנהיגות, ממבנים ארגוניים ומתהליכים, המבטיחים שטכנולוגיות המידע של הארגון יציבות ותומכות באסטרטגית הארגון וביעדיו.

תוכנית הביקורת (Engagement Work Program) – מסמך המפרט את התהליכים, שיש לפעול לפיהם במהלך ביצוע מטלת ביקורת, והמיועד להשיג את מטרות תוכניות העבודה של הביקורת הפנימית.

תיאבון לסיכון (Risk Appetite) – רמת הסיכון שארגון מוכן לקבל.

[1*] מדיניות לשכת המבקרים הפנימיים – ישראל, בצמידות לחוקי מדינת ישראל – הינה, כי מטלות ייעוץ אינן במסגרת הגדרת תפקידו של המבקר הפנימי, וכי ייעוץ הינו – הלכה למעשה – המלצת המבקר, הבאה בדוח ביקורת, שערך, לאור ממצאיו ומסקנותיו. המבקר הפנימי אינו יכול להיות יועץ, שאחרת יהיה בניגוד עניינים, בבואו לבקר את תוצאות הייעוץ, שנתן.

תקן / תקן מקצועי (Standard) – פרסום מקצועי המוכרז על-ידי לשכת המבקרים הפנימיים בישראל, ומתאר את הדרישות לביצוע תחום רחב של פעילויות ביקורת פנימית, ולהערכת ביצועי הביקורת הפנימית.

תקנים מקצועיים מקובלים – פרסומים מקצועיים, המוכרזים על-ידי לשכת המבקרים הפנימיים בישראל, וכוללים את הגדרת מקצוע הביקורת הפנימית, את הקוד האתי, את התקנים המקצועיים ואת ההנחיות המקצועיות, ומחייבים את העוסקים בביקורת פנימית.

תקנון הביקורת (Charter) – תקנון הביקורת הפנימית הוא מסמך פורמלי, המגדיר את המטרות, הסמכות והאחריות של הביקורת הפנימית. תקנון הביקורת הפנימית ממקם את הביקורת הפנימית באירגון, מתיר גישה לרשומות, לכוח אדם ולנכסים פיסיים, הרלוונטיים לביצוע הביקורת, ומגדיר את היקף פעילויות הביקורת הפנימית.

5. הנחיות מקצועיות

ההנחיות המקצועיות נכתבו על-ידי לשכת המבקרים הפנימיים בישראל, בהתבסס על ידע ועל ניסיון מקצועי ועל מקורות מגוונים, ובכללם:

- תקנים מקצועיים בינלאומיים לביקורת פנימית;
- ניירות עמדה, נוהלי יעץ והנחיות לפרקטיקה;
- חקיקה, תקינה, ופסיקה בישראל;
- ספרות מקצועית.

6. ניירות עמדה (Position Papers)

ניירות עמדה מסייעים למגוון רחב של גורמים מעוניינים בנושאי שליטה תאגידית (governance), ניהול סיכונים ובקרה. ניירות העמדה מתווים את התפקידים ומסגרת האחריות הקשורים בביקורת הפנימית. ניירות העמדה אינם מחייבים, ובמקרה של סתירה בינם לבין התקנים המקצועיים או ההנחיות המקצועיות - התקנים וההנחיות המקצועיות הם המחייבים.

7. נוהלי יעץ (Practice Advisories)

נוהלי היעץ משמשים כרקע עיוני לסיוע בהבנת התקנים המקצועיים לביקורת פנימית, בפרשנותם וביישומם.

נוהלי היעץ כוללים גישות, מתודולוגיות ושיקולים.

נוהלי היעץ נוהלי היעץ אינם מחייבים, ובמקרה של סתירה בינם לבין התקנים המקצועיים או ההנחיות המקצועיות - התקנים וההנחיות המקצועיות הם המחייבים.

8. הנחיות לפרקטיקה (Practice Guides)

הנחיות לפרקטיקה כוללות מידע מפורט כיצד לנהל פעילויות של ביקורת פנימית, כולל: תהליכים ונהלים, כלים וטכניקות, תוכניות, גישות ודוגמאות לדוחות.
הנחיות לפרקטיקה אינן מחייבות, ובמקרה של סתירה בינן לבין התקנים המקצועיים או ההנחיות המקצועיות - התקנים וההנחיות המקצועיות הם המחייבים.

9. תדריכי ביקורת ושאלונים (Audit Guides & Questionnaires)

תדריכי ביקורת ושאלונים נכתבו על-ידי המועצה המקצועית של לשכת המבקרים הפנימיים בישראל, בהתבסס על ידע, על ניסיון ועל חומר עיוני נוסף. מטרת תדריכי ביקורת ושאלונים היא לסייע למבקרים פנימיים בהבנה של נושאי תדריכי הביקורת והשאלונים, ולספק רשימות תיוג לביקורות בנושאים אלה.
תדריכי ביקורת ושאלות אינם מחייבים, ובמקרה של סתירה בינם לבין התקנים המקצועיים או ההנחיות המקצועיות - התקנים וההנחיות המקצועיות הם המחייבים.

10. הנוסח האנגלי של התקנים המקצועיים

להלן הנוסח האנגלי של התקנים המקצועיים כפי שפורסם על-ידי לשכת המבקרים הפנימיים העולמים ה-IIA.

Standards Introduction

Internal auditing is conducted in diverse legal and cultural environments; within organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. While differences may affect the practice of internal auditing in each environment, conformance with The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* is essential in meeting the responsibilities of internal auditors and the internal audit activity.

If internal auditors or the internal audit activity is prohibited by law or regulation from conformance with certain parts of the *Standards*, conformance with all other parts of the *Standards* and appropriate disclosures are needed.

If the *Standards* are used in conjunction with standards issued by other authoritative bodies, audit communications may also cite the use of other standards, as appropriate. In such a case, if inconsistencies exist between the *Standards* and other standards, internal auditors and the internal audit activity must conform with the *Standards,* and may conform with the other standards if they are more restrictive.

The purpose of the *Standards* is to:

1. Delineate basic principles that represent the practice of internal auditing.
2. Provide a framework for performing and promoting a broad range of value-added internal auditing.
3. Establish the basis for the evaluation of internal audit performance.
4. Foster improved organizational processes and operations.

The *Standards* are principles-focused, mandatory requirements consisting of:

- Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance, which are internationally applicable at organizational and individual levels.
- Interpretations, which clarify terms or concepts within the Statements.

The *Standards* employ terms that have been given specific meanings that are included in the Glossary. Specifically, the *Standards* use the word "must" to specify an unconditional requirement and the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

It is necessary to consider the Statements and their Interpretations as well as the specific meanings from the Glossary to understand and apply the *Standards* correctly.

The structure of the *Standards* includes Attribute, Performance, and Implementation Standards. Attribute Standards address the attributes of organizations and individuals performing internal audit services. The Performance Standards describe the nature of internal audit services and provide quality criteria against which the performance of these services can be measured. The

Attribute and Performance Standards apply to all internal audit services. The Implementation Standards expand upon the Attribute and Performance Standards, providing the requirements applicable to assurance (A) or consulting (C) activities.

Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusions regarding an entity, an operation, a function, a process, system, or other subject matter. The nature and scope of the assurance engagement are determined by the internal auditor. There are generally three parties involved in assurance services: (1) the person or group directly involved with the entity, operation, function, process, system, or other subject matter — the process owner, (2) the person or group making the assessment — the internal auditor, and (3) the person or group using the assessment — the user.

Consulting services are advisory in nature, and are generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Consulting services generally involve two parties: (1) the person or group offering the advice — the internal auditor, and (2) the person or group seeking and receiving the advice — the engagement client. When performing consulting services the internal auditor should maintain objectivity and not assume management responsibility.

The review and development of the *Standards* is an ongoing process. The Internal Audit Standards Board engages in extensive consultation and discussion prior to issuing the *Standards*. This includes worldwide solicitation for public comment through the exposure draft process. All exposure drafts are posted on The IIA's Web site as well as being distributed to all IIA institutes.

Suggestions and comments regarding the *Standards* can be sent to:

The Institute of Internal Auditors
Standards and Guidance
247 Maitland Avenue
Altamonte Springs, FL 32701-4201, USA
E-mail: guidance@theiia.org
Web: http://www.theiia.org

INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING (STANDARDS)

Attribute Standards

1000 – Purpose, Authority, and Responsibility
The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

Interpretation:
The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.

> **1000.A1 –** The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.
>
> **1000.C1 –** The nature of consulting services must be defined in the internal audit charter.

1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter
The mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* must be recognized in the internal audit charter. The chief audit executive should discuss the Definition of Internal Auditing, the Code of Ethics, and the *Standards* with senior management and the board.

1100 – Independence and Objectivity
The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Interpretation:
Independence is the freedom from conditions that threaten the ability of the internal audit activity or the chief audit executive to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

1110 – Organizational Independence
The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

> **1110.A1 –** The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

1111 – Direct Interaction with the Board
The chief audit executive must communicate and interact directly with the board.

1120 – Individual Objectivity
Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Interpretation:
Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.

1130 – Impairment to Independence or Objectivity
If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Interpretation:
Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity's and the chief audit executive's responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.

> **1130.A1 –** Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.
>
> **1130.A2 –** Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.
>
> **1130.C1 –** Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.
>
> **1130.C2 –** If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

1200 – Proficiency and Due Professional Care
Engagements must be performed with proficiency and due professional care.

1210 – Proficiency
Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Interpretation:
Knowledge, skills, and other competencies is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

1210.A1 – The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

1210.C1 – The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1220 – Due Professional Care
Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1 – Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives;
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

1220.A2 – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques**.**

1220.A3 – Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

1220.C1 – Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results;
- Relative complexity and extent of work needed to achieve the engagement's objectives; and
- Cost of the consulting engagement in relation to potential benefits.

1230 – Continuing Professional Development
Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

1300 – Quality Assurance and Improvement Program
The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Interpretation:
A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

1310 – Requirements of the Quality Assurance and Improvement Program
The quality assurance and improvement program must include both internal and external assessments.

1311 – Internal Assessments
Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic reviews performed through self-assessment or by other persons within the organization with sufficient knowledge of internal audit practices.

Interpretation:
Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

Periodic reviews are assessments conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

1312 – External Assessments
External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent external assessments; and
- The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

Interpretation:
A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the organizations that the reviewers have been associated with in relation to the organization for which the internal audit activity is being assessed, as well as the need for particular sector, industry, or technical knowledge.

An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs.

1320 – Reporting on the Quality Assurance and Improvement Program
The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

Interpretation:
The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the board and considers the responsibilities of the internal audit activity and chief audit executive as contained in the internal audit charter. To demonstrate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards, the results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results include the reviewer's or review team's assessment with respect to the degree of conformance.

1321 – Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"
The chief audit executive may state that the internal audit activity conforms with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support this statement.

1322 – Disclosure of Nonconformance
When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

Performance Standards

2000 – Managing the Internal Audit Activity
The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation:
The internal audit activity is effectively managed when:

- *The results of the internal audit activity's work achieve the purpose and responsibility included in the internal audit charter;*
- *The internal audit activity conforms with the Definition of Internal Auditing and the Standards; and*

- *The individuals who are part of the internal audit activity demonstrate conformance with the Code of Ethics and the Standards.*

2010 – Planning
The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:
The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board.

> **2010.A1 –** The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.
>
> **2010.C1 –** The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

2020 – Communication and Approval
The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2030 – Resource Management
The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Interpretation:
Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

2040 – Policies and Procedures
The chief audit executive must establish policies and procedures to guide the internal audit activity.

Interpretation:
The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

2050 – Coordination
The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

2060 – Reporting to Senior Management and the Board
The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks,

governance issues, and other matters needed or requested by senior management and the board.

Interpretation:
The frequency and content of reporting are determined in discussion with senior management and the board and depend on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management or the board.

2100 – Nature of Work
The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

2110 – Governance
The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

> **2110.A1 –** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.
>
> **2110.A2 –** The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.
>
> **2110.C1 –** Consulting engagement objectives must be consistent with the overall values and goals of the organization.

2120 – Risk Management
The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation:
Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- *Organizational objectives support and align with the organization's mission;*
- *Significant risks are identified and assessed;*
- *Appropriate risk responses are selected that align risks with the organization's risk appetite; and*
- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

> **2120.A1 –** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
>
> - Reliability and integrity of financial and operational information.

- Effectiveness and efficiency of operations.
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

2120.C1 – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

2130 – Control
The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – he internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

2130.A2 – Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.

2130.A3 – Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

2130.C1 – During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

2130.C2 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

2200 – Engagement Planning
Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

2201 – Planning Considerations
In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;

- The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and
- The opportunities for making significant improvements to the activity's risk management and control processes.

2201.A1 – When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

2210 – Engagement Objectives
Objectives must be established for each engagement.

2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

2210.A3 – Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.

2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

2220 – Engagement Scope
The established scope must be sufficient to satisfy the objectives of the engagement.

2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

2220.A2 – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

2220.C1 – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

2230 – Engagement Resource Allocation
Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

2240 – Engagement Work Program
Internal auditors must develop and document work programs that achieve the engagement objectives.

> **2240.A1 –** Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.
>
> **2240.C1 –** Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

2300 – Performing the Engagement
Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2310 – Identifying Information
Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Interpretation:
Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Reliable information is the best attainable information through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organization meet its goals.

2320 – Analysis and Evaluation
Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

2330 – Documenting Information
Internal auditors must document relevant information to support the conclusions and engagement results.

> **2330.A1 –** The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.
>
> **2330.A2 –** The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.
>
> **2330.C1 –** The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2340 – Engagement Supervision
Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

Interpretation:
The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit

activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.

2400 – Communicating Results
Internal auditors must communicate the engagement results.

2410 – Criteria for Communicating
Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

> **2410.A1 –** Final communication of engagement results must, where appropriate, contain internal auditors' overall opinion and/or conclusions.
>
> **2410.A2 –** Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.
>
> **2410.A3 –** When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.
>
> **2410.C1 –** Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

2420 – Quality of Communications
Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

Interpretation:
Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

2421 – Errors and Omissions
If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

2430 – Use of "Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*"
Internal auditors may report that their engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*", only if the results of the quality assurance and improvement program support the statement.

2431 – Engagement Disclosure of Nonconformance
When nonconformance with the Definition of Internal Auditing, the Code of Ethics or the *Standards* impacts a specific engagement, communication of the results must disclose the:

- Principle or rule of conduct of the Code of Ethics or *Standard(s)* with which full conformance was not achieved;

- Reason(s) for nonconformance; and
- Impact of nonconformance on the engagement and the communicated engagement results.

2440 – Disseminating Results
The chief audit executive must communicate results to the appropriate parties.

Interpretation:
The chief audit executive or designee reviews and approves the final engagement communication before issuance and decides to whom and how it will be disseminated.

2440.A1 – The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2 – If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization;
- Consult with senior management and/or legal counsel as appropriate; and
- Control dissemination by restricting the use of the results.

2440.C1 – The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2 – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

2500 – Monitoring Progress
The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

2600 – Resolution of Senior Management's Acceptance of Risks
When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

Glossary

Add Value
Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.

Adequate Control
Present if management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

Assurance Services
An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Board
A board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report.

Charter
The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

Chief Audit Executive
Chief audit executive is a senior position within the organization responsible for internal audit activities. Normally, this would be the internal audit director. In the case where internal audit activities are obtained from external service providers, the chief audit executive is the person responsible for overseeing the service contract and the overall quality assurance of these activities, reporting to senior management and the board regarding internal audit activities, and follow-up of engagement results. The term also includes titles such as general auditor, head of internal audit, chief internal auditor, and inspector general.

Code of Ethics
The Code of Ethics of The Institute of Internal Auditors (IIA) are Principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

Compliance
Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

Conflict of Interest
Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Consulting Services

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Control
Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Control Environment
The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

Control Processes
The policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.

Engagement
A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

Engagement Objectives
Broad statements developed by internal auditors that define intended engagement accomplishments.

Engagement Work Program
A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

External Service Provider
A person or firm outside of the organization that has special knowledge, skill, and experience in a particular discipline.

Fraud
Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

Governance
The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

Impairment
Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

Independence
The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

Information Technology Controls
Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

Information Technology Governance
Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology sustains and supports the organization's strategies and objectives.

Internal Audit Activity
A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

International Professional Practices Framework
The conceptual framework that organizes the authoritative guidance promulgated by The IIA. Authoritative Guidance is comprised of two categories – (1) mandatory and (2) strongly recommended.

Must
The *Standards* use the word "must" to specify an unconditional requirement.

Objectivity
An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires internal auditors not to subordinate their judgment on audit matters to others.

Residual Risk

The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

Risk
The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk Appetite
The level of risk that an organization is willing to accept.

Risk Management
A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

Should
The *Standards* use the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

Significance
The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

Standard
A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.

Technology-based Audit Techniques
Any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and computer-assisted audit techniques (CAATs).

***