שינויים בתקן ISO 27002 מהדורת 2022

24 מאי 2022

מבוא

עולם מערכות המידע האינטרנט ומרחב הסייבר מתפתח ושתנה במהירות מדהימה, לא כך התקנים שמלווים אותו. תקן הגנה על המידע ISO 27001 עומד להתעדכן באוקטובר 2022, אבל השינוי כבר כאן. התקן המשלים תקן ISO 27002 המשמש קוים מנחים ופרשנות באשר להטמעה ישום ומימוש הבקרות הטכנולוגיות כבר התעדכן בפברואר השנה.
יש להדגיש כי מדובר על ארגון מחדש ושינויים קלים ברשימת הבקרות, אולם בעקבות כך צפויים שינויים 27001 לצורך שמירת התאימות בין שני התקנים.

עיקר השינויים בגרסת 2022

מתוך 114 הבקרות במהדורת 2013 נוספו 11, 56 אוחדו ונוסחו מחדש כך שנותרו 24, ו- 1 פוצלה.
סה"כ במהדורה 2022 יש 93 בקרות בלבד.

114 controls in *ISO/IEC 27002:2013* + 11 additions - 56 merged + 24 condensed (+ 1 split - 1 already merged) = 93 controls in *ISO/IEC 27002:2022*

חשוב להדגיש כי השינוי במספר הבקרות אינו השינוי החשוב ביותר, הבשורה האמיתית היא הארגון מחדש של הנושאים (Domaine) והצמדת "תכונות" (Attributes) לכל בקרה. במקום 14 סעיפים הבקרות מחולקות ל 4 תחומים (Domaine):

5. ארגוני (37 בקרות)
6. אנשים (8 בקרות)
7. פיזי (14 בקרות)
8. טכנולוגי (34 בקרות)

בנוסף כדי לעזור בזיהוי הבקרות הרלוונטיות בתהליכי ניהול הסיכונים הבקרות מתוייגות עם "תכונות" (Attributes) בהתאם לאופיין על פי המפתח :

- **סוג בקרה** (#preventive, #detective, #corrective),
- **סיווג** (#availibility , #integrity , #confidentiality),
- **תפישת הגנת סייבר** (#identify, #protect, #detect, #respond, #recover)
- **ויכולות תפעוליות** (#governance, #asset_management, #information_protection, #human_resource_security, #physical_security, #system_and_network_security, #application_security, #secure_configuration, #identity_and_access_management, #threat_and_vulnerability_management, #continuity, #supplier_relationships_security, #legal).

הבקרות החדשות

כפי שצוין לעיל נוספו 11 בקרות חדשות שנראה כי הן עשויות לדרוש שינוי מסוים של היישום הקיים בארגונים ככל שהן כלולות בהצהרת הישימות הארגונית (SOA). להלן פרוט הסעיפים תוך ציון הבקרה התואמת במהדורה 2013.

א.לביא יעוץ וניהול (1996) בע"מ
אתר: www.lms.co.il
דוא"ל: info@lms.co.il

	ISO 27002:2022		ISO 27002:2013 שווה ערך
A.5.7	מודיעין איומים	A.6.1.4	צור קשר עם קבוצות אינטרס מיוחדות
A.5.16	ניהול זהויות	A.9.2.1	רישום משתמשים וביטול רישום
A.5.23	אבטחת מידע לשימוש בשירותי ענן	A.15.x	קשרי ספקים
A.5.29	אבטחת מידע במהלך שיבוש	A.17.1.x	המשכיות אבטחת מידע
A.5.30	מוכנות ICT להמשכיות עסקית	A.17.1.3	אימות, סקירה והערכה של רציפות אבטחת מידע
A.7.4	ניטור אבטחה פיזית	A.9.2.5	סקירה של זכויות גישה למשתמש
A.8.9	ניהול תצורה	A.14.2.5	עקרונות הנדסת מערכת מאובטחת
A.8.10	מחיקת מידע	A.18.1.3	הגנה על רשומות
A.8.11	מיסוך נתונים	A.14.3.1	הגנה על נתוני בדיקה
A.8.12	מניעת דליפות נתונים	A.12.6.1	ניהול פגיעויות טכניות
A.8.16	פעילויות ניטור	A.12.4.x	רישום וניטור
A.8.23	סינון אינטרנט	A.13.1.2	אבטחה של שירותי רשת
A.8.28	קידוד מאובטח	.14.2.1	מדיניות פיתוח מאובטחת

הערכות וניהול השינוי

המהדורה החדשה של תקן ISO 27002 פורסמה בפברואר 2022 ואילו העדכון המתבקש בתקן ISO 27001 צפוי להתפרסם באוקטובר 2022, למרות שתאריך מדוייק טרם הוכרז.
כפי שנזכר לעיל, השינויים העיקריים הצפויים בתקן 27001 הם שינויים צנועים הנוגעים בעיקר לארגון והגדרת הבקרות ועדכון נספח A להתאמה לבקרות החדשות שבתקן 27002.
ההערכות של כל ארגון למימוש השינוי תלויה בשלב בו הוא נמצא בתהליך ובדחיפות לקבלת התעדה רשמית.
ארגונים בעלי תעודת התאמה לתקן יסקרו על פי הנחיות גוף ההתעדה שלהם. תהליך הטמעת השינוי על ידי גופי ההתעדה נמשך כ 2-3 שנים במהלכן על הארגון לבצע את ההתאמות הנדרשות במערכת הניהול שלו. ההתאמות צפויות לכלול בין היתר התאמת תהליך הטיפול בסיכונים לבקרות החדשות, עדכון הצהרת הישימות (SOA) עדכון פסקאות ספציפיות בנהלים ובמסמכי המדיניות.
לארגונים הנמצאים בתהליך ולקראת התעדה בזמן הקרוב מוצע להצמד לדרישות ולבקרות של מהדורה 2013 ולקחת בחשבון את הצורך למפות ולהוסיף את הבקרות החדשות מראש כהכנה לקראת פרסום ISO 27001:2022.
לארגונים שאינם זקוקים להתעדה מידית מוצע להתחיל בתהליכי הטמעה של הבקרות הנחשבות עבורם לעיקריות בהתאם לניתוח הסיכונים ולהמתין עם תהליכי ההתעדה הרשמיים עד לפרסום רשמי של התקן.

התמיכה שלנו בתהליך

בין אם אתם בעלי התעדה וצריכים סיוע בשדרוג או שאתם מעונינים להתחיל בתהליך התעדה אנחנו כאן כדי לעזור. יש לנו את הידע הכישורים והיכולת לסיע לכם לעבור את התהליך בקלות ובפשטות או במילים אחרות במינימום מאמץ תוך ניצול כל היתרונות של חברה בעלת התעדה לתקן יוקרתי זה.

אבי לביא
יועץ לאיכות
א.לביא יעוץ בע"מ

א.לביא יעוץ וניהול (1996) בע"מ
אתר: www.lms.co.il
דוא"ל: info@lms.co.il