שיעור 5

הסמכות ומסגורים בינלאומיים:
ISO2700X, SOC2, CSA, GDPR ועוד

מטרת השיעור

הכרות עם תקנים ומסגורים מובילים בתחום אבטחת המידע בארגונים

- להכיר את התוכניות השונות ולהבין את מהותן.
- להבין את חשיבות העמידה בתקנים מחייבים ולא מחייבים.
- להבין כיצד התקנים תורמים לבניית אמון עם לקוחות, שותפים עסקיים ורגולטורים.
- לזהות מתי, איזה וכיצד (תקנים...).

תקנים ורגולציה באבטחת סייבר: מקומי, זר, בינלאומי

עיונים במסמך "תקנים ורגלוציה באבטחת סייבר" של מערך הסייבר הלאומי

- מבטיח שזה לא משעמם, באמת!

https://www.gov.il/BlobFolder/legalinfo/regulation/he/.0_תקנים%02ורגולציה pdf

מטרת השיעור

התקנים עליהם נדבר (בקצרה, כהקבלה לתכניות כמו NIST).

- ISO/IEC27001:2022 (ותקנים נלווים, למשל 27002, 27003).
- תקני SOC של הארגון האמריקאי American Institute of Certified Public Accountants (AICPA)
- תקן CSA.
- רגולציית ה-GDPR (שעצם היותה מחייבת הפכה למעין תקן).
- תקן PCI-DSS.
- תקנות הגנת הפרטיות (אבטחת מידע) - 2017 (נכנסו לתוקף ב-2018).

למה צריך תקנים?

למה צריך תקנים?

"התו היחיד המאשר כי שמן הזית נבדק כימית במעבדה ואורגנולפטית בפאנל טועמים מוסמך. תו האיכות מבטיח לכם שמקורו של שמן הזית שקניתם הוא מישראל ושמתחילת המסיק, דרך המעבר לבתי הבד ועד לצלחת שלכם – נשמרו תהליכי בקרה מוקפדים וברורים שנועדו להבטיח לכם שמן זית בריא, איכותי, טרי ומאה אחוז ישראלי."

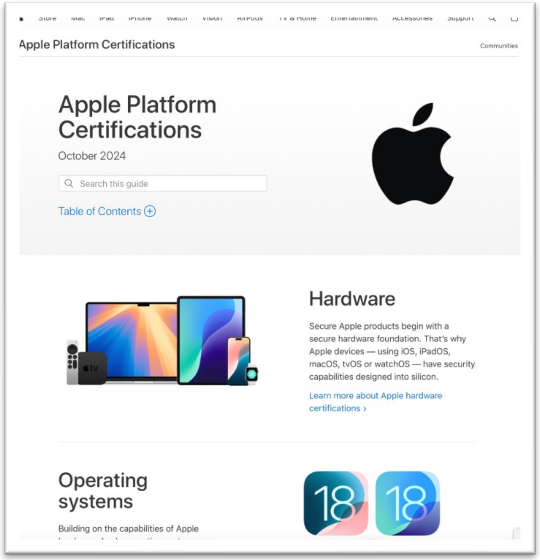
https://www.oliveboard.org.il/תו-האיכות/

מי צריך את התקנים האלה?

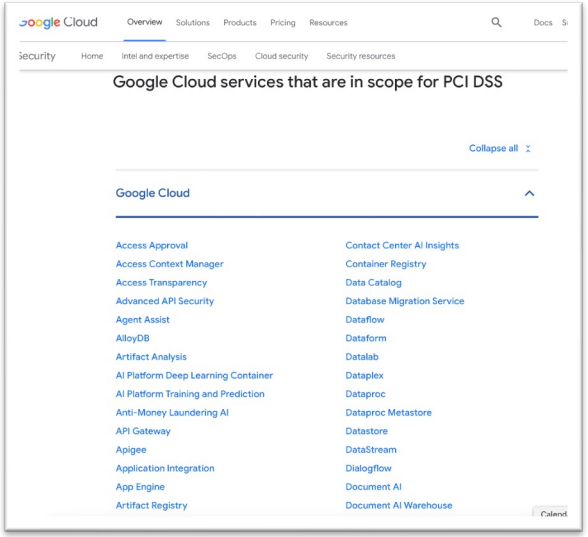
מטרת תקינה מקומית, זרה, בינלאומית

- שקיפות.
- אחידות (סטנדרטיזציה).
- הבטחה על עמידה ברמות איכות מסוימות.
- הקטנת סיכונים.
- אמון לקוחות.
- אמון שותפים עסקיים
- אמון רגולטורים (יכולים לוודא בקלות שהארגון עמד בדרישות מסוימות).
- חוק מחייב (לעיתים).

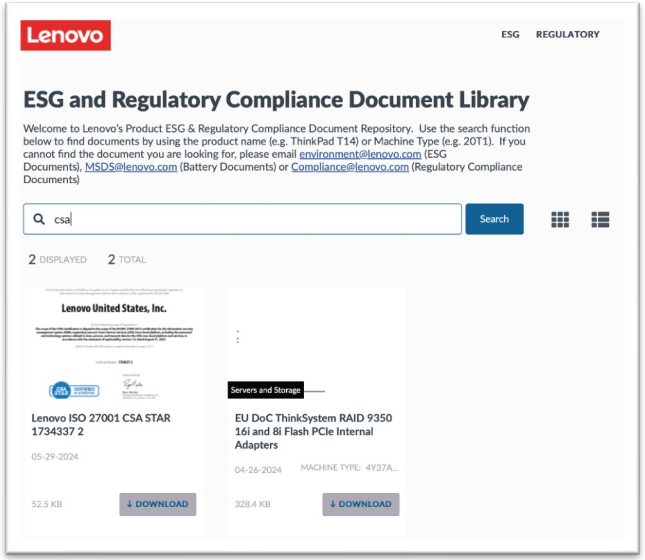
מי צריך את התקנים האלה? – בואו נראה...



https://support.apple.com/en-gb/guide/certifications/welcome/web



https://cloud.google.com/security/compliance/pci-dss



https://compliance.lenovo.com/content/esg-document-library/en/esg.html?layout=card&p.offset=0&p.limit=24

תקן/חוק	מחייב/לא מחייב	דרכי השגת התקן	קריטריונים	דוגמה	מהות
ISO/IEC 27001	לא מחייב (אלא אם נדרש רגולטורית)	הערכת סיכונים, יישום בקרות, ביקורת חיצונית	ניהול סיכונים, בקרות גישה, הצפנה, תיעוד נהלים	חברת טכנולוגיה המאבטחת נתוני לקוחות רגישים	מסגרת לניהול מערכת אבטחת מידע (ISMS)
SOC (AICPA)	לא מחייב (אך נדרש לשותפויות עסקיות מסוימות)	פנייה לרואי חשבון מוסמכים, ביקורת תקופתית	עמידה בבקרות על אבטחה, זמינות, וסודיות	ספק שירותי ענן המפיץ דוח SOC 2 ללקוחות	דוחות ביקורת לתהליכים ובקרות באבטחת מידע ושירותים עסקיים
CSA STAR	לא מחייב (אך מגדיל אמון לקוחות)	מילוי שאלון CAIQ, שילוב עם ISO 27001	שאלון הערכה עצמית ISO , 27001ניטור שוטף	חברת SaaS המציגה CSA STAR לאמינות בענן	הסמכה לאבטחת מידע בשירותי ענן
PCI-DSS	מחייב עבור ארגונים המעבדים עסקאות כרטיסי אשראי	הטמעת בקרות, בדיקות אבטחה, ביקורת חיצונית	הצפנת מידע, ניהול גישה, תיעוד עסקאות	אתר מסחר מקוון שמאבטח עסקאות כרטיסי אשראי	תקן דה-פקטו חובה לאבטחת עסקאות פיננסיות בין חברות
Common Criteria (CC)	לא מחייב (אך נדרש למכרזים ממשלתיים מסוימים)	הערכת המוצר על ידי גוף (מעבדות CC) מוכר	הערכת עמידות המוצר לקריטריונים בינלאומיים	מוצר Firewall שעבר הערכה וקיבל אישור CC	מסגרת להערכת ואישור מוצרי אבטחת מידע
GDPR	מחייב עבור ארגונים הפועלים באיחוד האירופי	מיפוי נתונים, כתיבת מדיניות פרטיות, יישום בקרות	שקיפות, הסכמה, דיווח הפרות, שמירה על זכויות	חברת מסחר אונליין המתאימה את פעילותה ל-GDPR	רגולציה להגנה על מידע אישי באיחוד האירופי
תקנות הגנת הפרטיות (ישראל)	מחייב עבור ארגונים עם מאגרי מידע אישי בישראל	יישום נהלים, ביקורת פנימית וחיצונית	רישום מאגרי מידע, בקרות גישה, הצפנה	חברה ישראלית הרשומה ברמו"ט כמנהלת מאגרי מידע	תקנות לאבטחת מאגרי מידע בישראל
ISO/IEC 27018	לא מחייב (אך חיוני לשירותי ענן המנהלים מידע אישי)	שילוב עם ISO 27001, יישום בקרות פרטיות, ביקורת חיצונית	יישום מדיניות פרטיות, הצפנה, ניהול הרשאות, שמירה על שקיפות מול לקוחות	ספק שירותי ענן המספק הצפנה וניהול שקוף של מידע אישי	תקן המוקדש להגנה על מידע אישי בסביבות ענן PII

ISO/IEC 27001

https://www.youtube.com/watch?v=jPA6gbsT2IQ

PCI-DSS

https://www.youtube.com/watch?v=szVmMxWORBc

GDPR

https://www.youtube.com/watch?v=j6wwBqfSk-o&t=75s

https://www.youtube.com/watch?v=j6wwBqfSk-o&t=75s

מי צריך את התקנים האלה?

- שקיפות.
- אחידות (סטנדרטיזציה).
- הבטחה על עמידה ברמות איכות מסוימות.
- הקטנת סיכונים.
- אמון לקוחות.
- אמון שותפים עסקיים
- אמון רגולטורים (יכולים לוודא בקלות שהארגון עמד בדרישות מסוימות).
- חוק מחייב (לעיתים).

Information Security Management ISO 27001 Certified

סיכום ושאלות

שיעור 6

מסגור אבטחת סייבר בראייה בינלאומית: בריטניה, סין, רוסיה