

שיעור 5

הסמכות ומוסגרים בינלאומיים:
יעוד ISO2700X, SOC2, CSA, GDPR

מטרת השיעור

הכרות עם תקנים ומוסגרים מובילים בתחום אבטחת המידע בארגונים

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

תקנים ורגולציה באבטחת סייבר: מקומי, זר, בינלאומי

עינויים במסמך "תקנים ורגולציה באבטחת סייבר" של מערך הסייבר הלאומי

- מבטיח שזה לא משעמם, באמת!

[תקנים ורגולציה באבטחת סייבר](https://www.gov.il/BlobFolder/legalinfo/regulation/he/.0_0.pdf)



מטרת השיעור

התקנים עליהם נדבר (בקצהה, כהקללה לתקנות כמו NIST).

- 
- IEC27001:2022 (ותקנים נלוים, למשל 27002, 27003).
 - תקני SOC של הארגון האמריקיקאי Accountants (AICPA)
 - תקן CSA.
 - רגולציה GDPR (שעزم הייתה מחייבת הפקה למעין תקן).
 - תקן PCI-DSS.
 - תקנות הגנת הפרטויות (אבטחת מידע) - 2017 (נכנו לתוכף ב-2018).

למה צריך תקנים?



למה צריך תקנים?



"התו היחד המאשר כי שמן הזית נבדק כימיית במעבדה אורגנולפטית באנל טועמים מוסמך.תו האיכות מבטיח לכם שמקורו של שמן הזית שקניתם הוא מישראל ושמתחילה 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/>

מי צריך את התקנים האלה?

מטרת תקינה מקומית, זרה, בינלאומית



- שקייפות.
- אחידות (סטנדרטיזציה).
- הבטחה על עמידה ברמות איכות מסוימות.
- הקטנת סיכוןים.
- אמון לקוחות.
- אמון שותפים עסקיים
- אמון רגולטורים (יכולים לוודא בקלות שהארגון עומד בדרישות מסוימות).
- חוק מחייב (לעתים).

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

Apple Platform Certifications

October 2024

Search this guide

Table of Contents

Hardware

Secure Apple products begin with a secure hardware foundation. That's why Apple devices — using iOS, iPadOS, macOS, tvOS or watchOS — have security capabilities designed into silicon.

Learn more about Apple hardware certifications >

Operating systems

Building on the capabilities of Apple

Google Cloud services that are in scope for PCI DSS

Collapsible sidebar: Google Cloud

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- AlloyDB
- Artifact Analysis
- AI Platform Deep Learning Container
- AI Platform Training and Prediction
- Anti-Money Laundering AI
- API Gateway
- Apigee
- Application Integration
- App Engine
- Artifact Registry
- Contact Center AI Insights
- Container Registry
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Databab
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- DataStream
- Dialogflow
- Document AI
- Document AI Warehouse

ESG REGULATORY

ESG and Regulatory Compliance Document Library

Welcome to Lenovo's Product ESG & Regulatory Compliance Document Repository. Use the search function below to find documents by using the product name (e.g. ThinkPad T14) or Machine Type (e.g. 20T1). If you cannot find the document you are looking for, please email environmental@lenovo.com (ESG Documents), MSDS@lenovo.com (Battery Documents) or Compliance@lenovo.com (Regulatory Compliance Documents)

Search: csa

2 DISPLAYED 2 TOTAL

Lenovo United States, Inc.

Lenovo ISO 27001 CSA STAR 1734337 2

05-29-2024

52.5 KB

Download

Servers and Storage

EU DoC ThinkSystem RAID 9350 16i and 8i Flash PCIe Internal Adapters

04-26-2024

328.4 KB

Download

<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.ofset=0&p.limit=24>

תקן/חוק	מחייב/לא מחייב	דרכי השגת התקן	דוגמה	מהות
ISO/IEC 27001	לא מחיב (אלא אם נדרש רגולטורית)	הערכת סיכון, ניהול סיכון, בקרות גישה, בקרות, ביקורת חיצונית	חברת טכנולוגיה המאבטחת נתונים ללקוחות רגילים אבטחת מידע (SMS)	מסגרת לניהול מערכת אבטחת מידע (SMS)
SOC (AICPA)	לא מחיב (אך נדרש ביקורת תקופתית לשוטפות עסקיות מסוימות)	פניה לרואי חשבון מוסמכים, עמידה בבדיקות על אבטחה, 2 SOC ללקוחות זמינות, וסודיות	ספק שירותי ענן המפיץ דוח ביקורת תקופתית	דוחות ביקורת לתהליכי אבטחת מידע ושירותים עסקיים
CSA STAR	לא מחיב (אך מגדיל אמון ללקוחות)	מילוי שאלון ISO 27001, CAIQ שלוב עם שאלון הערכת עצמית ISO , 1,000לניטור שוטף	חברת SaaS המציגה CSA STAR לאמינות בענן	הסכמה לאבטחת מידע בשירותי ענן
PCI-DSS	מחיב עבור ארגונים המעבדים עסקאות כרטיסי אשראי	הטמעת בקרות, בדיקות אבטחה, ביקורת חיצונית תעוד עסקאות	תקן דה-פקטו חובה לאבטחת עסקאות כרטיסי אשראי	תקן מסחר מקוון שמआבטח עסקאות פיננסיות בין חברות אשראי
Common Criteria (CC)	לא מחיב (אך נדרש למוצרים ממשלתיים מסוימים)	הערכת מוצר על ידי גופן לקריטריונים בינלאומיים (בדיקות CC) מוכר	מוצר Firewall שעבר הערכת קיבול אישור CC	מסגרת להערכת ואישור מוצר אבטחת מידע
GDPR	מחיב עבור ארגונים הפעילים באיחוד האירופי	מיפוי נתונים, כתיבת מדיניות שקייפות, הסכמה, דיווח הפרות, שימוש בקרות פרטיות, שימוש בזכויות המתאימה את פעילותה לא-	חברת מסחר אונליין באיחוד האירופי	רוגצ'יה להגנה על מידע אישי
תקנות הגנת הפרטיות (ישראל)	מחיב עבור ארגונים עם מאגרי מידע אישי בישראל	רישום מאגרי מידע, בקרות יישום פנימית גישה, הצפנה וחיצונית	חברה ישראלית הרשות ברמות'ט כמנהלת מאגרי מידע בישראל	תקנות לאבטחת מאגרי מידע
ISO/IEC 27018	לא מחיב (אך חיוני לשירותי ענן המנהלים מידע אישי)	ישום מדיניות פרטיות, שילוב עם ISO 27001 יישום מדיניות פרטיות, בקרות פרטיות, בקרות הצפנה, ניהול הרשות, שמירה על שקייפות מול לקוחות	ספק שירותי ענן המספק הצפנה וניהול שקוֹפֶשׁ למידע 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?

- 
- **שקייפות.**
 - **אחדות (סטנדרטיזציה).**
 - **הבטחה על עמידה בדרישות אינטראקטיביות.**
 - **הקטנת סיכוןם.**
 - **אמון ללקוחות.**
 - **אמון שותפים עסקיים**
 - **אמון רגולטורים (יכולים לוודא בקלות שהארגון עומד בדרישות מסויימות).**
 - **חוק מחייב (לעתים).**

סיכום ושאלות



שיעור 6

מסגר אבטחת סייבר בראשיה בינלאומי: בריטניה, סין,
רוסיה