



# PCI DSS Compliance Management<sup>®</sup>

## 2 napos szakmai tanfolyam



A fizetőkártya adatok kezelésével, feldolgozásával, tárolásával érintett társaságoknak (bankok, elszámolók, kereskedők) meg kell felelniük a Payment Card Industry Data Security Standard – **PCI DSS fizetőkártya biztonsági előírás** követelményeinek, és a megfelelést időszakiságosan igazolniuk is kell, amit a kártyatársaságok ellenőriznek.

A tanfolyam témája a **PCI DSS előírás**, az annak való megfelelés – a Compliance szint - elérése, auditálása, valamint a megfelelés igazolása, azaz együttesen a **PCI DSS Compliance Management**.

A tanfolyam tartalma az előzetes felkészülési követelmények alapján került összeállításra, és megadja az ahhoz szükséges ismereteket, hogy a tanfolyam elvégzését követően a hallgatók **PCI DSS Compliance** üzemeltetési környezeteket építhessenek ki, illetve az előírásoknak való megfelelést egy objektív, ismételhető módon ellenőrizhessék.

A tanfolyam mindazok számára nélkülözhetetlen, akiknek felelősségük vagy a feladatuk, hogy vállalatuknál a fizetőkártya adatok biztonságos kezelését megvalósítsák, felügyeljék, vagy bármilyen területen érintettek abban, hogy vállalatuk **PCI DSS Compliance** legyen.

A **PCI DSS Compliance Management** összetett tevékenység. A tanfolyam bemutatja a területeit, részletesen elemzi és értelmezi a megfelelési követelményeket, a kontrollokat, az audit szempontokat, a megfelelés szintjeit, valamint a **Compliance** szint elérésének gyakorlati lépéseit.

### A tanfolyamon a hallgatók

- megtanulják a PCI DSS keretrendszerét,
- megismerkednek a kontroll követelményekkel,
- útmutatást kapnak az elfogadható kontroll megoldásokról,
- és elsajátítják a biztonságos üzemeltetés feltételeit.

### Témakörök

- A PCI DSS és a Payment Card Industry üzleti szereplői,
- A kártyatársaságok megfelelési programjai,
- Kikre és hogyan vonatkozik az előírás, a nemmegfelelés következményei,
- A PCI DSS keretrendszere, az adatok, mit lehet megtartani és mit nem,
- Szegmentálás és az egyes rendszerkomponensek jelentősége,
- Sérülékenység menedzsment,
- Részletes előírások, kompenzációs kontrollok,
- A megfelelés ellenőrzése és igazolása,
- Az igazoló jelentések felépítése és tartalma, a QSA assessment,
- A Compliance szint elérésének lépései, prioritások.

### CPE credit

A tanfolyamon való részvételtől a résztvevők látogatási bizonyítványt kapnak. A tanfolyam a CISSP, CISA, CISM, CGEIT továbbképzésben résztvevő hallgatók számára 14 CPE óra teljesítését jelenti.

### A tanfolyam elvégzésével a hallgatók

- képessé válnak arra, hogy a szervezetüknél költséghatékony PCI DSS rendszert vezessenek be,
- alkalmassá válnak PCI DSS rendszerek belső ellenőrzésére, továbbfejlesztésére,
- felkészültek arra, hogy eredményesen együtt tudjanak működni a QSA auditorokkal.

### Akiknek a tanfolyam szól

**Fizetőkártya adatokat kezelő szervezetek – bankok, elszámolók, szolgáltatók, kártya elfogadó- és e-kereskedők munkatársai:**

- üzletági vezetők és PCI DSS felelősök,
- CIO-k, Security Officer-ek, Compliance Officer-ek, adatvédelmi- és adatbiztonsági felelősök,
- IT Security szakemberek, informatikai rendszergazdák,
- bankbiztonsági felelősök, internal auditorok és informatikai belső ellenőrök.

### Szükséges előképzettség

nincs, az adathálózatok és az IT security alapismerete ajánlott.

### Vizsga és PCI-CFO<sup>®</sup> oklevél

A tanfolyam végén lehetőség van vizsga letételére. Az írásbeli vizsgát sikeresen letett hallgatók Payment Card Industry Certified Field Officer - PCI CFO<sup>®</sup> - oklevelet kapnak.



## A PCI DSS

A fizetőkártya adatok jogtalan megszerzése, az adatokkal való visszaélés milliárdos pénzbeli veszteséget és ezzel összemérhető piacvesztést és erkölcsi károkat okoz évente a fizetőkártya társaságok számára. A szervezett bűnözői körök szakmailag felkészültek, felvenni velük a versenyt nehéz. A fizetőkártya csalásokkal valamint a kártya adatok eltulajdonításával kapcsolatos veszélyek megelőzésére alakították ki a piacvezető kártyatársaságok – MasterCard, Visa, Discover, JCB, AmEx – a **Payment Card Industry Data Security Standard - PCI DSS**- előírást.

Az előírás egy sor átfogó információbiztonsági követelmény teljesítését követeli meg minden olyan szervezettől, amelyek **fizetőkártyák adatainak kezelésével, azaz továbbításával, feldolgozásával vagy tárolásával** foglalkoznak, bankoktól, szolgáltatóktól, bolti- és elektronikus kereskedőktől egyaránt. Az előírás megköveteli a megfelelés rendszeres időközönkénti igazolását.

## PCI DSS Követelmények

### 1. Az adathálózat biztonsága

1. követelmény: A fizetőkártya adatokat tűzfal konfigurációval kell védeni
2. követelmény: Minden jelszót és biztonsági paramétert egyedileg be kell állítani

### 2. A kártyabirtokos adatainak a védelme

3. követelmény: A tárolás során az adatokat védelemmel kell ellátni
4. követelmény: A nyilvános hálózatokon az adatokat rejtjelezetten kell továbbítani

### 3. Sérülékenység menedzsment

5. követelmény: Rendszeresen frissített anti-vírus védelmet kell használni
6. követelmény: Biztonságos alkalmazásokat és rendszereket kell kifejleszteni és használni

### 4. Szigorú hozzáférés védelem alkalmazása

7. követelmény: Az adatokhoz való hozzáférés legyen üzletileg indokolt
8. követelmény: A felhasználói azonosítók legyenek személyhez kötöttek
9. követelmény: Az adatokhoz való fizikai hozzáférés legyen erősen korlátozott

### 5. Adathálózat felügyelete és ellenőrzése

10. követelmény: Minden adat hozzáférés legyen felügyelt és naplózott
11. követelmény: A biztonsági rendszerek és folyamatok kerüljenek rendszeresen tesztelésre

### 6. Informatikai biztonsági politika

12. követelmény: Vállalati-szintű előírással a dolgozóktól és a szerződéses partnerektől egyaránt követelni kell az informatikai biztonságot.

Jelentkezés: [www.hopet.hu](http://www.hopet.hu)



**HOPET**  
Számítástechnikai és Közgazdasági Kft.  
Iroda: 1149 Budapest,  
Pillangó Park 14/A.  
Telefon/Fax: +36-1-787-0740  
Email: hopet@hopet.hu  
Web: www.hopet.hu

A HOPET Kft. 2000-ben alakult. Kiemelt informatikai területünk az üzleti adatok biztonsága, az informatikai minőségirányítás, és a megfelelőség menedzsment. Tevékenységünket a hazai- és a nemzetközi előírások – mint pl. a PCI DSS -, és ajánlások alapján nyújtjuk. Sikereink forrását magasan képzett, nemzetközi szakmai minősítésekkel rendelkező munkatársaink jelentik, akik napi munkájuk során eredményesen ötvözik az informatikai és gazdasági ismereteiket, valamint vezető tanácsadói tapasztalataikat.