HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Hogyan érvényesülnek az Információbiztonsági kontrollok egy publikus felhőben.

Infokommunikáció szakmai tudományos konferencia
2023.november 15.

Oláh István – EIVOK alelnök, Óbudai Egyetem BDI.
HTE Információbiztonsági Szakosztály – EIVOK
istvan.olah@hte.hu; olah.istvan.op@gmail.com;
olah.istvan.gyorgy@uni-nke.hu; olah.istvan@uni-obuda.hu

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Mi a felhő ?

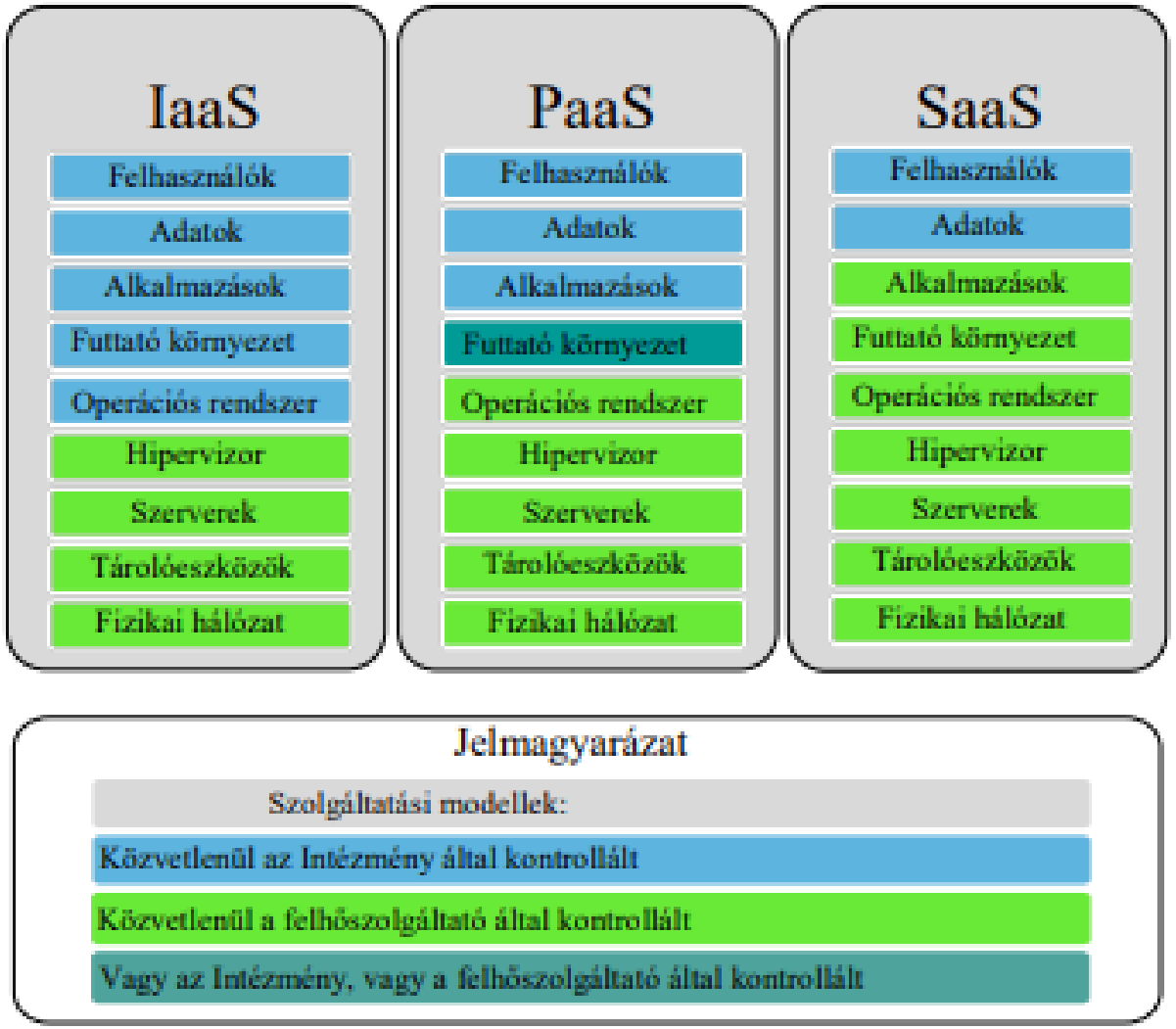
- Egy technológia,
- Erőforrás,
- Szolgáltatások,
- …
- A gyakorlatban sokan keverik ezeket a gondolkodásban
- A földön is lehet a felhő!

Forrás: https://www.usanotebook.hu/blog/mi-az-a-felho-es-miert-jo/467

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A felhő fogalma, és felelősségi kérdései?

- Privát, Publikus, Közösségi.
- Hibrid, Multi.
- A publikus felhőszolgáltatás öt lényegi ismérve a következő:
  - a szolgáltatás igény szerinti, akár önkiszolgáló módon való igénybevétele,
  - általános hálózati elérés,
  - megosztottan használt erőforrások,
  - a változó kapacitás-igények gyors lekövetése,
  - mért szolgáltatás (felhasználással arányos használati díj),
- The NIST Definition of Cloud Computing (SP 800-145).



Forrás:
https://www.mnb.hu/letoltes/4-2019-felho.pdf

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

XaaS ?

+ Address Verification as a Service
+ **Anything as a Service**
+ API as a service (APIaaS) Application
+ Delivery as a Service
+ Application Platform as a Service
+ Architecture as a Service
+ Authentication as a Service
+ Backend as a Service
+ Backup as a Service
+ Big Data as a Service
+ Broker as a Service
+ Business as a Service
+ Business Process as a Service
+ Cloud Load Balancers as a Service
+ Cloud Search as a Service
+ Collaboration-as-a-Service
+ Commerce as a Service
+ Communication as a Service
+ Computing as a Service
+ Contact Center as a Service
+ Conversations as a Service
+ Data as a service
+ Database as a service
+ Desktop as a Service
+ Development as a Service
+ DevTest as a Service
+ Disaster Recovery as a Service
+ Drupal as a Service
+ Email as a Service
+ Encryption as a Service
+ Enterprise Resource Management as a Service
+ Ethernet as a Service
+ **Everything as a Service**
+ Firewall as a Service
+ Framework as a Service
+ Globalization as a Service
+ Hadoop as a Service
+ Hardware as a Service
+ High Performance Computing as a Service
+ Identity as a Service
+ (Infrastructure PaaS)
+ Insight as a Service
+ Integrated Development Environment as a Service
+ Integration as a Service Integration Platform as a Service
+ Integration Platform as a Service
+ **IT as a Service**
+ Java Platform as a Service
+ Knowledge as a Service
+ Light as a Service
+ Logon as a Service Management as a Service
+ Mashups as a Service
+ Message Queuing as a Service
+ Metal as a Service
+ Mobility as a Service
+ Mobility Backend as a Service
+ Monitoring as a Service
+ Network Access Control as a Service
+ Network as a Service
+ Operations as a Service
+ Optimization as a Service
+ Payment as a Service
+ Quality as a Service
+ Query as a Service
+ Recovery as a Service
+ Remote Backup as a Service
+ Risk Assessment as a Service
+ Robot as a Service
+ Security as a service
+ Service Desk as a Service
+ Solutions as a Service
+ Storage as a Service
+ Telepresence as a Service
+ Test environment as a Service
+ Testing as a Service
+ Transport as a Service
+ Unified Communications as a Service
+ User Interface as a Service
+ Video Conferencing as a Service
+ Video Surveillance as a Service
+ Voice as a Service
+ Website as a Service

+ **Mélytanulás**
+ **Kvantumszámítástechnika**

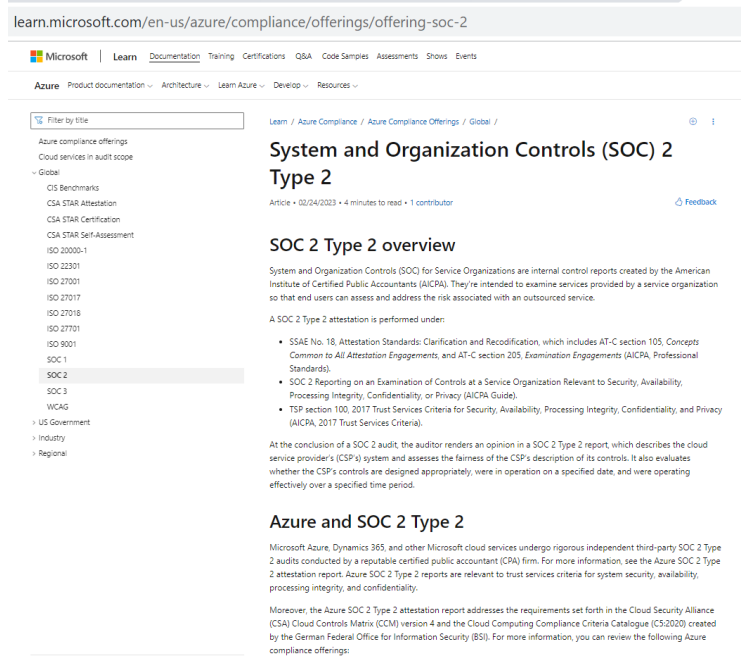
Forrás: Koczka Ferenc, okosóra előadása az OTP Bank Nyrt-ben

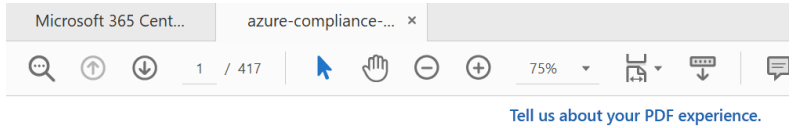
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő auditja I.

- Felhőszolgáltató igénybe vételével kapcsolatos beszerzéskor EIR-enként érdemes elkérni a szolgáltatást vizsgáló **auditok dokumentációját**.

- Akinek van, jellemzően a **tanúsítványt** publikálja az Interneten, de abból valójában semmit nem lehet megtudni, mert az értelmezésükhöz be kell szerezni a **vizsgálati profilt, módszertant és az audit tervet is.** Ezekből lehet látni a mit és milyen szinten tud nyújtani a szolgáltató ami általában nem az a szint amit hirdet magáról!





Azure, Dynamics 365, Microsoft 365, and Power Platform compliance offerings

Article • 02/24/2023 • 4 minutes to read

You're wholly responsible for ensuring your own compliance with all applicable laws and regulations. Information provided in Microsoft online documentation doesn't constitute legal advice, and you should consult your legal advisor for any questions regarding regulatory compliance.

Overview

Azure is a multi-tenant hyperscale cloud platform that is available in more than 60 regions worldwide. Most Azure services enable you to specify the region where your customer data will be located. Microsoft may replicate your customer data to other regions within the same geography for data resiliency but Microsoft won't replicate your customer data outside the chosen geography (for example, United States).

Forrás:https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

A Felhő auditja II.

- Felhőszolgáltató dokumentumai elérhetőek.
- Több ezer oldal 10% url.
- A dokumentumok dinamikusak !, de részei a szerződésnek!
- ISO 27017, 27018 (27015), SOC2-Type2,

Microsoft

EBA, EIOPA and ESMA guidelines that we have not included in the mapping below as these fall entirely within the responsibility scope of financial institutions' arrangements internally and are not specifically related to outsourcing.

4. While Microsoft provides a range of tools and information for customers and potential customers in its Compliance Documentation, on its Service Trust Portal and Trust Center to support firms through their regulatory due diligence and risk assessments, this mapping is a further tool intended to assist financial institutions interested in using Microsoft Online Services.

MAPPING

Item	Reference	Requirement	Microsoft commentary / How and where is this dealt with in the Microsoft Agreement?	Microsoft Agreement reference
		General		
1.	EBA 74 EIOPA 36 ESMA 26	**Rights and obligations** to be clearly allocated in a written agreement. The agreement for critical or important functions must set out:	The rights and obligations of the parties are set out in the Microsoft Agreement.	N/A
2.	EBA 75(a) EIOPA 37(a) ESMA 28(a)	**Services:** A clear description of the outsourced cloud services and type of support services;	The Online Services are described in the Microsoft Agreement. An online description is also available here: • Microsoft 365 Service Description • Dynamics 365 Service Description • Directory of Azure Cloud Services The support services, including Professional Services, are described in the DPA and in the Master Business Services Agreement. The Microsoft Cloud for Financial Services documentation provides capabilities to manage financial services data at scale and makes it easier for financial services organizations to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability.	N/A
3.	EBA 75(b) EIOPA 37(b) ESMA 28(b)	**Term:** Start and end date and notice periods;	Refer to the Microsoft Agreement. In general, standard EA Enrollments have a three-year term and may be renewed for a further three-year term.	N/A

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Ibtv. Megfelelés kontroll szinten- I

- Az azpolicyadvertizer-semicolon lapon az Azure policydefiníciók összefoglalása található meg. Az Azure védelmi profilok egyes adatai innen kerülnek az Azureba.
- Első lépésként célszerű *„az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet”* **kontrolljait NIST azonosítóval összerendelni, pl:**

BM rendelet				NIST
3.3.10.10.	A munkaszakasz zárolása	3.3.10.10.1. Az érintett szervezet: 3.3.10.10.1.1. meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést; 3.3.10.10.1.2. megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.		AC-11

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Ibtv. Megfelelés kontroll szinten-II

- **Második lépésben a NIST kód alapján az audit dokumentumokban megkeresni az adott kontrollt:**

NIST		
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

- ***Harmadik lépésben a kontrollal kapcsolatos előírás értékelése következik megfelel, vagy nem felel meg lehetőség szinten: IGEN!***
- **Negyedik lépésben, az adott kontroll kialakítását szükséges előírni a biztonsági rendszertervben.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Ibtv. Megfelelés kontroll szinten-III.

- Ötödik lépésben az Azure-ban az adott rendszere az érvényesítő paramétereket hangolni szükséges, azaz az alapbeállításokat kontrollonként végig kell gondolni, és a hangolást elvégezni.
- Az előíró jellegű lépések a forráshelyről pl. excel exportot alkalmazva úgy végezhetők el könnyedén, hogy egy „üres OVI” táblába az összerendelési logikát bevisszük, azaz az ovi táblát egy felhős + *„füllel”* látjuk el.
- Az adott rendszer biztonsági előírásait a kibővített „ovi” fájlban ugyanúgy lehet kezelni mint a többi kontrollt.
- Az előírt kontrollok paramétereit sem szükséges egyenként konfigurálni, mert a "M" (Mandatory), és az "O" (Optional) értékeket fileból be lehet olvasni, és az értékek benne lehetnek egy egy rendszer biztonsági leíró adatbázisában, akár az ovi táblájában is.
- A biztonságos környezet egyszerűen és gyorsan alakítható így ki, sőt a változásokra riasztás állítható be (Sentinel)

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Hol lehet a kontrollokat kialakítani?

MINDENHOL !

mert egy, egy kontroll nem szolgáltató és technologai függő!

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő egyéb kérdései

- Ki birtokolja az adatokat?
- KULCSOK KEZELÉSE!
- Késleltetés!
- Elnyomási hatás!
- Szerződési feltételek.
- A szolgáltató menedzsment és tulajdonosi szerkezet elemzése, mert sosem az semmi aminek elsőre látszik….,
- Politikai kockázat van-e? Oroszország esete!
- A Felhő és a TELKO üzemeltetői kollegái egyedi kockázatot jelentenek-e?
- … és….

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Köszönöm a megtisztelő jelenlétet és figyelmet!

https://www.hte.hu/eivok
https://www.hte.hu/esemenyek/-/esemeny/1/4876226/eivok-40--szakmai-est