Kockázatelemzés a gyakorlatban, egy Ibtv. érintett szervezetnél SeCube GRC támogató szoftverrel

Tóthmajor Máté
termékfejlszetési vezető
CISSP, CISA, CISM, PMP, ACP

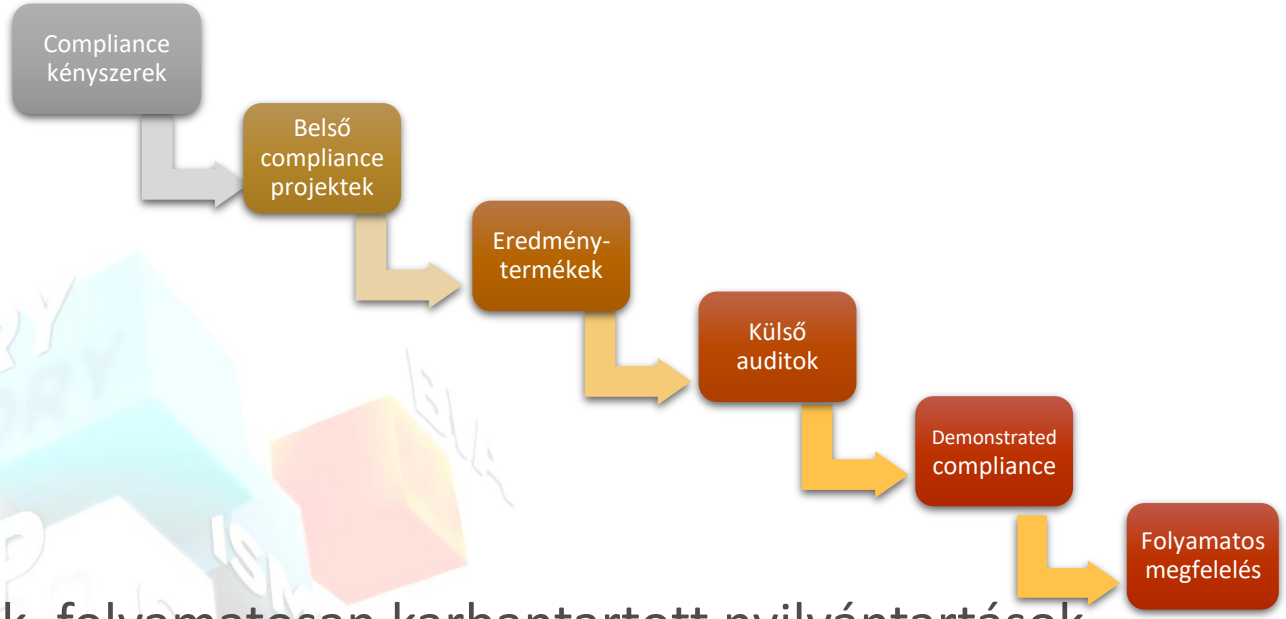
mate.tothmajor@kurt.hu

KÜRT Zrt.

KÜRT

- Információ biztonság
  - Adatvédelem cc
  - Governance Risk Compliance cc
  - Infrastruktúra menedzsment cc
  - Sérülékenység vizsgálat cc
  - SeCube GRC szoftver
  - SeConical log elemző szoftver
- Adatmentés
  - Hungary HQ
  - Germany office
  - Clean room lab class100

Növekvő Compliance nyomás



Érettség:

1. ***Projektszerű***
   Külön álló projektek, egyszeri eredmények
2. ***Integrált irányítás***
   Integrált projektek, összekapcsolt eredmények, folyamatosan karbantartott nyilvántartások, megfelelés riportok

   Nehézség: különböző eredmények konzisztens karbantartása (.xls .doc files)

   versus

   változó környezet és
   különböző felelős csoportok munkáinak **összehangolása, integrálása**
3. ***Folyamatosság, hatékonyság***
   Biztonság irányításának szoftveres támogatása -> ***GRC szoftverek***

Növekvő Compliance nyomás az információbiztonságon

- **§ IBTV, LRTV, NIS, GDPR, (MNB)**
- **Kritikus infrastruktúra - >** NIS **- > NIS2** (Network and Information Security Directive)
  - Formális jóváhagyás már folyamatban utána X + 2 éven belül kell implementálni tagállamokban
  - Szektorális (bővítés és automatikus „kijelölés") „nélkülözhetetlen" és „fontos" szervezetekre lesz érvényes, amelyek több mint 250 alkalmazottat foglalkoztatnak, és éves bevételük meghaladja a 10 millió eurót.
  - Birság: A vállalat éves bevételének 2 százaléka vagy 10 millió euró, illetve vezetői személyes felelősség.
  - Az irányelv bevezeti a **biztonsági kockázatelemzés** (bekövetkezési esetén **elhárítási tervek**) és **kiberbiztonsági belső auditokat** mint előírt rendszeres tevékenységek.
- **Pénzügyi szektor**
  - MNB 8/2020 és 11/2020 : Jelen ajánlás együttesen alkalmazandó az informatikai rendszer védelméről szóló 8/2020. (VI. 22.) MNB ajánlással, tekintettel arra, hogy ezek **együttesen** fedik le a **fizikai** és **logikai biztonsági**, valamint a **humánkockázatkezelési követelményrendszert**.
  - MNB 12/2022 a **belső védelmi vonalak** kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és **kontroll funkcióiról** szóló
    - 2023 Jan 1. hatályos. Az ajánlás átülteti az Európai Bankhatóság (a továbbiakban: EBH) 2021. július 2-án közzétett, a belső irányításról szóló iránymutatását.
  - **DORA** Digital Operational Resilience Act
    - Proposal elfogadva + 12 hónap
    - PÜ szektor és azok IT szolgáltatói - digitális működési ellenállóképesség.
    - DORA aims to ensure that all participants in the financial system have the necessary **safeguards in place to mitigate cyber-attacks and other risks**
- **Állami és köztulajdoni vállalati szektor**
  - **339/2019** és 370/2011 a köztulajdonban álló gazdasági társaságok / költségvetési szervek belső **kontroll** ~ és **integrált kockázatkezelési rendszeréről**

Biztonság irányítás integrációja

- **Egy vállalat egy biztonság irányítás**, különböző aspektusok és szakterületek
- **Integrált kockázat kezelés**
- Módszertanok, riportok, compliance folyamatok **egységesítése**

Első védelmi vonal

- a mindennapi operatív működés szintje
- a folyamatok és kockázatok menedzselése
- folyamatba épített kontrollok

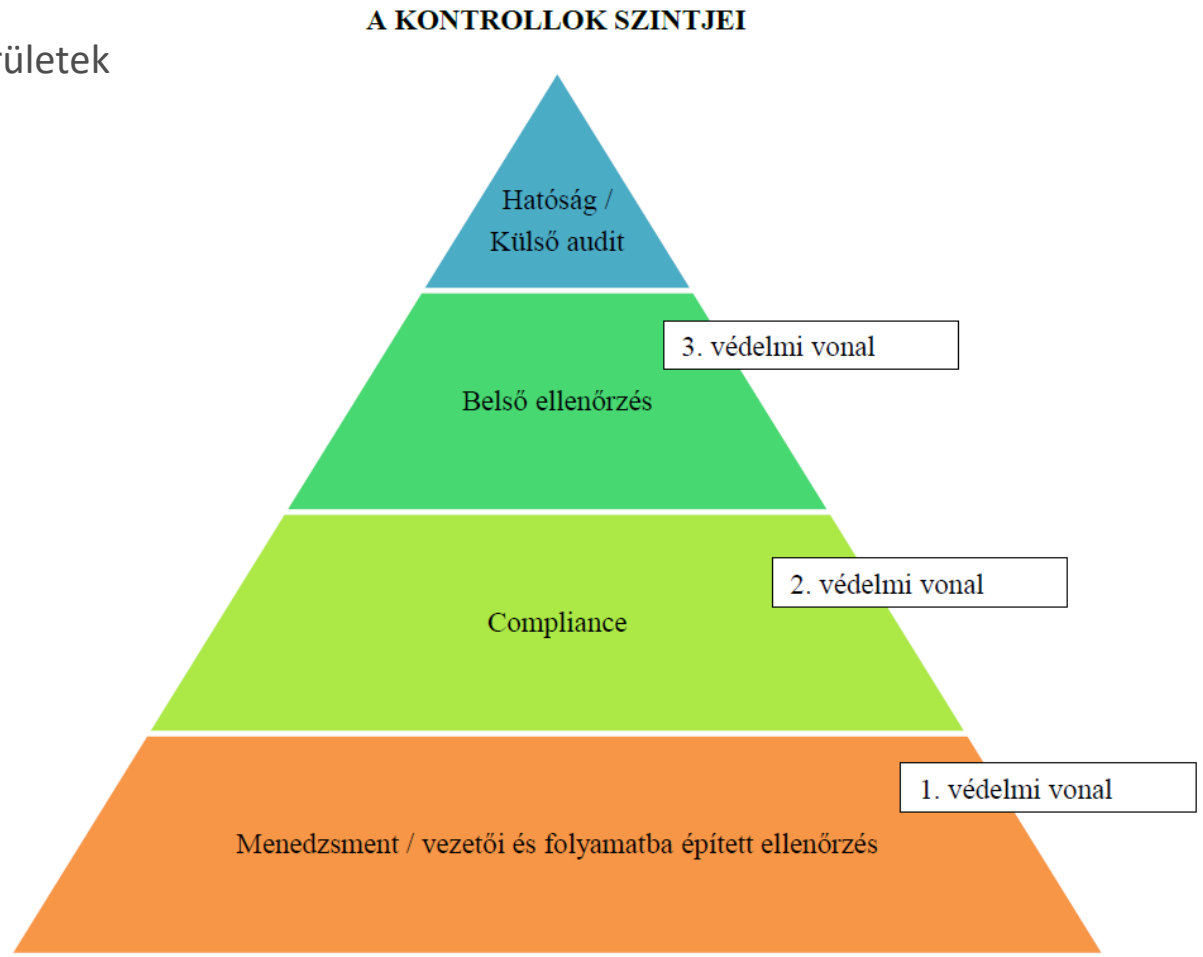
Második védelmi vonal

- szervezeti szintű kontrollok (pl. etikai kódex, belső szabályzatok)
- integrált kockázatkezelés
- megfelelés támogatás (compliance)
- biztonság
- informatika
- kontrolling
- monitoring

Harmadik védelmi vonal

Belső ellenőrzés

- bizonyosságnyújtás a belső kontrollrendszer megfelelő működéséről
- javaslatok kidolgozása a belső kontrollrendszer továbbfejlesztésére
- tanácsadó tevékenység
- független értékelés



Forrás: KÉZIKÖNYV a köztulajdonban álló gazdasági társaságok részére a belső kontrollrendszer kialakításához és működtetéséhez - 2021

Gartner®

ITRM products help security and risk management (SRM) leaders manage cyber and IT risks for these four common use cases:

- **IT Risk and Control Assessment** — Performing risk and control assessments across an organization's IT systems
- **Regulatory, Industry and Policy Compliance** — Managing the compliance of IT systems with regulatory and industry frameworks and standards
- **Cyber Risk Management** — Performing oversight of the cybersecurity function
- **Integrated into Enterprise Risk Management** — Leveraging risk insights to facilitate business decision making in mature **enterprise risk management (ERM) through an integrated risk management (IRM) approach** and technology

Figure 1: Magic Quadrant for IT Risk Management

Source: Gartner (September 2021)

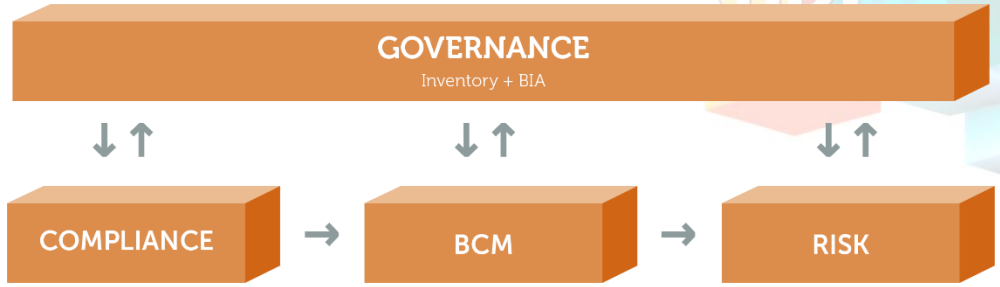
SeCube GRC – Kürt Zrt.

A **SeCube GRC** egy egységes keretrendszerben modulárisan összeilleszthető **biztonságirányítási, kockázat, compliance, audit** és **üzletmenet-folytonosság** menedzsment szoftver.

Célja egy vállalat különböző területeinek hatókörébe tartozó biztonsággal kapcsolatos elemzői, tervezői és fenntartási folyamatok integrált támogatása, ezáltal megteremtve a teljes vállalati biztonság átlátható és riportálható irányítását.

Szoftver szegmens: **GRC**, **IRM**, **ERM**, **BCM** software

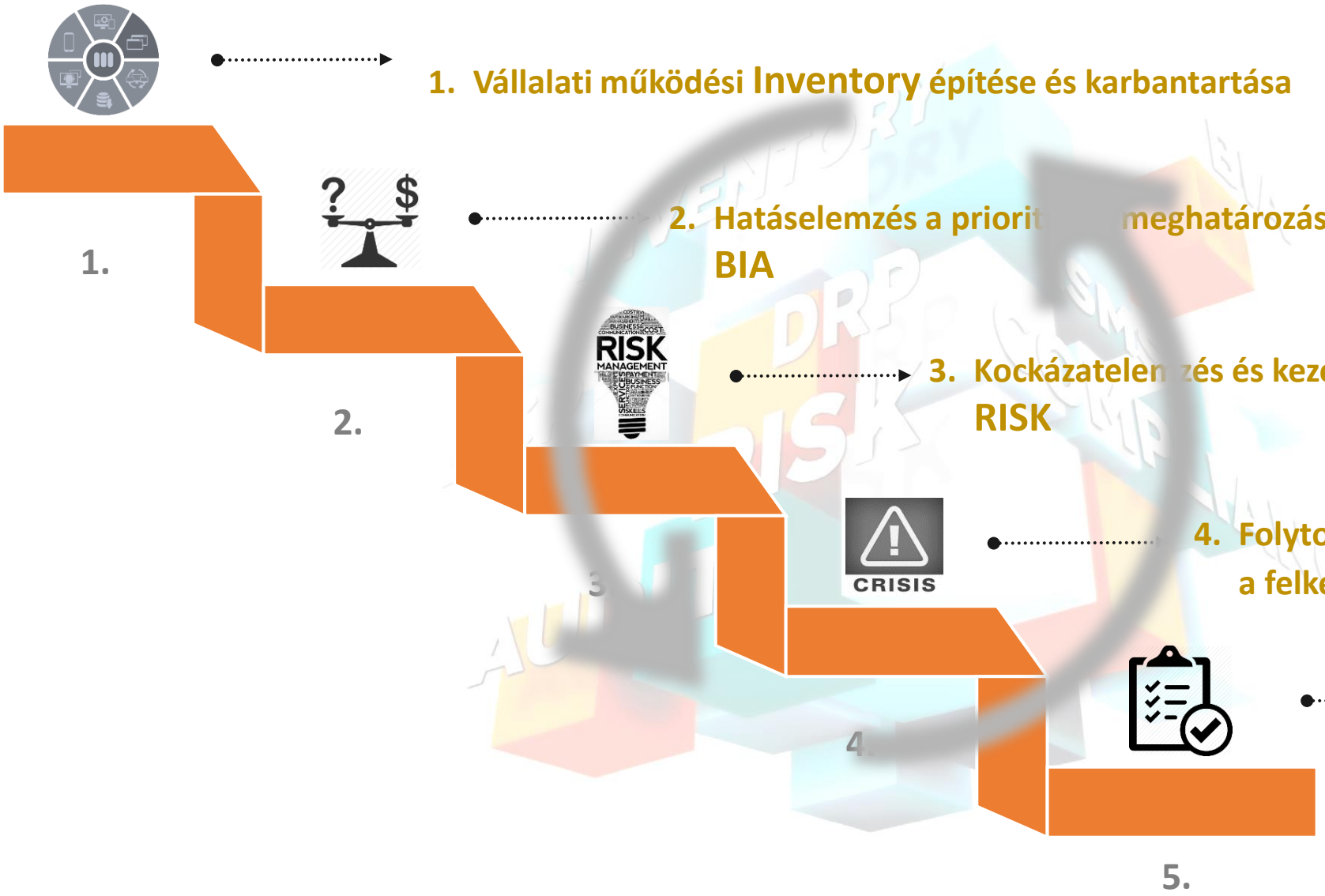
Kürt: **Szoftver** + **Knowhow** + **Terméktámogatás**



Mire nyújt megoldást a SeCube GRC?

- ✓ **Governance – Integrált biztonsági irányítási rendszer**
  ISO 27001 tanúsítás ás fenntartás - ISMS
- ✓ **Erőforrás nyilvántartás és vállalati működési modell**
  Erőforrások, szolgáltatások, adatvagyon, adatkezelési tevékenységek, üzleti folyamatok
- ✓ **RISK – Kockázatmenedzsment**
  Elemzés és kezelés (információbiztonsági, fizikai, humán, üzleti)
- ✓ **BCM - Működésfolytonosság-menedzsment**
  BCP/DRP tervezés és karbantartás
- ✓ **Compliance és Audit menedzsment**
  IBTV, LRTV, GDPR, MNB, ISO, Belső audit támogatás
- ✓ **GDPR Adatvédelem**
  Adatkezelési tevékenység nyilvántartás, DPIA, GDPR compliance vizsgálat

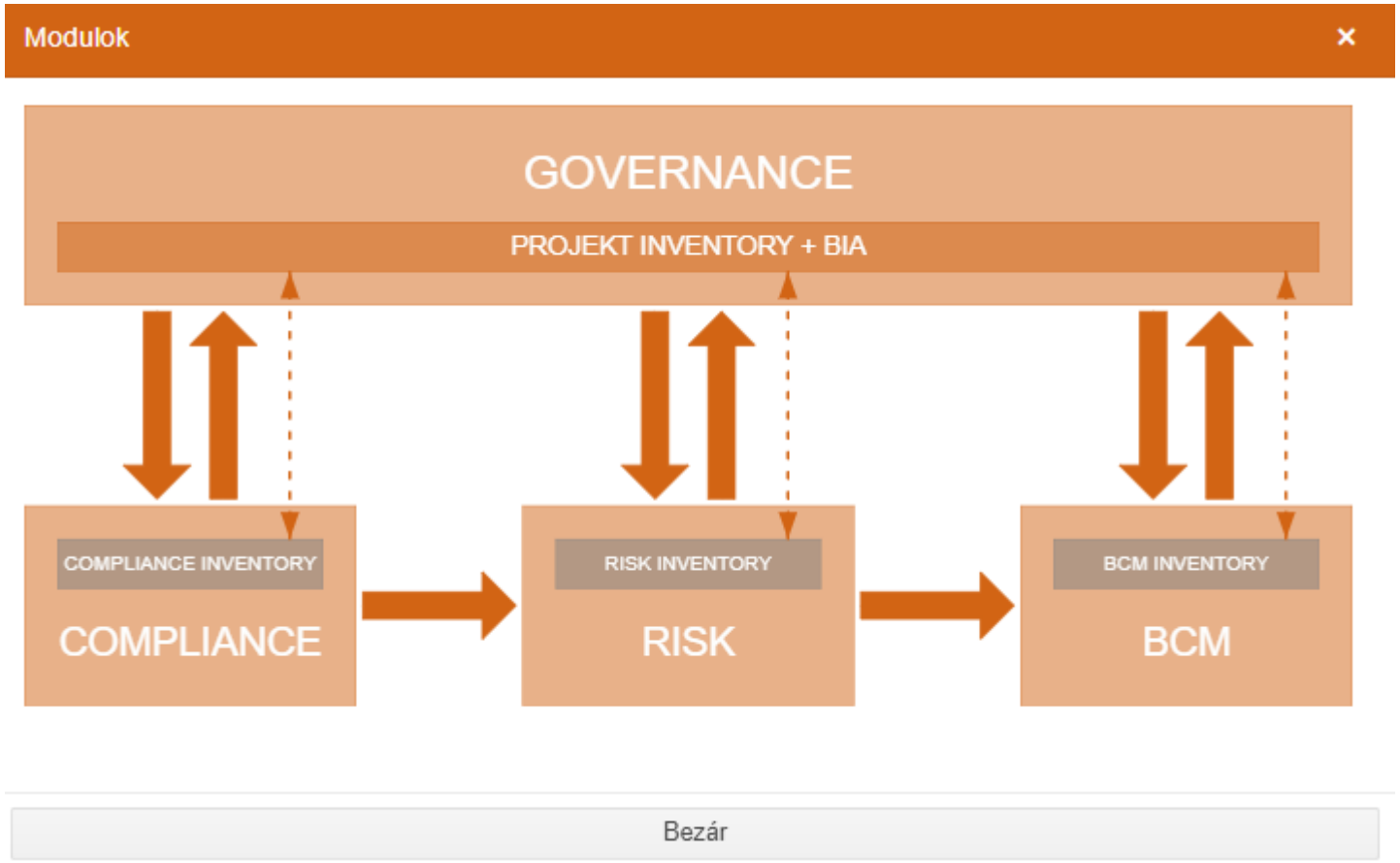
Cél: Vállati biztonság irányítás



1. Vállalati működési Inventory építése és karbantartása
2. Hatáselemzés a priorit meghatározásához, BIA
3. Kockázatelen zés és kezelés a tervszerű védelemért, RISK
4. Folytonossági és helyreállítás tervezés, a felkészültségért, BCM
5. Compliance célok Szabályzatok, audit

secube

Online bemutató



Biztonság irányítása – SeCube GRC

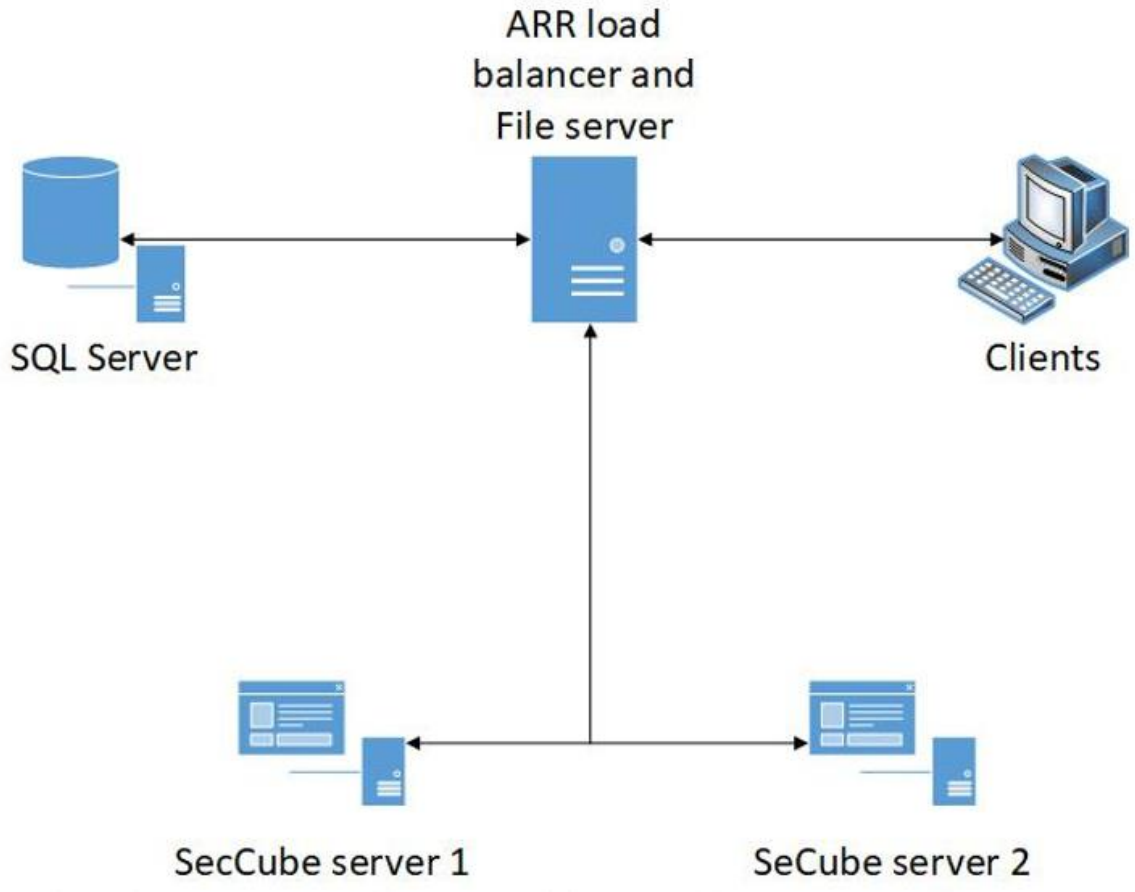
Az elérhető előnyök:

- ✓ **Közös tudásbázis** és **közös nyelv** kialakítása a szervezeten belül, integrált folyamatok és eredmények
- ✓ Validáció vizsgálatokkal ellenőrzött adatkonzisztenciák, **változások hatásainak figyelése**
- ✓ Inkompatibilis excel és word dokumentumok elhagyása, helyettük aktuális riportok generálása
- ✓ Az Excel riportokon felül átfogó szöveges Compliance, RISK jelentések, BCP és DRP tervek
- ✓ Compliance hatékony teljesítése
- ✓ Biztonsági döntések alátámasztása, „látható”, riportálható kockázatarányos védelem
- ✓ Feladatkezelés e-mailes figyelmeztetésekkel

A szakértői, illetve üzleti tudást nem helyettesítheti,
ugyanakkor kiterjesztheti azt, ráfordítást takaríthat meg és megteremtheti az átlátható kockázatarányos védelem integrált irányítását és fenntartását

SeCube GRC technikai információk

- MS SQL + MS IIS + (load balance) + webes böngészők kliens oldalon
- **MS AD integráció**
  - Authentikáció
  - User szinkronizáció
  - Jogosultsági szerepkörök AD csoportok alapján
- **Szerepkör alapú jogosultság kezelés**
  - Szabadon kialakítható szerepkörök – funkció mátrix alapján
  - Felelősség alapú jogosultság kezelés – funkción belül
- **Két faktoros** authentikáció (client cert)
- Rendszer sys logok + user művelet audit logok (felületen visszaállítható user tranzakciók)
- **Multitenantos** alkalmazás (több vállalat / projekt)
- **Email értesítők**
- **ETL** Extract Transfer Load import integráció (ütemezhető)



SeCube GRC termék információk

- On premise (örök) licenc vagy Kürt cloud service
- Licenc konfiguráció:
  - Függetlenül licenszelhető modulok - egységes keretrendszerben
  - Enabled userek
  - Projekt / vállalat tenantok
- Use case-k **integrált** támogatása
- Végfelhasználó vagy Tanácsadó
- Terméktámogatás
- Agilis fejlesztés
  - 2 havi ügyfél release vagy kritikus hiba javítás
  - Sérülékenység vizsgálatok:
    - Belső Kürt
    - Külsős főverzió váltáskor
    - Egyes ügyfeleink

https://secube.hu/services/uses-cases/

secube	SeCube GRC alapfunkció		SeCube választható Modulok				
USE CASE	Inventory (CMDB)		Governance GOV	Governance BIA	RISK (ERM)	Compliance (Audit)	BCM (BCP&DRP)
ISMS ISO27001	Polyamat és erőforrás nyilvántartás; Vállalati működési modell; Vizuális szimulációk; Védelmi intézkedések;	Vagyonelemleltár	Feladatkezelő és email emlékeztetők; Dokumentum tár; Biztonsági kivételek nyilvántartása; Incidens nyilvántartás; Több Inventory kezelése;	Üzleti hatáselemzés; BSR osztályozás;	Információbiztonsági kockázatelemzés és kockázatkezelés; ISO27005 támogatás;	Alkalmazhatósági nyilatkozat; IBSZ és vállalati szabályozás; Belső audit és Jelentések;	Működésfolytonosság - Üzletmenet (ügymenet) folytonosság tervezése; IT helyreállítás tervezés; Időcélok (RTO, RPO, MTPD); Felkészülési cselekvések menedzsmentje; Tesztelés;
IBTV		Elektronikus információs rendszer nyilvántartás			Információbiztonsági kockázatelemzés és kockázatkezelés	BSR osztálybasorolás OVI és SZVI felmérés Cselekvési tervezés	
LRTV		Létfontosságú rendszerelem nyilvántartás			KIV kockázatelemzés és kockázatkezelés	BSR osztálybasorolás OVI és SZVI felmérés Cselekvési tervezés	
MNB megfelelés		Folyamatok, rendszerek, adatvagyon működési modellezése			Információbiztonsági, humán, fizikai kockázatelemzés és kockázatkezelés;	Belső audit támogatás, valamint MNB megfelelés (pl.:8/11/12/2020)	
BCM (ISO22301)		Folyamatok és támogató erőforrások működési modellezése					
IT DRP		Erőforrások és IT rendszerek működési modellezése					
BIA		Folyamatok és támogató erőforrások működési modellezése					
ERM - Vállalati kockázat menedzsment		Területek, folyamatok, erőforrások			Üzleti/működési kockázatelemzés és kezelés		
339/2019 és 370/2011 belső kontrollrendszer		Szervezeti felépítés, folyamatok; védelmi intézkedések;			Integrált kockázatkezelési rendszer	Kontroll környezet; Belső audit; Eltérés kezelés;	
QM ISO9001		Vállalati folyamatok			Szervezeti kockázatelemzés	Belső audit és cselekvés tervezés	
GDPR		Adatkezelési tevékenység és személyes adatkör nyilvántartás			Adatvédelmi hatáselemzés (DPIA)	GDPR megfelelés vizsgálat	
Belső audit & compliance		Szervezeti erőforrások				Belső audit és cselekvés tervezés	

GONDOLKODJ KOMPLEXEN, **CSINÁLD EGYSZERŰEN.**

Tóthmajor Máté
termékfejlesztési vezető
CISSP, CISA, CISM, ACP, PMP

mate.tothmajor@kurt.hu
www.secube.hu

secube