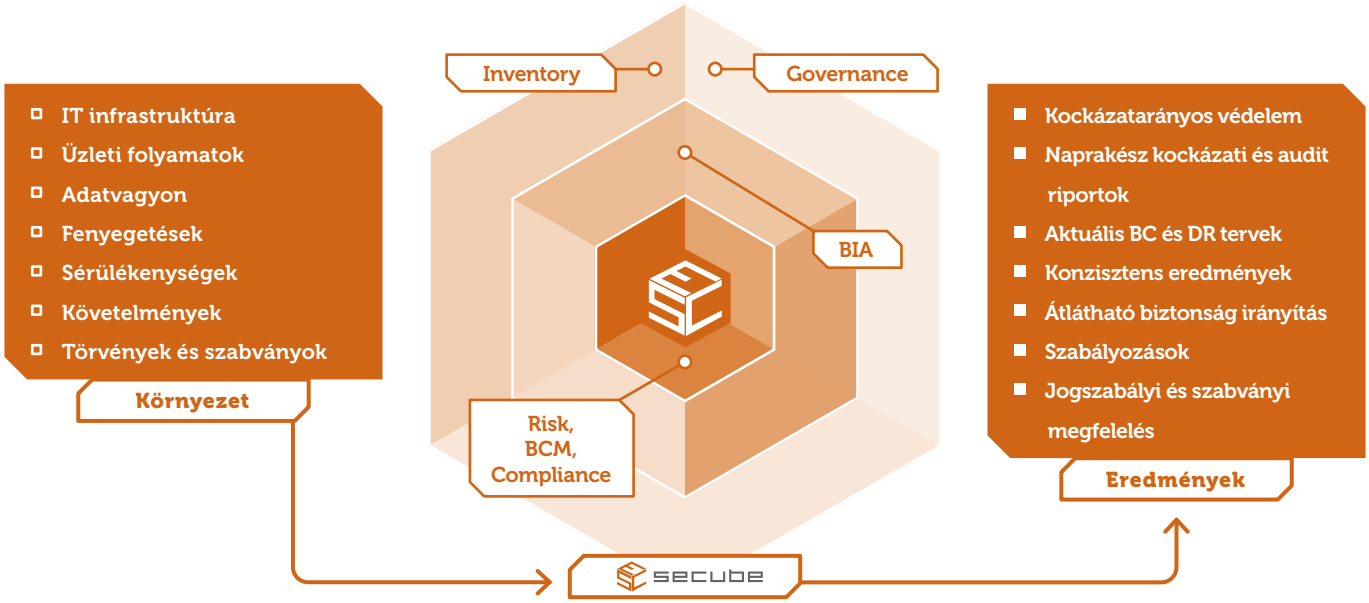
secube

GOVERN your RISK and COMPLIANCE think COMPLEX do EASY

secube@kurt.hu

www.secube.hu

KÜRT
INFORMÁCIÓMENEDZSMENT



Mi a SeCube?

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.

Kiknek készült a SeCube?

A SeCube célfelhasználói az **IT üzemeltetés**, a biztonság, az üzleti **folyamat felelősök, a belső ellenőrzés és a compliance** területek szakértői és vezetői. Egységes rendszerben képes a különböző szakmai területek akár nagy számú felhasználóinak a vállalat egészét átfogó, biztonsággal kapcsolatos tevékenységeit kezelni.

Mire nyújt megoldást a SeCube?

A SeCube GRC rendszerben **felépíthetjük vállalatunk működési modelljét** (erőforrások, rendszerek, adatok, folyamatok), **üzleti hatáselemzés** mentén értékelhetjük működésünk, **kockázatelemzések** mentén (információbiztonsági, fizikai, humán, üzleti) kezelhetjük kockázatainkat, **IT és üzletmenet-folytonosságot** tervezhetünk, valamint **belső audit** és **compliance** vizsgálatokat menedzselhetünk egységes moduláris rendszerben.

Vállalati biztonság integrált irányítása

- Kockázat, BCM és Compliance menedzsment egységes rendszerben, **kockázatarányos védelem** kialakítása és fenntartása.
- A szervezet működéséhez szükséges erőforrások, szolgáltatások, adatvagyon, üzleti folyamatok és ezek kapcsolatait leíró áttekinthető struktúra.
- **Egy vállalat egy biztonság irányítás.** Egységes és összeérő módszertanok, nyilvántartások, ezek mentén a különböző területek, folyamatok eredményeinek együttműködésének integrált támogatása, kompatibilitás és naprakész eredmények biztosítása.
- **Leszámolás az egyszeri eredmény-termékekkel.** A kockázatelemzési jelentés, a BCP, DRP, GDPR vagy a megfelelés jelentések már nem egyszeri eredmények, hanem **ráfordításhatékonyan** és könnyen karbantartható folyamatok, igény szerint generálható naprakész riportokkal.
- **Közös nyelv** megteremtése az üzleti területek és a belső szolgáltatók, mint IT és biztonság között. Kulcsemberektől való függőség csökkentése, **közös tudásbázis**.
- A korábban compliance kényszerből végrehajtott feladatok, a compliance megugráson túl, valós biztonsági irányítási **folyamatokká és auditálható eredményekké** válnak.

Használati esetek

Az önállóan is licencelhető moduláris felépítés rugalmas használati eset támogatást tesz lehetővé.

- ISMS ISO27001
- RISK – ERM
- IBTV
- LRTV
- GDPR
- MNB megfelelés 8/11/12/2020
- BIA
- BCM (ISO22301)
- IT DRP
- Audit & Compliance
- 339/2019 Belső kontrollrendszer
- ISO9001

Funkciók és modulok áttekintése

Inventory: A SeCube konfigurációs adatbázisában nyilvántartott erőforrásokat hierarchiába és kapcsolati viszonyba szervezhetjük. Az adatbázisban többek között a vállalat szervezeti felépítését, telephelyi struktúráját, technológiai és humán erőforrásait, rendszereit, szolgáltatásait, adatvagyonát, adatkezelési tevékenységeit és üzleti folyamatait rögzíthetjük, illetve ezek szerteágazó függőségi viszonyait ábrázolhatjuk, **vizualizálva vállalatunk működési modelljét**.

Governance: Az elemzési és tervezési funkciókon felül a szoftver kifejezett célja a biztonság irányítási rendszer folyamatos felügyelete és fenntartása is. Riportokkal és feladatkezelő funkciókkal támogatjuk a felelősségek és feladatok követését.

BIA - Üzleti hatáselemzés: Felméréseket készíthetünk az üzleti tevékenységek / adatok / rendszerek lehetséges sérülése mentén fellépő anyagi és immateriális kárhatásokról. A hatáselemzések alapján BSR osztályozhatjuk erőforrásainkat, illetve támogathatjuk a kockázatelemzési és üzletmenet-folytonosság tervezési feladatainkat.

RISK – Kockázatmenedzsment: A kockázatelemzés összekapcsolja vagyonelemeink sérülékenységeit és védelmi intézkedéseit a fenyegető veszélyekkel. Lehetséges bekövetkezésük esetén ok-okozati szimulációk mentén elemezhetjük a következményeket és a fellépő üzleti károkat. Egyszerre számos terület különböző típusú (**BSR információbiztonsági, humán, fizikai, üzleti, működési, ad-hoc, projekt alapú) kockázatelemzése is futhat párhuzamosan**, melyek eredményei egységesen is kezelhetők, ezáltal megvalósítva és támogatva az **integrált teljes vállalati kockázatmenedzsmentet** (**ERM** – Enterprise Risk Management). Folyamatos kockázatkezelési és jelentés készítő funkciók támogatják a vállalat kockázatarányos védelmének folyamatos irányítását.

Compliance & Audit: Rendszeres megfelelés és audit vizsgálatokat hajthatunk végre számos előre definiált **nemzetközi szabvány, biztonsági ajánlás és jogszabály** szerint, ugyanakkor tetszőleges audit/követelmény jegyzékeket is (pl. biztonsági szabályzatok, anyavállalati elvárások, belső audit követelmények) összeállíthatunk. A különböző megfelelés/audit vizsgálatokat akár párhuzamosan is kezelhetjük, a hiányosságokat pedig integrált cselekvési tervekkel kezelhetjük, részletes, akár időgép szerű riportolási és jelentés generálási lehetőségekkel.

A Létfontosságú infrastruktúra és az Információbiztonsági törvénynek (Ibtv) való megfelelés támogatása, osztályba sorolási megfelelés felmérési, kockázatelemzési és cselekvési tervezési funkciókkal akár százas nagyságrendű rendszer számmal, folyamatos karbantartás segítése és a **Hatósági (NKI, OKF) exportok** előállítása.

BCM - üzletmenet-folytonosság és IT helyreállítás menedzsment: A BCM modul képes egységes módon kezelni mind az üzletmenet-folytonosság, mind a technológiai helyreállítás tervezést, közös visszaállítási időcélok (RTO, MTPD, RPO) mentén. **Az üzletmenet-folytonosság tervezés (BCP)** során az üzleti folyamatokat támogató erőforrások (legyen az technológia, humán, létesítmény stb.) kiesésére definiálhatunk helyettesítő és megkerülő megoldásokat. **A helyreállítás (DRP)** és **szolgáltatásfolytonosság (SCM)** tervezés során a technológia erőforrások, rendszerek, szolgáltatások részletes helyreállítási és áthidalási tervezését hajthatjuk végre. Tervezőasztal szerű funkciókkal támogatott és rugalmasan kialakítható **szcenárió és terv rendszer** hozható létre, melyek folyamatos aktualitását felkészülési időszakban **változáskövetési, felülvizsgálati és tesztelési funkciók** biztosítják, word formátumban exportálható részletes tervekkel és teszt jegyzőkönyvekkel. Vészhelyzet esetén szimuláció vizsgálatok segítik a tervek helyes alkalmazását.

GDPR: Az adatvédelemre fokuszáló funkciók támogatják az adatkezelési tevékenységek, személyes adatkörök, incidensek nyilvántartását, adatvédelmi compliance vizsgálatok és kockázatelemzések (dpia) végrehajtását.

SeCube GRC keretrendszer kiemelt képességei

- **Multitenant:** SeCube keretrendszerben számos tanant/projekt indítható, mint önálló vállalatok (pl. leány vagy tag vállalatok).
- A tenantokban **önállóan is működni képes** funkcionális **modulok** indíthatók az aktuális felhasználási igényeknek megfelelően.
- Kiterjedt **validációs és konzisztencia vizsgálatok** üzleti logikák mentén, az adatok helyességének és naprakészségének érdekében.
- **Multiuser: Szerepkör, feladat és felelősség alapú jogosultság kezelés.** Kiosztható felmérési és eredmény karbantartási **feladatok**, email értesítőkkel.
- **Vizuális incidens szimulációs** képességek, érzékeny és egyedi hibapontok (SPoF) feltérképezése, fenyegetések rendszerelemek közötti terjedésének, következményeinek, üzleti hatásainak elemzése.
- Nemzetközi ajánlásokon alapuló és folyamatosan frissülő know how (fenyegetés, védelmi intézkedések, sérülékenységek stb.)
- **Valós testreszabhatóság, rugalmasság:** Akár mező szinten testre szabható nyilvántartások és paraméterezhető módszertani beállítások teszik lehetővé **meglévő vállalati gyakorlatokhoz, előírásokhoz való alkalmazkodást.**

SeCube bevezetés

A SeCube rendszer fejlesztője Magyarország egyik vezető információbiztonsági vállalata, a KÜRT Zrt. A széles portfólióval rendelkező, évtizedekre visszanyúló stabil vállalati háttér garanciát jelent a szoftvertámogatás és -követés szolgáltatások folytonos és magas szakmai minőségű fenntartására.

Mivel a **modulok önállóan is működni képesek**, ezért a részleges, egyes célterületekre, használati esetekre koncentráló licenc használat is támogatott.

A szoftver bevezetést a KÜRT Zrt. illetve kiterjedt SeCube Partneri hálózata végzi.

Használati mód

- On premise licenc, örök (lejárati idő nélkül)
- On premise licenc, bérlet
- Kürt Cloud szolgáltatás

Bevezetés, komplexitás sorrendben

1. Gyakorlati oktatások
2. Ősfeltöltés, kulcsrakész átadás
3. Kapcsolódó szakmai projekt (risk, compliance, bcm) végrehajtása

Gyártói terméktámogatás

A szoftverhez aktív gyártói terméktámogatás is tartozik (szupport, fejlesztési igény kezelés, frissítések, jogszabály és szabványkövetés, SeCube Store hozzáférés, oktató videók, webinárok), az első év mindig része a bevezetésnek.

Technikai részletek

- Magyar és Angol nyelvű
- **Multitenant keretrendszer**, több tag-leány vállalat támogatása
- MS IIS + SQL, több node-os load balancolható webes architektúra
- Szerepkör és felelősség alapú jogosultságkezelés
- Tranzakció szintű alkalmazás naplózás, visszaállítási funkciókkal
- Active Directory integráció, SSO, kétfaktoros authentikáció
- CMDB és Email integráció
- MS Excel addin interface (import/export)

Lépjen kapcsolatba velünk vagy Partnereinkkel:
www.secube.hu secube@kurt.hu