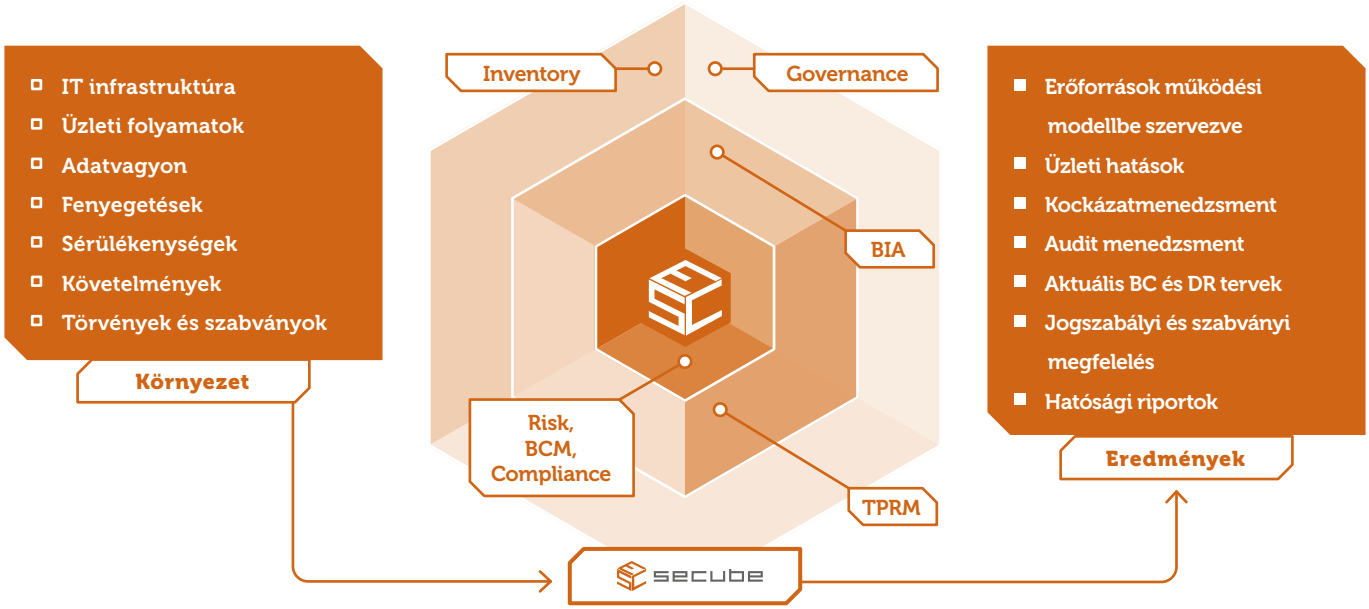
secube GRC

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, működési kockázat, third-party 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 vállalati biztonság, az üzleti folyamat felelősök, a belső ellenőrzés** és a **biztonsági 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, IKT szolgáltatások, adatok, folyamatok), **üzleti hatáselemzés** mentén értékelhetjük működésünket, **kockázatelemzések** mentén (információbiztonsági, third-party, fizikai, humán, üzleti) kezelhetjük kockázatainkat, **IT és üzletmenet-folytonosságot** tervezhetünk, valamint **belső audit** és **compliance** vizsgálatokat menedzselhetünk egységes moduláris rendszerben, megfelelve szabványi és jogszabályi előírásoknak.

Vállalati biztonság integrált irányítása

Kockázat, BCM, TPRM és Compliance menedzsment egységes rendszerben, kockázatarányos védelem kialakítása és fenntartása.

A szervezet működéséhez szükséges erőforrások, IKT szolgáltatások, adatvagyon, GDPR adatkezelések, üzleti folyamatok és ezek kapcsolatait leíró áttekinthető vállalati működési modell.

Egy vállalat egy integrált biztonság irányítás. Egységes és összeérő módszertanok, nyilvántartások, ezek mentén a **különböző szakmai területek,** folyamatok eredményeinek **együttműködésének integrált támogatása,** kompatibilitás, összeérő és **naprakész eredmények** biztosítása.

Közös nyelv megteremtése az üzleti területek az IT és a biztonsági területek között. Kulcsemberektől való függőség csökkentése, közös biztonságirányítási tudásbázis.

Leszámolás az egyszeri projekt alapú eredmény termékekkel. A működési vagy thid-party kockázatelemzési jelentések, a NIS2 vagy egyéb szabványi megfelelés jelentések vagy a BCM tervek már nem egyszeri eredmények, hanem ráfordításhatékonyan és könnyen karbantartható folyamatok, igény szerint generálható naprakész riportokkal.

A korábban **compliance** kényszerből végrehajtott projekt szerű feladatok, a compliance megugráson túl, **valós biztonsági irányítási folyamatokká** és auditálható eredményekké **válnak.**

Kiemelt használati esetek

- NIS2 – Kiberbiztonsági megfelelés
- DORA – MNB megfelelés
- CER - Kritikus szervezetek
- EU AI act
- RISK – ERM
- Third-Party Risk Management
- BIA & BCM
- IT DRP
- Audit & Compliance
- Belső kontrollrendszer
- GDPR
- ISO 27001
- Tisax

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, IKT 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 biztonsági irányítási rendszer folyamatos felügyelete és fenntartása is. Riportokkal, felülvizsgálati, incidens 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 (rendszerek, adatvagyon, folyamatok) 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, third-party, 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** (pl. NIST és ISO) **és biztonsági 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.

Hazai **kiberbiztonsági jogszabályok és Hatósági elvárások (SZTFH - kiberaudit, NKI-OVI és adatvagyon osztályozás, MNB, OKF)** kifejezett támogatása, akár százas nagyságrendű rendszer számmal. Folyamatos karbantartás és aktuális exportok támogatása. Megfelelési, kockázati és **Rendszerbiztonsági terv** riportok, cselekvési tervezéssel.

BCM - üzletmenet-folytonosság és IT helyreállítás menedzsment A BCM modul képes egységes módon kezelni mind az üzletmenet-folytonosság (BCP), mind az **IT és technológiai helyreállítás tervezést (DRP),** közös visszaállítási időcélok (RTO, MTPD, RPO) mentén. Tervezőasztal szerű funkciókkal támogatott, rugalmasan kialakítható **szcenáriók és tervek** rendszere hozható létre, melyek folyamatos **aktualitásának fenntartását, felülvizsgálatát és tesztelését** támogatja a rendszer auditálható módon.

Third-Party Risk Management (TPRM) A **vendorok** és az általuk nyújtott **szolgáltatásokat** értékelhetjük biztonsági szempontok alapján kérdőíves és hozzá kapcsolható kockázatelemzési folyamatok mentén. Menedzselhetjük a **szállítók** ciklikus és **automatikus kérdőíves biztonsági felmérését,** e-mail értesítőkkel, az eredmények ellenőrzési feladatait, a szükséges mitigációs feladatok meghozatalát és követését, és a szállítói **kockázatok kezelését.** Egyszerre **több különböző fajta felmérés** is támogatott (before live, active ICT service, end-of-service, cybersecurity, legal, etc.).

GDPR és Adatvédelem Az adatvédelemre fokuszáló funkciók támogatjuk a GDPR adatkezelési tevékenységek, személyes adatkörök, **minősített adatok (161/2010 rendelet),** incidensek nyilvántartását, valamint adatvédelmi compliance vizsgálatok végrehajtását.

SeCube GRC keretrendszer kiemelt képességei

Multitenant: SeCube keretrendszerben számos tenant/projekt indítható, mint önálló vállalatok (pl. leány vagy tag vállalatok), ezáltal akár több célra is használhatjuk a funkció modulokat, vagy több vállalatot is menedzselhetünk egy termékben.

Kiterjedt **validációs és konzisztencia vizsgálatok** üzleti logikák mentén, az adatok helyességének és naprakészségének érdekében.

Szerepkör és felelősség alapú jogosultság kezelés. Egyedi szerepkörök is létrehozhatóak. Testreszabható értesítő e-mail sablonokkal.

Integráció meglévő forrás rendszerekkel (pl. CMDB, AD) beolvasó interface funkciókkal. Kiterjedt export/import képességek (MS Excel addin) és kétfaktoros authentikáció lehetősége.

Vizuális incidens szimulációs képességek, érzékeny és egyedi hibapontok (SPoF) feltérképezése, fenyegetések rendszerelemek közötti terjedésének, következményeinek, üzleti hatásainak elemzése.

Valós testreszabhatóság, rugalmasság: Akár mező szinten testre szabható nyilvántartások és paraméterezhető módszertani beállítások teszik lehetővé **meglévő vállalati gyakorlatokhoz, előírásokhoz való alkalmazkodást.**

SeCube GRC bevezetés

A SeCube GRC 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 hosszútávú, 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. Ennek része lehet teljes ősfeltöltés és szakértői projektek végrehajtása, **kulcsrakész használatra átadással.**

Biztonságos használati mód

- Kürt Zrt. biztonságos SaaS szolgáltatás
- On-Premise licensz, ügyfél által üzemeltetve, opcionális támogatással

Főbb licensz paraméterek

- Tenantok és jogi entitások száma
- Userek száma
- Modulok:
  - Governance
  - RISK
  - Compliance
  - BCM
  - TPRM
  - ETL interface

Gyártói terméktámogatás

A szoftverhez aktív gyártói terméktámogatás is tartozik (szupport, fejlesztési igény kezelés, folyamatos funkció frissítések, jogszabály és szabványkövetés garanciával, SeCube Store hozzáférés, **oktató videók,** webinarok). A szoftver és támogató anyagok nyelve (integrált helpbook) angol és magyar.

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