GRC systém – řízení firmy už nemůže být jednodušší

Marian Němec I IT Security Consultant, AEC a.s.

Fakt, že správné informace jsou základem úspěšného byznysu, nelze zpochybnit. Informace chtějí všichni, a strategickou výhodou tak je schopnost získat informace ve správný okamžik. To samozřejmě platí nejen pro ekonomická a obchodní data, ale i pro informace potřebné k řízení provozu organizace. Informační systémy pro řešení problematiky GRC (Governance, Risk and Compliance) jsou právě k tomu určené.

Co je vlastně GRC?

Všichni známe mnoho různých typů systémů CRM, ERP, DMS, proto mnohé při pohledu na název GRC napadne, že je to jen jeden z dalších systémů. Takové zjednodušení však není úplně správné, zejména proto, že princip GRC je odlišný. Ono anglické Governance, Risk and Compliance ve své nejhlubší podstatě znamená přesně to, co znamená doslovný překlad těchto termínů: vládnutí, rizika a soulad. Tedy tři základní pilíře, které ve vzájemné provázanosti pomáhají managementu získat přehled nad tím, jak se jejich organizaci daří plnit cíle, které si stanovila.

Governance představuje celkový přístup k řízení organizace, který má manažerům a odpovědným osobám pomoci řídit a kontrolovat celou společnost. Hlavním cílem je umožnit vytvářet, získávat a předávat informace nezbytné pro efektivní rozhodování. Procesy a postupy k tomu určené jsou navázány na kontrolní mechanismy, které přispívají k celkové efektivitě předávání informací, a tím k efektivnějšímu řízení organizace.

Použitý termín Risk zase prezentuje komplexní systém řízení rizik organizace. Rizika na každou organizaci působí z různých stran. Může jít o právní rizika plynoucí ze smluvních záležitostí, ale také legislativní rizika, obchodní rizika, ekonomická, kybernetická a mnohá další. V GRC termín Risk vyjadřuje procesy a činnosti, které rizika identifikují, analyzují, pomáhají je řídit a evidovat, v neposlední řadě pomáhají k jejich případné eliminaci.

Compliance pak představuje způsob ověřování, že organizace plní všechny na ni kladené požadavky, jak externí (smlouvy, zákony, standardy), tak interní (směrnice, nařízení atd.). V rámci Compliance – shody se hodnotí stav dodržování definovaných požadavků, rizika a náklady vznikající jejich nedodržováním, ale také předpokládané náklady na zajištění plné shody s definovanými požadavky. To pomáhá stanovit priority kroků vedoucích ke splnění shody.

GRC lze proto považovat za metodu, která si klade za cíl synchronizovat informace a aktivity napříč organizací tak, aby fungovala s vyšší efektivitou. Specializované informační systémy pro GRC pak umožňují efektivní a včasné sdílení informací a kontrolování jednotlivých činností.

Má GRC reálný přínos?

Takto položená otázka nevystihuje správný stav věci. Jakýkoliv informační systém má jen takový přínos, nakolik správně je využíván. Pokud máte například sofistikovaný ERP informační systém, ve kterém však máte pouze inventurní evidenci majetku, tak mrháte potenciálem systému i vynaloženými zdroji. Přínos takového systému je v poměru k nákladům na pořízení a provoz minimální. V případě GRC je správná implementace stejně náročná.

GRC systémy jsou rovněž závislé na datech v nich ukládaných, na rozsahu a způsobu realizovaných činností a v neposlední řadě na integraci do struktury organizace. Jeho největší síla se ukáže v okamžiku, kdy je využíván komplexně, optimálně v celé organizaci. Jsou určeny odpovědnosti, definovány a naplánovány procesy, které se mají v systému realizovat. V neposlední řadě jsou důležití vlastní uživatelé systému. V takovém případě se GRC stává mocným nástrojem, který managementu společnosti na všech úrovních poskytuje relevantní informace.

Skvělým příkladem vhodného použití GRC je, pokud organizace vlastní certifikaci podle některého z ISO standardů nebo musí plnit povinnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Tento zákon vyžaduje po povinných subjektech provádění velkého množství činností, které se dotýkají různých částí organizace. Musejí být delegovány odpovědnosti a úkoly na jednotlivé zaměstnance a z těchto činností se musejí vytvářet záznamy. Velmi důležitým prvkem je zpracování analýz rizik, vedení evidence aktiv a dalších

souvisejících činností. To vše představuje pracovní, časovou i ekonomickou zátěž, jejíž velikost je závislá na velikosti organizace. Bez GRC se tyto činnosti provádějí často s využitím nástrojů jako excel, word apod., tedy v podstatě manuálně. I když to logicky neznamená, že by kvalita výstupů z analýzy rizik byla nižší, jejich další používání je mnohem složitější. Hlavní přínos informačního systému GRC je v takovém případě primárně v tom, že všechny potřebné informace a data jsou v jednom místě, snadno dostupná, jsou na ně navázány činnosti, lidé, úkoly a další. Systém pak dokáže sledovat stav plnění jednotlivých úkolů, zpracovávat a předávat informace ihned po vložení do systému a poskytovat relevantní podklady k manažerským rozhodnutím.

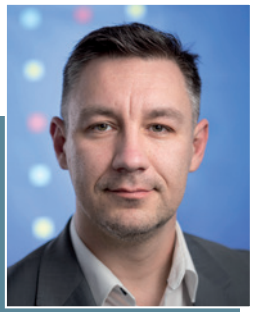
Další výhodou informačního systému GRC je možnost některé činnosti rychle a snadno opakovat. Pro kybernetickou bezpečnost je to třeba při realizaci opakovaných analýz rizik, auditů, hodnocení a dalších. Je tak možné sledovat změny a vývoj v čase. To vše víceméně téměř v reálném čase. Na každý výstup lze navázat další činnosti. Provázanost jednotlivých procesů a informací je tím silným argumentem, proč investovat čas a finanční prostředky do zakoupení GRC řešení.

Jak na to, když chci GRC?

Může se zdát, že zprovoznit GRC je věc poměrně snadná, ale spíše opak je pravdou. V první řadě je třeba si uvědomit, že to není řešení typu „nainstaluj a používej“. Stejně tak není kouzelný dodavatel, který přijde, nainstaluje, nastaví procesy a klient zázračně získá informace a fungující systém, aniž by musel cokoli udělat. Implementace GRC řešení se nikdy neobejde bez aktivního zapojení organizace samotné. Management si musí v prvé řadě uvědomit, které informace chce v GRC zpracovávat a jakým způsobem. To samozřejmě není snadné, už jen proto, že firma často nedisponuje potřebným know-how. Proto je prakticky nezbytné využít implementačního partnera, který má dostatečné zkušenosti se zaváděním GRC do firemního prostředí. Jeho odborný nadhled pomůže identifikovat klíčové procesy a informace, ty nadbytečné naopak vyřadit. To umožní vyhnout se problémům, které nesprávně provedená implementace GRC přináší. Ve výsledku jsou tak uspořeny významné finanční prostředky, které by byly nesprávnou implementací ztraceny.

Přes všechna rizika je GRC nástrojem, který je velmi účinný. Jeho plnohodnotné používání šetří čas i náklady, které jsou spojeny s procesy, jež dobře fungující organizace stejně musí provádět. Jedinou otázkou pak zůstává, jestli je chce realizovat tak, že zatěžuje zaměstnance dalšími úkoly, které jsou časově náročné a složité, takže se neobejdou bez asistence odborných pracovníků, nebo rychlým a efektivním způsobem, kdy se většina požadovaných úkonů provádí rychle a s minimálním vytížením zaměstnanců i odborných pracovníků. A takto získaná data jsou managementu dostupná téměř okamžitě, což přináší další úspory plynoucí ze správných rozhodnutí ve správném čase.

GRC je výborný sluha, který může být každé organizaci přínosem. Stejně tak ale může být velmi špatným pánem, zejména pokud se do něj vkládají nesprávná data nebo se používá nekoncepčně. Doporučení implementovat informační systém GRC pro potřeby organizace je přesto jednoznačně správné. Chybou by bylo podcenit rozsah a způsob implementace, zejména rozhodnutí nevyužít zkušeného implementátora.



Marian Němec

Marian Němec se v oblasti informačních technologií pohybuje celý svůj profesní život. Problematiku bezpečnosti IT začal řešit již v 90. letech minulého století z pozice informatika na městském úřadu. Později se podílel na vzniku Certifikační autority Czechia, aby se následně přes PKI systémy dostal k dalším bezpečnostním technologiím. Procesní bezpečnosti se pak věnuje od roku 2008. Podílel na mnoha projektech v oblasti implementace ISO27001 a systému ochrany osobních údajů, zejména ve veřejném sektoru. Ve volném čase se věnuje hlavně tréninku a výuce sebeobrany.