(Ne)lehká cesta k GRC…

Petr Nádeníček I Senior IT Security Consultant

GRC aktuálně patří k často diskutovaným tématům na pomezí řízení organizace a jejího IT (Governance), identifikace a řízení rizik (Risk) a zajištění souladu (Compliance). Pokud uvažujete o implementaci GRC ve své organizaci, možná vám přijde vhod pár tipů, na co si dát pozor.

Různé GRC nástroje (resp. SW) si stále častěji nacházejí cestu do všech typů organizací. Důvodem jejich nákupu a implementace často není ani tak snaha o další zlepšení systému řízení, ale (bohužel) spíše různé externí tlaky, jako např. potřeba splnění požadavků zákona o kybernetické bezpečnosti (181/2014 Sb. a souvisejících vyhlášek) nebo jiných regulativních požadavků, kterým konkrétní organizace podléhá. Je třeba podotknout, že jich neustále přibývá. Další požadavky můžeme čekat třeba v souvislosti s právě přicházející evropskou GDPR regulací. Nejde však jen o splnění regulativ. Osvícenější organizace již samy poznaly, že GRC nástroje dokáží automatizací některých procesů ušetřit nemálo času, a tedy i prostředků na jejich naplňování.

Těžká volba

Již samotný výběr řešení vhodného pro danou organizaci nebývá snadný. Je totiž třeba vzít v potaz řadu kritérií. Paradoxně, čím je organizace vyspělejší co do maturity svých GRC procesů, tím složitější a náročnější výběr je.

Teoreticky nejsnadnější se jeví implementace GRC takříkajíc „na zelené louce“, tzn. v organizaci, která dosud nenavrhla a nezavedla žádné vlastní procesy, tudíž může tyto procesy převzít z některého GRC řešení. Čím více vlastních procesů již organizace zavedla, tím důkladněji musí hledat řešení, které jí bude vyhovovat, a tím více bude muset investovat do jeho přizpůsobení (customizace).

Při výběru vhodného řešení je tedy většinou třeba zvážit celou řadu kritérií, počínaje celkovými náklady na jeho zakoupení, implementaci a provoz, přes technická hlediska až po specifické požadavky organizace, jako je např. soulad s vybranými standardy a metodikami. Pokud organizace bere výběr GRC řešení vážně, není neobvyklé, že výběr zabere minimálně půl roku i více. Určitě není na škodu již v této fázi provést důkladnou analýzu stávajících GRC procesů a její výstupy, kromě samotné implementace, využít i pro definici výběrových kritérií.

GRC je disciplína, která si klade za cíl synchronizovat informace a aktivity napříč oblastmi Governance, Risk a Compliance organizace. Cílem GRC je dosáhnout efektivního sdílení informací, efektivního provádění činností a omezení nehospodárného plýtvání zdroji. I když rozsah a smysl GRC může být v různých organizacích odlišný, typicky zahrnuje činnosti, jako jsou řídicí procesy (IT procesy, security procesy, business procesy), řízení podnikatelských rizik (ERM, bezpečnostní rizika, dodavatelská rizika) a zajištění souladu s relevantními zákony a předpisy.

Méně někdy znamená více

Jednou z prvních otázek, kterou si musíme položit již před tím, než začneme s výběrem konkrétního GRC řešení, je, jaký rozsah procesů a činností chceme implementovat. Můžeme se např. zaměřit pouze na proces analýzy rizik nebo můžeme např. zkusit pokrýt celé ISMS.

Pro úspěch implementačního projektu je nutné nevybírat příliš velký rozsah. Čím větší rozsah, tím je větší pravděpodobnost, že některou část nebo celou implementaci GRC nezvládneme. Nejčastější příčinou bývá kromě řady dalších faktorů jednoduše podcenění složitosti a náročnosti projektu.

Na druhou stranu, pokud vybereme příliš malý rozsah, může se stát, že i úspěšnou implementaci

v organizaci takříkajíc neobhájíme. Můžeme se např. dostat do situace, kdy vedení organizace nebude vnímat benefity řešení, bude jej považovat za málo efektivní apod.

Z vlastních zkušeností doporučuji provádět implementaci v několika navazujících fázích. V první fázi je vhodné začít s jedním, maximálně dvěma ne příliš složitými procesy. Tento přístup umožňuje pracovníkům organizace postupně se s řešením seznámit, což se vyplatí v dalších fázích, kdy už mohou přijít na řadu procesy složitější. Organizaci tento přístup přináší i větší flexibilitu, kdy je např. možné po první fázi revidovat cíle nebo i přístup k další implementaci. Může např. dojít k omezení angažmá externího dodavatele a předání implementace internímu týmu, nebo se naopak může organizace přiklonit k plnému outsourcingu další implementace a provozu řešení. To ale vždy záleží na celé řadě individuálních faktorů.

A co data?

Při implementaci GRC je nutné dobře si uvědomit i to, že implementujeme nejen procesy, ale abychom je dokázali implementovat, musíme do GRC řešení dostat i odpovídající data, se kterými dané procesy pracují. Pokud např. implementujeme procesy v oblasti IT GRC, určitě se neobejdeme bez dat o infrastruktuře (počítače, servery, síťové prvky, datová úložiště, aplikace, software…). Pokud implementujeme procesy související s managementem rizik, pravděpodobně budeme potřebovat i některá business data (procesy, informační aktiva, služby, finanční informace apod.).

Bohužel se stává, že i když organizace v dobré víře považuje svoje data za kvalitní a snadno dosažitelná, ve skutečnosti to bývá méně ideální. A dopady na projekt implementace mohou být velmi citelné. Typickým příkladem je situace, kdy se snažíte dostat do GRC řešení data z více zdrojů a na první pohled bezvýznamné chyby (jako je např. (ne)používání diakritiky v určitých položkách) znemožňují jejich vzájemné provázání nebo update. Důsledkem pak může být výrazný nárůst manuální práce s těmito daty, nebo dokonce zjištění, že jsou naprosto nepoužitelná a je nutné je přepracovat včetně dalších oblastí mimo původní rozsah implementace GRC.

Implementace dodavatelem, nebo vlastními silami?

Dalším logickým klíčovým rozhodnutím při implementaci GRC je, zda se pustíme do implementace vlastními silami, nebo společně s externím dodavatelem. Minimálně pro první fázi implementace není první varianta příliš pravděpodobná a je spíše vhodné angažovat dodavatele, který nám s implementací pomůže.

Nepočítejte ale s tím, že vám dodavatel přinese kompletní řešení, jak se říká, „na stříbrném podnose“, to snad jedině v případě, že implementace probíhá „na zelené louce“ (bylo zmíněno výše). Uvědomte si, že implementace vašich interních procesů do jakéhokoliv GRC nástroje se bez účasti interních lidí prostě neobejde, a pokud ano, skončí to s velkou pravděpodobností ne úplně dobře.

Pokud vybíráte dodavatele pro implementaci GRC, vždy se ptejte nejen na to, zda má zkušenost s konkrétním řešením/nástrojem, ale hlavně zda rozumí implementovaným procesům. Nedostanete se tak do situace, kdy vám např. bezpečnostní procesy implementuje pracovník dodavatele, který je sice zkušený analytik, ale s bezpečností nemá zkušenosti vůbec

žádné. Zejména v situaci, kdy k implementaci GRC přistupujete zároveň i jako k příležitosti pro změnu/úpravu implementovaných procesů, je přiměřená odbornost na straně dodavatele naprosto nezbytná.

Pozor na dobré nápady!

Možná to bude znít na první pohled divně, ale je to tak – příliš mnoho „dobrých" nápadů při implementaci GRC řešení může vést k velkým obtížím. Projekt implementace GRC totiž často doslova provokuje invenci zainteresovaných lidí a ti pak dokáží generovat spoustu báječných nápadů, jak by implementovaný proces mohl v GRC nástroji vypadat, jak by bylo dobré ho upravit atd. Částečně je to asi způsobeno i tím, že nástroje již v základním stavu často obsahují určité předem definované struktury procesů (např. řešení RSA Archer již v surové instalaci poskytuje spoustu tzv. „Out-of-the-Box" obsahu, ať již jde o nastavení jednotlivých procesů, workflow či vazeb mezi informacemi apod.).

Pokud těmto tendencím vedení projektu nedokáže efektivně čelit, může se stát, že se pod vlivem těchto „dobrých nápadů" budeme k některým částem GRC řešení neustále vracet, předělávat již jednou dokončené komponenty a ve výsledku se budeme dostávat do zpoždění. Nepromyšlené zásahy byť jen do malých částí GRC řešení navíc mohou mít nemalé dopady na související komponenty, což může dále zvyšovat pracnost a snižovat efektivnost celého komplexního systému.

A co podpora?

Dejme tomu, že se nám podařilo GRC řešení úspěšně implementovat, stojíme na prahu produkčního provozu řešení a zvažujeme, jakou podporu budeme pro jeho bezproblémové využívání potřebovat.

Pokud jste se s implementovaným nástrojem během implementace neskamarádili tak, že byste měli oprávněný pocit, že jej dokonale znáte a dokážete vyřešit většinu krizových situací, do kterých se při jeho provozu můžete dostat, je vhodné si alespoň nějakou externí podporu zajistit. Většinou se organizace s tímto požadavkem zcela logicky obrátí na implementátora řešení.

Rozsah zajišťované podpory by měl být úměrný kritičnosti procesů, které jsme do GRC implementovali. Pokud na nich bezprostředně závisí provoz vaší organizace, je nutná vyšší míra podpory, navíc ošetřená dostatečnými SLA. Pokud jde spíše o běžné podpůrné procesy, určitě postačí např. podpora 8×5 s přiměřenou reakční dobou pro zahájení řešení požadavku.

Celkově vzato…

A co říci závěrem? Snad jen to, že dnešní doba je pro implementaci GRC nástrojů v rámci organizací velmi příhodná. Potýkáme se totiž nejen s nutností stále větší optimalizace našich GRC procesů, ale navíc jsme vystaveni stále většímu tlaku různých regulativ (kybernetický zákon, GDPR…). A s tímto vším nám vhodný GRC nástroj může pomoci se do budoucna efektivně vypořádat. Jeho implementace sice nebývá jednoduchá, ale pokud do ní investujeme svůj čas a prostředky, vrátí se nám to především ve formě celkově efektivnějších procesů s menší celkovou časovou zátěží pro jejich realizaci. Správně implementovaný GRC nástroj nám také navíc poskytuje schopnost řídit dané procesy v reálném čase a bezprostředně reagovat, což např. v případě bezpečnosti je v dnešním světě opravdu k nezaplacení.

Ing. Petr Nádeníček

Senior IT Security Consultant, AEC a.s., absolvent Fakulty elektrotechniky a informatiky a Fakulty podnikatelské Vysokého učení technického v Brně. Od roku 2001 se věnuje informační bezpečnosti ve firmě AEC na různých pozicích, již téměř 15 let na pozici konzultanta informační bezpečnosti. Zaměřuje se především na problematiku řízení informační bezpečnosti, ISMS, GRC a související oblasti.