Používáte vhodné nástroje k budování důvěry zákazníků?

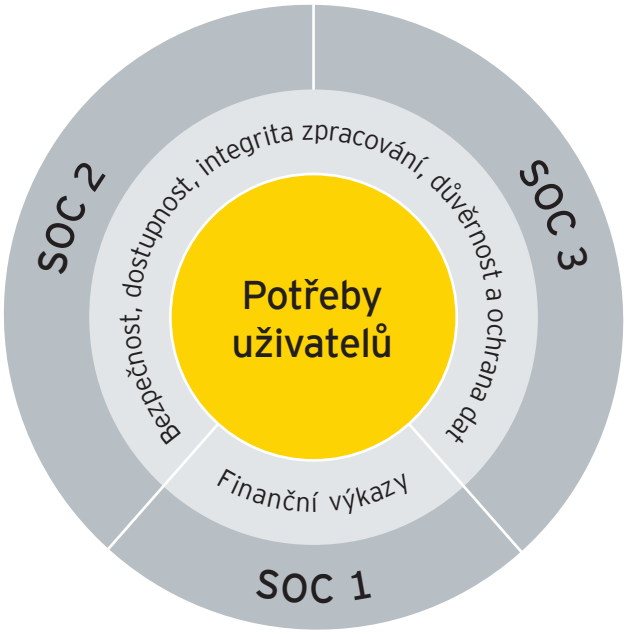
SOC 2 – Kritéria služeb vytvářejících důvěru
(Trust Services Criteria)

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

Demystifikace SOC 2

Co znamená, pokud po vás vaši klienti požaduji SOC 2 report? Jaké máte možnosti a jakou variantu SOC 2 reportu můžete zvolit? Co se skrývá za zkratkami SSAE 18, TSC nebo ISAE 3000? Tyto otázky si naši klienti často kladou v momentě, kdy začnou uvažovat o SOC 2 atestaci pro svou organizaci. Příprava na vydání SOC 2 reportu vyžaduje čas, obvykle nejméně několik měsíců. Na začátku je vhodné si stanovit, která varianta SOC 2 reportu je nejvhodnější pro vás, vaše klienty a realisticky dosažitelná pro vaši organizaci.



Typy SOC reportů

SOC 1

Poskytuje informace o kontrolách v servisní organizaci, které jsou relevantní pro finanční auditory (report má omezené použití).

SOC 2

Poskytuje informace o efektivitě kontrol, které pomáhají servisní organizaci splnit závazky na základě platných kritérií pro oblast bezpečnosti, dostupnosti, integrity zpracování, důvěrnosti nebo ochrany dat (report má omezené použití).

SOC 3

Je nadstavbou SOC 2 reportu, jen neposkytuje tolik informací jako SOC 2. Zpravidla je veřejným marketingovým dokumentem doplňujícím SOC 2 report (report lze veřejně sdílet).

Budování důvěry prostřednictvím SOC reportu

SOC reporty vedou k budování důvěry. Servisní organizace získávají důvěru splněním svých závazků, transparentností operací, řízením rizik a nezávislým auditem. Vaši klienti v mnoha případech používají SOC reporty k prokázání splnění požadavků regulatorních orgánů a orgánů dohledu.

Lepší komunikace se zainteresovanými stranami prostřednictvím SOC 2 reportu

SOC 2 reporty vám pomohou budovat důvěru zainteresovaných stran a umožní identifikovat oblasti, které je třeba zlepšit. Slouží k pochopení interních kontrol servisní organizace a souvisejících kritérii, jako je bezpečnost, dostupnost, integrita zpracování, důvěrnost a ochrana dat.

SOC 2: Kritéria služeb vytvářejících důvěru (Trust Services Criteria – TSC)

Zatímco SOC 1 reporty poskytují ujištění pouze ve vztahu k procesům významným z hlediska finančního auditu, SOC 2 reporty mohou nabídnout záruku ohledně procesů, které nesouvisí s financemi. SOC 2 reporty poskytují ujištění ve vztahu k jedné nebo několika z pěti kategorií služeb vytvářejících důvěru:

Bezpečnost	Dostupnost	Integrita zpracování	Důvěrnost	Ochrana dat
Informace a systémy jsou chráněny před neoprávněným přístupem, zveřejněním a poškozením systémů.	Informace a systémy jsou k dispozici za účelem provozu a použití.	Systémové zpracování je úplné, platné, přesné, včasné a oprávněné.	Informace označené jako důvěrné jsou chráněny.	Osobní údaje jsou řádně shromažďovány, používány, uchovávány, zveřejňovány a mazány.

Kritéria pro oblast bezpečnosti (Common Criteria) jsou základem každého SOC 2 reportu. Ostatní čtyři kategorie jsou volitelné. Nejčastěji v SOC 2 reportu vidíme kombinaci kritérií pro bezpečnost a dostupnost (Security/Common Criteria and Availability). SOC 2 report je možné vydat podle amerického standardu SSAE 18, který definovala AICPA, nebo podle mezinárodního standardu ISAE 3000. V obou případech se reportuje na základě vybraných kategorií pro kritéria služeb vytvářejících důvěru (Trust Services Criteria). Volba standardu obvykle záleží na potřebách vašich klientů.

Výhody SOC 2

SOC 2 je příležitostí k získání záruky ohledně širší škály poskytovaných služeb, než je pouhé účetní výkaznictví. K výhodám SOC 2 patří:

1. Budování konkurenční výhody a využití reportu pro odlišení na trhu
2. Pomoc klientům s aktivitami v oblasti dohledu nad dodavateli a splnění smluvních závazků
3. Zlepšení komunikace klientů a zvýšení transparentnosti externě zajišťovaných interních kontrol
4. Udržení stávajících klientů a získání nových klientů
5. Snížení nákladů, jelikož bez SOC 2 reportu může být organizace předmětem auditu ze strany auditorů různých klientů
6. Lepší řízení a kontrola rizik, kdy nezávislý tým provede hodnocení a identifikuje příležitosti ke zlepšení

Kterým servisním organizacím může SOC 2 přinést výhody?

- Poskytovatel hostingových služeb datového centra
- Poskytovatelé cloudových služeb zodpovídající za integritu zpracování, bezpečnost a dostupnost (v souladu se standardy Cloud Security Alliance)
- Poskytovatel zdravotní péče podávající hlášení ohledně dodržování předpisů [např. požadavků amerického zákona o nakládání se zdravotními informacemi (HIPAA) nebo organizace HITRUST]
- Zpracovatelé kreditních karet nebo poskytovatelé platebních služeb [podobné bezpečnostním standardům pro odvětví platebních karet (PCI DSS)]
- Uživatel externích služeb poskytovatele aplikačních služeb
- Společnosti poskytující služby Blockchain-as-a-Service (BaaS) nebo využívající k poskytování služeb zákazníkům nové technologie, jako je blockchain a umělá inteligence
- Společnosti pro ověřování informací nebo poskytovatelé služeb ověřování identity

Věděli jste, že SOC 2+ reporty mohou kombinovat více standardů?

Report typu SOC 2+ („SOC 2 Plus“) může zahrnovat výrok auditora služeb ohledně dalších oblastí, což přispívá k větší flexibilitě reportu a ke spokojenosti zákazníka. Spolu se SOC 2 reportem lze použít jiné rámce pro ověřování, jako je ISO 27001, GDPR, Cloud Controls Matrix (CCM), NIST (NIST CSF), HIPAA a HITRUST. SOC 2+ tak umožňuje využít jediný soubor testů k získání ujištění a záruk z hlediska různých standardů. Místo několika atestací a certifikací stačí jeden report.

SOC 2 report lze také přizpůsobit tak, aby vyhovoval potřebám konkrétních odvětví. Nejnovější verze reportů, jako je SOC pro dodavatelský řetězec, SOC pro kybernetickou bezpečnost a SOC pro integritu dat, přispívají k větší důvěře interních a externích zainteresovaných stran.

Přístup a metody EY v oblasti SOC 2

Stanovení očekávání	Hodnocení připravenosti na SOC 2 audit (volitelné)	Plánování SOC 2 auditu	Realizace SOC 2 auditu	Příprava a vydání SOC 2 reportu
▸ Regulatorní požadavky ▸ Vaše potřeby ▸ Potřeby vašich klientů ▸ Definice očekávání a způsobu komunikace	▸ Představení SOC 2 konceptu ve vaší organizaci ▸ Pomoc se zacílením rozsahu reportu tak, aby odpovídal vašim potřebám a potřebám klientů ▸ Série workshopů mapující připravenost vaší organizace na SOC 2 požadaky ▸ Seznam doporučení pro odstranění nedostatků a přípravu kontrolního rámce (SOC 2 kontroly)	▸ Pochopení klíčových procesů, potřeb a očekávání ▸ Stanovení rozsahu auditu ▸ Stanovení podrobných metod testování a plánu prací	▸ Posouzení systému hodnocení rizik ▸ Testování SOC 2 kontrol ▸ Kontrola výsledků společně s vedením ▸ Souhrnné informace pro výkonné vedení a výbor pro audit	▸ Formulace případných nálezů a vyhodnocení jejich dopadu na výrok auditora ▸ Příprava a vydání SOC 2 reportu k určitému datu (Type I) nebo za určité období (Type II, obvykle za 6–12 měsíců) ▸ SOC 2 report

Kontaktujte nás a zjistěte více o vaší připravenosti na SOC 2 audit. Uspořádáme pro vás nezávazný workshop.

EY | Building a better working world

Smyslem EY je přispívat k tomu, aby svět fungoval lépe. Proto pomáháme klientům, našim zaměstnancům i širšímu společenství vytvářet dlouhodobé hodnoty a posilovat důvěru v kapitálové trhy.

Týmy odborníků EY, vybavené nejmodernějšími technologiemi, působí ve více než 150 zemích celého světa – provádějí audity a poskytují klientům širokou poradenskou podporu, která jim umožňuje růst, transformovat se a efektivně fungovat.

Naši auditoři, konzultanti, právní a daňoví poradci i odborníci na strategické a transakční poradenství si kladou ty správné otázky a dokážou najít ty správné odpovědi na složité problémy dnešního světa.

O SOC reportingu v EY
Organizace EY hraje důležitou mezinárodní roli v oblasti ověřovacích zpráv podle standardu SOC (zejména SSAE18, ISAE 3402, ISAE 3000). Naši zástupci jsou členy pracovních skupin, které definují profesionální standardy používané pro SOC reporty. Po celém světě máme odborníky, jejichž každodenní prací je zpracování ověřovacích zpráv pro klienty EY. Díky tomu může naše organizace fungovat jako myšlenkový lídr v oblasti SOC reportingu. Myšlenkové vedení je zajištěno prostřednictvím odborníků EY, kteří denně spolupracují na vývoji efektivního a účinného procesu podávání zpráv SOC pro naše klienty.

ED None.

Tento materiál má pouze všeobecný informační charakter, na který není možné spoléhat se jako na poskytnutí účetního, daňového ani jiného odborného poradenství. V případě potřeby se prosím obraťte na svého konkrétního poradce.

ey.com

David Kesl
partner
david.kesl@cz.ey.com
+420 731 627 226

Soňa Flieglová
manažer
sona.flieglova@cz.ey.com
+420 730 191 987