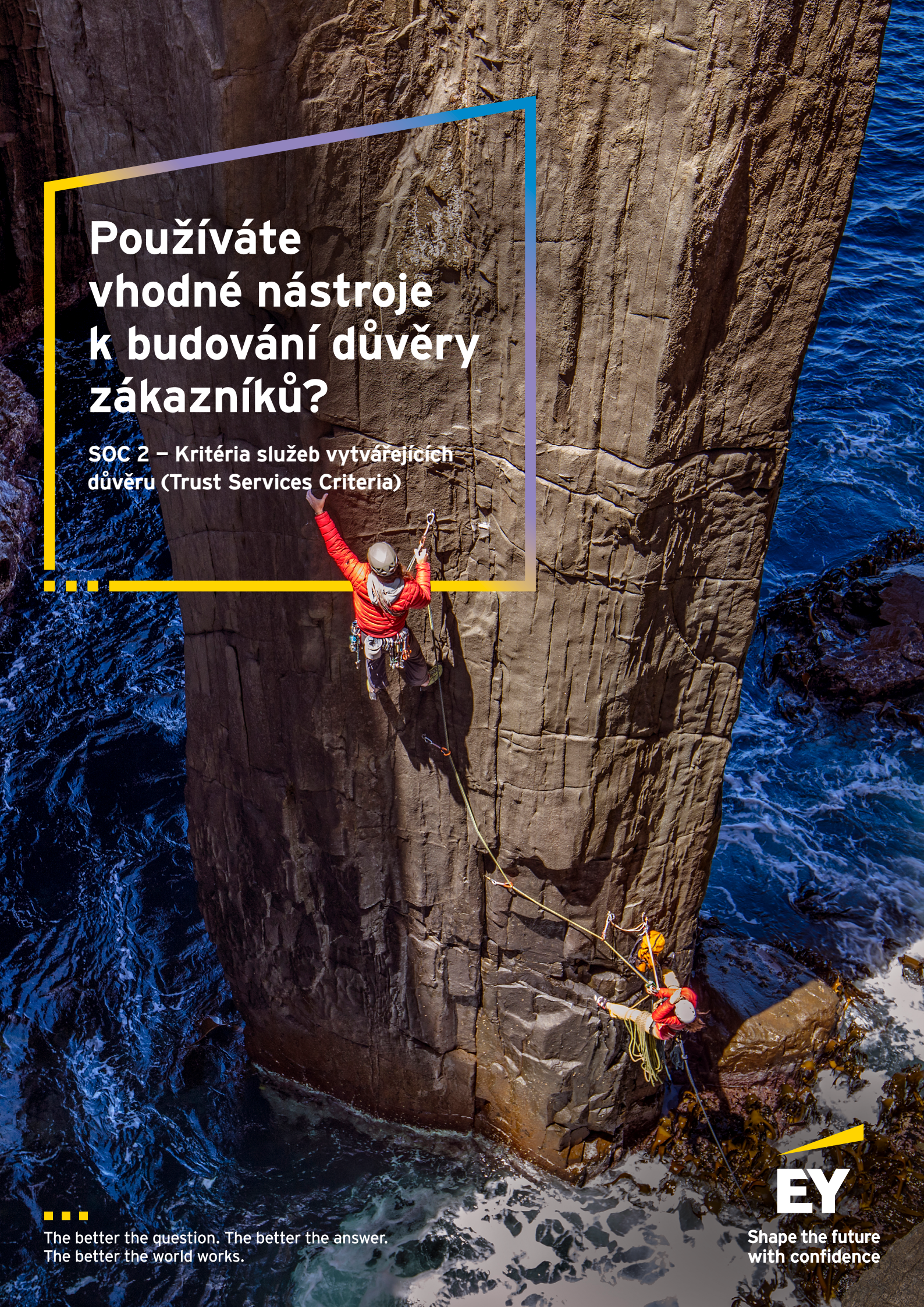


A full-page background image showing two rock climbers on a steep, dark rock face. One climber in a red jacket is higher up, reaching for a hold, while another is lower down. The sea is visible at the base of the cliff.

# 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.



Shape the future  
with confidence



# Demystifikace SOC 2

Co znamená, pokud po vás vaši klienti požadují 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

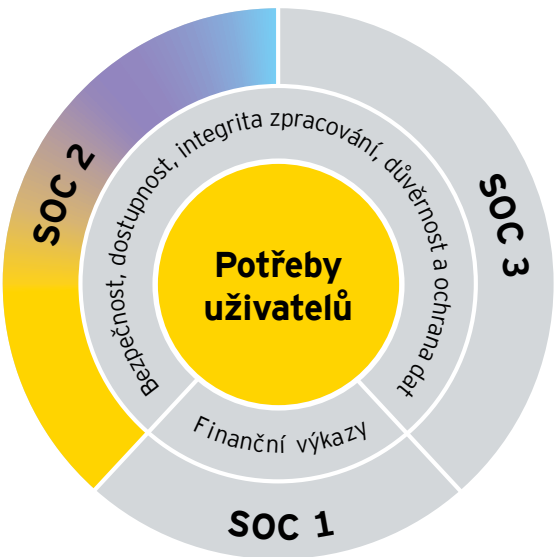
Poskytuje informace o kontrolách v servisní organizaci, které jsou relevantní pro finanční auditory (report má omezené použití).

### 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 kritérií, 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

## 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.

## 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

# 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                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Regulační požadavky</li><li>Vaše potřeby</li><li>Potřeby vašich klientů</li><li>Definice očekávání a způsobu komunikace</li></ul> | <ul style="list-style-type: none"><li>Představení SOC 2 konceptu ve vaší organizaci</li><li>Pomoc se zacílením rozsahu reportu tak, aby odpovídal vašim potřebám a potřebám klientů</li><li>Série workshopů mapující připravenost vaší organizace na SOC 2 požadavky</li><li>Seznam doporučení pro odstranění nedostatků a přípravu kontrolního rámce (SOC 2 kontroly)</li></ul> | <ul style="list-style-type: none"><li>Pochopení klíčových procesů, potřeb a očekávání</li><li>Stanovení rozsahu auditu</li><li>Stanovení podrobných metod testování a plánu prací</li></ul> | <ul style="list-style-type: none"><li>Posouzení systému hodnocení rizik</li><li>Testování SOC 2 kontrol</li><li>Kontrola výsledků společně s vedením</li><li>Souhrnné informace pro výkonné vedení a výbor pro audit</li></ul> | <ul style="list-style-type: none"><li>Formulace případných nálezů a vyhodnocení jejich dopadu na výrok auditora</li><li>Příprava a vydání SOC 2 reportu k určitému datu (Type I) nebo za určité období (Type II, obvykle za 6–12 měsíců)</li><li>SOC 2 report</li></ul> |



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



## **Jan Železný**

vedoucí partner  
v oddělení Technology Risk

[jan.zelezny@cz.ey.com](mailto:jan.zelezny@cz.ey.com)

EY | Building a better working world

EY přispívá k lepšímu fungování světa tím, že vytváří hodnotu pro klienty, zaměstnance, společnost i celou planetu a buduje důvěru na kapitálových trzích.

Týmy odborníků EY s využitím dat, umělé inteligence a pokročilých technologií pomáhají klientům s důvěrou a sebedůvěrou utvářet budoucnost a nacházet odpovědi na ty nejnaléhavější výzvy dneška a zítřka.

Díky detailní znalosti různých ekonomických odvětví, globálně propojené multidisciplinární síti a ekosystému nejrozličnějších partnerských organizací mohou týmy našich auditorů, konzultantů, daňových poradců i odborníků na strategické a transakční poradenství poskytovat komplexní služby ve více než 150 zemích a teritoriích.

**All in to shape the future with confidence.**

Název EY zahrnuje celosvětovou organizaci a může zahrnovat jednu či více členských firem Ernst & Young Global Limited, z nichž každá je samostatnou právnickou osobou. Ernst & Young Global Limited je britská společnost s ručením omezeným garancí, která neposkytuje služby klientům. Informace o tom, jak EY shromažďuje a používá osobní údaje, a o právech fyzických osob stanovených právními předpisy o ochraně osobních údajů jsou k dispozici na [ey.com/privacy](https://ey.com/privacy). Členské firmy EY neposkytují právní služby v zemích, kde to zákon neumožňuje. Podrobnější informace o naší organizaci najdete na našich webových stránkách [ey.cz](https://ey.cz).

© 2026 Ernst & Young, s.r.o. | Ernst & Young Audit, s.r.o. |  
E & Y Valuations s.r.o. | EY Law advokátní kancelář, s.r.o.

Všechna práva vyhrazena

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

[ey.com](https://ey.com)



## **Josef Duben**

senior manažer v oddělení  
Technology Risk

[josef.duben@cz.ey.com](mailto:josef.duben@cz.ey.com)