

Řízení souladu a rozvoj kybernetické bezpečnosti liniových staveb

Asociace pro rozvoj infrastruktury

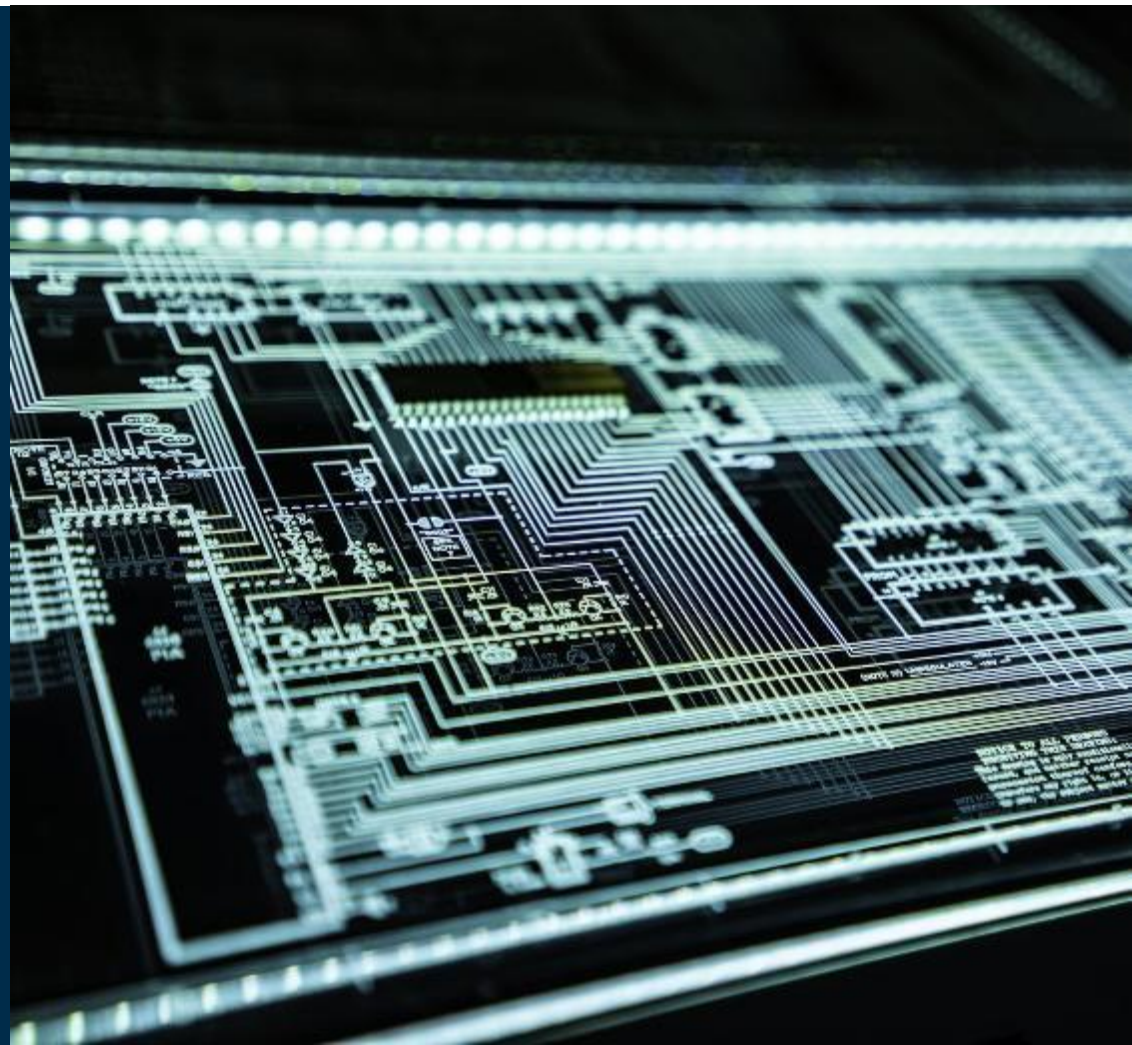
Corpus Solutions, a. s.

23. 4. 2026

Kybernetická bezpečnost v projektech liniových staveb

▪ Body prezentace:

- Jak navázat řízení souladu na fáze projektu
- Jak prakticky zahájit řízení souladu - roadmap
- Co má ověřit gap analýza
- Jak zjištění převést do priorit a roadmapy
- Jaké projekty z toho typicky vzniknou
- Kdo za co odpovídá
- Co je potřeba stihnout v prvním roce



Co je roadmap kybernetické bezpečnosti a jak ji koncipovat?



Dopravní a řídicí technologie



Bezpečnostní a informační prvky



Konektivita a přístupy

Roadmapa kybernetické bezpečnosti jako plán řízení souladu

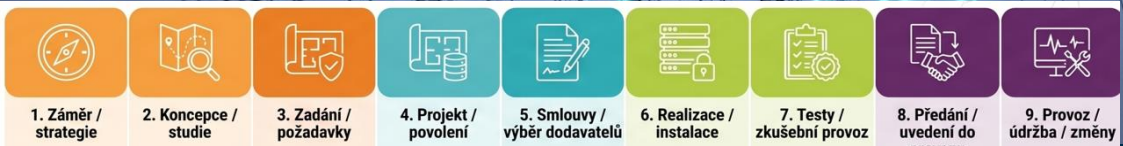


PŘÍPRAVA ROADMAP
PLNĚNÍ ROADMAP

Řízení souladu a rozvoj KyBe neběží mimo projekt. Musí být navázány na životní cyklus liniové stavby.

- **Fáze 1–3 | Příprava a požadavky**
vzniká rozsah, cíle, rizikové scénáře a očekávaný cílový stav
- **Fáze 4–5 | Projekt a smluvní zajištění**
bezp. požadavky se převádějí do architektury, dokumentace, zadání a smluv
- **Fáze 6–7 | Realizace a ověření**
probíhá impl. opatření, integrace, testování a ověření souladu
- **Fáze 8–9 | Předání a ostrý provoz**
nastavuje se monitoring, provozní řízení, reakce na incidenty a průběžné zlepšování

Roadmapa se navrhuje na začátku projektu, ale její realizace typicky probíhá **minimálně 12 měsíců** a často zasahuje až do předání a prvního období provozu. Pokud je stavba hotova, musí se vypracovat soulad s novým zákonem/vyhláškou okamžitě po rozhodnutí o registraci identifikaci. Pak už nejde o „security by design“, ale o řízení retrofit bezpečnosti za provozu.



První krok: vymezení chráněného prostředí

Bez přesně definovaného rozsahu nelze efektivně řídit soulad ani plánovat projekty. Tento proces propojuje regulované služby s konkrétními technologiemi a určuje hranice mezi interními systémy a externími dodavateli.

Analýza a Identifikace Aktiv



Vazba služby na technologie

Propojení regulovaných služeb s konkrétními technologiemi v organizaci



Primární a podpůrná aktiva

Identifikace klíčových aktiv a prvků, které je technicky podporují.



Výběr pro roadmapu

Rozhodnutí, která aktiva a procesy musí být prioritně zahrnuty do plánu rozvoje.

Vymezení Hranic a Závislosti



Interní systémy:
Provozní technologie (OT) a firemní infrastrukturu.

Externí entity:
Cloudové služby a přístupy servisních organizací.

Dodavatelé:
Smluvní vztaby a vymezení odpovědnosti za aktiva.



Mapování kritických rozhraní

Detailní popis klíčových závislostí nezbytných pro následnou analýzu rizik.

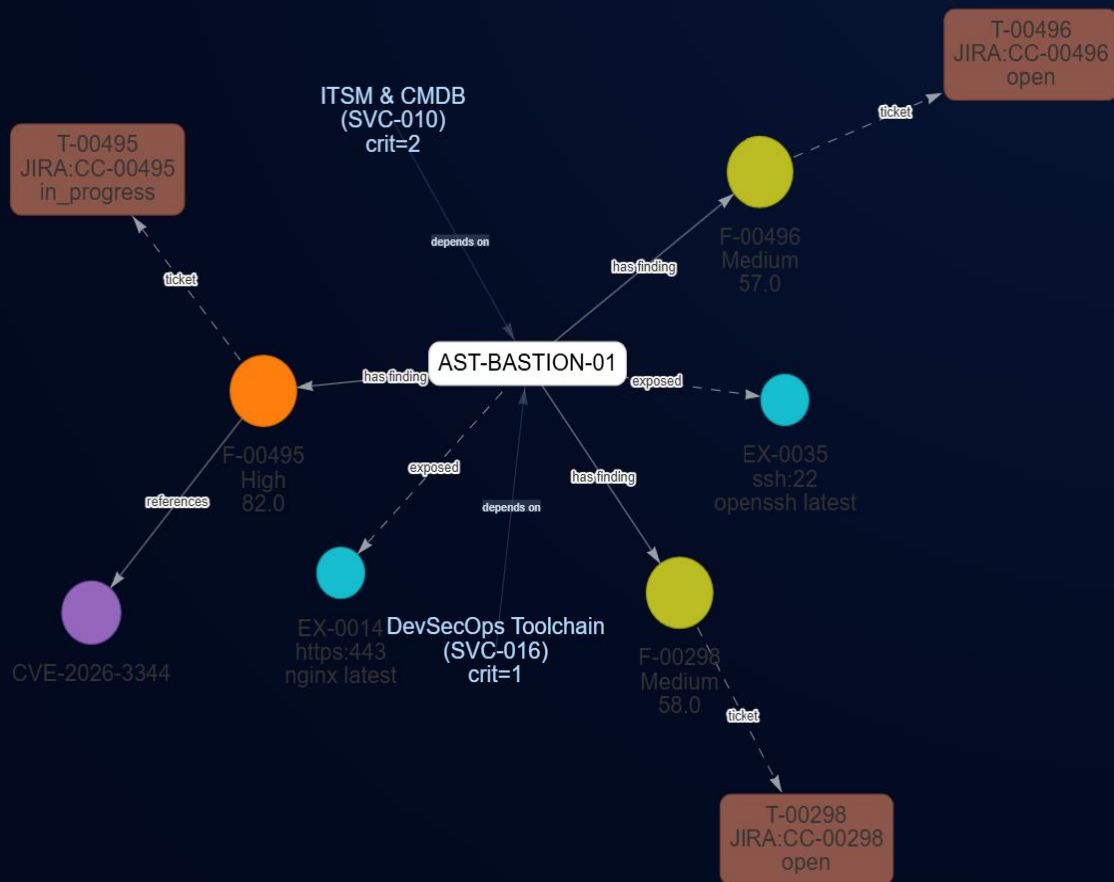


Základ pro Gap analýzu

Jasný výstup, na který přímo navazuje analýza rizik a nápravné projekty.

Gap analýza: co má skutečně ověřit

Vztahy mezi aktivy



Gap analýza nemá jen zkontrolovat dokumenty, ale odhalit, co chybí pro reálný bezpečný provoz.

- governance, role a odpovědnosti
- přehled aktiv, architektury a vazeb na službu
- řízení rizik a návaznost na provozní scénáře
- technická a organizační opatření
- monitoring, logování a detekce událostí
- řízení přístupů a privilegovaných účtů
- dodavatelé, servisní zásahy a vzdálené přístupy
- kontinuita provozu, obnova a cvičení
- dokumentace, auditní průkaznost a akceptace změn

Výstup gap analýzy:

ne seznam paragrafů, ale konkrétní nedostatky, rizika a témata pro další projekty.



Jak z gap analýzy udělat priority a roadmapu

Zjištění je potřeba převést do řízené roadmapy, návrhu opatření v podobě projektů:

- seskupit zjištění do logických oblastí a projektů a hodnotit je podle:
 - dopadu na službu
 - rizika
 - náročnosti
 - závislostí na jiných činnostech
- rozlišit:
 - rychlá opatření (evidence, směrnice, MFA pro remote access)
 - systémové změny (centrálně řízený VPN přístup, řízení změn OT)
 - dlouhodobé architektonické projekty (nasazení PAM / bastion hostu pro privilegované a dodavatelské přístupy, segmentace, SOC)
- určit, co musí být navrženo hned a co může být realizováno postupně
- sladit roadmapu s reálnými fázemi stavby, rozpočtem a kapacitami

Realizace roadmapy typicky trvá **nejméně 1 rok** a často pokračuje i po spuštění ostrého provozu.



Typické projekty rozvoje kybernetické bezpečnosti

Servisní VPN login → přístup do OT → změna PLC konfigurace → SCADA alarm / výpadek technologie.

Z gap analýzy obvykle nevznikne jedno opatření, ale sada navazujících projektů.

- inventarizace a klasifikace aktiv
- **segmentace sítí IT/OT a ochrana kritických rozhraní**
- řízení identit, účtů a privilegovaných přístupů
- **bezpečné vzdálené přístupy dodavatelů**
- centralizace logů, monitoring a dohled
- hardening technologií a vulnerability management
- **řízení změn a bezpečnostní akceptace**
- **monitoring servisních zásahů, incident response a krizové scénáře**
- BCM/DR pro provozně významné technologie
- promítnutí bezpečnostních požadavků do zadání, smluv a dokumentace
- **privilegovaný přístup a dohled nad činností**
- **kontinuita a obnova po chybné změně**

Typický charakter těchto projektů:

část lze udělat rychle, ale část vyžaduje koordinaci s projektantem, integrátorem i provozem a běží déle.

Definice projektů Realizace projektů



4. Projekt / povolení
5. Smlouvy / výběr dodavatelů



6. Realizace / instalace
7. Testy / zkušební provoz
8. Předání / uvedení do provozu
9. Provoz / údržba / změny

Jak má vypadat definice projektu roadmapy

ZÁKLADNÍ PARAMETRY PROJEKTU



Název projektu

Zavedení řízeného vzdáleného přístupu dodavatelů a servisních organizací.



Hlavní cíl

Zajistit, aby všechny vzdálené přístupy byly řízené, schvalované, auditovatelné a bezpečné.



Popis řešení

Zavedení centrálního přístupového bodu, vícefaktorová autentizace (MFA), evidence relací, oddělení rolí a časově omezený přístup pouze na definované systémy.

REALIZAČNÍ A PROVOZNÍ ASPEKTY

Implementační náročnost




Odhadováno v závislosti na počtu lokalit, dodavatelů a složitosti prostředí.

Orientační cena



Přibližně podle zvoleného technologického řešení a požadavků na záznam relací.

Přehled fází a rolí

Kategorie	Detaily z dokumentace
Implementační kroky 	1. Mapování přístupů, 2. Identifikace kritických systémů, 3. Návrh architektury, 4. Výběr VPN/PAM řešení, 5. Nastavení rolí a MFA, 6. Integrace IT/OT, 7. Logování, 8. Pilotní provoz, 9. Převod dodavatelů, 10. Dokumentace a školení.
Role pro realizaci 	Bezpečnostní a síťový architekt, OT specialista, správce identit, administrátor technologií, projektový manažer, zástupci dodavatelů.
Role pro provoz 	Správce platformy, SOC dohled, provozní správce OT/ITS, vlastník služby, schvalovatelé přístupů, interní audit.

BEZPEČNOSTNÍ DOPADY A RIZIKA



Přínos pro bezpečnost

Vyšší kontrola nad zásahy dodavatelů, dohledatelnost činnosti a snížení rizika kompromitace OT/ITS prostředí.



Snížení rizika

Prevence neoprávněného přístupu, kompromitace účtů, neauditovaných změn a laterálního pohybu mezi sítěmi.



Rizika implementace

Možný odpor dodavatelů ke změně, nekompatibilita starších technologií, neúplný přehled stávajících přístupů nebo chybějící interní kapacity.

„Roadmapa nemá být jen seznam témat. Musí být tvořena konkrétními projekty, které mají jasný cíl, rozsah, odpovědnosti, návaznosti, náročnost a přínos pro snížení rizik.“

Kdo za co odpovídá

Vedení organizace

Investor / zadavatel

V praxi je dobré se u každého zásadního bezpečnostního požadavku ptát:

*kdo to zadal,
kdo to navrhl,
kdo to dodal,
kdo to ověřil,
kdo to bude dlouhodobě provozovat.*

Projektant / architekt

Provozovatel Dodavatel / integrátor

Největší riziko bývá tam, kde odpovědnost není jasně přiřazena.

- **Vedení organizace**
schvaluje směr, priority, rozpočet a akceptaci rizik
- **Investor / zadavatel**
přenáší bezpečnostní požadavky do zadání, smluv a akceptačních kritérií
- **Projektant / architekt**
promítá požadavky do návrhu, architektury, dokumentace a technických standardů
- **Provozovatel**
potvrzuje provozní realitu, scénáře použití a udržitelnost opatření
- **Dodavatel / integrátor**
dodává bezpečně provozovatelné řešení, konfiguraci a potřebné důkazy o splnění

Klíčové pravidlo:

bezpečnost nesmí zůstat „mezi rolemi“ — jinak se ztratí mezi projektem, dodávkou a provozem. **Největší bezpečnostní selhání často nevznikají kvůli chybě technologie, ale kvůli chybě řízení odpovědnosti**



Strategická kybernetická roadmapa: 10 kroků k odolnosti



1. Definice účelu a rozsahu

Vymezení prostředí, služeb a rozhodnutí, která má dokument podpořit.



2. Metodika a standardy

Výběr hodnotícího rámce (např. NIST CSF, ISO 27001) a metodiky rizik.



3. Kontext hrozeb a regulací

Popis relevantních scénářů útoků a technologických trendů v sektoru.



4. Analýza současného stavu a aktiv

Systematické vyhodnocení bezpečnosti a analýza aktiv (primární i podpůrná).



5. Témata změny

Seskupení zjištěných mezer (gaps) do logických celků pro budoucí projekty.



6. Definice cílového stavu

Návrh realistické architektury založené na principech Zero Trust a XDR.



7. Identifikace projektů

Převod opatření do konkrétních projektů s jasným popisem a přínosem.



8. Prioritizace

Sefazení projektů podle dopadu na riziko, rozpočtu a provozní proveditelnosti.



9. Časová roadmapa

Rozvržení do fází: Stabilizace, Konsolidace a Pokročilá automatizace.



10. Zdroje a investice

Kalkulace interních rolí, pracovní v člověkodnech a celkových finančních nákladů.

Co musí organizace stihnout v prvním roce



Protected Environment



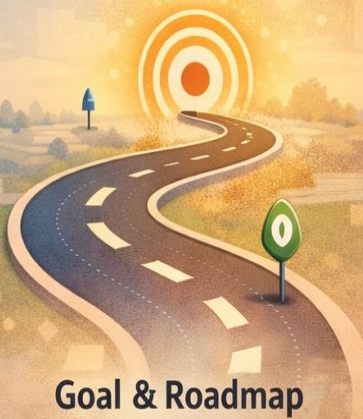
Risk Analysis



Governance



Security Projects



Goal & Roadmap



Monitoring &
Incident Response

První rok je rozhodující pro nastavení směru, priorit a spuštění klíčových projektů.

- potvrdit rozsah chráněného prostředí
- provést gap analýzu a řízení rizik
- definovat cílový stav a roadmapu
- promítnout požadavky do projektu, změn a smluv
- nastavit governance, reporting a kontrolní mechanismy
- zahájit prioritní bezpečnostní projekty
- připravit monitoring, incident response a základní cvičení
- nastavit průběžné vyhodnocování souladu a další rozvoj

Soulad není jednorázový dokument. Je to řízený program technických a organizačních projektů, který se musí navrhnout včas a realizovat v návaznosti na celý životní cyklus liniové stavby.

Jak průběžně hlídat a kontrolovat soulad

Řídicí výbor

měsíční stav projektů, rizik, rozpočtu, rozhodnutí

Compliance dashboard

stav paragrafů, důkazy, otevřené úkoly, termíny

Risk register

top rizika, plán zvládnání, výjimky, akceptace

Architecture & change board

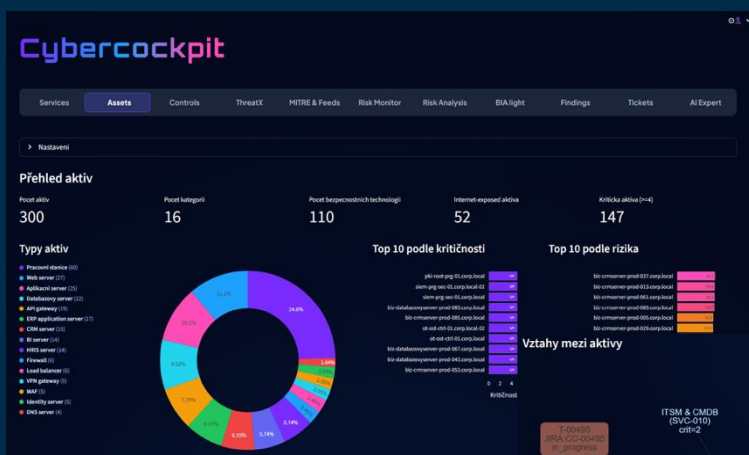
dopad změn na regulovanou službu a bezpečnost

SOC / incident reporting

detekce, eskalace, lessons learned, trendy

Audit cycle

interní kontroly, cvičení, testy obnovy, readiness



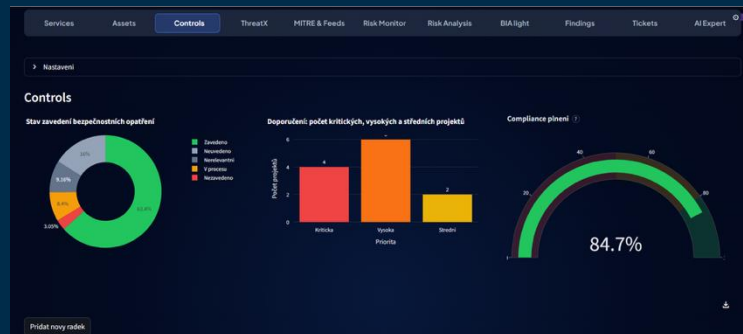
Detail souladu podle frameworku

Procesní compliance (manuální): 4.8% (22/457)

ENISA_EU_2024_2690 ISO_27002 NIS2_VOKB_409_2025 NIS2_VOKB_410_2025

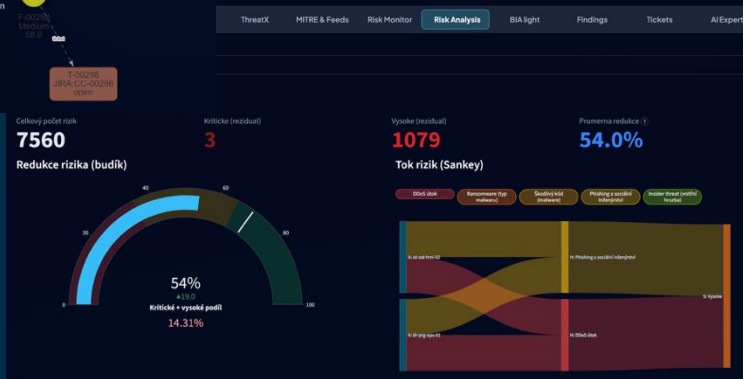
Tabulka je editovatelná. Povelový status: splněno, neuspělo, zčásti.

ID	Typ pozadavku	Bezpečnostní opatření	Hierarchie	Pozadavek	Pozadované opatření
311	TECHNICE	§ 24 Aplikáční bezpečnost	(5) Povinná osoba v rámci	c) provádí v souladu s ods.	§ 24 Aplikáční bezpečno
312	TECHNICE	§ 24 Aplikáční bezpečnost	(3) Povinná osoba v rámci	d) v obdobných případech	§ 24 Aplikáční bezpečno
313	TECHNICE	§ 24 Aplikáční bezpečnost	(1) Povinná osoba v rámci	e) u pověřených testů v s.	§ 24 Aplikáční bezpečno
314	TECHNICE	§ 24 Aplikáční bezpečnost	(6) Povinná osoba proved.	b) nouzovou komunikaci v	§ 24 Aplikáční bezpečno
315	TECHNICE	§ 25 Kryptografické algorit.	(1) Povinná osoba při zapř.	a) používá pouze aktuáln.	§ 25 Kryptografické algorit.
316	TECHNICE	§ 25 Kryptografické algorit.	(1) Povinná osoba při zapř.	b) používá bezpečné na.	§ 25 Kryptografické algorit.
317	TECHNICE	§ 25 Kryptografické algorit.	(1) Povinná osoba při zapř.	c) zotezňuje dostupnost.	§ 25 Kryptografické algorit.
318	TECHNICE	§ 25 Kryptografické algorit.	(7) Povinná osoba zapřít.	a) hlasovou, audiovizuáln.	§ 25 Kryptografické algorit.
319	TECHNICE	§ 25 Kryptografické algorit.	(2) Povinná osoba zapřít.	b) nouzovou komunikaci v	§ 25 Kryptografické algorit.
320	TECHNICE	§ 25 Kryptografické algorit.	(3) Povinná osoba v přípa.	a) pouze aktuálně ověř.	§ 25 Kryptografické algorit.
321	TECHNICE	§ 25 Kryptografické algorit.	(3) Povinná osoba v přípa.	1. zapřít generování, dist.	§ 25 Kryptografické algorit.
322	TECHNICE	§ 25 Kryptografické algorit.	(3) Povinná osoba v přípa.	2. umožnit kontrolu a audit a	§ 25 Kryptografické algorit.
323	TECHNICE	§ 25 Kryptografické algorit.	(1) Povinná osoba v přípa.	3. zapřít důvěrnost a integ.	§ 25 Kryptografické algorit.
324	TECHNICE	§ 26 Zajištění dostupno.	(1) Povinná osoba zavře.	a) dostupnost regulovan.	§ 26 Zajištění dostupno.
325	TECHNICE	§ 26 Zajištění dostupno.	(1) Povinná osoba zavře.	b) oddělené resoursování sá.	§ 26 Zajištění dostupno.



Upr. v. Nutí měnit pozadavky v. stav. bezpeč. v. Počet bezpečnostních opatření v. Termín zav. v. priorita. zav. v. Odpovědnost v. sledovat v. koment.

id	Upr.	Nutí měnit pozadavky	v. stav. bezpeč.	v. Počet bezpečnostních opatření	v. Termín zav.	v. priorita. zav.	v. Odpovědnost	v. sledovat	v. koment.
1	nan	Povinná osoba při zapřít.	Zavazeno	Jako zavedení přehledně be.	Jedná se o st.	Vysoká	Osoba pověřená z. a.	nan	na nepř.
2	nan	Zavazeno a prováděno bezpeč.	Zavazeno	Veliká bezpečnostní bez.	Jedná se o st.	Vysoká	Osoba pověřená z. a.	nan	na nepř.
3	nan	Zavazeno a prováděno bezpeč.	Zavazeno	Veliká bezpečnostní bez.	Jedná se o st.	Vysoká	Osoba pověřená z. a.	nan	na nepř.



Děkujeme vám za pozornost

jan.kriz@corpus.cz

corpus.cz