Metodika pro výkon auditu kybernetické bezpečnosti IS VaVaI

Metodika definující způsob naplnění vybraných povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti v oblasti identifikace, analýzy a řízení rizik informačního systému pro výzkum, vývoj a inovace (IS VaVaI)

Zpracoval: Tomáš Bezouška, garant aktiva IS VaVaI

Schválil: doplnit

Verze: 0.1

Datum: 22. června 2017

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
KB	Kybernetická bezpečnost
ÚV ČR	Úřad vlády České republiky
RVVI	Rada pro vědu, výzkum a inovace, poradní orgán Vlády České republiky
IS VaVaI	Informační systém výzkumu, vývoje a inovací
ZKB	Zákon o kybernetické bezpečnosti
ISMS	Systém řízení bezpečnosti informací
Sb.	Sbírka zákonů České republiky
ČR	Česká republika
VIS	Významný informační systém
NCKB	Národní centrum kybernetické bezpečnosti
RACI	Matice odpovědností
IT	Informační technologie
EU	Evropská unie
ISO	Mezinárodní organizace pro standardizaci
IEC	International Electrotechnical Commission

1 Úvod

1.1 Poslání a postavení auditu KB

Pro účely vykonávání auditu kybernetické bezpečnosti IS VaVaI byl v souladu se zákonem č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vypracován tento Metodické pokyny pro výkon auditu kybernetické bezpečnosti. Metodický pokyn dále vychází z Bezpečnostní politiky informací IS VaVaI a Bezpečnostní politika ochrany IS ÚV ČR.

1.2 Postavení auditora

Auditor kybernetické bezpečnosti je osoba odpovědná za formální i věcně správné a úplné provedení auditu kybernetické bezpečnosti. Prověřuje fungování systémů řízení informační bezpečnosti v souladu se zákonem o kybernetické bezpečnosti, vyhlášek ke kybernetické bezpečnosti, přijatými mezinárodními ISO normami, případně s relevantními zásadami, standardy a směrnicemi, kontroluje dodržování platných zákonů a procesních postupů stanovených interními akty řízení, ověřuje vedení evidencí, realizaci předepsaných školení a reportování identifikovaných kybernetických bezpečnostních událostí.

Auditora kybernetické bezpečnosti jmenuje ředitel Sekce pro vědu, výzkum a inovace ÚV ČR. Při jmenování musí respektovat zákonné požadavky na kvalifikaci auditora a ustanovení o neslučitelnosti rolí v rámci systému řízení kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti zodpovídá zejména za:

- plánování kontrolních činností a auditů v oblasti kybernetické bezpečnosti resortu,
- hodnocení míry souladu systému řízení bezpečnosti informací a realizovaných bezpečnostních opatření s definovanými požadavky, stanovenými bezpečnostními politikami a vhodnými bezpečnostními standardy,
- vedení dokumentace o průběhu auditu podle stanovených metodik,
- vyhodnocování shromážděných nálezů z auditu a jejich srovnávání s kritérii auditu,
- sdělování výsledků auditu a navrhování doporučení,
- zpracování závěrečných zpráv z auditu,
- kontrolování účinnosti přijatých opatření.

Role Auditora kybernetické bezpečnosti je neslučitelná s členstvím ve Výboru pro řízení kybernetické bezpečnosti, s rolí Manažera kybernetické bezpečnosti, Architekta kybernetické bezpečnosti a Garanta aktiva. Auditor kybernetické bezpečnosti vykonává svou roli nestranně.

Musí být garantována nezávislost auditora vůči předmětu auditu. Roli Auditora KB lze obsadit i externím pracovníkem při splnění požadavku na řízení rizik spojených s tímto krokem.

2 Plánování auditu KB

Audit kybernetické bezpečnosti se provádí nejméně jednou ročně. Za jeho provedení odpovídá jmenovaný auditor KB a jeho výsledky předkládá Garantovi aktiva IS VaVaI a po jejich schválení na vědomí Výboru pro řízení kybernetické bezpečnosti ÚV ČR.

3 Postupy a techniky pro provádění auditu KB

Auditor kybernetické bezpečnosti při své činnosti postupuje v souladu s platnými právními předpisy, zejména pak zákonem č. 255/2012 Sb., o kontrole, a vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) a vnitřními předpisy ÚV ČR.

Auditor se rozhoduje samostatně jaké postupy a techniky nebo jejich kombinaci při provádění auditu použije.

Auditor primárně vyhodnotí soubor otázek (check list), který je uveden jako příloha tohoto dokumentu. K tomu účelu použije níže uvedené auditní techniky.

Při provádění auditu se používají takové techniky, které zabezpečí splnění cíle auditu. V Metodickém pokynu jsou uvedeny pouze některé z vybraných technik:

- kontrola dokumentace (náležitostí, úplnosti,…),
- řízené pohovory s osobami odpovědnými za danou problematiku a osobami, které se účastní procesu zajištění bezpečnosti,
- místní šetření.

4 Základní náležitosti při provádění interního auditu

Pověřený auditor se seznámí s prostředím, informačními toky a dokumenty, které jsou předmětem ověřování pro účely posouzení kybernetické bezpečnosti. Identifikuje zdroje, ze kterých bude vycházet při vyhodnocování jednotlivých témat check listu. Zdroje a informace z nich získané pak využije k zodpovězení jednotlivých otázek check listu, který je přílohou tohoto dokumentu. K získání odpovědí na jednotlivé otázky dotazníku využije výše uvedené techniky.

V průběhu provádění auditu KB auditor získává, ověřuje a analyzuje získané informace, které shromažďuje a zakládá do auditní dokumentace.

Na základě těchto podkladů je pak formulováno zjištění a z něj vyplývající závěr o stavu auditované oblasti, včetně návrhu doporučení k odstranění zjištěných nedostatků.

Zjištěné skutečnosti jsou v průběhu auditu projednávány s příslušným odpovědným vedoucím zaměstnancem.

V případě, že program auditu je splněn, zpracuje auditor písemnou Zprávu z auditu.

Pokud dojde k porušení zásady funkčnosti a nezávislosti při přípravě nebo výkonu auditu, uvede se ve zprávě tato skutečnost a její dopady na tento audit.

V písemné zprávě se auditor soustředí zejména na:

- zjištění z provedeného auditu obsahující zejména negativní výsledky procesů, t.j. zjištěné nedostatky při prověřování a vyhodnocení zjištěných skutečností v porovnání s objektivně stanovenými kontrolními kritérii,
- rizika vyplývající ze zjištění, včetně dopadu na auditovanou oblast,
- doporučení k odstranění zjištěných nedostatků a ke zdokonalení kvality sytému kybernetické bezpečnosti a předcházení nebo zmírnění zjištěných rizik (doporučení by měla být popsána srozumitelně, musí mít konkrétního adresáta odpovědného za realizaci doporučení a náklady na realizaci doporučení by měly být úměrné riziku vyplývajícímu ze zjištění.
- závěry obsahující výrok auditora ve vztahu k auditované oblasti, pozitivní a negativní zjištění.

Zpráva z auditu musí být objektivní, jasná, stručná, výstižná, konstruktivní a průkazná.

Auditor předloží závěrečné znění zprávy manažerovi kybernetické bezpečnosti, po schválení závěrečné zprávy je tato předložena Výboru pro řízení kybernetické bezpečnosti ÚV ČR na vědomí.

Zpráva z auditu se stává součástí dokumentace kybernetické bezpečnosti ÚV ČR a je uložena v souladu se stanovenými pravidly pro tuto dokumentaci. Současně je jeden stejnopis zprávy uložen na odboru bezpečnosti a krizového řízení.

5 Uložení dokumentace auditu

Dokumenty získané v průběhu auditu jsou součástí spisu auditu a jsou také souhrnně označovány jako auditorská dokumentace.

Do auditorské dokumentace je ukládána veškerá dokumentace a materiály vzniklé v průběhu auditu (záznamy z interview, kopie materiálů a dokladů získaných při auditu atp.). Součástí auditorské dokumentace se stává i zpráva z auditu.

6 Seznam příloh

Příloha č. 1: Etický kodex auditora kybernetické bezpečnosti

Příloha č. 2: Checklist auditora kybernetické bezpečnosti

Příloha 1: Etický kodex auditora kybernetické bezpečnosti

Auditor KB:

1. postupuje při plnění svých povinností a úkolů vždy objektivně, s patřičnou důkladností, prozíravostí a čestností,
2. oznámí řediteli odboru bezpečnosti a krizového řízení, že nemůže přijmout konkrétní úkol, neboť se jeho realizací může dostat do rozporu s nezávislým plněním jemu stanovené funkční náplně,
3. nikdy se vědomě nezapojí do žádné nezákonné či nepatřičné činnosti, která by diskreditovala jeho, jeho profesi či organizaci, jejímž je zaměstnancem,
4. zdrží se jakékoli činnosti, která by mohla být v rozporu se zájmy zaměstnavatele a která by mohla nepříznivě ovlivnit jeho schopnost plnit objektivně své úkoly a povinnosti,
5. nepřijme od zaměstnance, klienta, zákazníka, dodavatele nebo obchodního partnera peněžní ani nepeněžní plnění, které by mohlo narušit nebo být považováno za schopné narušit jeho profesní úsudek,
6. sdělí řediteli odboru bezpečnosti a krizového řízení, že nemůže přijmout stanovený úkol, neboť může reálně předpokládat, že jej nedokáže splnit na profesionální úrovni a ve stanoveném termínu,
7. při plnění povinností zachází opatrně a obezřetně s informacemi, které získá v průběhu své činnosti. Nesmí používat důvěrných informací v ničí prospěch, ani způsobem, který by byl v rozporu se zákonem nebo by byl na škodu zaměstnavatele,
8. dodržuje vysokou úroveň způsobilosti, morálky a důstojnosti, zásadu mlčenlivosti o informacích získaných v průběhu své práce, pokud k tomu neobdrží výslovné svolení, příp. pokud mu to neukládá zákonná nebo profesní povinnost,
9. sdělí při vykazování výsledků své práce všechna důležitá fakta, která zjistil a která, nebudou-li sdělena, mohou buď zkreslit zprávy o posuzovaných skutečnostech nebo mohou zakrývat nezákonné machinace,
10. průběžně usiluje o zvyšování své odbornosti, efektivnosti a kvality vlastní práce,
11. v zájmu objektivnosti nesmí auditovat činnosti, za jejichž výkon nesl v minulosti odpovědnost,
12. jedná při své pracovní činnosti vždy korektně s ostatními zaměstnanci i se zaměstnanci jiných úřadů či orgánů,
13. řeší záležitosti spojené s výkonem auditu KB vždy objektivně bez zbytečných průtahů na základě skutkové podstaty, nikdy svévolně k újmě kohokoliv, ať již fyzické či právnické osoby,
14. zásadně nepřipustí, aby došlo ke střetu jeho soukromého zájmu s postavením interního auditora, v případě jakýchkoliv pochybností projedná konkrétní záležitost se svým nadřízeným,

15. nevykonává takové politické či veřejné činnosti, které by mohly narušit důvěru v jeho schopnost nestranně vykonávat povinnosti auditora KB,
16. ve svém soukromém životě se bude rovněž vyhýbat takovým činnostem, chování či jednání, které by mohly ve svých důsledcích vést ke snížení důvěry či dokonce být příčinou jeho vydírání,
17. vynakládá přiměřené úsilí, aby zajistil maximálně efektivní a ekonomické využívání svěřených finančních zdrojů, zařízení a služeb,
18. v případě, že je požádán o jednání v rozporu s platnými zákony či vnitřními pokyny nebo které ve svých důsledcích může vést ke zneužití úřední moci, je povinen takové jednání odmítnout a současně neprodleně informovat o celé záležitosti svého nejbližšího nadřízeného, příp. vedení ministerstva zdravotnictví,
19. v případě zjištění skutečností nasvědčujících podezření ze spáchání trestného činu nebo přestupku, zabezpečí zajištění příslušných dokladů, připraví podklady pro podání oznámení orgánům činným v trestním řízení a bez zbytečného odkladu informuje ředitele odboru bezpečnosti a krizového řízení.

Příloha 2: Checklist auditora kybernetické bezpečnosti

Reference	Otázka	ANO	NE	N/A
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)				
181/2014 Sb. §2	Má organizace kritickou informační infrastrukturu?			
181/2014 Sb. §2	Má organizace významný informační systém?			
181/2014 Sb. §2	Má organizace správce informačního systému, který určuje účel zpracování informací a podmínky provozování IS?			
181/2014 Sb. §2	Má organizace správce komunikačního systému, který určuje účel využití a podmínky provozování KS?			
181/2014 Sb. §2	Má organizace správce elektronických komunikací (buď zajišťující přímé zahraniční připojení do veřejných komunikačních sítí nebo připojení ke kritické informační infrastruktuře?			
181/2014 Sb. §2	Má organizace významnou síť?			
181/2014 Sb. §3	Je organizace poskytovatel služeb elektronických komunikací nebo poskytovatel zajišťující síť elektronických komunikací?			
181/2014 Sb. §3	Je organizace zajišťující významnou síť (pokud není správce komunikačního systému kritické infrastruktury) správce informačního systému kritické informační infrastruktury?			
181/2014 Sb. §3	Je organizace správce komunikačního systému kritické informační infrastruktury?			
181/2014 Sb. §3	Je organizace správce významného informačního systému?			

Reference	Otázka	ANO	NE	N/A
181/2014 Sb. §4 odst. 2	Pokud je organizace správcem informačního systému KIS, příp. Správce komunikačního systému KIS nebo správce významného IS má zavedena bezpečnostní opatření pro informační systém KIS, KII, VIS?			
181/2014 Sb. §4 odst. 2	Pokud je organizace správcem informačního systému KIS, příp. Správce komunikačního systému KIS nebo správce významného IS provádí bezpečnostní opatření pro informační systém KIS, KII, VIS?			
181/2014 Sb. §4 odst. 3	Pokud je organizace správcem informačního systému KIS, příp. Správce komunikačního systému KIS nebo správce významného IS má zohledněny požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů?			
181/2014 Sb. §5 odst. 2	Má organizace organizačně zajištěna opatření systému řízení bezpečnosti informací?			
181/2014 Sb. §5 odst. 2	Má organizace organizačně zajištěné řízení rizik?			
181/2014 Sb. §5 odst. 2	Má organizace definovánu bezpečnostní politiku?			
181/2014 Sb. §5 odst. 2	Má organizace definovánu organizační bezpečnost?			
181/2014 Sb. §5 odst. 2	Má organizace stanoveny bezpečnostní požadavky pro dodavatele?			
181/2014 Sb. §5	Jsou v organizaci řízena aktiva?			

Reference	Otázka	ANO	NE	N/A
odst. 2				
181/2014 Sb. §5 odst. 2	Má organizace řízenu bezpečnost lidských zdrojů?			
181/2014 Sb. §5 odst. 2	Má organizace zavedeno řízení provozu a komunikací KIS nebo VIS?			
181/2014 Sb. §5 odst. 2	Má organizace zavedeno řízení přístupu osob ke KIS nebo VIS?			
181/2014 Sb. §5 odst. 2	Má organizace zabezpečenu akvizici, vývoj a údržbu KIS a VIS?			
181/2014 Sb. §5 odst. 2	Má organizace zabezpečeno zvládání kybernetických bezpečnostních událostí a incidentů?			
181/2014 Sb. §5 odst. 2	Má organizace zabezpečeno řízení kontinuity činností?			
181/2014 Sb. §5 odst. 2	Má organizace zabezpečenu kontrolu a audit KIS a VIS?			
181/2014 Sb. §5 odst. 3	Má organizace technicky zabezpečenu fyzickou bezpečnost?			
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro ochranu integrity komunikačních sítí?			
181/2014 Sb. §5	Má organizace nástroj pro ověřování identity uživatelů?			

Reference	Otázka	ANO	NE	N/A
odst. 3				
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro řízení přístupových oprávnění?			
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro ochranu před škodlivým kódem?			
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro zaznamenávání činností KIS a VIS, jejich uživatelů a administrátorů?			
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro detekci kybernetických bezpečnostních událostí?			
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí?			
181/2014 Sb. §5 odst. 3	Má organizace zavedenu aplikační bezpečnost?			
181/2014 Sb. §5 odst. 3	Používá organizace kryptografické prostředky?			
181/2014 Sb. §5 odst. 3	Má organizace nástroj pro zajišťování úrovně dostupnosti informací?			
181/2014 Sb. §5 odst. 3	Má organizace zajištěnu bezpečnost průmyslových a řídících systémů?			
181/2014 Sb. §8	Má organizace zavedeno hlášení kybernetických bezpečnostních incidentů provozovateli			

Reference	Otázka	ANO	NE	N/A
odst. 2	národního CERT?			
181/2014 Sb. §8 odst. 3	Má organizace zavedeno hlášení kybernetických bezpečnostních incidentů Národnímu bezpečnostnímu úřadu?			
181/2014 Sb. §11 odst. 3a	Pokud organizace spadá mezi orgány a osoby uvedené v §3 písm. a) a b) je schopna za stavu kybernetického nebezpečí nebo nouzového stavu vyhlášeného na základě žádosti §21 odst. 6 provádět reaktivní opatření?			
181/2014 Sb. §11 odst. 3b	Pokud organizace spadá mezi orgány a osoby uvedené v §3 písm. c) až e) je schopna provádět reaktivní opatření?			
181/2014 Sb. §11 odst. 4	Pokud organizace spadá mezi orgány a osoby uvedené v §3 písm. c) až e) je schopna provádět ochranná opatření?			
181/2014 Sb. §13 odst. 4	Má organizace nebo osoba uvedená v §3 zabezpečeno oznámení o provedení reaktivního opatření a jeho výsledku na NBÚ?			
181/2014 Sb. §14 odst. 1	Pokud NBÚ uložil na základě vyřešeného kybernetického bezpečnostního incidentu provedení ochranné opatření obecné povahy, byla tato ochranná opatření provedena?			
181/2014 Sb. §14 odst. 2	Pokud NBÚ stanovil orgánům nebo osobám dle §3 písm. c) až e) způsob zvýšení ochrany IS nebo sítí elektronických komunikací, byla tato opatření provedena ve stanovené lhůtě?			
181/2014 Sb. §16 odst. 2a	Oznámil orgán nebo osoba uvedená v §3 písm. a) a b) kontaktní údaje definované v §16 provozovateli národního CERT (§29 nejpozději do 30 dnů od nabytí účinnosti zákona)?			
181/2014 Sb. §16 odst. 2b	Oznámil orgán nebo osoba uvedená v §3 písm. c) až e) kontaktní údaje definované v §16 NBÚ?			

Reference	Otázka	ANO	NE	N/A
181/2014 Sb. §24 odst. 2	Dokáže zajistit orgán nebo osoba uvedena v §3 přestat používat KII, KIS nebo VIS pokud NBÚ zakáže jeho použití?			
181/2014 Sb. §29 odst. 1	Oznámil orgán nebo osoba uvedená v §3 písm. a) a b) kontaktní údaje podle §16 nejpozději do 30 dnů ode dne nabytí účinnosti zákona?			
181/2014 Sb. §29 odst. 2	Dokáže organizace nebo osoba uvedena v §3 písm. b) zajistit plnění povinnosti stanovené §8 odst. 1 a 2 (hlášení bezp. Incidentů) nejpozději do 1 roku ode dne nabytí účinnosti zákona?			
181/2014 Sb. §30 písm. a)	Nahlásil orgán nebo osoba uvedená v §3 písm. c) a d) kontaktní údaje (§16) nejpozději do 30 dnů ode dne určení informačního systému nebo komunikačního systému kritickou informační infrastrukturou?			
181/2014 Sb. §30 písm. b)	Dokáže / Dokázal orgán nebo osoba uvedená v §3 písm. c) a d) plnit povinnost stanovenou v §8 odst. 1 a 3. (hlášení bezp. Incidentů) do 1 roku ode dne určení informačního systému nebo komunikačního systému kritickou informační infrastrukturou?			
181/2014 Sb. §30 písm. c)	Zavede / Zavedl orgán nebo osoba uvedená v §3 písm. c) a d) bezpečnostní opatření dle §4 odst. 2 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou?			
181/2014 Sb. §31 písm. a)	Nahlásil orgán nebo osoba uvedená v §3 písm. e) kontaktní údaje (§16) nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému?			

Reference	Otázka	ANO	NE	N/A
181/2014 Sb. §31 písm. b)	Dokáže / Dokázal orgán nebo osoba uvedená v §3 písm. e) plnit povinnost stanovenou v §8 odst. 1 a 3. (hlášení bezp. Incidentů) do 1 roku ode dne naplnění určujících kritérií významného informačního systému?			
181/2014 Sb. §31 písm. c)	Zavede / Zavedl orgán nebo osoba uvedená v §3 písm. e) bezpečnostní opatření dle §4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému?			
Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)				
316/2014 Sb. §3 odst. 1 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) stanovenu s ohledem na aktiva a organizační bezpečnost rozsah a hranice systému řízení bezpečnosti informací, ve kterých je určeno, kterých organizačních částech a technických prvků se řízení bezpečnosti týká?			
316/2014 Sb. §3 odst. 1 písm. b)	Řídí orgán nebo osoba uvedená v §3 písm. c) a d) rizika podle §4 odst. 1			
316/2014 Sb. §3 odst. 1 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) a d) vytvořenu a schválenu bezpečnostní politiku v oblasti řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik. Má stanovenu bezpečnostní politiku v dalších oblastech podle § 5 a zavedena příslušná bezpečnostní opatření?			
316/2014 Sb. §3 odst. 1 písm. d)	Monitoruje orgán nebo osoba uvedená v §3 písm. c) a d) účinnost bezpečnostních opatření?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §3 odst. 1 písm. e)	Vyhodnocuje orgán nebo osoba uvedená v §3 písm. c) a d) vhodnost a účinnost bezpečnostní politiky podle §5			
316/2014 Sb. §3 odst. 1 písm. f)	Zajišťuje orgán nebo osoba uvedená v §3 písm. c) a d) provádění auditu kybernetické bezpečnosti podle §15, a to nejméně jednou ročně?			
316/2014 Sb. §3 odst. 1 písm. g)	Zajišťuje orgán nebo osoba uvedená v §3 písm. c) a d) vyhodnocení účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně jednou ročně?			
316/2014 Sb. §3 odst. 1 písm. h)	Aktualizuje orgán nebo osoba uvedená v §3 písm. c) a d) systém řízení bezpečnosti informací a příslušnou dokumentaci na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami?			
316/2014 Sb. §3 odst. 1 písm. i)	Řídí orgán nebo osoba uvedená v §3 písm. c) a d) provoz a zdroje systému řízení bezpečnosti informací, zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik?			
316/2014 Sb. §3 odst. 2 písm. a)	Řídí orgán nebo osoba uvedená v §3 písm. e) rizika podle §4 odst. 1			
316/2014 Sb. §3	Má orgán nebo osoba uvedená v §3 písm. e) vytvořenu a schválenu bezpečnostní politiku			

Reference	Otázka	ANO	NE	N/A
odst. 2 písm. b)	v oblasti řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik. Má stanovenu bezpečnostní politiku v dalších oblastech podle § 5 a zavedena příslušná bezpečnostní opatření?			
316/2014 Sb. §3 odst. 2 písm. c)	Aktualizuje orgán nebo osoba uvedená v §3 písm. e) zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plán zvládání rizik a plán rozvoje bezpečnostního povědomí a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami?			
316/2014 Sb. §4 odst. 1 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) stanovenu metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik?			
316/2014 Sb. §4 odst. 1 písm. b)	Identifikuje a hodnotí orgán nebo osoba uvedená v §3 písm. c) a d) důležitost aktiv, která patří do rozsahu systému řízení bezpečnosti informací, podle § 8 v rozsahu přílohy č. 1 k této vyhlášce a výstupy zapracovává do zprávy o hodnocení aktiv a rizik?			
316/2014 Sb. §4 odst. 1 písm. c)	Identifikuje a hodnotí orgán nebo osoba uvedená v §3 písm. c) a d) rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce, určí a schválí přijatelná rizika a zpracuje zprávu o hodnocení aktiv a rizik?			
316/2014 Sb. §4 odst. 1 písm. d)	Zpracovává orgán nebo osoba uvedená v §3 písm. c) a d) na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a uvedených bezpečnostních opatření?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §4 odst. 1 písm. e)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zpracován a zaveden plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními?			
316/2014 Sb. §4 odst. 1 písm. f)	Zohledňuje orgán nebo osoba uvedená v §3 písm. c) a d) bez zbytečného odkladu reaktivní a ochranná opatření vydaná Národním bezpečnostním úřadem (dále jen Úřad) v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik? Je doplněn plán zvládání rizik?			
316/2014 Sb. §4 odst. 2 písm. a)	Má orgán nebo osoba uvedená v §3 písm. e) stanovenu metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik?			
316/2014 Sb. §4 odst. 2 písm. b)	Identifikuje a hodnotí orgán nebo osoba uvedená v §3 písm. e) důležitost primárních aktiv, která patří do rozsahu systému řízení bezpečnosti informací, podle § 8 v rozsahu přílohy č. 1 k této vyhlášce a výstupy zapracovává do zprávy o hodnocení aktiv a rizik?			
316/2014 Sb. §4 odst. 2 písm. c)	Identifikuje a hodnotí orgán nebo osoba uvedená v §3 písm. e) rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce, určí a schválí přijatelná rizika a zpracuje zprávu o hodnocení aktiv a rizik?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §4 odst. 2 písm. d)	Zpracovává orgán nebo osoba uvedená v §3 písm. e) na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření?			
316/2014 Sb. §4 odst. 2 písm. e)	Má orgán nebo osoba uvedená v §3 písm. e) zpracován a zaveden plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními?			
316/2014 Sb. §4 odst. 2 písm. f)	Zohledňuje orgán nebo osoba uvedená v §3 písm. e) bez zbytečného odkladu reaktivní a ochranná opatření vydaná Národním bezpečnostním úřadem (dále jen Úřad) v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik? Je doplněn plán zvládání rizik?			
316/2014 Sb. §4 odst. 3	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zajištěno řízení rizik jiným způsobem, než jak je stanoveno v 316/2014 Sb. §4 odst. 1 a 2 s použitím opatření zajišťující stejnou nebo vyšší úroveň řízení rizik?			
316/2014 Sb. §4 odst. 4 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů?			
316/2014 Sb. §4 odst. 4 písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik poškození nebo selhání technického anebo programového vybavení?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §4 odst. 4 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zneužití identity fyzické osoby?			
316/2014 Sb. §4 odst. 4 písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik užívání programového vybavení v rozporu s licenčními podmínkami?			
316/2014 Sb. §4 odst. 4 písm. e)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik kybernetický útok z komunikační sítě?			
316/2014 Sb. §4 odst. 4 písm. f)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik škodlivý kód (např. viry, spyware, trojské koně)?			
316/2014 Sb. §4 odst. 4 písm. g)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému?			
316/2014 Sb. §4 odst. 4 písm. h)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik narušení fyzické bezpečnosti?			
316/2014 Sb. §4 odst. 4 písm. i)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie?			
316/2014 Sb. §4 odst. 4 písm. j)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zneužití nebo neoprávněné modifikace údajů?			
316/2014 Sb. §4	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik			

Reference	Otázka	ANO	NE	N/A
odst. 4 písm. k)	trvale působící hrozby?			
316/2014 Sb. §4 odst. 4 písm. l)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik odcizení nebo poškození aktiva?			
316/2014 Sb. §4 odst. 5 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatečnou ochranu vnějšího perimetru?			
316/2014 Sb. §4 odst. 5 písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatečné bezpečnostní povědomí uživatelů a administrátorů?			
316/2014 Sb. §4 odst. 5 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatečnou údržbu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému?			
316/2014 Sb. §4 odst. 5 písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nevhodné nastavení přístupových oprávnění?			
316/2014 Sb. §4 odst. 5 písm. e)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů?			
316/2014 Sb. §4 odst. 5 písm. f)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §4 odst. 5 písm. g)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí?			
316/2014 Sb. §4 odst. 6 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátorů kritické informační infrastruktury?			
316/2014 Sb. §4 odst. 6 písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu pochybení ze strany zaměstnanců?			
316/2014 Sb. §4 odst. 6 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu zneužití vnitřních prostředků a sabotáž?			
316/2014 Sb. §4 odst. 6 písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu dlouhodobého přerušení poskytování služeb elektronických komunikací, dodávek elektrické energie nebo jiných důležitých služeb?			
316/2014 Sb. §4 odst. 6 písm. e)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu nedostatku zaměstnanců s potřebnou úrovní?			
316/2014 Sb. §4 odst. 6 písm. f)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu cíleného kybernetického útoku pomocí sociálního inženýrství a použití špionážních technik?			
316/2014 Sb. §4 odst. 6 písm. g)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženy při hodnocení rizik zváženu hrozbu zneužití vyměnitelných technických nosičů dat?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §4 odst. 7 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženu při hodnocení rizik zranitelnost nedostatečné ochrany prostředků KIS?			
316/2014 Sb. §4 odst. 7 písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženu při hodnocení rizik zranitelnost nevhodné bezpečnostní architektury?			
316/2014 Sb. §4 odst. 7 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženu při hodnocení rizik zranitelnost nedostatečné míry nezávislé kontroly?			
316/2014 Sb. §4 odst. 7 písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zváženu při hodnocení rizik zranitelnost neschopnosti včasného odhalení pochybení ze strany zaměstnanců?			
316/2014 Sb. §5 odst. 1 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti systému řízení informací?			
316/2014 Sb. §5 odst. 1 písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti organizační bezpečnosti?			
316/2014 Sb. §5 odst. 1 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti řízení vztahů s dodavateli?			
316/2014 Sb. §5 odst. 1 písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti klasifikace aktiv?			
316/2014 Sb. §5 odst. 1 písm. e)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti bezpečnosti lidských zdrojů?			
316/2014 Sb. §5 odst. 1 písm. f)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti řízení provozu komunikací?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §5 odst. 1 písm. g)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti řízení přístupu?			
316/2014 Sb. §5 odst. 1 písm. h)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti bezpečného chování uživatelů?			
316/2014 Sb. §5 odst. 1 písm. i)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti zálohování a obnovy?			
316/2014 Sb. §5 odst. 1 písm. j)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti bezpečného předávání informací?			
316/2014 Sb. §5 odst. 1 písm. k)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti řízení technických zranitelností?			
316/2014 Sb. §5 odst. 1 písm. l)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti bezpečného používání mobilních zařízení?			
316/2014 Sb. §5 odst. 1 písm. m)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti poskytování a nabývání licencí programového vybavení a informací?			
316/2014 Sb. §5 odst. 1 písm. n)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti dlouhodobého ukládání a archivaci informací?			
316/2014 Sb. §5 odst. 1 písm. o)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti ochrany osobních údajů?			
316/2014 Sb. §5 odst. 1 písm. p)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti fyzické bezpečnosti?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §5 odst. 1 písm. q)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti bezpečnosti komunikační sítě?			
316/2014 Sb. §5 odst. 1 písm. r)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti ochrany před škodlivým kódem?			
316/2014 Sb. §5 odst. 1 písm. s)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí?			
316/2014 Sb. §5 odst. 1 písm. t)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí?			
316/2014 Sb. §5 odst. 1 písm. u)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona stanovenu bezpečnostní politiku v oblasti používání kryptografické ochrany?			
316/2014 Sb. §5 odst. 2 písm. a)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti systému řízení informací?			
316/2014 Sb. §5 odst. 2 písm. b)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti organizační bezpečnosti?			
316/2014 Sb. §5 odst. 2 písm. c)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti řízení vztahů s dodavateli?			
316/2014 Sb. §5 odst. 2 písm. d)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti klasifikace aktiv?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §5 odst. 2 písm. e)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti bezpečnosti lidských zdrojů?			
316/2014 Sb. §5 odst. 2 písm. f)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti řízení provozu komunikací?			
316/2014 Sb. §5 odst. 2 písm. g)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti řízení přístupu?			
316/2014 Sb. §5 odst. 2 písm. h)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti bezpečného chování uživatelů?			
316/2014 Sb. §5 odst. 2 písm. i)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti zálohování a obnovy?			
316/2014 Sb. §5 odst. 2 písm. j)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti poskytování a nabývání licencí programového vybavení a informací?			
316/2014 Sb. §5 odst. 2 písm. k)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti ochrany osobních údajů?			
316/2014 Sb. §5 odst. 2 písm. l)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti používání kryptografické ochrany?			
316/2014 Sb. §5 odst. 2 písm. m)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti ochrany před škodlivým kódem?			
316/2014 Sb. §5 odst. 2 písm. n)	Má orgán nebo osoba uvedená v §3 písm. e) zákona stanovenu bezpečnostní politiku v oblasti nasazení a používání nástroje pro detekci kybernetických bezpečnostních			

Reference	Otázka	ANO	NE	N/A
	událostí?			
316/2014 Sb. §5 odst. 3	Hodnotí pravidelně orgán nebo osoba uvedená v §3 písm. c) až e) zákona účinnost bezpečnostní politiky a aktualizuje ji?			
316/2014 Sb. §6 odst. 1	Má orgán nebo osoba uvedená v §3 písm. c) až e) zavedenu organizaci řízení bezpečnosti informací, v rámci které určila výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury, komunikačním systémem kritické informační infrastruktury nebo významným informačním systémem?			
316/2014 Sb. §6 odst. 2 písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až d) určenu bezpečnostní roli manažer kybernetické bezpečnosti?			
316/2014 Sb. §6 odst. 2 písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až d) určenu bezpečnostní roli architekt kybernetické bezpečnosti?			
316/2014 Sb. §6 odst. 2 písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až d) určenu bezpečnostní roli auditor kybernetické bezpečnosti?			
316/2014 Sb. §6 odst. 2 písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až d) určenu bezpečnostní roli garant aktiva podle §2 písm. m)?			
316/2014 Sb. §6 odst. 3	Má orgán nebo osoba uvedená v §3 písm. e) určeny bezpečnostní role přiměřené podle §6 odst. 2?			
316/2014 Sb. §6 odst. 4	Má orgán nebo osoba určenu roli manažera kybernetické bezpečnosti s odpovědností za systém řízení bezpečnosti informací? Je pro tuto činnost vyškolen? Má pro tuto činnost			

Reference	Otázka	ANO	NE	N/A
	prokázanou odbornou praxí po dobu nejméně tří let?			
316/2014 Sb. §6 odst. 5	Zajišťuje architekt kybernetické bezpečnosti návrh a implementaci bezpečnostních opatření? Je pro tuto činnost vyškolen a má prokázánu odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let?			
316/2014 Sb. §6 odst. 6	Je osoba provádějící audit kybernetické bezpečnosti (Auditor) pro tuto činnost vyškolena a má prokázánu odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let? Je tato role nestranná a výkon oddělen od rolí uvedených v odst. 2 písm. a) b) a d)?			
316/2014 Sb. §6 odst. 7	Má orgán nebo osoba zřízen výbor pro řízení kybernetické bezpečnosti?			
316/2014 Sb. §6 odst. 8	Má orgán nebo osoba uvedená v §3 písm. c) až e) zajištěna odborná školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle §9 odst. 1 písm. b)?			
316/2014 Sb. §7 odst. 1	Má orgán nebo osoba uvedená v §3 písm. c) až e) zavedena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a zohlední je u dodavatelů nebo jiných osob, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného			

Reference	Otázka	ANO	NE	N/A
	informačního systému prokazatelně dokumentuje orgán a osoba uvedená v § 3 písm. c) až e) zákona smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.			
316/2014 Sb. §7 odst. 2) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona u dodavatelů uvedených v §7 odst. 1 zabezpečeno před uzavření smlouvy hodnocení rizik podle přílohy č. 2 k této vyhlášce?			
316/2014 Sb. §7 odst. 2) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona u dodavatelů uvedených v §7 odst. 1 zabezpečeno uzavření smlouvy o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření?			
316/2014 Sb. §7 odst. 2) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zabezpečeno provádění pravidelného hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky odstraňuje nebo po dohodě s dodavatelem zajistí jejich odstranění?			
316/2014 Sb. §8 odst. 1) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení aktiv identifikována a evidována primární aktiva?			
316/2014 Sb. §8 odst. 1) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení aktiv určeny garanty aktiv, kteří jsou zodpovědní za primární aktiva?			
316/2014 Sb. §8 odst. 1) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení aktiv zhodnocenu důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a jsou tato aktiva zařazena do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k této			

Reference	Otázka	ANO	NE	N/A
	vyhlášce?			
316/2014 Sb. §8 odst. 2) písm. a)	Má orgán nebo osoba při hodnocení aktiv posouzen rozsah a důležitost osobních údajů nebo obchodního tajemství?			
316/2014 Sb. §8 odst. 2) písm. b)	Má orgán nebo osoba při hodnocení aktiv posouzen rozsah dotčených právních povinností nebo závazků?			
316/2014 Sb. §8 odst. 2) písm. c)	Má orgán nebo osoba při hodnocení aktiv posouzen narušení vnitřních řídících a kontrolních činností?			
316/2014 Sb. §8 odst. 2) písm. d)	Má orgán nebo osoba při hodnocení aktiv posouzeno poškození veřejných, obchodních nebo ekonomických zájmů?			
316/2014 Sb. §8 odst. 2) písm. e)	Má orgán nebo osoba při hodnocení aktiv posouzeny možné finanční ztráty?			
316/2014 Sb. §8 odst. 2) písm. f)	Má orgán nebo osoba při hodnocení aktiv posouzen rozsah narušení běžných činností orgánu a osoby uvedené v §3 písm. c) až e) zákona?			
316/2014 Sb. §8 odst. 2) písm. g)	Má orgán nebo osoba při hodnocení aktiv posouzeny dopady spojené s narušení důvěrnosti, integrity a dostupnosti?			
316/2014 Sb. §8 odst. 2) písm. h)	Má orgán nebo osoba při hodnocení aktiv posouzeny dopady na zachování dobrého jména nebo ochranu dobré pověsti?			
316/2014 Sb. §8 odst. 3) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona identifikována podpůrná aktiva?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §8 odst. 3) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona určeny garanty aktiv, kteří jsou odpovědni za podpůrná aktiva?			
316/2014 Sb. §8 odst. 3) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona určeny vazby mezi primárními a podpůrnými aktivy a zhodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy?			
316/2014 Sb. §8 odst. 4) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona stanovena pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv? Jsou určeny způsoby rozlišování jednotlivých úrovní aktiv? Jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv? Jsou stanoveny přípustné způsoby používání aktiv?			
316/2014 Sb. §8 odst. 4) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zavedena pravidla ochrany odpovídající úrovni aktiv?			
316/2014 Sb. §8 odst. 4) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv?			
316/2014 Sb. §9 odst. 1) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §9 odst. 1) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů v souladu s plánem rozvoje bezpečnostního povědomí zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných □školení?			
316/2014 Sb. §9 odst. 1) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů zajištěnu kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role?			
316/2014 Sb. §9 odst. 1) písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení bezpečnosti lidských zdrojů zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role?			
316/2014 Sb. §9 odst. 2)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona veden o školení podle §9 odst. 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly?			
316/2014 Sb. §9 odst. 3) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů?			
316/2014 Sb. §9 odst. 3) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona hodnocenu účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí?			
316/2014 Sb. §9 odst. 3) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §9 odst. 3) písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona zajištěnu změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role?			
316/2014 Sb. §10 odst. 1)	Má orgán nebo osoba uvedená v §3 písm. c) až e) zákona v rámci řízení provozu a komunikací pomocí technických nástrojů uvedených v §21 až 23 detekovány kybernetické bezpečnostní události a pravidelně vyhodnoceny získané informace? Je na tyto nedostatky reagováno v souladu s §13?			
316/2014 Sb. §10 odst. 2)	Orgán nebo osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení provozu a komunikací dále zajištěn bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem stanovena provozní pravidla a postupy?			
316/2014 Sb. §10 odst. 3) písm. a)	Obsahují provozní pravidla a postupy orgánu nebo osoby uvedené v §3 písm. c) a d) práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů?			
316/2014 Sb. §10 odst. 3) písm. b)	Obsahují provozní pravidla a postupy orgánu nebo osoby uvedené v §3 písm. c) a d) postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů?			
316/2014 Sb. §10 odst. 3) písm. c)	Obsahují provozní pravidla a postupy orgánu nebo osoby uvedené v §3 písm. c) a d) postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech?			
316/2014 Sb. §10 odst. 3) písm. d)	Obsahují provozní pravidla a postupy orgánu nebo osoby uvedené v §3 písm. c) a d) spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných			

Reference	Otázka	ANO	NE	N/A
	systémových nebo technických potíží?			
316/2014 Sb. §10 odst. 3) písm. e)	Obsahují provozní pravidla a postupy orgánu nebo osoby uvedené v §3 písm. c) a d) postupy řízení a schvalování provozních změn?			
316/2014 Sb. §10 odst. 3) písm. f)	Obsahují provozní pravidla a postupy orgánu nebo osoby uvedené v §3 písm. c) a d) postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů?			
316/2014 Sb. §10 odst. 4)	Řídí orgány nebo osoby uvedené v §3 písm. c) až e) zákona provoz, který spočívá v provádění pravidelného zálohování a prověřování použitelnosti provedených záloh?			
316/2014 Sb. §10 odst. 5) písm. a)	Má orgán nebo osoba uvedené v §3 písm. c) a d) zákona řízen provoz pomocí oddělení vývojového, testovacího a produkčního prostředí?			
316/2014 Sb. §10 odst. 5) písm. b)	Má orgán nebo osoba uvedené v §3 písm. c) a d) zákona řízen provoz pomocí řešení reaktivních opatření vydaných Úřadem (NBÚ)? Má posouzeny očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnoceny možné negativní účinky a bez zbytečného odkladu je oznamuje Úřadu? Stanovuje způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určuje časový plán jeho provedení?			
316/2014 Sb. §10 odst. 6) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona v rámci řízení komunikací zajištěnu bezpečnost a integritu komunikačních sítí a bezpečnost komunikačních služeb podle § 17?			
316/2014 Sb. §10	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona v rámci řízení komunikací			

Reference	Otázka	ANO	NE	N/A
odst. 6) písm. b)	určena pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi?			
316/2014 Sb. §10 odst. 6) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona v rámci řízení komunikací prováděnu výměnu a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla zdokumentována?			
316/2014 Sb. §10 odst. 6) písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona v rámci řízení komunikací s ohledem na klasifikaci aktiv prováděnu výměnu a předávání informací na základě písemných smluv, jejíchž součástí je ustanovení o bezpečnosti informací?			
316/2014 Sb. §11 odst. 1)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona na základě provozních a bezpečnostních potřeb řízen přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a přidělen každému uživateli jednoznačný identifikátor?			
316/2014 Sb. §11 odst. 2)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle § 18 a 19, a která brání ve zneužití těchto údajů neoprávněnou osobou?			
316/2014 Sb. §11 odst. 3) písm. a)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona dále v rámci řízení přístupu přidělena přistupujícím aplikacím samostatný identifikátor?			
316/2014 Sb. §11 odst. 3) písm. b)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona dále v rámci řízení přístupu omezeno přidělování administrátorských oprávnění?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §11 odst. 3) písm. c)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona dále v rámci řízení přístupu přidělována a odebírána přístupová oprávnění v souladu s politikou řízení přístupu?			
316/2014 Sb. §11 odst. 3) písm. d)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona dále v rámci řízení přístupu prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích?			
316/2014 Sb. §11 odst. 3) písm. e)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona dále v rámci řízení přístupu použit nástroj pro ověřování identity uživatelů podle § 18 a nástroj pro řízení přístupových oprávnění podle § 19?			
316/2014 Sb. §11 odst. 3) písm. f)	Má orgán nebo osoba uvedená v §3 písm. c) a d) zákona dále v rámci řízení přístupu zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.			
316/2014 Sb. §12 odst. 1)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou tyto požadavky zahrnuty do projektu akvizice, vývoje a údržby systému?			
316/2014 Sb. §12 odst. 2) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury? Pro postupy hodnocení a řízení rizik jsou použity metodiky podle § 4 odst. 1 písm. a)?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §12 odst. 2) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona zajištěnu bezpečnost vývojového prostředí a zajištěnu ochranu používaných testovacích dat?			
316/2014 Sb. §12 odst. 2) písm. c)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona provedeno bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu?			
316/2014 Sb. §13 písm. a)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů přijata nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních vede záznamy?			
316/2014 Sb. §13 písm. b)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů připraveno prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle § 21 až 23, provádí jejich vyhodnocení a identifikuje kybernetické bezpečnostní incidenty?			
316/2014 Sb. §13 písm. c)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů provedenu klasifikaci kybernetických bezpečnostních incidentů, přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, provádí hlášení kybernetického bezpečnostního incidentu podle § 32 a zajistí sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního			

Reference	Otázka	ANO	NE	N/A
	incidentu?			
316/2014 Sb. §13 písm. d)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu, vyhodnocenu účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanovena nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu?			
316/2014 Sb. §13 písm. e)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona při zvládání kybernetických událostí a incidentů zdokumentováno zvládání kybernetických bezpečnostních incidentů?			
316/2014 Sb. §14 odst. 1) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení kontinuity činností stanovena práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role?			
316/2014 Sb. §14 odst. 1) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení kontinuity činností stanoveny cíle řízení kontinuity činností formou určení 1. minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému? 2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury,			

Reference	Otázka	ANO	NE	N/A
	komunikačního systému kritické informační infrastruktury nebo významného informačního systému? 3. doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu?			
316/2014 Sb. §14 odst. 1) písm. c)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci řízení kontinuity činností stanovenu strategii řízení kontinuity činností, která obsahuje naplnění cílů podle písm. b)?			
316/2014 Sb. §14 odst. 2) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona vyhodnoceny a zdokumentovány možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností?			
316/2014 Sb. §14 odst. 2) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury?			
316/2014 Sb. §14 odst. 2) písm. c)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona realizována opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a je využíván nástroj pro zajišťování úrovně dostupnosti podle § 26?			
316/2014 Sb. §14 odst. 2) písm. d)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona stanoveny a aktualizovány postupy pro provedení opatření vydaných Úřadem (NBÚ) podle § 13 a 14 zákona, ve kterých jsou zohledněny 1. výsledky hodnocení rizik provedení opatření, 2. stav dotčených bezpečnostních opatření a			

Reference	Otázka	ANO	NE	N/A
	3. vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury?			
316/2014 Sb. §15 odst. 1) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci kontroly a auditu kritické informační infrastruktury a významných informačních systémů (dále jen audit kybernetické bezpečnosti) posouzen soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a určena opatření pro jeho prosazování?			
316/2014 Sb. §15 odst. 1) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci kontroly a auditu kritické informační infrastruktury a významných informačních systémů (dále jen „audit kybernetické bezpečnosti“) prováděny a zdokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik?			
316/2014 Sb. §15 odst. 2)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona zajištěno provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6, která hodnotí správnost a účinnost zavedených bezpečnostních opatření?			
316/2014 Sb. §15 odst. 3)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona dále pro informační systém kritické informační infrastruktury a komunikační systém kritické informační infrastruktury prováděnu kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reaguje na zjištěné zranitelnosti?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §16 odst. 1) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci fyzické bezpečnosti přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému?			
316/2014 Sb. §16 odst. 1) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci fyzické bezpečnosti přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému?			
316/2014 Sb. §16 odst. 1) písm. c)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci fyzické bezpečnosti předcházení poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému?			
316/2014 Sb. §16 odst. 2) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů?			
316/2014 Sb. §16 odst. 2) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §16 odst. 3) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - mechanické zábranné prostředky?			
316/2014 Sb. §16 odst. 3) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - zařízení elektrické zabezpečovací signalizace?			
316/2014 Sb. §16 odst. 3) písm. c)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - prostředky omezující působení požárů?			
316/2014 Sb. §16 odst. 3) písm. d)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - prostředky omezující působení projevů živelných událostí?			
316/2014 Sb. §16 odst. 3) písm. e)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - systémy pro kontrolu vstupu?			
316/2014 Sb. §16 odst. 3) písm. f)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - kamerové systémy?			
316/2014 Sb. §16 odst. 3) písm. g)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - zařízení pro zajištění ochrany před selháním dodávky elektrického napájení?			
316/2014 Sb. §16 odst. 3) písm. h)	Má orgán a osoba uvedená v § 3 písm. c) a d) zákona uplatňovány prostředky fyzické bezpečnosti - zařízení pro zajištění optimálních provozních podmínek?			
316/2014 Sb. §17 odst. 1) písm. a)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavedeno řízení bezpečného			

Reference	Otázka	ANO	NE	N/A
	přístupu mezi vnější a vnitřní sítí?			
316/2014 Sb. §17 odst. 1) písm. b)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavedenu segmentaci zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí?			
316/2014 Sb. §17 odst. 1) písm. c)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavedeny kryptografické prostředky (§ 25) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií?			
316/2014 Sb. §17 odst. 1) písm. d)	Má orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavedena opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě?			
316/2014 Sb. §18 odst. 1)	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému?			
316/2014 Sb. §18	Zajišťuje nástroj pro ověřování identity uživatelů a administrátorů ověření identity			

Reference	Otázka	ANO	NE	N/A
odst. 2)	uživatelů a administrátorů před zahájením jejich aktivit v informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury a významném informačním systému?			
316/2014 Sb. §18 odst. 3) písm. a)	Zajišťuje nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem minimální délku hesla osm znaků?			
316/2014 Sb. §18 odst. 3) písm. b)	Zajišťuje nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících 4 požadavků (Nejméně jedno velké písmeno, nejméně jedno malé písmeno, nejméně jednu číslici, nejméně jeden speciální znak odlišný od požadavků uvedených v bodech 1 - 3)?			
316/2014 Sb. §18 odst. 3) písm. c)	Zajišťuje nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů? (Tento požadavek není vyžadován pro samostatné identifikátory aplikací).			
316/2014 Sb. §18 odst. 4) písm. a)	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona nástroj pro ověření identity, který zamezí opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin a provádí opětovné ověření identity po určené době nečinnosti?			
316/2014 Sb. §18 odst. 4) písm. b)	Využívá orgán a osoba uvedená v § 3 písm. c) až d) nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c)?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §18 odst. 5)	Je nástroj pro ověřování identity uživatelů zajištěn i jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, pokud orgán a osoba uvedená v § 3 písm. c) až e) zákona zabezpečí, že používá opatření zajišťující stejnou nebo vyšší úroveň odolnosti hesla?			
316/2014 Sb. §19 odst. 1)	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění: a) pro přístup k jednotlivým aplikacím a datům a b) pro čtení dat, pro zápis dat a pro změnu oprávnění?			
316/2014 Sb. §19 odst. 2)	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona dále nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik?			
316/2014 Sb. §20	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona pro řízení rizik spojených s působením škodlivého kódu nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu a) komunikace mezi vnitřní sítí a vnější sítí, b) serverů a sdílených datových úložišť a c) pracovních stanic? Provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem, jeho definic a signatur?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §21 odst. 1)	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajistí: a) sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a b) ochranu získaných informací před neoprávněným čtením nebo změnou?			
316/2014 Sb. §21 odst. 2)	Zaznamenává orgán a osoba uvedená v § 3 písm. c) až e) zákona dále pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému: a) přihlášení a odhlášení uživatelů a administrátorů, b) činnosti provedené administrátory, c) činnosti vedoucí ke změně přístupových oprávnění, d) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů, e) zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, f) automatická varovná nebo chybová hlášení technických aktiv, g) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a			

Reference	Otázka	ANO	NE	N/A
	h) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení?			
316/2014 Sb. §21 odst. 3)	Uchovává orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle §21 odstavce 2 nejméně po dobu 3 měsíců?			
316/2014 Sb. §21 odst. 4)	Zajišťuje orgán a osoba uvedená v § 3 písm. c) až e) zákona nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému?			
316/2014 Sb. §22 odst. 1)	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí?			
316/2014 Sb. §22 odst. 2)	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona dále nástroj pro detekci kybernetických bezpečnostních událostí, které zajistí ověření, kontrolu a případně zablokování komunikace: a) v rámci vnitřní komunikační sítě a b) serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury?			
316/2014 Sb. §23 odst. 1)	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajistí: a) integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z			

Reference	Otázka	ANO	NE	N/A
	informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury, b) poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury a c) nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí?			
316/2014 Sb. §23 odst. 2)	Zajišťuje orgán a osoba uvedená v § 3 písm. c) a d) zákona dále: a) pravidelnou aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování, a b) využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury?			
316/2014 Sb. §24 odst. 1)	Provádí orgán a osoba uvedená v § 3 písm. c) až e) zákona bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů?			
316/2014 Sb. §24 odst. 2)	Zajišťuje orgán a osoba uvedená v § 3 písm. c) a d) zákona dále v rámci aplikační bezpečnosti trvalou ochranu: a) aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou a			

Reference	Otázka	ANO	NE	N/A
	b) transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním?			
316/2014 Sb. §25 odst. 1) písm. a)	Stanoví orgán a osoba uvedená v § 3 písm. c) až e) zákona a) pro používání kryptografické ochrany stanoví 1. úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a 2. pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat?			
316/2014 Sb. §25 odst. 1) písm. b)	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona v souladu s bezpečnostními potřebami a výsledky hodnocení rizik kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a průkaznou identifikaci osoby za provedené činnosti.			
316/2014 Sb. §25 odst. 2) písm. a)	Stanoví orgán a osoba uvedená v § 3 písm. c) a d) zákona pro používání kryptografických prostředků systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů?			
316/2014 Sb. §25 odst. 2) písm. b)	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem?			
316/2014 Sb. §26 odst. 1)	Používá orgán a osoba uvedená v § 3 písm. c) až e) zákona v souladu s bezpečnostními potřebami a výsledky hodnocení rizik nástroj pro zajišťování úrovně dostupnosti informací?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §26 odst. 2)	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona nástroj pro zajišťování úrovně dostupnosti informací, který zajistí: a) dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností, b) odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost, a c) zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury: 1. využitím redundance v návrhu řešení a 2. zajištěním náhradních technických aktiv v určeném čase.			
316/2014 Sb. §27	Používá orgán a osoba uvedená v § 3 písm. c) a d) zákona pro bezpečnost průmyslových a řídicích systémů, které jsou informačním systémem kritické informační infrastruktury nebo komunikačním systémem kritické informační infrastruktury anebo jsou jejich součástí, nástroje, které zajistí: a) omezení fyzického přístupu k síti a zařízením průmyslových a řídicích systémů, b) omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů, c) ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých zranitelností a d) obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu?			
316/2014 Sb. §28 odst. 1)	Vede a aktualizuje orgán a osoba uvedená v § 3 písm. c) a d) zákona bezpečnostní dokumentaci, která obsahuje:			

Reference	Otázka	ANO	NE	N/A
	a) bezpečnostní politiku podle § 5 odst. 1, b) zprávy z auditu kybernetické bezpečnosti podle § 3 odst. 1 písm. f), c) zprávy z přezkoumání systému řízení bezpečnosti informací podle § 3 odst. 1 písm. g), d) metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik, e) zprávu o hodnocení aktiv a rizik, f) prohlášení o aplikovatelnosti, g) plán zvládání rizik, h) plán rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. a), i) zvládání kybernetických bezpečnostních incidentů podle § 13 písm. e), j) strategii řízení kontinuity činností podle § 14 odst. 1 písm. c) a k) přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků podle § 15 odst. 1 písm. a)?			
316/2014 Sb. §28 odst. 2)	Vede a aktualizuje orgán a osoba uvedená v § 3 písm. e) zákona bezpečnostní dokumentaci, která obsahuje: a) bezpečnostní politiku podle § 5 odst. 2, b) metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik podle § 4 odst. 2 písm. a), c) zprávu o hodnocení aktiv a rizik podle § 4 odst. 2 písm. b) a c), d) prohlášení o aplikovatelnosti podle § 4 odst. 2 písm. d), e) plán zvládání rizik podle § 4 odst. 2 písm. e), f) plán rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. a), g) zvládání kybernetických bezpečnostních incidentů podle § 13 písm. e), h) strategii řízení kontinuity činností podle § 14 odst. 1 písm. c) a			

Reference	Otázka	ANO	NE	N/A
	i) přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků podle § 15 odst. 1 písm. a).?			
316/2014 Sb. §28 odst. 3)	Vede orgán a osoba uvedená v § 3 písm. c) až e) zákona bezpečnostní dokumentaci tak, aby záznamy o provedených činnostech byly úplné, čitelné, snadno identifikovatelné a aby se daly snadno vyhledat. Dokumentuje opatření potřebná k identifikaci, uložení, ochraně, vyhledání, době platnosti a uspořádání záznamů o provedených činnostech?			
316/2014 Sb. §29	Je zahrnut orgán a osoba uvedená v § 3 písm. c) až e) zákona, jejíž informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém do rozsahu systému řízení bezpečnosti informací, který byl certifikován podle příslušné technické normy akreditovaným certifikačním orgánem, a která vede dokumenty obsahující: a) popis rozsahu systému řízení bezpečnosti informací, b) prohlášení politiky a cílů systému řízení bezpečnosti informací, c) popis použité metody hodnocení rizik a zprávu o hodnocení rizik, d) prohlášení o aplikovatelnosti, e) certifikát systému řízení bezpečnosti informací splňující požadavky příslušné technické normy zabývající se bezpečností informací, f) záznam o přezkoumání systému řízení bezpečnosti informací včetně souvisejících vstupů a výstupů přezkoumání a g) zprávu z auditů provedených certifikačním orgánem včetně příslušných záznamů o			

Reference	Otázka	ANO	NE	N/A
	nápravě zjištěných neshod s příslušnou normou? Splňuje požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky?			
316/2014 Sb. §30 odst. 1)	Jsou rozděleny kybernetické bezpečnostní incidenty podle příčiny do následujících typů: a) kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb, b) kybernetický bezpečnostní incident způsobený škodlivým kódem, c) kybernetický bezpečnostní incident způsobený překonáním technických opatření, d) kybernetický bezpečnostní incident způsobený porušením organizačních opatření, e) kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb a f) ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem?			
316/2014 Sb. §30 odst. 2)	Jsou rozděleny kybernetické bezpečnostní incidenty podle dopadu do následujících typů: a) kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv, b) kybernetický bezpečnostní incident způsobující narušení integrity aktiv, c) kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv, nebo d) kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených v písmenech a) až c)?			
316/2014 Sb. §31 odst. 1)	Jsou rozděleny pro potřeby zvládání kybernetických bezpečnostních incidentů podle následků a negativních projevů kybernetické bezpečnostní incidenty do následujících kategorií: a) Kategorie III - velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i			

Reference	Otázka	ANO	NE	N/A
	potenciálních škod. b) Kategorie II - závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod c) Kategorie I - méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod?			
316/2014 Sb. §31 odst. 2)	Je zohledněna u orgánů a osob uvedených v § 3 písm. c) až e) zákona při kategorizaci jednotlivých kybernetických bezpečnostních incidentů podle odstavce 1: a) důležitost dotčených aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, b) dopady na poskytované služby informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, nebo významného informačního systému, c) dopady na služby poskytované jinými informačními systémy kritické informační infrastruktury, komunikačními systémy kritické informační infrastruktury, nebo významnými informačními systémy a d) předpokládané škody a další dopady?			

Reference	Otázka	ANO	NE	N/A
316/2014 Sb. §32 odst. 1)	Dovede orgán a osoba uvedená v § 3 písm. c) až e) zákona nahlásit kybernetický bezpečnostní incident a) v elektronické podobě prostřednictvím 1. elektronického formuláře zveřejněného na internetových stránkách Úřadu, 2. emailu na adresu elektronické po□ty Úřadu určené pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněné na internetových stránkách Úřadu, 3. datové zprávy do datové schránky Úřadu, nebo 4. prostřednictvím určeného datového rozhraní, jehož popis je zveřejněn na internetových stránkách Úřadu, anebo b) v listinné podobě na adresu Národního centra kybernetické bezpečnosti, zveřejněné na internetových stránkách Úřadu?			
316/2014 Sb. §32 odst. 3)	Dovede orgán a osoba uvedená v § 3 písm. c) až e) zákona nahlásit kybernetický bezpečnostní incident dle přílohy č. 5 této vyhlášky?			
316/2014 Sb. §33	Dovede orgán a osoba uvedená v § 3 písm. c) až e) zákona oznámit provedení reaktivního opatření a jeho výsledek na formuláři, jehož vzor je uveden v příloze č. 6 k této vyhlášce?			