Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu	
Pro řádek 10.1 přílohy č. 2 k této vyhlášce	Tři záznamy o provedení skenu zranitelností provedených maximálně 3 měsíce před podáním žádosti o zápis do katalogu cloud computingu nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 3 skeny zranitelností maximálně 3 měsíce před podáním žádosti o zápis do katalogu cloud computingu.
Pro řádek 10.2 přílohy č. 2 k této vyhlášce	Zprávu o provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM, provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis do katalogu cloud computingu.
Pro řádek 10.3 přílohy č. 2 k této vyhlášce	Zpráva o provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis do katalogu cloud computingu.
Poskytovatel dodá každých 24 měsíců evidence služby cloud computingu v katalogu cloud computingu Ministerstvu vnitra	
Pro řádek 10.1 přílohy č. 2 k této vyhlášce	Čtyři záznamy o provedení skenu zranitelností provedených každých 6 měsíců evidence v katalogu cloud computingu nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 4 skeny zranitelností každých 6 měsíců evidence v katalogu cloud computingu.
Pro řádek 10.2 přílohy č. 2 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM, provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 23 měsíců od zápisu do katalogu cloud computingu nebo dodání předchozí zprávy o provedení penetračního testu.
Pro řádek 10.3 přílohy č. 2 k této vyhlášce	Zprávu o provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 23 měsíců od zápisu do katalogu cloud computingu nebo dodání předchozí zprávy o provedení penetračního testu.