Od regulace k praxi
zkušenosti SPCSS

SPCSS
Státní pokladna
Centrum sdílených služeb

TLP: GREEN

19.5.2026

Pavlína Havelková

vedoucí odboru Kompetenční centrum kybernetické bezpečnosti

pavlina.havelkova@spcss.cz

Úsek bezpečnosti SPCSS

Regulace SPCSS

- Poskytovatel regulovaných služeb
  - Cloud Computing
  - Datové centrum
  - Řízená služba
  - Řízená bezpečnostní služba
- Prováděcí nařízení (EU) 2024/2690
- ISO 27001, 27017 a 27018
- 1 rok (od 5.2.2026)

Provozní a technické změny?

Žádné …

- Datová centra jsou postavena
- Infrastrukturu a technologie máme
- Bezpečnostní procesy jsou zavedené
- Role a odpovědnosti jsou rozdělené

Nestartujeme od nuly

… vše existovalo před účinností zákona

Co se skutečně změnilo?

Nová legislativa = nová realita

- Struktura bezpečnostní dokumentace
- Obsah bezpečnostní dokumentace
- Terminologie
- Řízení dodavatelů
- Smluvní vztahy

Je nezbytné prokázat, že to není jen na papíře …

Od regulace k praxi

	A	B	C	D	E	F	G	H	I	J	K
1	Commission Implementing		European and internation standards & frameworks					National frameworks			
2	Point No	Title	ISO standard 27001:2022	NIST Cybersecurity Framework v2.0	ETSI Standard EN 319 401 V3.1.1	CEN/TS 18026:2024	BE-CyFun®2023	FI-Kybermittari	EL- Ministerial decision 1689/2025	ENS-Royal Decree 311/2022	FR
3	1.1	Policy on the security of network and information systems	5.2, A.5.1, A.5.36, A.5.4, 9.3	PR.AT-02, GV.PO-01, GV.PO-02, GV.OC-03, GV.RM-03, GV.OC-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	REQ 6.1-02, REQ 6.1-06, REQ 6.1-07, REQ 6.1-08, Clause 6.3	ISP-01, ISP-02, OPS-01, OPS-02, OPS-03	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-1.2, PR.IP-5.1, PR.IP-6.1, PR.PT-2.1, PR.AT-4.1 ESSENTIAL: PR.PT-3.3, PR.PT-4.3	WORKFORCE-3, PROGRAM-1, PROGRAM-2, Management activities, CRITICAL-2, ARCHITECTURE-1	Ministerial decision 1689/2025: articles 6a, 6b, 6c Cybersecurity handbook: Part A: 2, Part B: 1.1, 1.5, 2.1, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1 Self assessment tool: 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 2.1, 2.2, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1,	Article 5, Article 6, Article 10, Article 12, Article 27, Annex II: [org.1] Security policy, [org.2] Security regulations, [org.3] Security procedures	2.B.1-IE/EE 2.B.2-IE/EE 2.B.3-IE/EE 2.B.4-IE/EE 2.B.5-IE/EE 2.C.1-IE/EE 2.C.2-IE/EE 2.C.3-IE/EE
4	1.2	Roles, responsibilities and authorities	5.3, A.5.2, A.5.3, A.5.4	GV.RR-02, GV.SC-02, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	REQ-7.1.2-01, REQ-7.2-01X, REQ-7.2-03X, REQ 7.2-07X, REQ 7.2-08X, REQ 7.2-09X, REQ 7.2-10X, REQ 7.2-11X, REQ 7.2-12X, REQ 7.2-13X, REQ-7.2-14X, REQ-7.2-15X	ISP-02, OIS-02	BASIC: RS.RP-1.1 IMPORTANT: ID.AM-6.1, PR.AT-2.1, PR.AT-4.1, PR.AT-5.1, RS.CO-1.1	PROGRAM-1, PROGRAM-2, CRITICAL-2, WORKFORCE-2 WORKFORCE-3	Ministerial decision 1689/2025: articles 7a, 7b, 7c Cybersecurity handbook: Part A: 2, Part B: 1.1, 2.1, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1 Self assessment tool: 1.1, 1.2, 1.3, 1.4, 1.5	Article 11, Article 13 Annex II: [org.1] Security policy	2.A.1-IE/EE 2.A.2-EE 2.A.3-IE/EE 2.B.2-IE/EE 4.3-EE 4.4-IE/EE 4.5-IE/EE
5	2.1	Risk management framework	6.1, 6.1.2, 6.1.3, 6.2, 8.2, 8.3, A5.7, A.5.19, A.5.20, A.5.21	ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, ID.RM-01, GV.RM-06, GV.RR-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	Clause 5, Clause 6.3	OIS-01, RM-01, RM-02, RM-03	BASIC: ID.GV-4.1, ID.RA-5.1 IMPORTANT: ID.BE-4.1, ID.GV-4.2, ID.RA-5.2, ID.RA-6.1, ID.RM-1.1, ID.RM-2.1, ID.RM-3.1, ID.SC-2.1, ID.SC-3.1, PR.AC-7.1, DE.CM-6.2, RS.MI-1.1 ESSENTIAL: ID.RA-5.3, ID.SC-1.1, PR.AC-1.5, DE.AE-4.1	CRITICAL-2, RISK-1, RISK-2, RISK-3, RISK-4, RISK-5, THIRD-PARTIES-2, WORKFORCE-3, WORKFORCE-4	Ministerial decision 1689/2025: articles 5.1a, 5.1b, 5.1c, 5.1d, 5.2 Cybersecurity Handbook: Part A: 2 Self assessment tool: 1.15, 1.16, 1.17, 1.18, 1.19	Article 7, Article 14, Annex II: [op.pl.1] Risk analysis, [op.mon.2] Metrics system, [op.ext.3] Protection of the supply chain	3.A.IE/EE 16.1-EE 16.2-EE 16.3-EE 16.4-EE 20.2-EE
6	2.2	Compliance monitoring	9.2, A.5.31, A.5.35, A.5.36	GV.OV-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	Clause 7.13, REQ-6.3-06X , REQ-6.3-07X, REQ-6.1-08	CO-01, DOC-03, INQ-01, INQ-02, INQ-03	BASIC: RS.IM-1.1 IMPORTANT: ID.GV-1.2, ID.GV-3.2, ID.SC-4.1, PR.AT-3.3, PR.IP-9.1, DE.DP-3.1, DE.DP-5.1, RS.IM-1.2, RC.IM-1.1 ESSENTIAL: ID.SC-4.2, PR.AT-3.4, PR.IP-7.2, PR.IP-9.2, DE.DP-5.2	PROGRAM-1, PROGRAM-2	Ministerial decision 1689/2025: articles 9a, 9b, 9c Cybersecurity Handbook: Part A: 2 Self assessment tool: 1.11, 1.12, 1.19, 1.20	Article 10, Article 28, Article 31, Article 32 Technical Security Instruction on Safety Status Report. Technical Security Instruction on Information Systems Security Auditing ANNEX III - Security audit	2.A.1-IE/EE 2.B.2-IE/EE 2.B.4-IE/EE 2.C.1-IE/EE 2.C.2-IE/EE 2.C.3-IE/EE 3.B.1-IE/EE 3.B.2-IE/EE
7	2.3	Independent review of information and network security	9.2, 10.1, A.5.35, A.8.34	GV.OV-02, ID.IM-01	Clause 7.13, REQ-7.2-11X , REQ-7.2-14X (d)	CO-01, CO-02, CO-03, CO-04	ESSENTIAL: ID.SC-4.2, PR.IP-7.2, DE.DP-5.2, DE.CM-2.2	PROGRAM-2	Ministerial decision 1689/2025: articles 8a, 8b, 8c, 8d Cybersecurity Handbook:- Self assessment tool: 15.2	Article 31 ANNEX III - Security audit, National Security Framework Compliance, sections V (National Security Framework Compliance) and VI (Requirements of the certifier bodies) Technical Security Instruction on Information Systems Security Auditing Technical Security Instruction for compliance with the	3.B.2-EI/EE 17.2-EE
	3.1	Incident handling policy	A.5 .24	GV.SC-08, RS.MA-01, RS.MA-05, RS.MI-01, RS.MI-02, ID.IM-01, ID.IM-04	REQ-7.9.2-12X, REQ-7.9.2-01X, REQ-7.9.2-04X, REQ-7.9.2-05X, REQ-7.9.2-12X, REQ-7.9.2-06X, REQ-7.9.2-08X , REQ-7.9.3-01X	ISP-02, IM-01, IM-07	BASIC: RS.RP-1.1 IMPORTANT: ID.AM-6.1, PR.IP-9.1, RS.CO-1.1, RS.MI-1.1, RC.RP-1.1	RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-5, CRITICAL-3	Ministerial decision 1689/2025: articles 24a, 24f Cybersecurity Handbook: Part B: 17.1 Self-assessment tool: 18.1	Article 12, Article 24, Article 25, Article 33, Article 34, Technical Security Instruction for Notification of Security Incidents , Annex II: [op.exp.7] Incident management, [op.exp.9] Incident management record, [op.mon.1] Intrusion	2.C.1-IE/EE 2.C.2-IE/EE 2.C.3-IE/EE 12.1-EE 12.2-EE

Mapovací tabulka ENISA

SPCSS

Náš postup

	A	B	C
1	ID podle ISO 27001 přílohy A	Název podle ISO 27001 přílohy A	Maping dle PN 2690/2024
3	5.1	Politiky pro informační bezpečnost	1.1.
4	5.2	Role a odpovědnosti v oblasti informační bezpečnosti	1.2.
5	5.3	Oddělení povinností	1.2. + 11.2.
6	5.4	Odpovědnosti vedení	1.1. + 1.2.
9	5.7	Zpravodajství o hrozbách	2.1.
11	5.9	Evidence informací a dalších souvisejících aktiv	12.1. + 12.2. + 12.4.
12	5.10	Přípustné používání informací a dalších souvisejících aktiv	12.2.
13	5.11	Vrácení aktiv	12.5.
14	5.12	Klasifikace informací	12.1.
50	7.1	Perimetry fyzické bezpečnosti	13.3.
51	7.2	Fyzický vstup	11.1. + 13.3.
52	7.3	Zabezpečení kanceláří, místnosti a vybavení	13.2.
53	7.4	Monitorováni fyzické bezpečnosti	13.3.
54	7.5	Ochrana před fyzickými a přírodními hrozbami	13.2.
56	7.7	Prázdný stůl a prázdná obrazovka	12.3.
59	7.10	Paměťová média	12.2. + 12.3.
60	7.11	Podpůrné služby	13.1.
62	7.13	Údržba zařízení	6.4.
66	8.2	Privilegovaná přístupová práva	11.3. + 11.4.
67	8.3	Omezení přístupu k informacím	11.1.
69	8.5	Bezpečná autentizace	11.7.

	A	B	C	D	F
1	ID podle ISO 27001 přílohy A	Název podle ISO 27001 přílohy A	Maping dle PN 2690/2024	Přiřazeno	Popis implementace
2	5	Organizační opatření	Není mapováno	Celá kapitola 1	Požadavek není mapován samostatně; vztahuje se k celé kapitole 1.
7	5.5	Kontakt s autoritami	Není mapováno	1.1.2. + 1.1.3.	Požadavek je pokryt v kap. 1.1.2 a 1.1.3, které upravují kontakt s autoritami a spolupráci s orgány veřejné moci.
8	5.6	Kontakt se zvláštními zájmovými skupinami	Není mapováno	1.1.4.	Téma je ve směrnici zmíněno, ale detailní obsah je řešen odkazem na Směrnici k řízení kybernetických incidentů.
10	5.8	Informační bezpečnost v řízení projektů	Není mapováno	6.2 + 6.3.2	Požadavek je pokryt nepřímo v kap. 6.2 a 6.3.2, které řeší bezpečný vývoj, oddělení prostředí a roli garanta bezpečnosti v projektovém řízení.
35	5.33	Ochrana záznamů	Není mapováno	3.2. + 3.2.5 + 6.4.1 + 1.1. + "12"	Ochrana záznamů je pokryta v kap. 3.2, 3.2.5, 6.4.1 a 1.1, které řeší vedení, archivaci, ochranu a klasifikaci logů a auditních záznamů.
36	5.34	Soukromí a ochrana PII	Není mapováno	1.1.3 + 10.1.2 + 8.1 + 10.2.4	Ochrana soukromí a PII je pokryta přes roli pověřence, prověřování osob a bezpečný režim práce s neveřejnými informacemi v kap. 1.1.3, 10.1.2, 8.1 a 10.2.4.
39	5.37	Dokumentované provozní postupy	Není mapováno	6.4.1 + 3.2.1	Požadavek je pokryt v kap. 6.4.1 a návazně 3.2.1; dokument popisuje provozní postupy, provozní deník i metodiku vedení dokumentace.
40	6	Opatření v oblasti lidských zdrojů	Není mapováno	10	Opatření v oblasti lidských zdrojů jsou pokryta v kap. 10 Politika bezpečnosti lidských zdrojů.
46	6.6	Dohody o důvěrnosti nebo mlčenlivosti	Není mapováno	10.2.5 + 10.2.3 + 10.3 + "12"	Mlčenlivost a NDA jsou řešeny v kap. 10.2.5, navazují na ně postupy při ukončení pracovního poměru a disciplinární řízení v kap. 10.2.3 a 10.3.
47	6.7	Práce na dálku	Není mapováno	10.2.4 + 8.1.1 +8.1.2 + 8.1.3	Práce na dálku je pokryta v kap. 10.2.4 a podpořena požadavky na bezpečné používání mobilních zařízení v kap. 8.1.1 až 8.1.3.

SPCSS

Služba Kompetenční centrum KB

GAP analýza dle 409/2025 Sb.

	A	B	C	D	E	F	G
1	**GAP analýza**					Opatření je aplikováno v plném rozsahu	
2						Opatření je aplikováno částečně	
3						Opatření není aplikováno	
4	**82/2018 Sb. vs 409/2025 Sb.**					Nový bod ve vyhlášce 409/2025 Sb.	
5						Opatření není relevantní	
6	§				**Název §**	**Text §**	**Plně**
77	§ 6	(1)			**4. Řízení bezpečnostní politiky a bezpečnostní dokumentace**	Povinná osoba stanoví bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti a vede bezpečnostní politiku a bezpečnostní dokumentaci k relevantním bezpečnostním opatřením uvedeným v § 3 až 27.	
78	§ 6	(2)				Povinná osoba dodržuje pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci podle odstavce 1.	
79	§ 6	(3)				Povinná osoba pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajišťuje jejich aktuálnost a jejich relevantní oblasti zahrnuje do provozní dokumentace, pravidel a postupů.	
80	§ 6	(4)				Povinná osoba určí osobu odpovědnou za pravidelný přezkum a aktualizaci bezpečnostní politiky a bezpečnostní dokumentace podle odstavce 3.	
81	§ 6	(5)				Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly	
82	§ 6		a)			dostupné v elektronické nebo listinné podobě,	
83	§ 6		b)			dotčené osoby v rámci povinné osoby informovány o právech, povinnostech a postupech v nich obsažených,	
84	§ 6		c)			přiměřeně dostupné dotčeným osobám,	
85	§ 6		d)			chráněny z pohledu důvěrnosti, integrity a dostupnosti a	
86	§ 6		e)			informace v nich obsažené úplné, čitelné, snadno identifikovatelné a vyhledatelné.	
87							
88	§ 7				**5. Řízení aktiv**	Povinná osoba v návaznosti na stanovení rozsahu řízení kybernetické bezpečnosti podle § 12 zákona	
93	§ 7	e)				posuzuje při hodnocení primárních aktiv alespoň oblasti uvedené v příloze č. 1 k této vyhlášce,	
94	§ 7	f)				určuje a eviduje vazby mezi aktivy, která mají vliv na bezpečnost regulované služby,	
95	§ 7	g)				hodnotí podpůrná aktiva a vychází přitom zejména z určených vazeb na primární aktiva a	
96	§ 7	h)				pro jednotlivé úrovně aktiv podle písmene b) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, integrity a dostupnosti, která obsahují alespoň	
99	§ 7		3.			pravidla pro klasifikaci informací,	
100	§ 7		4.			pravidla pro označování aktiv,	
101	§ 7		5.			pravidla správy výměnných médií a	

Statistika plnění dle 409/2025 Sb.

	A	B	C	D	E	F
1	**Bod**	**Typ opatření**	**Název**	**Počet bodů v rámci §**	**Plněných bodů**	**Plněno (%)**
2	§ 3	Organizační opatření	Systém řízení bezpečnosti informací	19	12	63
3	§ 4		Požadavky na vrcholné vedení	29	3	10
4	§ 5		Stanovení bezpečnostních rolí	9	6	67
5	§ 6		Řízení bezpečnostní politiky a bezpečnostní dokumentace	9	4	44
6	§ 7		Řízení aktiv	13	8	62
7	§ 8		Řízení rizik	23	15	65
8	§ 9		Řízení dodavatelů	15	7	47
9	§ 10		Bezpečnost lidských zdrojů	17	10	59
10	§ 11		Řízení změn	10	9	90
11	§ 12		Akvizice, vývoj a údržba	8	2	25
12	§ 13		Řízení přístupu	12	10	83
13	§ 14		Zvládání kybernetických bezpečnostních událostí a incidentů	16	15	94
14	§ 15		Řízení kontinuity činností	8	7	88
15	§ 16		Provádění auditu kybernetické bezpečnosti	11	6	55
16	§ 17	Technická opatření	Fyzická bezpečnost	9	7	78
17	§ 18		Bezpečnost komunikačních sítí	9	7	78
18	§ 19		Správa a ověřování identit	32	29	91
19	§ 20		Řízení přístupových práv a oprávnění	3	3	100
20	§ 21		Detekce kybernetických bezpečnostních událostí	11	10	91
21	§ 22		Zaznamenávání událostí	26	21	81
22	§ 23		Vyhodnocování kybernetických bezpečnostních událostí	8	3	38
23	§ 24		Aplikační bezpečnost	15	9	60
24	§ 25		Kryptografické algoritmy	9	5	56
25	§ 26		Zajišťování dostupnosti regulované služby	10	5	50
26	§ 27		Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	N/A		
27						
28			**Celkové plnění v rámci 409/2025 Sb.**	331	213	64

Co umíme nabídnout?

Praktická pomoc s plněním povinností

- Podpora při implementaci požadavků ZoKB
- Tvorba a správa bezpečnostní dokumentace
- Nastavení procesů, rolí a odpovědností
- Zpracování analýzy rizik
- Školení a vzdělávání
- Podpora při kontrolách a auditech

Služba Cloud computingu a smlouvy

Henry Ford

„Každý zákazník si může vybrat jakoukoliv barvu auta …

jestliže to bude černá“

Cloud Computing

Do jakých mantinelů se musíme vejít?

- Rozsah zapsaný v katalogu CC
- Služba je definována katalogovým listem
- Požadavky nad rámec katalogu
  - Podléhají samostatnému posouzení
  - Jsou samostatně naceněny
- Bezpečnostní a technické parametry
  - Nelze snižovat oproti standardu a zlevňovat tak službu

„Každý zákazník si může vybrat libovolnou cloudovou službu … přesně takovou, jaká je v katalogu CC“

Sledujte nás

Spolehlivý

Poskytovatel

Cloudových

Služeb

Státu

SPCSS
Státní pokladna
Centrum sdílených služeb

spcss.cz/**cloud**

@spcss

@spcss_sp

@spcss_sp

@SPCSSsp